Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification

Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance

1008122

Final Report, November 2004

Cosponsor
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585-1290

EPRI Project Manager
J. Naser

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

MPR Associates, Inc.

Brookhaven National Laboratory

ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Orders and Conferences, 1355 Willow Way, Suite 278, Concord, CA 94520, (800) 313-3774, press 2 or internally x5379, (925) 609-9169, (925) 609-1310 (fax).

CITATIONS

This report was prepared by

MPR Associates, Inc.
320 King Street
Alexandria, VA 22314

Principal Investigators
R. Fink
D. Hill

Brookhaven National Laboratory
Building 130
32 Lewis Street
Upton, NY 11973

Principal Investigator
J. O'Hara

This report describes research sponsored by EPRI, and the U.S. Department of Energy.
(Award No. DE-FC07-03ID14536. Task FY03-4).

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors(s) and do not necessarily reflect the views of the Department of Energy.

The report is a corporate document that should be cited in the literature in the following manner:

Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance, EPRI, Palo Alto, CA, the U.S. Department of Energy, Washington, DC: 2004. 1008122.

REPORT SUMMARY

Operators of nuclear power plants face a significant challenge designing and modifying control rooms that will be produced at various stages of instrumentation and control modernization. This report provides guidance on planning, specifying, designing, implementing, operating, maintaining, and training for modernized control rooms and digital human-system interfaces. Much of the guidance also will support new plant control rooms. This report also presents detailed information and guidelines on specific technologies such as information display systems, soft controls, alarms, and computer-based procedures.

Background

A significant challenge facing plants and system designers is incorporating good human factors engineering and meeting human performance goals with hybrid (part analog and part digital) and full digital control rooms produced at various stages of I&C modernization. Careful design of human-system interfaces (HSIs) incorporating digital technology and integrating these interfaces into control rooms can allow personnel to accomplish their tasks more effectively. Tasks include process and equipment monitoring, fault detection and diagnosis, situation assessment, and response planning and execution. Results can be reduced human errors, improved performance, and, thus, enhanced plant safety and improved availability, reliability, and efficiency.

Objectives

To help nuclear power plant operators and suppliers plan, specify, design, implement, operate, maintain, and train for the modernization of control rooms and other HSI in a way that takes advantage of digital system and HSI technologies, reflects practical constraints associated with modernizing existing control rooms and I&C systems, and addresses issues concerning hybrid and fully digital control room HSI.

Approach

Supported by a working group of utility and industry representatives, the project team developed 31 guidelines and the technical bases for them. Each guideline was developed by part of the development team, then reviewed and commented on by the entire team. After these comments were resolved, the guidelines were sent to the entire working group for additional peer review and comments. When this process was complete, the guideline is considered ready for use. Additional feedback as guidelines are applied will be used later to enhance the guidelines. Working-group plants farthest along in I&C modernization provided input on major issues and stumbling blocks faced in planning control room and HSI changes. Additional related inputs came from lessons learned at plants with completed modernization projects. Regulators provided input on regulatory requirements and expectations related to modernized control rooms. Vendors and other industry representatives provided input on design approaches and control room issues.

Results

This report provides the guidance and technical bases that will help plant operators, suppliers, and supporting third parties 1) plan changes to main control rooms and HSIs that address obsolescence issues and the need for new capabilities and 2) meet plant goals of improved availability, reliability, and cost-effectiveness while meeting Nuclear Regulatory Commission (NRC) safety requirements. These guidelines are on 31 topics grouped in the areas of 1) control room modernization planning to help utilities develop plant-specific plans (for example, endpoint definition, human factors engineering program – including a methodology for a graded effort approach), 2) human factors engineering design analyses and tools with most of these including what is needed to be done under the graded effort approach (for example, function analysis and allocation, task analysis, HSI and procedure design), 3) detailed human factors engineering guidelines including design principles, checklists, and additional information sources for designers (for example, information display systems, soft controls, alarms, computer-based procedures), 4) regulatory and licensing activities (for example, regulatory requirements and expectations, engineering evaluations related to licensing), and 5) special topics related to operations and maintenance (for example, training considerations unique to digital I&C modernization programs, safety monitoring and control in modernized control rooms). These guidelines and technical bases will be the main support for utilities as they modernize control rooms, HSIs, and I&C systems. Much of the guidance also will support new plant control rooms and HSI. The document's primary use will be as a reference that is accessed and used when specific needs arise such as guidance for computer-based procedures. It is not anticipated the document will be read from cover to cover. Thus, when users are in a specific section of interest, the document contains extensive electronic cross-referencing to related sections in other parts of the document.

EPRI Perspective

The full promise of reducing human errors and increasing plant and human performance may not be achieved unless the specification, design, implementation, operation, maintenance, and training for new digital systems and HSIs take into account human cognitive aspects. This project has developed necessary guidelines and technical bases to support these areas. Guidance is of five types: 1) control room modernization planning, 2) human factors engineering design analyses and tools, 3) detailed human factors engineering guidelines, 4) regulatory and licensing activities, and 5) special topics related to operations and maintenance. The project's overall aim is to support operational requirements of power plants while improving their availability, reliability, and cost-effectiveness and meeting NRC safety requirements. This report provides guidance that is useful for operating plants that are modernizing control rooms and HSI, and for new plant designs. Related EPRI reports are *Nuclear Power Plant Control Room Modernization Planning* (1003569), *Technical Material for a Workshop on Control Room Upgrades* (1007795), *Information Display Considerations for Designing Modern Computer-Based Display Systems* (1002830), and *Alarm Processing Methods: Improving Alarm Management in Nuclear Power Plant Control Rooms* (1003662). This report greatly extends and replaces *Interim Human Factors Guidance for Hybrid Control Rooms* (1003696).

Keywords

Control room design, Control room planning, Digital systems, Human factors engineering
Human-system interface, Hybrid control rooms, Instrumentation and control systems, Simulator

EXECUTIVE SUMMARY

In recent years, plants have been modernizing their instrumentation and control (I&C) systems and the interfaces that plant personnel use to perform their tasks. The latter are referred to as human-system interfaces (HSIs) and include resources such as alarms, displays, and controls that are located in the main control room and numerous local control stations situated throughout the plant. There are many reasons for these modernization activities, including:

1. To address obsolescence and lack of spare parts
2. To meet the need for equipment replacement due to high maintenance cost or lack of vendor support for existing equipment
3. To implement new functionality necessary for adding beneficial capabilities
4. To improve plant performance, HSI functionality, and reliability
5. To enhance operator performance and reliability
6. To address the difficulties in finding young professionals with education and experience with older analog technology

The scope of these plant modernization activities includes a broad spectrum of potential modifications, from the replacement of a few individual obsolete components with newer digital devices to a modernization program that leads to a fully digital control room and digital I&C system HSIs over several years. These new HSIs are computer-based and may incorporate features such as on-screen soft controls, computer-based procedures, touch-screen interfaces, sit-down workstations, and large-screen overview displays. The guidance in this document can be used to support this entire spectrum of plant modernization, as well as new plant control room and HSI design.

The benefits of the new I&C systems and HSIs are significant. New digital systems provide the opportunity to give personnel information they did not have with conventional systems. Improved instrumentation and signal validation techniques can help ensure that the information is more accurate, precise, and reliable. In addition, data processing techniques and the flexibility of computer-based information presentation enable designers to present information in ways that are much better suited to personnel tasks and information processing needs to achieve more efficient, cost-effective power production. The result should be more efficient operations and maintenance, leading to improved power plant availability and safety through the avoidance of transients, forced outages, and unnecessary shutdowns. The potential benefits also include increased efficiency and power output as well as reduced operating costs.

It is equally important to recognize that, if poorly designed and implemented, there is the potential to negatively impact performance that can result in a detrimental effect on safety and cost-effective power production.

Human factors engineering (HFE) is used to help meet this challenge and to ensure that the benefits of the new technology are realized, while potential problems are avoided. The main contributions of HFE are to help ensure that:

1. The role of personnel is well defined and their tasks are clearly specified
2. The numbers of staff, their functions, and qualifications are adequate to fulfill the human roles in the plant
3. The HSIs, procedures, and training meet task performance requirements and are designed to be consistent with human cognitive and physiological characteristics

The guidance provided in this document will help utilities, their suppliers, and their contractors to integrate HFE activities into their overall design efforts to ensure that the contributions of modern I&C and HSI systems are realized.

This document was developed over several years with extensive review and input from multiple facets of the nuclear industry both national and international, including: utilities, vendors /suppliers, researchers, and regulatory personnel. As a result, this document is unique as compared to other HFE standards and guidance documents:

- First, most HFE documents are oriented toward design of a new control room. This document specifically addresses the modification and upgrading of existing control rooms. Thus, the unique issues associated with modification projects are identified and addressed. However, it should be noted that many of the guidelines in this document will also support the design of a new control room.
- Second, most HFE documents are fairly high-level. For example, they may specify that certain analyses should be performed, such as task analysis, but they do not provide a specific methodology to do so. This document provides detailed methodologies that can be used by utility personnel.
- Third, most documents focus largely on HSI design, while this document addresses a broader range of plant modernization considerations - from planning to monitoring the modifications once they are in place.
- Fourth, the structure of this document and the guidance it provides has been intentionally designed to meet regulatory guidance and expectations. No other document provides guidance that so clearly interprets and clearly defines the regulatory and licensing issues that need to be considered as part of control room modernization.

The document can be used to develop a variety of products as part of an I&C modernization program, including:

- An endpoint vision for the control room and other changes to the HFE aspects of the plant
- A migration plan for implementing the endpoint vision over a series of modifications

- Plant-specific HFE procedures
- HSI specifications
- Detailed HSI designs
- Tests and evaluations of designs
- Training program modifications

The document is divided into six sections. They are briefly summarized below.

Section 1 – Introduction

This section introduces HFE and lays out the scope of the document. The contents of the rest of the document are briefly summarized. The section also identifies the intended users who include:

- Plant personnel, including operators, engineers, maintainers, and managers responsible for modernization projects
- I&C designers
- Control system suppliers
- Third party implementers

Section 2 – Control Room Modernization Planning

A significant I&C and HSI modernization project, which may extend over multiple outages, is a major undertaking. It becomes more difficult when the technology employed in the modification is relatively unfamiliar to the utility undertaking the modernization project. Thus, planning is essential.

The key aspects of planning addressed in this document include:

- Developing an vision for what the utility would like the final control room and HSI to look like
- Developing a "migration plan" for modifications that will occur over several outages so that each "interim configuration" produced in the migration will support human performance during periods of operation between outages.
- Developing a HFE program to ensure that the integration of HFE into the plant design and modification process will support the development, design, evaluation, and modification of HSIs. An important aspect of HFE planning is establishing a methodology for grading the level of HFE effort, i.e., ensuring that the level of HFE effort is commensurate with the importance of the modification.
- Establishing a licensing plan, including when and how to interact with the regulatory authority, what the scope of the regulatory review will be, and what documentation will be necessary.

Section 3 – HFE Design, Analyses, and Tools

The section begins with a discussion of how HFE fits into the overall design process and provides guidance for planning the application of HFE for individual modifications. This section then describes the HFE activities that contribute to the design process. It also discusses how to identify which activities are needed for a particular modification. The topics discussed are:

- Implementing HFE in the Design Process for Individual Modifications
- Operating Experience Review (OER)
- Function Analysis and Allocation
- Task Analysis
- Staffing, Qualifications, and Integrated Work Design
- Human Error Analysis
- Human-System Interface and Procedure Design
- HFE Verification and Validation
- In-Service Monitoring
- Methods and Tools for Collecting Information from Users

The methods in these sections are graded into three levels reflecting the overall grading approach determined in Section 2.4.

Section 4 – Detailed HFE Guidelines

HFE guidelines provide principles for the design of computer-based HSIs. The guidelines are organized into the following sections:

- Information Display
- User-Interface Interaction and Management
- Soft Control Systems
- Alarm Systems
- Computer-Based Procedures
- Computerized Operator Support Systems
- Communications
- Workstation and Workplace Design

Each guidance section contains an introduction that characterizes the key features of the HSI technology, the appropriate HFE guidelines organized by that characterization, and design principles and supplemental information that provides further information about the guideline and how it can be applied. The sections also contain a checklist of the guidelines and give additional sources of information that the designer can consult.

Section 5 – Regulatory and Licensing Activities

Regulatory and licensing activities are an important part of any modernization program. Up-front planning can help reduce the cost of activities related to regulatory compliance and can minimize licensing risk. Guidance on licensing activities specific to the human performance considerations related to I&C, control rooms, and HSI modernization is provided.

Section 6 – Special Topics Related to Operations and Maintenance

This section provides guidance for several special topics related to I&C and HSI modernization:

- Human Factors Engineering for the Maintenance of Digital Systems
- Human Factors Engineering for Configuration Management
- Training Considerations Unique to Digital I&C Modernization Programs
- Safety Monitoring and Control in Modernized Control Rooms

Using this Document

It is anticipated that the primary use of this document will be as a reference that is accessed and used when specific needs arise. For example, the guidelines in Section 4.4, Alarm Systems, will be accessed when the designer is developing an alarm specification, a plant-specific guidance document describing the characteristics and functions of how their computer-based alarms should function, or a checklist for alarm system evaluation. That guidance can also be used when future modifications of the alarm system are being planned and implemented.

In light of this concept of usage, it is not anticipated that the document will be read from cover to cover. Thus, when the user is in a specific section of interest such as Section 4.5 Computer-Based Procedures, the document contains extensive cross-referencing to related sections users should be aware of in other parts of the document. As this is an electronic document, these cross-references are hyperlinked for easy access.

ACKNOWLEDGMENTS

This report was prepared with guidance and input from the Hybrid Control Room Working Group. The membership of this Working Group is shown below:

Jay Amin, Chairman	TXU Electric
Karen Arciszewski	Bruce Power
Mike Bailey	Duke Energy
Leo Beltracchi	Consultant
Oivind Berg	Halden Reactor Project
John Blevins	AmerenUE
Jim Bongarra	Nuclear Regulatory Commission
Louis Bosch	San Onofre Nuclear Generating Station
Ronald Bradford	STP Nuclear Operating Company
Warren Busch	FPL
Peter Carpenter	APS
Bob Contratto	Framatome ANP
Ray DiSandro	Exelon
Viktoria Doumtchenko	MPR Associates
Keith Duncan	AmerenUE
Kenneth Dunham	Omaha PPD

Jim Easter	Consultant
Dick Eckenrode	Nuclear Regulatory Commission
Larry Erin	Westinghouse
Bob Evans	Nuclear Energy Institute
Stan Farlow	American Electric Power
Bob Fink	MPR Associates
Genevieve Filippi	Electricité de France
Jim Gallman	TXU Electric
Lew Hanes	Consultant
Dwight Harrison	MPR Associates
Daryl Harmon	Westinghouse
Scott Helm	TXU Electric
Doug Hill	MPR Associates
David Hooten	Progress Energy
Jun Ikeda	Toshiba
Ron Jarrett	Tennessee Valley Authority
Steve Kenney	FPL
Stephen Kerch	Westinghouse
Phil Knobel	Invensys
Bill Kurth	Exelon
Doug Lenker	Constellation
Paul Loeser	Nuclear Regulatory Commission

Troy Martel	Invensys
Pat McKenna	AmerenUE
James McQuighan	Constellation
Mike Miller	Duke Energy
Glenn Morris	Department of Energy
Randy Morrison	TXU Electric
Paul Moore	MPR Associates
Joseph Naser	EPRI
Mark Norris	British Energy Generation
John O’Connor	PSE&G
John O’Hara	Brookhaven National Lab
Julius Persensky	Nuclear Regulatory Commission
Mike Pinion	Dominion
Dominique Pirus	Electricité de France
Jeff Porter	PSE&G
Nick Rakos	TXU Electric
Joe Ruether	Nuclear Management Company
Hiroshi Sakamoto	Toshiba
Patrick Salaun	Electricité de France
Robert Scanlan, Vice Chairman	Dominion
Ken Scarola	Consultant
Rick Scofield	Omaha PPD
Clayton Scott	Invensys

Bruce Sheffel	Detroit Edison
Bobby Shewmake	Southern Nuclear
Bob Starkey	Framatome ANP
Chris Sterba	Omaha PPD
Jeff Summy	San Onofre
Dale Walling	TXU Electric
Les Ward	Omaha PPD
David Whitsitt	TXU Electric
Dan Wingbermuehle	AmerenUE

Special thanks go to the following individuals who have been particularly active in reviewing drafts and providing comments and suggestions to the project team as the guidance has been developed: Jay Amin, John Blevins, Ron Bradford, Keith Duncan, Jim Easter, Dick Eckenrode, Daryl Harmon, Bill Kurth, Jim McQuighan, Mike Miller, Bob Scanlan, Bob Starkey, Les Ward, and Dave Whitsitt.

Also, in addition to Brookhaven National Lab and MPR Associates the following are members of the overall project team who have contributed to the development of the guidance in this document:

Leo Beltracci, consultant

Lew Hanes, consultant

Oivind Berg and colleagues at Halden Reactor Project (Norway)

Dominique Pirus and colleagues at EDF (France)

Special thanks go to Christie Mar and Monique Neaves for their invaluable contribution for the organization, assembly, and production of the final report.

CONTENTS

1 **INTRODUCTION 1-1**

1.1 Background 1-1

1.2 Scope of this Document.. 1-3

1.3 Introduction to Human Factors Engineering and Human Performance 1-4

1.3.1 What Human Factors Engineering (HFE) is and why it is Important 1-4

1.3.2 How HFE Relates to Human Performance 1-5

1.3.3 The Role of HFE in the Design Process 1-5

1.3.4 Basic Human Performance Concepts Used in this Document 1-7

1.4 Organization of this Document.. 1-9

1.5 Intended Users of this Document...1-14

1.6 How to Use this Document 1-15

1.7 Relationship to Other HFE Guidelines and Standards 1-17

2 **CONTROL ROOM MODERNIZATION PLANNING 2-1**

2.1 Management Considerations.. 2-5

2.1.1 The Need for Planning 2-5

2.1.2 Objectives of the Planning Effort 2-6

2.1.3 Minimum Planning Activities 2-7

2.1.4 Levels of I&C and HSI Modernization.. 2-7

2.1.5 Interaction between I&C and HSI Modernization Planning 2-9

2.1.6 Concept of Operations 2-10

2.1.7 Importance of Involving Operations Personnel...2-11

2.1.8 Consideration of Available Systems and Equipment 2-12

2.1.9 Scheduling Challenges 2-13

2.1.10 Documentation of the Planning Effort...2-14

2.1.11 Human Factors Engineering...2-14

2.1.12 Licensing Considerations 2-15

2.2 Endpoint Definition 2-16

2.2.1 Gathering Inputs 2-18

2.2.2 Understanding New HSI Technologies and Modern Control Rooms 2-19

2.2.3 Key Operational and Design Considerations..2-24

2.2.4 Defining the Endpoint Concept..2-32

2.2.5 Potential Benefits of Control Room Modernization 2-36

2.2.6 Costs and Constraints..2-40

2.2.7 Comparison of Conventional and Modernized Control Rooms 2-42

2.2.8 Worksheets for Development of Endpoint Concept 2-43

2.3 Migration Strategy 2-75

2.3.1 Gathering Inputs 2-77

2.3.2 Guidelines for HSI Migration 2-78

2.3.3 Planning and Evaluating the HSI Transitions at Each Migration Step..................2-79

2.3.4 Ensuring Adequacy of Interim Hybrid HSIs 2-85

2.3.5 Conceptual Design of HSI Changes...2-90

2.3.6 Evaluating Costs and Minimizing Project Risk...2-91

2.3.7 Licensing Evaluations 2-96

2.4 Human Factors Program Planning...2-96

2.4.1 HFE Program Elements 2-97

2.4.2 A Graded Approach to HFE 2-101

2.4.3 Sources of Additional Information 2-107

2.4.4 Appendix – Example of HFE Procedure for Modifications 2-107

2.5 Planning for Regulatory and Licensing Activities 2-113

2.5.1 Frequently Asked Questions 2-113

2.5.2 Planning for Licensing Activities...2-119

2.5.3 Sources of Additional Information 2-121

3 **HFE DESIGN, ANALYSES, AND TOOLS 3-1**

3.1 Implementing HFE in the Design Process for Individual Modifications 3-5

3.1.1 Introduction 3-6

3.1.2 Design Process Steps.. 3-6

3.1.3 Basic Application of HFE in Design Processes 3-7

3.1.4 Planning for HFE Activities in Individual Modifications 3-12

3.1.5 Appendix – Example HFE-Related Portion of Modification Checklist...................3-17

3.2 Operating Experience Review 3-18

3.2.1 Introduction...3-18

3.2.2 Design Process Steps 3-18
3.2.3 Basic Application of HFE in Design Processes 3-19
3.2.4 Documentation...3-29
3.2.5 Grading the OER Effort 3-30
3.2.6 Use of the Results..3-30
3.2.7 Appendix – HFE-Related Issues Arising in Plant Modernization Programs 3-31
3.3 Function Analysis and Allocation 3-34
3.3.1 Introduction 3-35
3.3.2 Objective..3-40
3.3.3 Methodology 3-40
3.3.4 Documentation...3-47
3.3.5 Grading the Function Analysis and Allocation Effort...3-47
3.3.6 Use of the Results..3-48
3.4 Task Analysis 3-48
3.4.1 Introduction 3-49
3.4.2 Objectives 3-49
3.4.3 Methodology 3-50
3.4.4 Documentation...3-60
3.4.5 Establishing the Task Risk Level and Grading the Task Analysis Effort 3-61
3.4.6 Use of the Results..3-63
3.5 Staffing, Qualifications, and Integrated Work Design 3-64
3.5.1 Introduction 3-64
3.5.2 Design Process Steps..3-65
3.5.3 Methodology 3-65
3.5.4 Documentation...3-71
3.5.5 Grading the Staffing Analysis Effort...3-71
3.5.6 Use of the Results..3-71
3.6 Human Error Analysis...3-72
3.6.1 Introduction 3-72
3.6.2 Objectives 3-73
3.6.3 Methodology 3-73
3.6.4 Documentation...3-77
3.6.5 Grading the Human Error Analysis Effort 3-78
3.6.6 Use of the Results..3-78

3.7 Human-System Interface and Procedure Design 3-85
3.7.1 Introduction 3-86
3.7.2 Design Process Steps..3-88
3.7.3 Methodology 3-88
3.7.4 Documentation...3-120
3.7.5 Grading the HSI Design Effort..3-120
3.7.6 Use of the Results...3-121
3.7.7 Appendix – Vendor HSI Evaluation Questionnaire 3-121
3.8 HFE Verification and Validation Processes...3-132
3.8.1 Introduction 3-132
3.8.2 Objectives 3-134
3.8.3 Methodology 3-134
3.8.4 Documentation...3-148
3.8.5 Grading the HFE Verification and Validation Effort.......................................3-148
3.9 In-Service Monitoring of Modifications 3-149
3.9.1 Introduction 3-149
3.9.2 Objective...3-150
3.9.3 Methodology 3-151
3.9.4 Use of the Results...3-156
3.9.5 Grading the In-Service Monitoring Effort 3-156
3.10 Methods and Tools for Collecting Information from Users....................................3-157
3.10.1 Introduction 3-157
3.10.2 General Approaches to Information Collection 3-159
3.10.3 Methodological Considerations for Collecting Information..............................3-167
3.10.4 Appendix – Rating Scale for General HSI Evaluation....................................3-183
3.10.5 Appendix – Questions for Detailed Usability Evaluation 3-184

4 HFE GUIDELINES 4-1
4.1 Information Display... 4-9
4.1.1 Overview...4-10
4.1.2 Display Guidelines Checklist...4-13
4.1.3 Display Functions..4-60
4.1.4 Display Pages...4-92
4.1.5 Display Formats..4-99
4.1.6 Display Elements 4-127

4.1.7 Data Quality and Update Rate 4-157
4.1.8 Sources of Additional Information 4-160
4.2 User Interface Interaction and Management..4-165
4.2.1 Section Overview 4-165
4.2.2 Description of User Interface Interaction and Management..............................4-166
4.2.3 Interface Management Guidelines Checklist 4-167
4.2.4 General Interface Design Objectives..4-215
4.2.5 Interface Management Functions...4-239
4.2.6 Interacting with Interface Components..4-298
4.2.7 Sources of Additional Information 4-313
4.3 Soft Control Systems..4-314
4.3.1 Overview..4-314
4.3.2 Soft Controls Guidelines Checklist 4-317
4.3.3 Deciding Whether to Use Hard or Soft Controls 4-321
4.3.4 Selection Displays..4-326
4.3.5 Control Displays...4-329
4.3.6 Feedback and Monitoring...4-339
4.3.7 Sources of Additional Information 4-341
4.3.8 Appendix: Error Tolerant Design 4-342
4.4 Alarm Systems 4-345
4.4.1 Overview..4-345
4.4.2 Display Guidelines Checklist..4-350
4.4.3 General Considerations for Alarm Modifications 4-357
4.4.4 Alarm Definitions...4-359
4.4.5 Alarm Prioritization and Processing...4-360
4.4.6 Alarm Display...4-364
4.4.7 Alarm Control and Management 4-377
4.4.8 Alarm Response Procedures 4-380
4.4.9 Sources of Additional Information 4-382
4.5 Computer-Based Procedure Systems..4-383
4.5.1 Overview..4-383
4.5.2 Computer-Based Procedures Guidelines Checklist..4-387
4.5.3 Scope and Functionality of the CBP System 4-393
4.5.4 Display of Procedures...4-396

4.5.5 Interaction with CBPs........4-403
4.5.6 CBP Functions........4-405
4.5.7 Degraded Conditions and CBP Failure........4-408
4.5.8 Sources of Additional Information........4-409
4.5.9 Appendix: Initial Implementation and Maintenance of CBP........4-410
4.6 Computerized Operator Support Systems (COSS)........4-414
4.6.1 Overview........4-415
4.6.2 COSS Guidelines Checklist........4-418
4.6.3 Deciding if COSS is Needed........4-420
4.6.4 COSS Design and Integration........4-421
4.6.5 Modes of Operation........4-422
4.6.6 User Control of Interaction........4-422
4.6.7 Appendix – Examples of COSS Applications........4-423
4.7 Communication Systems........4-431
4.7.1 Overview........4-431
4.7.2 Display Guidelines Checklist........4-434
4.7.3 Main Aspects of Communication System Design........4-439
4.7.4 Communication System Design........4-440
4.7.5 Control Room Design and Communication System........4-446
4.8 Workstations and Workplaces........4-447
4.8.1 Overview........4-448
4.8.2 Workstations and Workplaces Guidelines Checklist........4-450
4.8.3 General Considerations........4-455
4.8.4 Workstation Design........4-456
4.8.5 Workplace Design........4-463
4.8.6 Managing the Impact of Modifications........4-472
4.8.7 Sources of Additional Information........4-475

_5_ REGULATORY AND LICENSING ACTIVITIES........5-1
5.1 Regulatory Requirements and Expectations........5-6
5.1.1 Roadmap to the Relevant Documents........5-7
5.1.2 NRC HFE Reviews........5-8
5.2 Engineering Evaluations Related to Licensing........5-15
5.2.1 HFE Evaluations and Hybrid HSI Issues........5-16
5.2.2 System Failure Analysis........5-21

5.2.3 Defense-in-Depth and Diversity (D3) Evaluation 5-22
5.2.4 Digital System Dependability Evaluations 5-27
5.2.5 Modern Safety Monitoring and Control Solutions 5-27
5.2.6 Interaction with PRA 5-28
5.3 10 CFR 50.59 Evaluations....5-34
5.3.1 Screening....5-35
5.3.2 CFR 50.59 Evaluation....5-38
5.4 Licensing Submittals and Other NRC Interactions 5-41
5.4.1 License Amendment Requests 5-41
5.4.2 Other NRC Interaction for Major HSI Changes....5-42
5.5 Appendix – Roadmap to HFE-Related Regulatory Requirements and Guidance....5-44

6 SPECIAL TOPICS RELATED TO OPERATIONS AND MAINTENANCE.... 6-1
6.1 Human Factors Engineering for the Maintenance of Digital Systems.... 6-2
6.1.1 Overview.... 6-3
6.1.2 Maintainability Checklist.... 6-7
6.1.3 General Design for Maintainability 6-16
6.1.4 Detailed Design Features for Maintainability 6-17
6.1.5 Diagnosis and Testing....6-21
6.1.6 Maintenance Performance....6-25
6.1.7 Maintainability in Procurement and Plant Changes 6-27
6.1.8 Sources of Additional Information 6-28
6.2 Human Factors Engineering for Configuration Management 6-34
6.2.1 Overview....6-34
6.2.2 Configuration Management Guidelines Checklist....6-35
6.2.3 General Configuration Control Guidance 6-38
6.2.4 Configuration Change Control Guidance....6-38
6.2.5 Control of User-Defined Interface Features....6-41
6.3 Training Considerations Unique to Digital I&C Upgrades....6-43
6.3.1 Introduction....6-44
6.3.2 Objectives....6-45
6.3.3 New Training Topics 6-45
6.3.4 Use of Full Scope Simulator and Other Training Tools....6-57
6.3.5 Sources of Additional Information 6-66
6.3.6 Case Study: Training and Simulation for a Turbine Controls Upgrade....6-67

6.4 Safety Monitoring and Control in Modernized Control Rooms......6-78

6.4.1 Introduction......6-78

6.4.2 Key Documents......6-80

6.4.3 Designing Modernized HSIs for Safety Monitoring and Control......6-87

***A* ACRONYMS** **A-1**

***B* GLOSSARY** **B-1**

***C* REFERENCES** **C-1**

***D* CHECKLISTS** **D-1**

D.1 Information Display......D-1

D.1.1 Display Guidelines Checklist......D-1

D.2 User Interface Interaction and Management......D-39

D.2.1 Display Guidelines Checklist......D-39

D.3 Soft Controls......D-77

D.3.1 Display Guidelines Checklist......D-77

D.4 Alarms......D-82

D.4.1 Display Guidelines Checklist......D-82

D.5 Computer-Based Procedures......D-89

D.5.1 Display Guidelines Checklist......D-89

D.6 Computerized Operator Support Systems (COSS)......D-95

D.6.1 Display Guidelines Checklist......D-95

D.7 Communication Systems......D-96

D.7.1 Display Guidelines Checklist......D-96

D.8 Workstations and Workplaces......D-100

D.8.1 Display Guidelines Checklist......D-100

D.9 Human Factors Engineering for the Maintenance of Digital Systems......D-104

D.9.1 Display Guidelines Checklist......D-104

D.10 Human Factors Engineering for Configuration Management......D-111

D.10.1 Display Guidelines Checklist......D-111

LIST OF FIGURES

Figure 1-1 Hybrid Control Room in Beznau Plant in Switzerland 1-2
Figure 1-2 Organization of Section 1 1-9
Figure 1-3 Organization of Section 2 1-10
Figure 1-4 Organization of Section 3 1-11
Figure 1-5 Organization of Section 4 1-12
Figure 1-6 Organization of Section 5 1-13
Figure 1-7 Organization of Section 6 1-14
Figure 1-8 Context-Sensitive Search Results 1-16
Figure 2-1 HSI Modernization Planning Process 2-4
Figure 2-2 Levels of Modernization of the I&C Systems and the Control Room/HSI: Equipment, Architecture, and Integration/Automation 2-8
Figure 2-3 Evolution of the Control Room Concept of Operations 2-11
Figure 2-4 Defining a Control Room Endpoint 2-18
Figure 2-5 Photo of an Existing U.S. Nuclear Power Plant Control Room 2-20
Figure 2-6 Artist's Rendition of a Modern Control Room for Japanese Plants 2-21
Figure 2-7 Photo of a Modern Control Room Built in France 2-21
Figure 2-8 Example of an Existing Control Room Layout 2-24
Figure 2-9 Example Concept Showing Operator Desks Converted to Workstations 2-25
Figure 2-10 3D View of the Concept Shown in the Layout of Figure 2-9 (Benchboard and Vertical Panel Controls and Indicators Not Shown) 2-26
Figure 2-11 HSI Migration Planning 2-77
Figure 3-1 HFE Activities 3-1
Figure 3-2 Elements of a Generic Digital I&C Modification 3-8
Figure 3-3 Basic HFE Activities Performed in the Design Modification Process 3-11
Figure 3-4 Overview of Operating Experience Review 3-20
Figure 3-5 Prioritization of Operating Experience Review Items 3-28
Figure 3-6 Documentation of OER Items 3-29
Figure 3-7 High-Level Functions of a Nuclear Plant 3-36
Figure 3-8 Generic Activities Performed by Agents 3-38
Figure 3-9 Examples of Allocations 3-39
Figure 3-10 Overview of Function Analysis and Allocation 3-40
Figure 3-11 Identify Changes to F/T Allocations 3-42

Figure 3-12 F/T Allocation Analysis....3-44
Figure 3-13 F/T Allocation Analysis....3-48
Figure 3-14 Overview of Task Analysis....3-51
Figure 3-15 Hierarchical Levels of Analysis....3-55
Figure 3-16 System Start-Up Task Decomposition....3-56
Figure 3-17 Evaluation of Staffing and Qualifications Considerations....3-66
Figure 3-18 Human Error Analysis Process....3-74
Figure 3-19 General Aspects of HSI Design....3-87
Figure 3-20 HSI Design Methodology....3-90
Figure 3-21 Style Guide Development....3-96
Figure 3-22 Style Guide Source Materials....3-98
Figure 3-23 Examples of Level of Specificity from High-Level HFE Guideline to Style Guide Level....3-103
Figure 3-24 Steps in the Design of Error Tolerant HSIs....3-108
Figure 3-25 Basic HFE Activities Performed in the Design Modification Process....3-118
Figure 3-26 Overview of Verification and Validation Activities in the I&C Design Process....3-135
Figure 3-27 Conditions for Integrated System Validation....3-145
Figure 3-28 Example of a Rating Scale....3-161
Figure 3-29 NASA Task Load Index Rating Scales....3-180
Figure 4-1 HFE Guidance for HSI Design.... 4-6
Figure 4-2 Display Design Considerations Addressed in this Section....4-11
Figure 4-3 Plant Abstraction Hierarchy for Supplying Power to Grid....4-67
Figure 4-4 Plant Abstraction Hierarchy for Maintain Safety....4-67
Figure 4-5 Partial Hierarchy Based on PWR Frontline and Support Systems....4-69
Figure 4-6 Representing High-Level Status of Multiple Systems....4-73
Figure 4-7 Displaying Status and Performance Indicators....4-74
Figure 4-8 Alerting User to Changes in Higher and Lower Level Displays (Note: Example uses the Containment Heat Removal Function in a BWR Plant)....4-79
Figure 4-9 On-Screen Navigation to Lower and Upper Level Displays....4-80
Figure 4-10 Characteristics of Information Display Systems....4-93
Figure 4-11 Placement of Heading Above Data Fields....4-107
Figure 4-12 Placement of Heading Adjacent to Data Fields....4-107
Figure 4-13 Example of a Horizontal Bar Chart....4-109
Figure 4-14 Example of a Deviation Bar Chart....4-110
Figure 4-15 Example of a Segmented Bar Chart....4-110
Figure 4-16 Example of an Aid for Reading Exact Values from a Line Graph....4-113
Figure 4-17 Example of a Linear Profile Chart....4-114
Figure 4-18 Example of a Segmented Curve Graph....4-115
Figure 4-19 Example of a Mimic Display....4-118

Figure 4-20 Examples of Configural Displays for Normal (Left) and Abnormal (Right) Conditions 4-123
Figure 4-21 Use of Color to Code the Magnitude of a Parameter 4-147
Figure 4-22 Use of Monochromatic Variations (‘Density’) to Code the Magnitude of a Parameter 4-148
Figure 4-23 Example of Redundant Pattern Coding With Color Coded Indicators 4-152
Figure 4-24 User Interface Interaction and Management 4-166
Figure 4-25 Examples of Broad and Shallow Menu Structures 4-248
Figure 4-26 Layered and Tiled Windows 4-300
Figure 4-27 Examples of Open Window Indications 4-301
Figure 4-28 Examples of Different Applications with Separate Menu Bars 4-302
Figure 4-29 Example of Figure Animation 4-305
Figure 4-30 Soft Control Design Considerations Addressed in this Section 4-315
Figure 4-31 Deciding Between Types of Controls 4-321
Figure 4-32 Two Displays for Selecting Items to be Controlled (With On-Screen Cursor) 4-328
Figure 4-33 Soft Control Input Field is a Window within the Selection Display 4-330
Figure 4-34 Soft Control Input Field and Selection Display are on Separate Display Devices 4-331
Figure 4-35 High-Level Controls 4-332
Figure 4-36 Alarm Design Process 4-349
Figure 4-37 Alarms Integrated into a Process Display 4-369
Figure 4-38 CBP Design and Implementation Considerations 4-384
Figure 4-39 CBP Workstation for the Westinghouse COMPRO System 4-397
Figure 4-40 Main Procedure Display for the Westinghouse COMPRO System 4-397
Figure 4-41 Main Procedure Display for the Forsmark CBP using COPMA 4-398
Figure 4-42 COSS Design and Implementation Considerations 4-416
Figure 4-43 COSS for Operations and Maintenance 4-417
Figure 4-44 Communication System Design 4-433
Figure 4-45 Overview of Workstation and Workplace Design 4-449
Figure 4-46 The Overall Layout of Workstations should Reflect the Ways in which Users are Expected to Work 4-459
Figure 4-47 In Hybrid or Interim Control Room Configurations, Operators may be Positioned at Computer Equipment Placed Atop Former Laydown Space Located Opposite the Control Boards 4-461
Figure 4-48 The Arrangement of Workstations in Hybrid or Interim Control Rooms should take into Account the Operators’ Continuing need to Access the Boards as well as the Computer-Mediated Controls and Displays 4-466
Figure 4-49 The Overall Layout of Workstations should Reflect the ways in which Users are Expected to Work 4-467
Figure 4-50 The Operators’ Workstations should be Designed to Allow an Unobstructed View of Wall-Mounted Displays 4-468

Figure 4-51 Operators may be Positioned at Computer Equipment Placed Atop Former Laydown Space Opposite the Control Boards 4-474

Figure 5-1 Overview of the Licensing Process 5-2

Figure 5-2 Regulatory Requirements and Expectations Related to Determining when a Digital I&C Change Requires Prior NRC Approval.. 5-8

Figure 5-3 Regulatory Requirements and Expectations Related to Human Factors Engineering and Changes Affecting Human Actions 5-9

Figure 5-4 Regulatory Requirements and Expectations Related to HSI Design......................5-10

Figure 5-5 Defense-in-Depth and Diversity Evaluation 5-25

Figure 5-6 Interactions with PRA/HRA 5-29

Figure 5-7 10 CFR 50.59 Screening – Addressing HSI Changes 5-36

Figure 5-8 HFE Plans and Activities for a Large-Scale Modernization Program 5-43

Figure 6-1 Maintainability 6-6

Figure 6-2 Configuration Management...6-35

Figure 6-3 Timeline of Training and Related Activities for the Turbine Controls Upgrade 6-69

Figure 6-4 Full-Scope Training Simulator Configured for Training on New DCS-Based Turbine Control System...6-73

Figure 6-5 Classroom Simulator for Hands-On Training...6-74

LIST OF TABLES

Table 1-1 Examples of General and Plant-Specific HSI Guidelines.. 1-6

Table 2-1 Features of a Fully Modernized Control Room 2-23

Table 2-2 Major Cost Drivers and Constraints...2-41

Table 2-3 Concept of Operations 2-44

Table 2-4 Failure Management 2-55

Table 2-5 Worksheet 1: Concept of Operations for the Endpoint Vision 2-59

Table 2-6 Worksheet 2: HSI Design Concepts for Endpoint Vision..2-67

Table 2-7 Worksheet 3: HSI Failure Management Concepts for Endpoint Vision 2-72

Table 2-8 Guidelines for HSI Migration 2-79

Table 2-9 Advantages and Disadvantages of Different Migration Approaches for Control Panels/Boards..2-81

Table 2-10 Phased Implementation of HSI Changes...2-84

Table 2-11 Specific Hybrid Issues for Individual HSI Elements 2-88

Table 2-12 Major Cost Drivers and Constraints...2-92

Table 2-13 Grading Modifications Based on Nuclear Safety Risk Significance.....................2-103

Table 2-14 Grading Modifications Based on Nuclear Safety Risk Significance, Risk to Power Production and Personnel Safety 2-106

Table 3-1 HF Planning Activities 3-13

Table 3-2 Scope of OER..3-20

Table 3-3 Level 2 OER Methodology 3-30

Table 3-4 Use of OER Information 3-31

Table 3-5 HFE-Related Issues Found in Plant Modernization Programs................................3-31

Table 3-6 Comparison of Task Analysis Techniques..3-50

Table 3-7 Task Description Elements...3-53

Table 3-8 Possible Relationships Between Task Elements 3-58

Table 3-9 General Task Requirements Considerations 3-59

Table 3-10 Task Requirements for System Start-Up 3-60

Table 3-11 Sample Questions for Human Error Analysis 3-75

Table 3-12 Interface Characteristics that can Induce Errors...3-76

Table 3-13 Human Error Identification...3-79

Table 3-14 General Characteristics of a Well-Designed HSI 3-88

Table 3-15 Examples of General and Plant-Specific HSI Guidelines......................................3-93

Table 3-16 Examples of General and Plant-Specific HSI Guidelines......................................3-98
Table 3-17 Detailed HFE Guidelines in Section 4..3-102
Table 3-18 Suggested Error Tolerant Design Approaches for Key Task Elements...............3-110
Table 3-19 HF Planning Activities 3-158
Table 3-20 Guidelines for Interacting with Personnel 3-168
Table 3-21 Guidelines for Interacting with Personnel 3-170
Table 3-22 Examples of Types of Actions Taken by Users 3-176
Table 3-23 Examples of Measures of Task Performance...3-177
Table 3-24 Examples of Situation Awareness Questions 3-179
Table 3-25 Establishing Performance Criteria 3-182
Table 4-1 HSI Resources Supporting Crew Cognitive Activities 4-60
Table 4-2 NRC HFE Guidance for SPDS Review...4-76
Table 4-3 Information Grouping Principles 4-161
Table 4-4 Formats for Displaying Verbal Information..4-161
Table 4-5 Data Display Formats and Usage Notes 4-162
Table 4-6 Suitability of Data Display Formats by Data and Use 4-163
Table 4-7 Examples of Typical Color Meanings 4-164
Table 4-8 Functions for the Control of Processing Commands...4-219
Table 4-9 Functions for the Control of Entering Information 4-220
Table 4-10 Users of HSI Flexibility 4-238
Table 4-11 Dialogue Formats for Representative User Tasks 4-240
Table 4-12 Reducing Navigation Demands in Large Displays..4-272
Table 4-13 Maximum and Preferred System Response Times...4-285
Table 4-14 Typical Profile of Hard and Soft Control Features...4-324
Table 4-15 Typical Profile of Hard and Soft Control Features...4-330
Table 4-16 Considerations for Sharing Alarms..4-373
Table 4-17 Factors Influencing the Decision to Computerize Procedures.............................4-394
Table 4-18 Classes of Techniques for Condition Monitoring, Fault Detection, and Diagnosis 4-427
Table 4-19 Available Guidance for Communciation...4-441
Table 4-20 Available Guidance for Workstation Configuration...4-457
Table 4-21 Available Guidance for Control and Display Device Layout 4-462
Table 4-22 Available Guidance for Labels and Demarcations 4-463
Table 4-23 Available Guidance for Control Room Layout and Configuration 4-464
Table 4-24 Available Guidance for Control Room Environment...4-469
Table 4-25 Available Guidance for Local Control Stations...4-472
Table 5-1 Specific Hybrid Issues for Individual HSI Elements 5-19
Table 5-2 Sample List of Operator Actions and Importance Measures for a Pressurized Water Reactor (PWR)..5-32

Table 5-3 Sample List of Operator Actions and Importance Measures for a Boiling Water Reactor (BWR) 5-33

Table 6-1 Examples of Potential Operator Training Needs for an Analog-to-Digital System Upgrade Includeing a Modernized HSI 6-63

Table 6-2 Tradeoffs Between Use of Existing (Conventional) or New (Computer-Based) Qualified HSIs 6-94

1
INTRODUCTION

1.1 Background

Nuclear power plant personnel play a vital role in the productive, efficient, and safe generation of electric power. Operators monitor and control the plant to ensure it is functioning properly. Test and maintenance personnel help ensure that plant equipment is functioning properly and restore components when malfunctions occur.

Personnel performance, and resulting plant performance, is influenced by many aspects of plant design, including the level of automation, personnel training, and the interfaces provided for personnel to interact with the plant. The latter are referred to as human-system interfaces (HSIs) and include resources such as alarms, displays, and controls that are located in the main control room and numerous local control stations situated throughout the plant. HSIs are also located in support facilities such as the technical support center.

In recent years, plants have been modernizing their instrumentation and control (I&C) systems and HSIs. There are many reasons for these modernization activities, including:

1. To address obsolescence and lack of spare parts
2. To meet the need for equipment replacement due to high maintenance cost or lack of vendor support for existing equipment
3. To implement new functionality necessary for adding beneficial capabilities
4. To improve plant performance, HSI functionality, and reliability
5. To enhance operator performance and reliability
6. To address the difficulties in finding young professionals with education and experience with older analog technology

These modifications can affect personnel in various ways. They can impact the role of personnel, the tasks to be performed, the way their tasks are performed, and the knowledge, skills and training required of personnel. As part of modernization, HSIs are becoming more computer-based, incorporating features such as soft controls, computer-based procedures, touch-screen interfaces, sit-down workstations, and large-screen overview displays. As computer-based technologies are integrated into control rooms that were largely based on conventional technology, hybrid HSIs are created (see Figure 1-1).

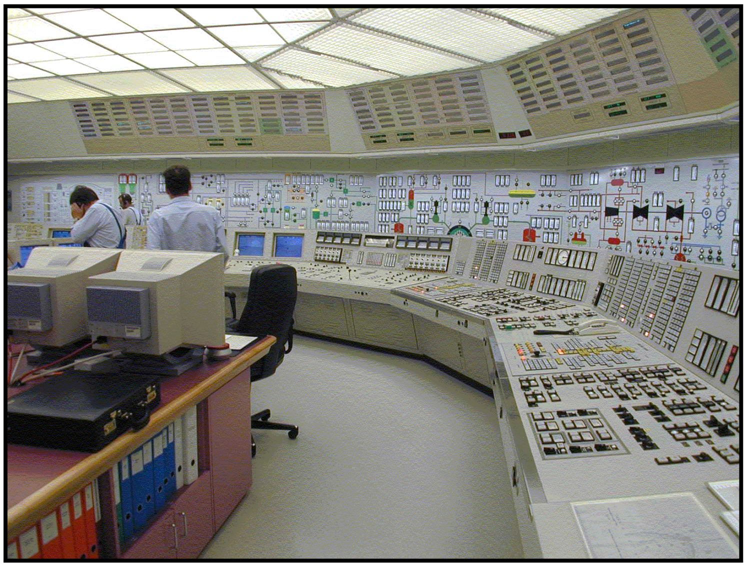


Figure 1-1
Hybrid Control Room in Beznau Plant in Switzerland
(Photo courtesy of Nordostschweizerische Kraftwerke AG)

The potential benefits of modernization are compelling and should result in more efficient operations and maintenance, leading to improved power plant availability and safety through the avoidance of transients, forced outages, and unnecessary shutdowns. The potential benefits also include increased efficiency and power output as well as reduced operating costs. New digital systems provide the opportunity to give personnel information they did not have with conventional systems. Improved instrumentation and signal validation techniques can help ensure that the information is more accurate, precise, and reliable. In addition, data processing techniques and the flexibility of computer-based information presentation enable designers to present information in ways that are much better suited to personnel tasks and information processing needs to achieve more efficient, cost-effective power production.

While plant modernization can greatly improve personnel and plant performance, it is important to recognize that, if poorly designed and implemented, there is the potential to negatively impact performance, increase errors, and reduce human reliability resulting in a detrimental effect on safety and cost-effective power production. Human Factors Engineering (HFE) is needed to ensure that the benefits of the new technology are realized and problems with its implementation are minimized. (See the Appendix of Section 3.2 for a discussion of some of the issues that arise when HFE is not properly addressed).

The guidance provided in this document will help utilities, their suppliers, and their contractors to recognize these potential impacts and to establish design and implementation efforts that address the important human factors aspects of the modernization process in order to achieve the potential benefits of the modernization.

1.2 Scope of this Document

This document provides HFE guidance to help ensure that the HFE aspects of the plant that are affected by I&C and HSI modernization are well designed and, thus, improve overall plant operations, reliability, and safety, i.e., realize the benefits of digital I&C and HSI technology. The HFE aspects of the plant, as used in this document, include:

- the roles and responsibilities of plant personnel as determined by the functions allocated to personnel and automatic systems
- the tasks necessary to accomplish personnel functions
- the staffing and teamwork necessary to perform tasks
- the HSIs, support systems, procedures, and training used by personnel to perform their tasks, both individually and as a team.

Plant modifications can affect all of these HFE aspects of plant design. For example, changes to systems and components can impact the role of personnel and the way their tasks are performed. Even when the tasks stay the same, their characteristics and demands may be changed in ways that can impact human performance. HFE and the guidance provided in this document help utilities address these effects as part of the overall design process.

One significant impact of a modification is the change to HSIs. For example, control rooms are modified to reduce the presence of conventional HSIs and replace them with computer-based HSIs. The guidance in this document can be used to support the design of new HSIs and can be used to address a broad spectrum of potential modifications, from the replacement of a few individual obsolete components with newer digital devices, to a modernization program that leads to a fully digital control room over several years.

To understand the scope of the guidance provided herein, it is useful to know what is not addressed:

- The hardware aspects of computer technology (such as monitors, mice, and keyboards) are not addressed. These are addressed by recent national and international standards and appropriate references to these documents, such as EPRI NP-3659 (EPRI, 1984) and NUREG-0700 (NRC, 2002), are provided in this document.
- Conventional HSI technology (such as j-handles, position switches, pushbuttons, gauges and dials) is not addressed. Such guidance is readily available in other nuclear industry HFE guidance documents (such as the documents listed in the first bullet above).
- The establishment of a training program, e.g., implementation of a systems approach to training, is not addressed here. However, training issues that arise related to the new technology are addressed, as is the coordination of training needs with simulator and plant modifications (see Section 6.3).
- While Section 5 addresses HFE-related regulatory and licensing issues, this document is not a general guide for the overall design or licensing of digital I&C systems. Other industry documents cover the hardware, software and systems aspects of digital upgrades (e.g., digital I&C system hardware and software design, system architecture, performance, commercial grade item dedication, qualification, and licensing). These other documents are referenced where appropriate.

1.3 Introduction to Human Factors Engineering and Human Performance

1.3.1 What Human Factors Engineering (HFE) is and why it is Important

Knowledge about human performance comes from many scientific disciplines, including physiology, medicine, psychology, and sociology. The term “human factors” refers to this body of information. “Human factors engineering” refers to the application of this knowledge to plant and equipment design.

HFE is an engineering discipline like many others involved in the design and modification of nuclear power plants. Thus, just as engineering principles and methods from other disciplines are applied in the design of plant systems and equipment, HFE principles and methods are applied when designing or modifying the HFE aspects of the plant.

The main contributions of HFE are to help ensure that:

1. The role of personnel is well defined and their tasks are clearly specified.
2. The numbers of staff, their functions, and qualifications are adequate to fulfill the human roles in the plant.
3. The HSIs, procedures, and training meet task performance requirements and are designed to be consistent with human cognitive and physiological characteristics.

HFE is a basic element of the design of many complex human-machine systems, such as aircraft, military systems, computer systems, process control facilities, and medical devices. In fact, it is most prominently applied in systems requiring high reliability where failures can have significant consequences.

Commercial nuclear facilities are no different in this regard from other complex systems. HFE has been applied to commercial nuclear power plants in a formal, regulated manner since the accident at Three Mile Island. Lessons learned from subsequent modernization programs also illustrate the importance of the HFE aspects of the plant and of recognizing the unique challenges and opportunities associated with digital upgrades. The main purpose of including HFE as part of the overall design process is to help ensure that the process identifies and addresses the requirements, design, and evaluation of the HFE aspects of plant design. The result will be an overall design that meets personnel needs, supports efficient human performance, minimizes human error, and reduces training burden. As noted earlier, when the HFE aspects of the plant are well designed, the net result should be improved power plant availability and safety through the avoidance of transients, forced outages, and unnecessary shutdowns, as well as increased cost-effective operation and power generation.

HFE is also important in helping utilities to meet the U.S. Nuclear Regulatory Commission’s expectations (discussed further in Section 5).

1.3.2 How HFE Relates to Human Performance

The term "human performance" has two related meanings. In its general usage, it broadly refers to the performance of plant personnel in completing their tasks and the factors that influence that performance. It is primarily in this context that human performance is used within this document. In the nuclear industry, human performance has a more specific meaning as well. Many plants have Human Performance departments or groups that conduct activities to monitor and maintain good human performance at the plant. In that role, they may be involved in related activities as well, such as personnel selection, training, job performance aids, human performance evaluation, safety culture, and root cause analysis. However, this is not the context of this document.

The activities involved in human factors engineering and human performance (HP) are closely related and overlap, in some areas. The major distinction is one of focus. The focus of HFE is on design that supports human performance (in the broad context). Human performance may be measured as part of defining design requirements, obtaining user input and feedback, and design evaluation, but the focus is mainly on the suitability of the design from the user's perspective. The primary focus of HP professionals is on personnel performance itself. Although, both are very much involved with the factors that influence and support plant personnel performance, this document only addresses the former.

1.3.3 The Role of HFE in the Design Process

A central tenet of this guidance document is that HFE should be fully integrated into the engineering design process. IEEE 1220-1998 states that "the design of the products and life cycle processes should consider the human as an element of the system in terms of operators, maintainers, manufacturing personnel, training personnel, etc. for the purpose of understanding the human/system integration issues and ensuring that the system products are producible, maintainable, and usable" (IEEE, 1999, p. 3-4). The HFE activities described in this document associated with planning, design, and evaluation provide the means to accomplish this objective. Thus, it is important that these HFE activities be a part of the overall plant modification process.

The basic steps common to engineering design processes can be expressed in terms of the concept of CReDITS,[1] where the letters of CReDITS represent basic design steps:

- Project planning/design concept development (C)
- Requirements definition (Re)
- Design (D)
- Design implementation (I)
- Design testing (T)
- Design support during operation and maintenance (S)

[1] The acronym CReDITS was used in an EPRI workshop given in 2003 on control room upgrades to show that HFE is a process that is familiar to any engineer/designer. The workshop material is available in EPRI Report 1007795, *Technical Material for a Workshop on Control Room Upgrades*, EPRI, Palo Alto, CA: 2003.

The CReDITS concept as it relates to the HFE activities discussed in this document is shown in Table 1-1.

Table 1-1
Examples of General and Plant-Specific HSI Guidelines

CReDITS	HFE Activity	Section
C	HFE Planning	Section 2 and Section 3.1
Re	Operating Experience Review Function Analysis and Allocation Task Analysis Staffing and Qualification Analysis Human Error Analysis	Section 3.2 Section 3.3 Section 3.4 Section 3.5 Section 3.6
D	HSI and Procedure Design Training Program Development	Section 3.7 Section 6.3
I	HSI and Procedure Design	Section 3.7
T	HSI and Procedure Design HFE Verification and Validation Test Methods and Tools	Section 3.7 Section 3.8 Section 3.10
S	In-Service Monitoring	Section 3.9

This concept has been promulgated in international standards and guidance documents for general product design (e.g., ISO 13407), general control room design (e.g., ISO 11064), and nuclear plant design (e.g., IEC 964 and NUREG-0711). Four key principles for addressing the human factors aspects of design are:

- *Integrate HFE into the design process (as discussed above)* – For HFE to have the greatest impact, it should be fully integrated into the overall plant engineering process. This will help ensure timely and complete interaction with other engineering activities. Experience has shown that when HFE activities are performed independently from other engineering activities, their effectiveness is lessened. The integration of HFE and overall design is discussed in greater detail in Section 3.1, HFE in the Design Process.

- *Use a "top-down" hierarchical approach* – The HFE aspects of the plant should be developed, designed, and evaluated on the basis of a systems analysis that uses a "top-down" approach. Top-down refers to an approach starting at the "top" of the hierarchy with the plant's high-level mission and goals. These are divided into the functions necessary to achieve the goals. Functions are allocated to human and system resources. Each function can be broken down into tasks. The tasks are analyzed to identify the alarms, displays, procedures, and controls that will be required for task performance. Task requirements reflect performance demands imposed by the detailed design of the plant. Tasks are arranged into meaningful jobs to be performed by plant personnel. The HSIs, support systems, procedures, and training are designed to best support personnel in performing their tasks. The detailed design (of the HSI, support systems, procedures, and training) is the "bottom" of the top-down process. Of course, there are also requirements that stem from the detailed design of individual systems and components. These are captured when personnel tasks are analyzed.

- *Apply HFE throughout the life cycle* – HFE should also be considered for the full plant life cycle; i.e., from concept planning through operations and ultimately decommissioning. HFE is sometimes thought of a "usability" check of the final design. However, if user needs are to be considered during decisions, e.g., how much automation to incorporate into the modification, HFE activities have to be performed early on. In fact, the thorough integration of personnel considerations at every step in the process can help ensure that good HSI support systems are developed.
- *Grade the HFE effort to focus on the areas of greatest significance* – HFE activities should be graded. This means that a process is in place to evaluate proposed modifications and adjust the level of HFE design and evaluation effort to the importance of the change. Such an approach enables the application of HFE to be directed to where it will have the most impact. Section 2.4 addresses the grading process in detail and defines a recommended grading approach, which is then applied in detail on appropriate topics in Section 3.

1.3.4 Basic Human Performance Concepts Used in this Document

In this section, some of the basic concepts of human performance that are used throughout this document are briefly discussed.

In carrying out their roles and responsibilities, nuclear plant personnel perform two types of tasks: *primary tasks* and *secondary tasks* (for the sake of this HFE discussion). Primary tasks include activities such as monitoring steam flow, starting pumps, and aligning valves. Secondary tasks are mainly "interface management tasks," as discussed below. Primary tasks can be broken down into the following cognitive elements:

- *Monitoring and detection* – monitoring of plant performance and detection of abnormalities when they arise
- *Situation assessment* – evaluating current situations and determining the underlying causes of abnormalities when they occur (the term "situation awareness" is used to refer to the understanding that personnel have of the plant's current situation)
- *Response planning* – determining the actions to take in order to achieve a desired situation or goal, often with the aid of procedures
- *Response implementation* – performing the actions specified by response planning

Some primary tasks are fairly routine and part of the normal operations, such as start-up, power changes, realignments to support maintenance, and test and maintenance activities. These tasks are well planned and often guided by procedures. Other tasks are much more difficult to plan for, such as trouble shooting and diagnosing a complex plant disturbance. Given the unpredictable nature of plant disturbances, these activities are far less structured than the routine tasks.

To perform their primary tasks, personnel interact with the plant through the HSIs. The main HSIs include alarms, displays, and controls. Use of HSIs can be influenced directly by factors such as:

- The organization of HSIs into workstations (e.g., consoles and panels).
- The arrangement of workstations and supporting equipment into facilities such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility.

- The environmental conditions in which the HSIs are used, including temperature, humidity, ventilation, illumination, and noise.

To perform their primary tasks successfully, personnel must perform secondary tasks or "interface management tasks." In a computer-based control room, secondary tasks include activities such as navigating or accessing information at workstations and arranging various pieces of information on the screen. In part, these tasks are necessitated by the fact that operators view only a small amount of information at any one time through their video display units. Therefore, they must perform interface management tasks to retrieve and arrange the information. These tasks are called secondary because they are not directly associated with monitoring and controlling the plant.

The distinction between primary and secondary tasks is important in HSI design because of the ways they can interact. Secondary tasks may take so much attention and effort away from primary tasks that primary task performance declines. Alternatively, operators may decide not to access additional information because the retrieval effort may detract from their primary tasks (note the lesson learned related to this is that "*Personnel do not always use HSIs in the way designers expect* "). However, this situation may leave important information out of the operator's decision-making. Thus, secondary tasks are important and need to be carefully addressed in the design.

An HSI is most effective when it is almost transparent to its users[2]; i.e., the secondary tasks they impose demand little attention. Transparency enables users to devote their complete attention to the primary tasks. This is the essence of what it means for an interface to be "user friendly." To the extent that users must stop and think about how to interact with the HSI, attention is directed away from the primary tasks. At best, this can lead to frustration. The user's task has shifted from starting the pump to figuring out how to use the HSI. At worst, it can lead to error, which in turn can cause problems such as delaying a startup or damaging equipment. Additional characteristics of a well-designed HSI are presented in Section 4.0. The detailed guidelines in Section 4 address the design of HSI resources, such as alarms, displays, and soft controls, from an HFE perspective.

The discussion above focuses on the primary and secondary tasks that operators perform. In actual plant operation, individual operators typically do not perform these tasks alone. Instead, the tasks are accomplished by the coordinated activity of multi-person teams. Crewmembers may perform a task cooperatively from one location, such as the main control room, while in other cases a control room operator may have to coordinate tasks with personnel in a remote location. Relative to conventional control rooms, computer-based control rooms can impact teamwork in two ways: changes to the physical layout and characteristics of the workplace, and changes to the functionality of the HSIs such that activities previously performed by a crewmember are now performed by the HSI. Thus, new technology impacts teamwork, and supporting teamwork is an important design activity.

[2] The term "users" refers to the users of the plant HSIs. This mainly includes operations and maintenance personnel; although to a lesser extent, engineering and administrative staff may also be users. For the sake of simplicity, all of these personnel are collectively referred to as "users."

It is important to design the HSIs so that they enable users to efficiently and safely perform their tasks both individually and as a team.

1.4 Organization of this Document

The document is divided into six sections, including this introduction. Figure 1-2 illustrates the relationship between the sections of this Introduction. A brief description and diagram of the contents of each section is provided below.

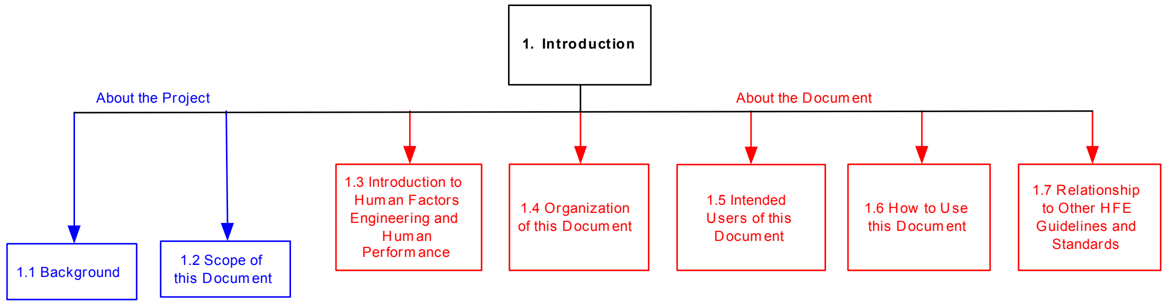

1. Introduction
About the Project
About the Document
1.1 Background
1.2 Scope of this Document
1.3 Introduction to Human Factors Engineering and Human Performance
1.4 Organization of this Document
1.5 Intended Users of this Document
1.6 How to Use this Document
1.7 Relationship to Other HFE Guidelines and Standards

Figure 1-2
Organization of Section 1

Section 2 – Control Room Modernization Planning

A significant I&C and HSI modernization project, which may extend over multiple outages, can be a challenging undertaking. It becomes more difficult when the technology employed in the modification is relatively unfamiliar to the utility undertaking the modernization project. Thus, planning is essential.

During the planning process, an endpoint vision is developed for what the utility would like the final HSI to look like. For example, the endpoint may be a computer-based control room with operator workstations, it may be a relatively unchanged control room with focused replacements of a relatively small number of HSIs such as replacing meters and recorders with computer displays of the same information, or the endpoint may be anywhere in between.

The HFE guidelines contained in Section 4 of this document support the planning process by providing planners with information about what the technology can do, i.e., its features, functions, and limitations. By understanding the capabilities and limitations of the technology, planners can determine what should be incorporated into the endpoint vision. Review of the HFE guidelines also can help planners understand some of the key design decisions involved with various elements of the HSI, e.g., strategies for presentation of alarm information or decisions on use of computer-based procedures or task-based displays.

For those projects that extend over multiple outages, a utility will have to plan for how much of a change will be made to the control room at each outage and how this will be coordinated with the I&C system upgrades. The overall sequence of modification phases or stages should lead ultimately to the desired endpoint vision for the control room. This “migration strategy” must ensure that each “interim configuration” produced in the migration will support human performance during periods of operation between outages.

As part of the overall modification planning process, utilities need to ensure that the appropriate features of an HFE program are in place to support the HFE aspects of upgrades. Utilities also need to ensure that the integration of HFE in the plant design and modification process is appropriate to support the development, design, evaluation, and modification of HSIs. An important aspect of HFE planning is establishing a methodology for grading the HFE effort. Less important modifications may need limited HFE, while a "high risk" modification may need considerably more HFE. This overall grading is addressed in Section 2.4. It is also addressed at the level of individual HFE activities in Section 3.

Another key planning consideration is determining and planning for the impact of the I&C and HSI modernization project on licensing. Planning should include when and how to interact with the regulatory authority, what the scope of the regulatory review will be, and what documentation will be necessary.

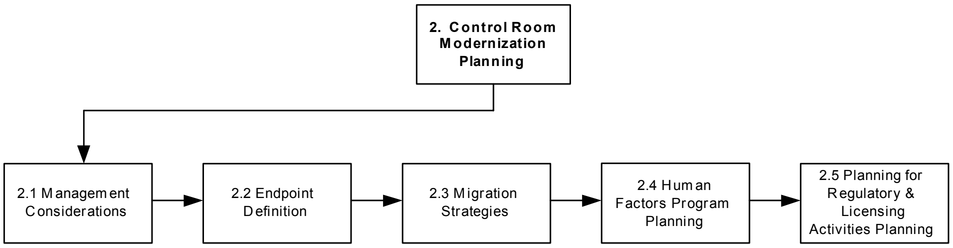

2. Control Room Modernization Planning
2.1 Management Considerations
2.2 Endpoint Definition
2.3 Migration Strategies
2.4 Human Factors Program Planning
2.5 Planning for Regulatory & Licensing Activities Planning

Figure 1-3
Organization of Section 2

Section 3 – HFE Design, Analyses, and Tools

This section describes the HFE activities and analyses that should be performed as part of the design process. The section begins with *Implementing HFE in the Design Process for Individual Modifications,* which provides a discussion of how HFE fits into the overall design process and provides guidance for planning the application of HFE for individual modifications. Then each activity is described in terms of its objectives, methods, use of results, and documentation. The methods are graded into three levels reflecting the overall grading approach determined in Section 2.4. The activities and analyses discussed are:

Operating Experience Review (OER) – this activity is performed to understand (1) current work practices so the potential impact of planned changes can be assessed, (2) operational problems and issues in current designs that may be addressed in the modernization program, and (3) relevant industry experience with candidate technological approaches to system and HSI technology.

Function Analysis and Allocation – this activity is performed to specify the roles and responsibilities of plant personnel in the performance of plant functions and tasks and how they may be changed as a result of the modification.

Task Analysis – this activity is performed to specify the requirements for successful task performance, e.g., what alarms, information, and controls are needed.

Staffing, Qualifications, and Integrated Work Design – this activity is performed to allocate new tasks to crewmembers and determine their impact on job qualifications.

Human Error Analysis – this activity is performed to evaluate the potential for human error in plant operation and maintenance and to define the circumstances surrounding an error specifically enough so that means for reducing the error can be identified.

Human-System Interface Design – this activity is performed to develop HSI and procedures that (1) reflect the plant's functional and physical design, (2) meet personnel task requirements, (3) exhibit the general characteristics of a well-designed HSI, and (4) are easy to use and learn.

HFE Verification and Validation – these activities are performed to ensure:

- the HSI supports task requirements
- the HSI is designed to accommodate human capabilities and limitations
- the integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and acceptably supports safe and economical operation of the plant

In-Service Monitoring – this activity is performed to identify and address issues and lessons learned that arise once the new systems are used on a "day-to-day" basis.

A final subsection, *Methods and Tools for Collecting Information from Users,* presents information on methods to collect information from users and test and evaluation tools and techniques.

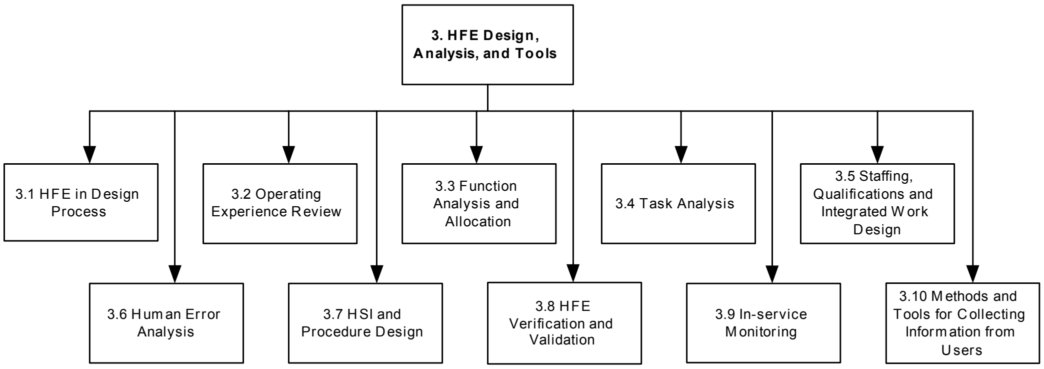

3. HFE Design, Analysis, and Tools
3.1 HFE in Design Process
3.2 Operating Experience Review
3.3 Function Analysis and Allocation
3.4 Task Analysis
3.5 Staffing, Qualifications and Integrated Work Design
3.6 Human Error Analysis
3.7 HSI and Procedure Design
3.8 HFE Verification and Validation
3.9 In-service Monitoring
3.10 Methods and Tools for Collecting Information from Users

Figure 1-4
Organization of Section 3

Section 4 – Detailed HFE Guidelines

HFE guidelines are principles for the design of HSI characteristics and functions to support human performance. The guidelines are divided into the following sections:

- Information Display
- User-Interface Interaction and Management

- Soft Controls
- Alarms
- Computer-Based Procedures
- Computerized Operator Support Systems
- Communications
- Workstation and Workplace Design

Each guidance section contains an introduction that characterizes the key features of the HSI technology and the appropriate HFE guidelines organized by that characterization. Each guideline contains design principles and supplemental information that provides further information about the guideline and how it can be applied. The sections also contain a checklist of the guidelines and additional sources of information that the designer can consult.

The HFE guidelines have broad applicability in the modernization process including supporting the development of an endpoint vision, providing the basis for style guide development, and providing criteria for design verification.

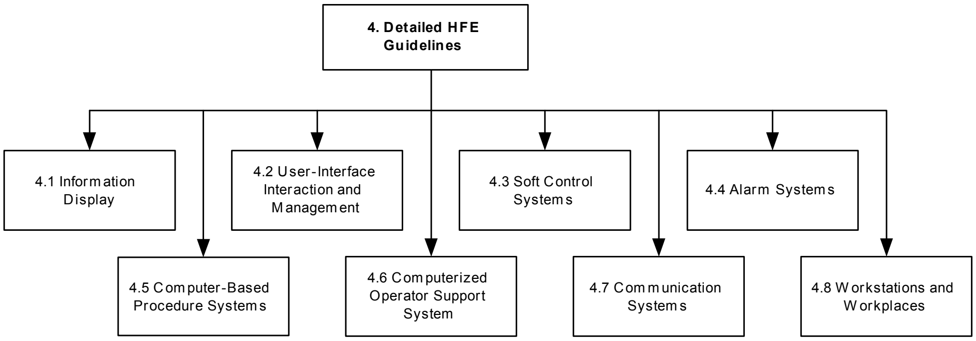

4. Detailed HFE Guidelines
4.1 Information Display
4.2 User-Interface Interaction and Management
4.3 Soft Control Systems
4.4 Alarm Systems
4.5 Computer-Based Procedure Systems
4.6 Computerized Operator Support System
4.7 Communication Systems
4.8 Workstations and Workplaces

Figure 1-5
Organization of Section 4

Section 5 – Regulatory and Licensing Activities

Regulatory and licensing activities are an important part of any modernization program. Up-front planning can help reduce the cost of activities related to regulatory compliance and can minimize licensing risk. Guidance on licensing activities specific to the human performance considerations related to I&C, control room, and HSI modernization is provided.

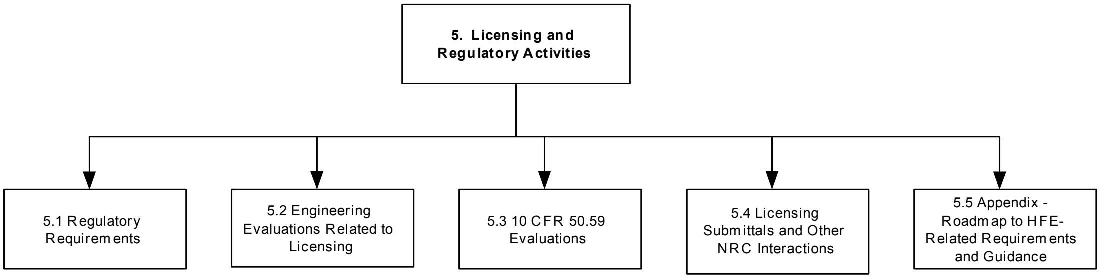

5. Licensing and Regulatory Activities
5.1 Regulatory Requirements
5.2 Engineering Evaluations Related to Licensing
5.3 10 CFR 50.59 Evaluations
5.4 Licensing Submittals and Other NRC Interactions
5.5 Appendix - Roadmap to HFE-Related Requirements and Guidance

Figure 1-6
Organization of Section 5

Section 6 – Special Topics Related to Operations and Maintenance

This section provides guidance for several special topics related to I&C and HSI modernization. They are briefly described below.

Human Factors Engineering for the Maintenance of Digital Systems (Section 6.1) – A key driver for the transition from analog to digital systems is the potential for reduced operations and maintenance costs. These reductions may be in the form of labor savings, hardware savings, or reduced threats to plant availability or safety during maintenance operations. For digital systems to achieve these improvements in the most cost efficient manner, maintainability must be formally emphasized in all phases of the design process. This section provides human factors guidance for the maintenance of digital systems, and the effects of I&C modernization on maintenance of human system interfaces and special considerations for the design of maintainers' HSIs.

Human Factors Engineering for Configuration Management (Section 6.2) – This section addresses those aspects of configuration management of a digital upgrade modification that may affect the performance of human tasks at the system interfaces, other information or data that is used in the tasks at the human system interfaces to operate or service the plant, and the human factors issues in controlling the configuration and use of user-definable features.

Training Considerations Unique to Digital I&C Modernization Programs (Section 6.3) – New digital I&C and computer-based HSIs will impose new demands on training programs to address their operation and maintenance. The new systems may significantly alter the way tasks are performed and may result in new tasks for which training needs to be developed. Two unique aspects need to be considered:

- New issues that need to be addressed in training related to the impact of digital I&C and computer-based HSIs on operations and maintenance
- Managing and scheduling changes to the simulator while supporting training and qualification of the operators on the existing and modified designs, especially when changes extend over multiple outages and multi-unit plants are involved

This section addresses the training considerations related to new digital I&C systems and computer-based HSIs.

Safety Monitoring and Control in Modernized Control Rooms (Section 6.4) – In most plants there are many different systems that have HSI aspects related to monitoring and control of plant safety functions, including SPDS, PAMS (PAMI), RPS (RTS), ESFAS, and BISI. There has not been a uniform or consistent approach applied to the design of these HSIs. As a result, they tend to be separate and isolated systems that are rarely used and that may not follow the conventions of the other control room HSIs. Also, the regulatory guidance applicable to these areas was written long ago and was based primarily on the analog technology prevalent in control rooms at that time. With I&C and HSI modernization, better and more integrated approaches are possible.

This section addresses these issues. It also considers the need to provide diverse HSI capabilities that allow the operators to cope with postulated failures or degradation of the HSIs that are normally used, while still providing a well-integrated HSI for both normal and emergency plant operating conditions.

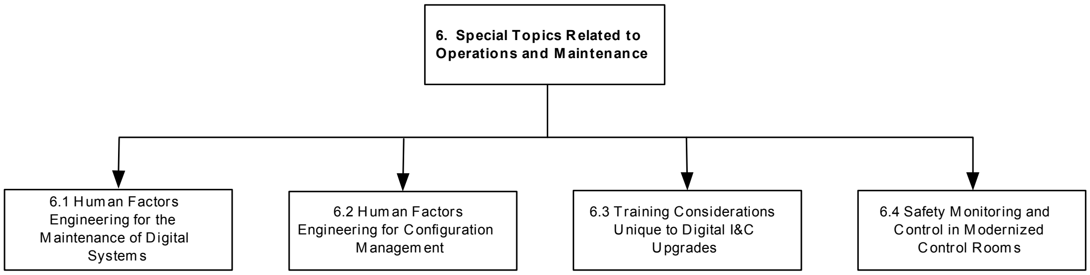

6. Special Topics Related to Operations and Maintenance
6.1 Human Factors Engineering for the Maintenance of Digital Systems
6.2 Human Factors Engineering for Configuration Management
6.3 Training Considerations Unique to Digital I&C Upgrades
6.4 Safety Monitoring and Control in Modernized Control Rooms

Figure 1-7
Organization of Section 6

1.5 Intended Users of this Document

The intended users of this guidance are:

- plant personnel, including operators, engineers, maintainers, and managers responsible for modernization projects
- I&C designers
- control system suppliers
- third party implementers

This document was developed for use by the organizations and design team members responsible for designing and evaluating the HFE aspects of the plant I&C modernization. For significant modifications, it is expected that the individuals using this guidance will be part of a multidisciplinary design team (this is discussed further in Section 2).

While the main users should be knowledgeable in HFE, they are not expected to be human factors experts. The guidance is intended to help users identify when the assistance of such experts would be beneficial.

1.6 How to Use this Document

This document can be used to develop a variety of products as part of an I&C modernization program, including:

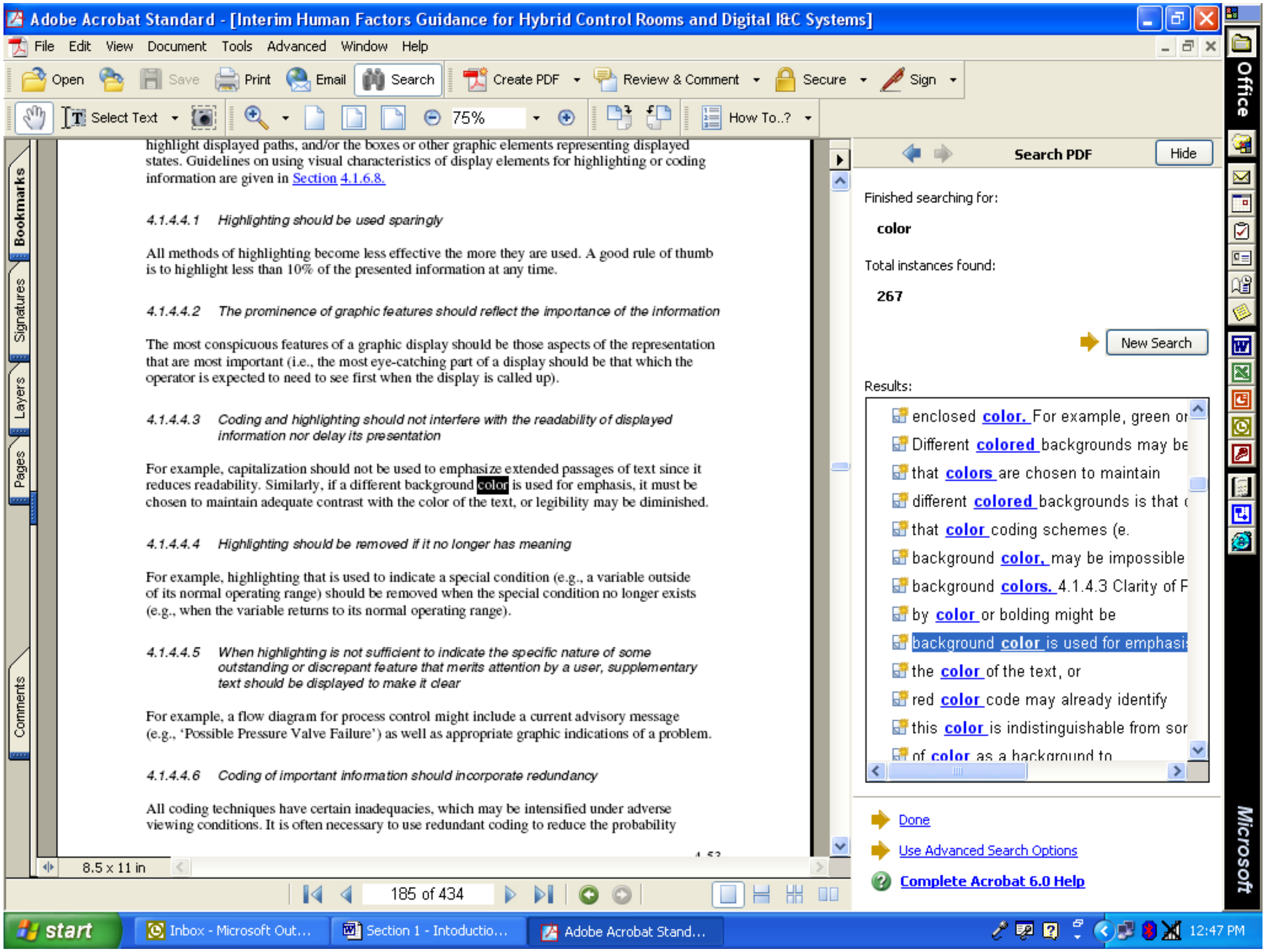
- An endpoint vision for the control room and other changes to the HFE aspects of the plant
- A migration plan for implementing the endpoint vision over a series of modifications
- Plant-specific HFE procedures
- HSI specifications
- Detailed HSI designs
- Tests and evaluations of designs
- Training program modifications

HFE documents are needed to support the planning, design, evaluation, and implementation of the HFE aspects of a plant modernization program. Plant specific documentation can be developed directly from the material contained herein by tailoring the guidance provided to the unique engineering procedures and design goals of individual utilities.

It is anticipated that the primary use of this document will be as a reference that is accessed and used when specific needs arise. For example, the guidelines in Section 4.4, Alarm Systems, will be accessed when the designer is developing an alarm specification, a plant-specific guidance document describing the characteristics and functions of how their computer-based alarms should function, or a checklist for alarm system evaluation. That guidance can also be used when future modifications of the alarm system are being planned and implemented.

In light of this concept of usage, it is not anticipated that the document will be read from cover to cover. Thus, when the user is in a specific section of interest such as Section 4.5 Computer-Based Procedures, the document contains extensive cross-referencing to related sections users should be aware of in other parts of the document. As this is an electronic document, these cross-references are hyperlinked for easy access.

Another important feature is the ability to find information of interest (which may be in multiple sections). To support the user in this type of search, a context-sensitive search feature is provided. That is, a desired term can be entered into the document's search function and the results (displayed on the right-hand side of the screen) show each instance of the desired term along with the surrounding text where that instance occurs (see Figure 1-8). Thus, it is easy for the user to locate the specific instances where the term appears in the desired context.


Adobe Acrobat Standard - [Interim Human Factors Guidance for Hybrid Control Rooms and Digital I&C Systems]
File Edit View Document Tools Advanced Window Help
Open Save Print Email Search Create PDF Review & Comment Secure Sign
Select Text 75% How To..?
Bookmarks Signatures Layers Pages Comments
8.5 x 11 in
185 of 434
Search PDF Hide
New Search
Done
Use Advanced Search Options
Complete Acrobat 6.0 Help
Office Microsoft
start Inbox - Microsoft Out... Section 1 - Intoductio... Adobe Acrobat Stand...
12:47 PM

highlight displayed paths, and/or the boxes or other graphic elements representing displayed states. Guidelines on using visual characteristics of display elements for highlighting or coding information are given in Section 4.1.6.8.

4.1.4.4.1 *Highlighting should be used sparingly*

All methods of highlighting become less effective the more they are used. A good rule of thumb is to highlight less than 10% of the presented information at any time.

4.1.4.4.2 *The prominence of graphic features should reflect the importance of the information*

The most conspicuous features of a graphic display should be those aspects of the representation that are most important (i.e., the most eye-catching part of a display should be that which the operator is expected to need to see first when the display is called up).

4.1.4.4.3 *Coding and highlighting should not interfere with the readability of displayed information nor delay its presentation*

For example, capitalization should not be used to emphasize extended passages of text since it reduces readability. Similarly, if a different background color is used for emphasis, it must be chosen to maintain adequate contrast with the color of the text, or legibility may be diminished.

4.1.4.4.4 *Highlighting should be removed if it no longer has meaning*

For example, highlighting that is used to indicate a special condition (e.g., a variable outside of its normal operating range) should be removed when the special condition no longer exists (e.g., when the variable returns to its normal operating range).

4.1.4.4.5 *When highlighting is not sufficient to indicate the specific nature of some outstanding or discrepant feature that merits attention by a user, supplementary text should be displayed to make it clear*

For example, a flow diagram for process control might include a current advisory message (e.g., 'Possible Pressure Valve Failure') as well as appropriate graphic indications of a problem.

4.1.4.4.6 *Coding of important information should incorporate redundancy*

All coding techniques have certain inadequacies, which may be intensified under adverse viewing conditions. It is often necessary to use redundant coding to reduce the probability

4-53

Finished searching for:

color

Total instances found:

267

Results:

- enclosed color. For example, green or
- Different colored backgrounds may be
- that colors are chosen to maintain
- different colored backgrounds is that
- that color coding schemes (e.
- background color, may be impossible
- background colors. 4.1.4.3 Clarity of F
- by color or bolding might be
- background color is used for emphasis
- the color of the text, or
- red color code may already identify
- this color is indistinguishable from sor
- of color as a background to

Figure 1-8
Context-Sensitive Search Results

1.7 Relationship to Other HFE Guidelines and Standards

There are many HFE standards and guidance documents available. This document is different from most of the others in several important respects:

- First, most HFE documents are oriented toward design of a new control room. This document specifically addresses the modification and upgrading of existing control rooms. Thus, the unique issues associated with modification projects are identified and addressed. Further, maximum attention is focused on integrating the HFE activities with existing plant processes. However, it should be noted that many of the guidelines in this document would also support the design of a new control room.
- Second, most HFE documents are fairly high-level. For example, they may specify that certain analyses should be performed, such as task analysis, but they do not provide a specific methodology to do so. This document provides detailed methodologies that can be used by utility personnel.
- Third, most documents focus on design of HSIs, while this document addresses a broader range of plant modernization considerations - from planning to monitoring the modifications once they are in place.

While most of the information contained in this document can be used in stand-alone fashion, there are places where the user is directed to other documents, such as NUREG-0700 and EPRI NP-3659. This practice is limited and occurs where material is relevant to the discussion, but is out of the scope of this document. An example is the design of conventional HSIs. The focus of this document is on computer-based HSIs, so the user is directed to other HFE documents that address conventional HSIs. Another situation where the user is directed to another document occurs when very detailed and readily usable guidance is available in the other document. An example of this is detailed guidelines related to the auditory characteristics of alarms.

With respect to NRC HFE review documents, both NUREG-0711 and -0700 were used in the development of this document. For example, NUREG-0711 was used in the development of Section 3. However, the NRC guidance provides review criteria and not specific methodologies to use. This document provides specific methodologies that should be generally consistent with the review criteria.

NUREG-0700 was a source of information in Section 4. However, the guidance given here was developed to support a design effort rather than a design review, many guidelines have been updated based on new information not reflected in NUREG-0700, and the guidelines were further modified because of the extensive industry review and revision process that was used during the development of this guidance. As a result, the specific criteria used by the NRC in a review or inspection may be somewhat different from the guidelines contained here. However, use of the guidelines contained in this document should provide a good HFE design that meets regulatory requirements and expectations.

2
CONTROL ROOM MODERNIZATION PLANNING

This section provides guidance on planning the modernization of the main control room and other human-system interfaces (HSIs). This includes defining a target endpoint or vision for the control room that will result from the modernization program. Guidance is also provided on developing a migration strategy – a plan for how the control room will evolve over time to reach the chosen endpoint.

An objective of this guidance is to help plants plan control room changes that make appropriate use of modern technologies, minimize the likelihood of human errors, and make substantive improvements in human performance. The guidance is intended to cover a broad spectrum of potential changes to the control room. Such changes range from the replacement of a few obsolete components with newer digital devices, up to a full modernization program that makes incremental changes over a number of years to arrive at a much more advanced control room with compact, computer-based work stations.

Modernization planning for the control room and other HSIs should be done in concert with planning of the overall I&C modernization and upgrade. The focus of the discussion in this section is on the HSI design, human factors engineering (HFE), and human performance considerations including issues specifically associated with hybrid HSIs. Some limited guidance is provided on the interaction between control room modernization planning and modernization planning for the instrumentation and control systems.

Intended Users of the Guidance in this Section

The planning guidance in this section is intended primarily for those plants that have not yet determined an endpoint or a plan for their control room modernization. However, the guidance also can be used by plants that have already set a direction and vision for the modernized control room. It can be used to help evaluate and strengthen the endpoint conceptual design and its technical basis, develop a migration strategy, identify hard spots or difficulties that may be encountered, and define the potential benefits that might be achieved with the chosen approach. Also, the guidance can be used to re-assess the endpoint vision and migration strategy when necessary as plant conditions, priorities, and available technologies change over time.

The planning effort should include input and participation by all of the key stakeholders in the control room modernization. Typically this will include at a minimum plant operators, I&C design engineers, human factors engineers, human performance group, systems engineers, training, purchasing, and plant maintenance personnel. The guidance given here is intended for use by this entire team, with particular emphasis on operations, human factors engineering, human performance, and design. In addition to plant personnel, it is expected that this guidance will be used by vendors and suppliers who will provide I&C and HSI systems and perform design and applications engineering in support of the plant's modernization program.

Managers responsible for I&C and control room upgrade projects also can benefit from the guidance given here, particularly Section 2.1, Management Considerations.

Additional Sources of Guidance

Other important industry documents that are sources of guidance and should be used in conjunction with the planning guidance given here include:

EPRI TR-102348 (NEI 01-01). This is the industry guideline on design and licensing of digital I&C systems. It covers the overall I&C upgrade design process, dealing with digital systems issues such as software common mode failure, diversity and defense-in-depth. It specifically addresses digital issues in the context of 10 CFR 50.59 evaluations and determining the need for license amendments when making changes to the I&C systems and human-system interfaces. TR-102348/NEI 01-01 was endorsed by NRC in Regulatory Issue Summary RIS 2002-22.

NUREG 0800 (Standard Review Plan). The SRP provides guidance to NRC reviewers, but it also provides a source of guidance and understanding of NRC expectations related to I&C and HSI upgrades. Chapter 7 covers the I&C systems, and Chapter 18 covers human factors and the human-system interface. It is expected that NUREG 0711 (cited below) will be incorporated into NUREG 0800 in the future.

NUREG 0711. This document describes the NRC expectations for a plant’s human factors program and appropriate HFE design and evaluation processes. Originally written primarily for application to new plant designs, a recent revision added more guidance related to plant upgrades and modifications. This document is referenced by the Standard Review Plan, NUREG 0800.

IEEE Std 1023. This standard addresses planning and application of human factors engineering in the design, operation, testing and maintenance of nuclear power plant facilities, systems and equipment.

IEC 62096. This new international standard provides guidance on decisions related to modernization. It provides high-level guidance on overall I&C modernization, as well as some guidance related to modernizing the control room/HSI.

This list identifies only the primary nuclear industry and NRC guidance documents that relate to HSI modernization planning. There are many other references, standards and guidance documents covering related topics and providing more detailed guidance that can be used as needed during the planning and design of HSI modifications. For example, NUREG 0700 is a key source of detailed human factors guidelines useful for design and evaluation of HSIs. The references listed above are those that are considered most useful during the planning stage.

The Planning Process

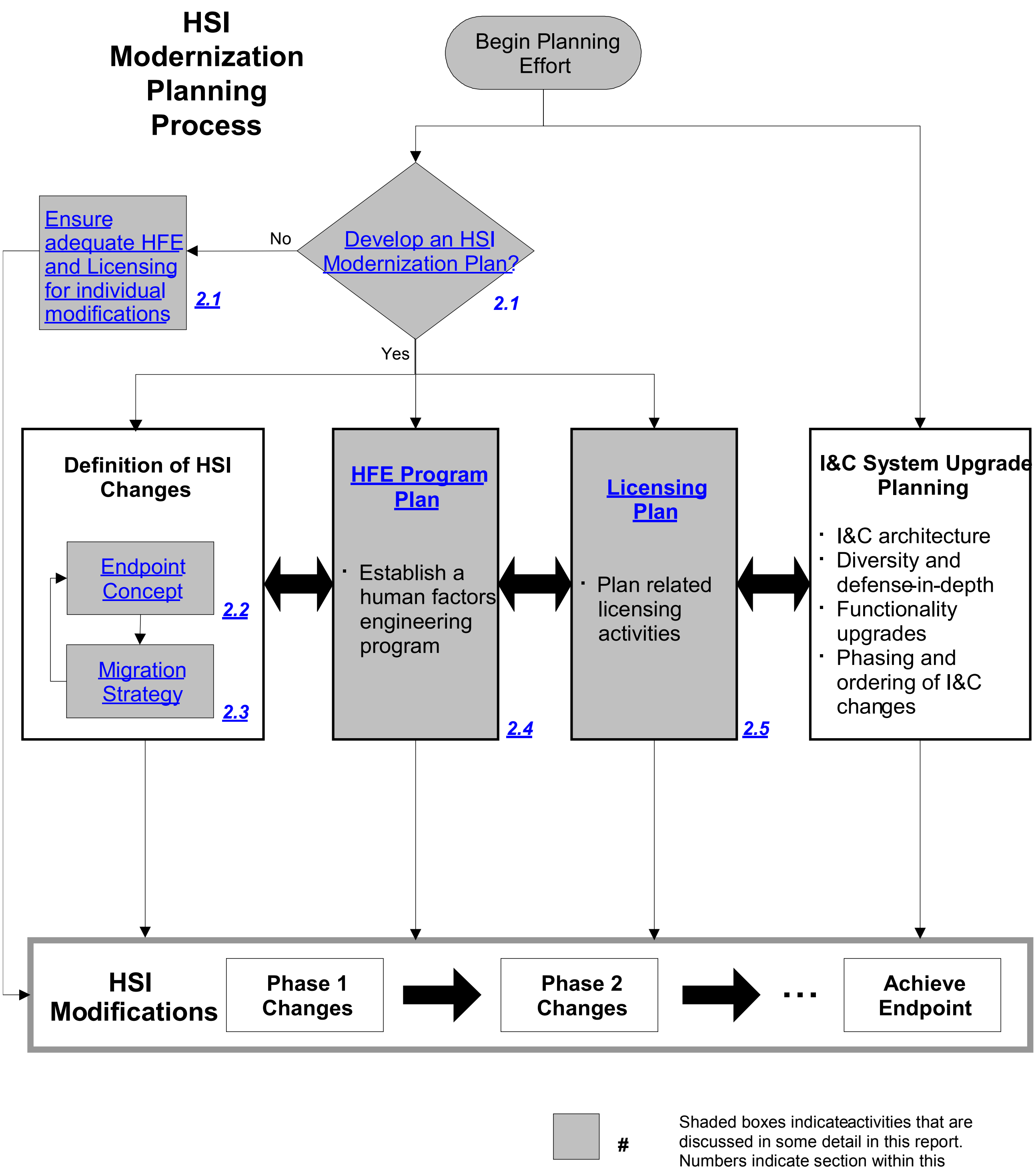
Figure 2-1 illustrates the overall HSI modernization planning process. Objects that are shaded in the figure represent activities that are addressed specifically in this section (the corresponding section number is shown next to the object in the diagram). These include:

- Making a **decision** on whether to develop an overall HSI modernization plan before proceeding with the modifications. This and other management considerations are discussed in Section 2.1 of this document.
- Definition of a control room **endpoint** or vision. Defining an endpoint or vision for the desired control room/HSI will help guide the changes that are made, and can help ensure that they are accomplished in an orderly and efficient manner. An important part of this is defining a "concept of operations" for the updated control room – how the plant will be operated under normal and abnormal conditions, and how the operators' roles and responsibilities may change with the modernized control room and HSI equipment. This includes consideration of operation under conditions of failed or degraded I&C systems or human-system interfaces (e.g., failure of workstation displays). Guidance on endpoint definition is given in Section 2.2 of this document.
- Definition of a **migration path**, or series of steps to be taken to achieve or work toward the desired endpoint. HSI changes will be driven primarily by the strategy chosen for phasing or staging of the I&C upgrades. Nevertheless, decisions will have to be made regarding how far and how fast the plant should go in modernizing the control room and HSI equipment as the I&C changes are made over time. This includes ensuring that interim, hybrid configurations are self-consistent and incorporate good human factors engineering to support operation until the next set of changes is made. Guidance on developing a migration strategy is provided in Section 2.3 of this document.
- Development of an overall **human factors program** and plans and procedures for individual modifications that will be made as part of the migration strategy, including internal HFE practices and procedures, plant-specific design guidelines that will be followed, graded approach for application of HFE activities and analyses, interaction with procedures and training, etc. Guidance on human factors program planning is provided in Section 2.4.
- Development of a **licensing plan**, or an approach to address licensing issues related to the HSI changes considering 10 CFR 50.59 requirements, submittals that may be required, and impact of the changes on operator qualification and licensing. Guidance on developing a licensing plan is provided in Section 2.5.

Planning of the control room modernization should be done in concert with development of an I&C system upgrade or modernization plan. Interaction between I&C upgrade planning and HSI modernization planning is discussed in this section, but I&C planning itself is not directly addressed in this document. EPRI has produced a number of other guidance documents related to I&C upgrades and development of upgrade plans.

The double arrows shown in the diagram are meant to illustrate the interaction among these various activities. All of these are interdependent and typically are performed iteratively as part of the overall planning process.

Also, note that although Figure 2-1 shows the HSI changes being made in several steps or phases, this is not to preclude the possibility of implementing all the changes in one large modification, e.g., during an extended outage. The guidance on migration strategy provided in Section 2.3 includes considerations related to the number of steps to take in modernizing the HSI.


HSI Modernization Planning Process
Begin Planning Effort
Develop an HSI Modernization Plan?
2.1
No
Ensure adequate HFE and Licensing for individual modifications
2.1
Yes
Definition of HSI Changes
Endpoint Concept
2.2
Migration Strategy
2.3
HFE Program Plan
· Establish a human factors engineering program
2.4
Licensing Plan
· Plan related licensing activities
2.5
I&C System Upgrade Planning
· I&C architecture
· Diversity and defense-in-depth
· Functionality upgrades
· Phasing and ordering of I&C changes
HSI Modifications
Phase 1 Changes
Phase 2 Changes
. . .
Achieve Endpoint
#

▨ # Shaded boxes indicateactivities that are discussed in some detail in this report. Numbers indicate section within this document where the topic is addressed.

Figure 2-1
HSI Modernization Planning Process

2.1 Management Considerations

2.1.1 The Need for Planning
2.1.2 Objectives of the Planning Effort
2.1.3 Minimum Planning Activities
2.1.4 Levels of I&C and HSI Modernization
2.1.4.1 I&C Modernization Levels
2.1.4.2 HSI Modernization Levels
2.1.5 Interaction between I&C and HSI Modernization Planning
2.1.6 Concept of Operations
2.1.7 Importance of Involving Operations Personnel
2.1.8 Consideration of Available Systems and Equipment
2.1.9 Scheduling Challenges
2.1.10 Documentation of the Planning Effort
2.1.11 Human Factors Engineering
2.1.12 Licensing Considerations

Modernization of the instrumentation and controls and human-system interfaces of a nuclear power plant is a major undertaking with the potential to make significant improvements in human performance and plant operation. There are a number of things to consider from a management standpoint when embarking on an HSI modernization program. These are discussed briefly below.

2.1.1 The Need for Planning

In the past, changes to the instrumentation and control systems and human-system interface have been made largely in a piecemeal fashion, with each individual change designed and implemented on its own. This process can continue with further changes made piecemeal as the I&C systems are modernized. However, for most plants this is not the most cost effective or efficient way to make the changes.

In addition, past history has shown that modifications have been a significant source of human factors deficiencies in nuclear plant control rooms. Changes that are made in a piecemeal fashion tend not to be well integrated or even consistent in their human-system interface characteristics. Also, when they are done individually without an overall HSI modernization plan, they typically are “shoe-horned” into the existing control room with inevitable compromises in human factors and human performance aspects of the changes. Over time the changes can degrade the overall effectiveness of the control room, have a negative impact on operations due to the lack of an overall operational concept for the modified control room, and result in significant re-work down the road. Also, if the HSI aspects of the changes are not properly planned, this can negate the advantages that would be expected from the implementation of newer digital technologies.

The best approach is to plan the HSI changes that will take place as I&C systems are upgraded and modernized. This is particularly important for plants that are committed to or considering plant life extension, but it is beneficial for any plant faced with a series of I&C changes and upgrades. It is mandatory for plants that want to make significant improvements in human performance and take maximum advantage of the I&C and HSI technologies that will be introduced as the systems are modernized.

2.1.2 Objectives of the Planning Effort

An HSI modernization planning effort performed up-front can help the plant accomplish a number of important objectives. For example, the planning effort should help:

- Define key operational, economic and human performance **objectives and ground rules** for the modernization, consistent with the overall goals of plant Management
- Ensure that the changes fit the Operations group's overall **concept of plant operations** and how they envision it should evolve as modernization progresses
- Make sure that the changes made over time fit a **common vision for the control room** and plant operation, minimizing re-work as much as possible to keep costs down
- Ensure that each of the steps taken to achieve the modernization is **consistent with the resources available** at the time, including finances, time (e.g., outage time) and people (engineering, operations, maintenance, training, etc.)
- Ensure **consistency and integration** of the modifications that may be made over many years
- Complete some of the **HFE planning** and process definition once up-front, consistent with good design practice and NRC expectations, and then use and re-use this as each modification is made, including large upgrade steps and smaller component-level replacements – this includes defining a **graded approach** to application of HFE (this is discussed in Section 2.4)
- Ensure that existing **human factors/human performance problems** are addressed and, where practical, resolved by the modifications
- Take advantage of opportunities to make further improvements in the human-system interface and control room through **appropriate use of technology**, with the aim of achieving economic benefits as part of the modernization
- Appropriately address issues related specifically to **hybrid HSIs** (examples of these are given in Section 2.3, Migration Strategy)
- Develop a plan for licensing that will **minimize licensing risk** (note that the HSI licensing plan will be a subset of the overall I&C licensing plan)
- Ensure that the final endpoint of the modernization, and the **interim configurations** or stopping points along the way, are well planned and self-consistent, and meet the applicable regulatory requirements and expectations
- Ensure that operator **training and procedures**, changes to the simulator, and operator licensing issues are properly addressed at each step in the modernization

- Develop the plans such that there is **flexibility for change** as plant conditions change, budgets and priorities are modified, and technologies evolve over the time it takes to complete the modernization.

2.1.3 Minimum Planning Activities

Some plants may choose to short cut the planning process and proceed with individual I&C and HSI changes in the absence of an overall HSI plan. This path is shown on the far left-hand side of Figure 2-1. If this option is chosen, it is important at a minimum to ensure that:

- Appropriate human factors engineering processes and principles are applied in the design and implementation of the changes
- Hybrid HSI issues are adequately addressed (examples of these are provided in Section 2.3)
- Consistency and cumulative effects of changes made over time are considered as each change is made, and
- The pertinent regulatory requirements are met.

Although this option is not recommended, those plants that choose it or whose circumstances force them to proceed with some initial modifications and postpone the overall planning to a later phase, should ensure that these items are adequately addressed. The guidelines in Sections 3 and 4 of this document should still be used when designing and evaluating the individual modifications.

The most effective and highly recommended approach is to first develop an overall HSI modernization plan following the process outlined in the main path of Figure 2-1. The plant can then proceed with a set of well-planned changes that are coordinated with the plant's I&C upgrade program and that best support the plant's operational, economic and safety goals.

2.1.4 Levels of I&C and HSI Modernization

The guidance in this document assumes that the plant has developed or is developing a long-range plan for addressing I&C obsolescence. This includes development of an overall strategy and architecture for the I&C, a prioritization of the needed I&C system upgrades, and an I&C upgrade or modernization plan. The planning process for the human-system interface needs to be coordinated with the I&C system upgrade planning.

Just as there are different levels of modernization that can be pursued for the I&C systems, there are different levels to which the HSI can be modernized as well. The level of HSI modernization that can be achieved depends on the degree to which the I&C systems are modernized.

Figure 2-2 illustrates this. For the sake of simplicity, the figure shows three levels of upgrade or modernization for the I&C and HSI systems.

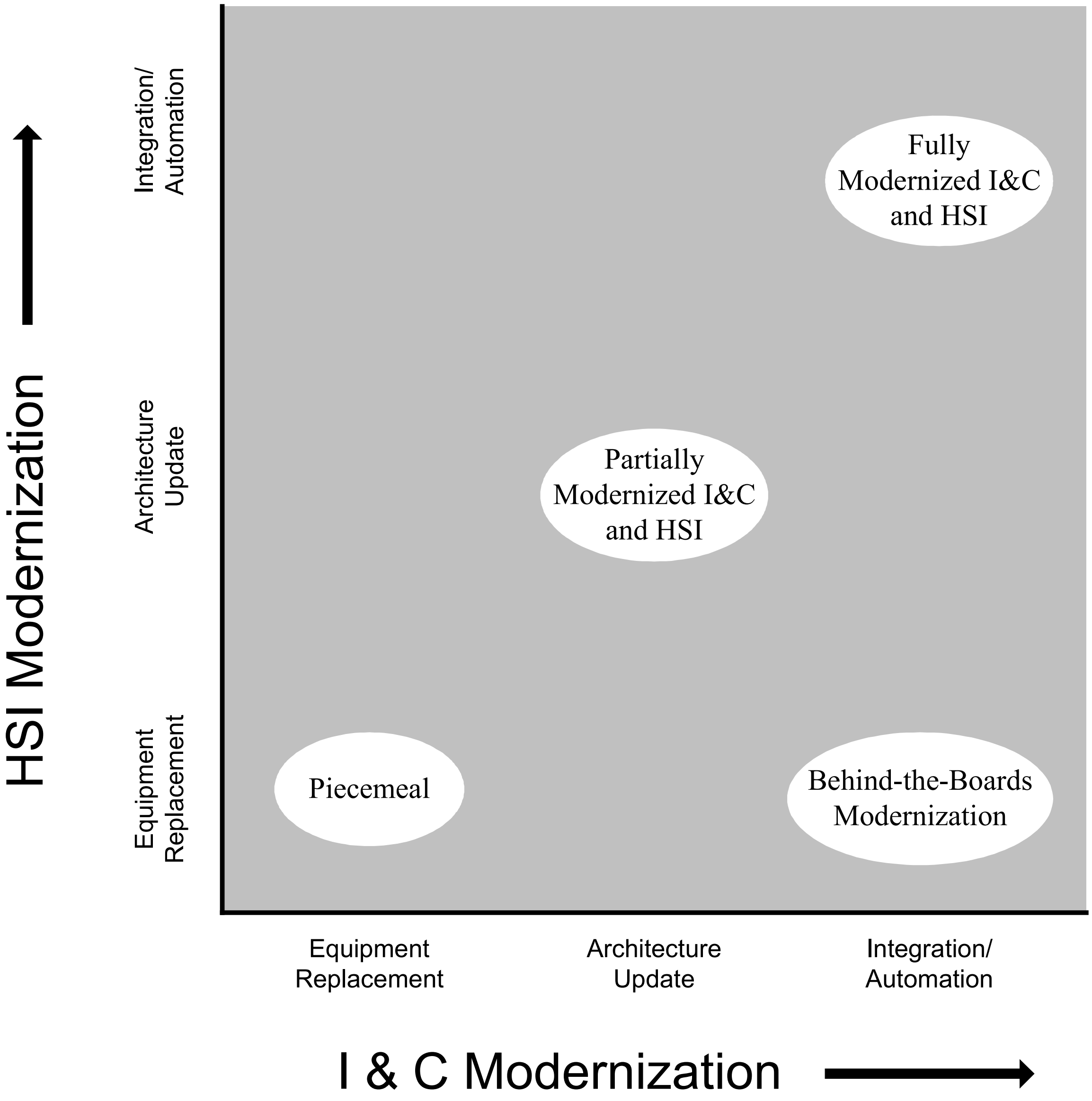


Figure 2-2
Levels of Modernization of the I&C Systems and the Control Room/HSI: Equipment, Architecture, and Integration/Automation

2.1.4.1 I&C Modernization Levels

- Equipment replacement – individual pieces of equipment are replaced with more modern devices, without any significant change in functionality. Some level of standardization may also be accomplished as the equipment is replaced.
- Architecture update – an updated architecture is implemented for the monitoring, control and protection systems that provides additional flexibility and functionality, and achieves further standardization through use of common platforms.

- Integration and automation – I&C systems are integrated functionally to achieve specific performance improvements, and additional automation is implemented in the control systems and HSI.

The extent of the changes needed and the benefits achieved vary significantly for these different levels of I&C modernization.

There are similar levels that can be pursued for HSI modernization. Again, for simplicity it is useful to think of three levels of modernization:

2.1.4.2 HSI Modernization Levels

- Equipment replacement – as with the I&C, the HSI equipment and devices on the control panels, benchboards, etc., can be replaced individually without any significant change in functionality. A level of standardization also might be achieved (e.g., standardizing on a particular type of digital meter or recorder).
- Architecture update – in existing plants, not only is the HSI equipment outdated, but the overall architecture of the human-system interface and main control room is obsolete by modern-day standards. By HSI architecture we mean the configuration and arrangement of the interfaces. Compared to a conventional control room with many discrete controls, indicators and annunciators spread out along panels, a modernized control room consolidates these at seated workstations with soft controls, video displays of information, and alarm information screens.
- Integration and automation – a further level of advancement is functional integration of the various HSI elements. An example is a computerized procedure system that, in addition to presenting and allowing execution of a procedure, also integrates the display of relevant information, provides needed control capabilities, and provides alarms pertinent to each step. In addition, a higher level of automation can be implemented, including automation of data collection, data recording, and checking as well as automation of control actions. Also, more intelligence can be provided in alarm processing, information display, support of control actions and tasks, etc. This can be integrated functionally into the primary HSI as opposed to use of standalone operator aids or operator support systems.

Note that there are many variations within each of these three “levels.” As noted above for the I&C, the extent of the modifications needed to modernize the HSI and the benefits achieved from the modernization (in this case, improvements in human performance) vary widely depending on the level of modernization that is undertaken.

2.1.5 Interaction between I&C and HSI Modernization Planning

Although there is some flexibility in choosing how far to go with the HSI, the degree to which it can be modernized clearly depends on the level of I&C modernization. For example, upgrading to compact workstations providing plant-wide access to controls and information requires an I&C communications and control architecture that allows access to multiple systems and functions across the plant. Decisions made regarding defense-in-depth and diversity and plans for backup controls and indications will impact the HSI architecture due to the need to integrate the diverse backups into the overall HSI. Decisions on which HSIs will be implemented using qualified (safety-related) equipment may have an impact. Also, when changes are made in steps or phases, the I&C changes made at each step must support the HSI upgrades that are to be made.

Clearly the I&C upgrade plans will be a major driver of the HSI changes. However, the interaction goes both ways. Human factors and Operations considerations, and the plant's choice of a control room endpoint and method for migrating toward the endpoint can, and should have a significant impact on the I&C upgrade plans. It is particularly important that an overall "concept of operations" be defined for the modernized control room, and the plans for individual I&C upgrades and HSI changes consider how this concept of operations will evolve over time until the endpoint is reached.

2.1.6 Concept of Operations

Concept of operations refers to the way in which the operating crew is organized and monitors and controls the plant under normal and abnormal conditions. This includes items such as:

- Crew size and makeup (number of reactor operators, senior reactor operators, supervisors, etc.)
- Main control room (MCR) functions and responsibilities (e.g., degree of centralization of functions in the MCR)
- Allocation of functions to the operating crew versus automated systems
- Assignment of duties and stations to members of the crew under different operating conditions
- Crew coordination and supervision
- Operation under failed or degraded I&C/HSI conditions
- How the MCR crew interacts with other personnel such as equipment operators, maintenance technicians, engineers, emergency personnel, etc.

It is important to understand how the concept of operations may change as the control room and other HSIs are modernized. Roles and responsibilities of the operator change as modern I&C and HSI systems are introduced, particularly as systems and lower-level HSI functions are automated and information, controls, and procedures are integrated in a modern control room.

Figure 2-3 illustrates this, using the levels of I&C and HSI modernization identified above. As the HSI is modernized, the operator spends less time on low-level tasks such as getting readings from individual sensors, checking status indicators, making logs, and performing sequences of low-level control actions (e.g., system line-ups). Higher-level information and task support and automation are provided that allow the operator to monitor the plant at a higher level and act more as a supervisor of automated systems. Experience in plants that have operated with modern control rooms has shown that the division of responsibility and allocation of tasks among the operators change when greater automation is introduced. Automation of previously manual HSI functions and use of computer-based procedures integrated into the HSI tend to make the computer system act essentially as another member of the crew. This should be reflected in the allocation of tasks to the human operators. The concept of operations is discussed further in Section 2.2 on endpoint definition.

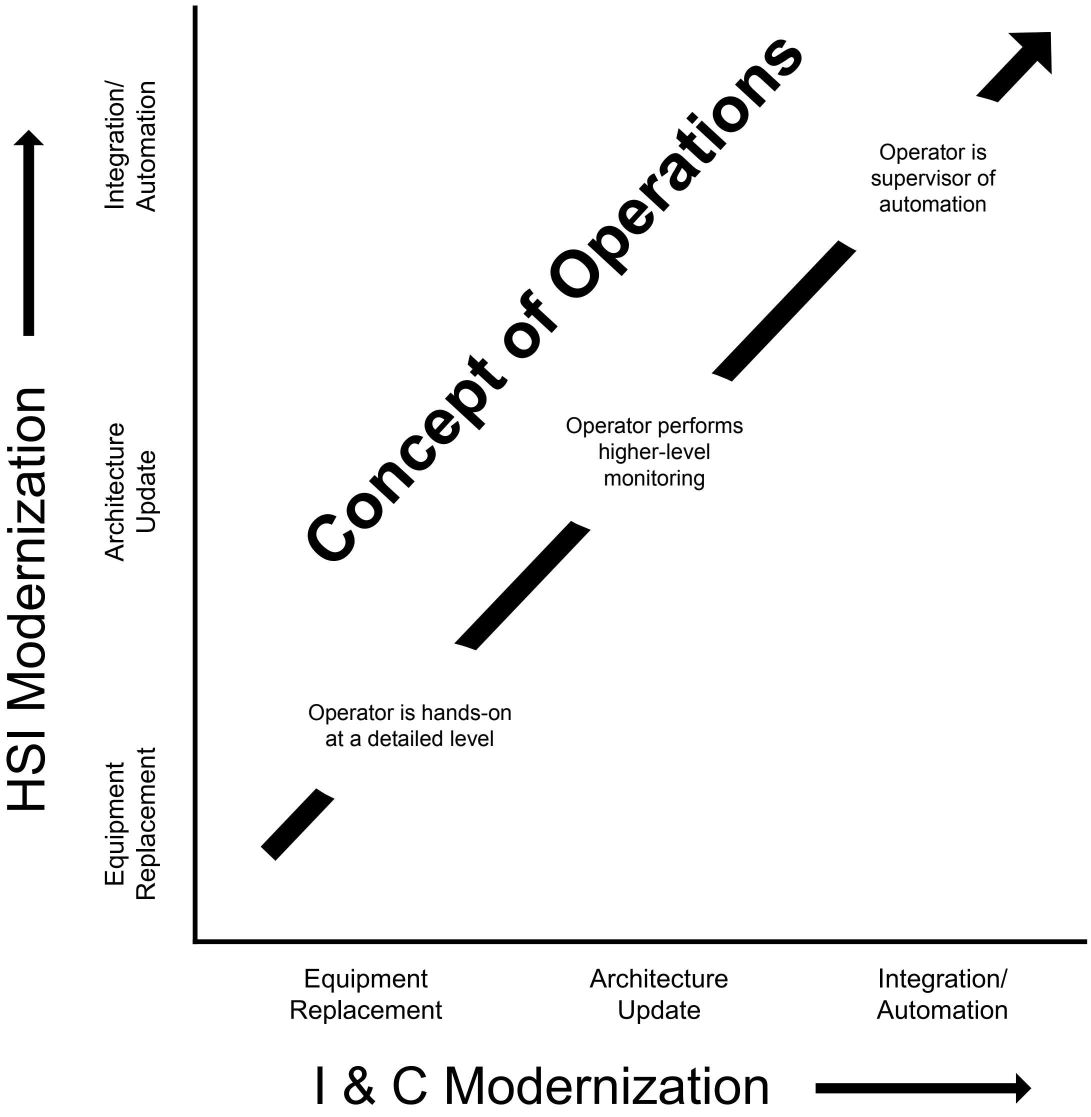


Figure 2-3
Evolution of the Control Room Concept of Operations

2.1.7 Importance of Involving Operations Personnel

The importance of direct involvement of Operations personnel including licensed operators in the HSI modernization planning cannot be over-stated. Experience has shown many times over that user involvement is critical to the success of a human-system interface design or modification. In other industries, such as aviation, it has been recognized that designs need to be "human-centered" in order to be effective (see, for example, ISO 13407). Creating a human-centered design requires getting users involved in the design effort.

This is true for new designs, but it is even more important for modifications such as those that will be undertaken to modernize an operating plant's control room. Typically, only operations personnel fully understand integrated plant operations. This is because as the plant has operated over time the operators have developed methods of operation, preferred work practices, and their own mental models of the plant and its operation. Some of this has been driven by the original design or standard approaches used by the industry. However, each plant has developed its own practices based on the specific plant and systems design, modifications made over the years, experience gained from operation including unusual events and upsets, and the particular people involved. This has led to a concept of operations that is plant-specific, not fully documented, but well understood and ingrained in the operating crews. Determining the specifics of the existing concept of operations as it may impact the HSI modifications, and developing a new concept of operations for the modified control room, both require extensive input from the operators.

Consideration of failure modes and degraded I&C and HSI conditions is very important and again requires operator involvement. Conversion to digital instrumentation and control systems and human-system interfaces introduces different failure modes with sometimes subtle and wide-ranging effects. Evaluating the effects of failures on plant operation, and developing concepts for how operation will be conducted under conditions of failed or degraded instrumentation or HSI equipment require significant Operations input.

In addition, identifying and addressing issues associated with hybrid interfaces, which will necessarily result as the modifications are made, requires Operations review and input. It is much better to identify these up-front during the planning stage, rather than deal with them after the modifications have been made or in final training before operation. Hybrid HSI issues are discussed further in Section 2.3 on migration strategy.

Finally, operators can identify opportunities for human performance improvements and ways to take advantage of the new technologies, which can be built into the endpoint design.

For more information on human-centered design processes, see the international standard ISO 13407.

2.1.8 Consideration of Available Systems and Equipment

It is important to examine the HSI features and capabilities of the systems and equipment available from vendors and suppliers. As the planning progresses and the endpoint vision is defined, the capabilities of the systems and equipment offered need to be evaluated in more detail to determine whether the desired features can be implemented, and to estimate the cost and difficulty of doing so – preferably before selecting a vendor. The evaluation should consider items that can be major cost and schedule drivers:

- What capabilities are offered "out of the box" versus those that require custom development.
- The need for specialized interfaces to existing plant equipment and the vendor's ability to develop them in a timely manner.
- The flexibility of the system and the vendor to adapt the available (typically commercial) system to the plant's particular conventions and practices – for example, symbols, color

choices, and computer-based procedure formats. Compatibility with existing HSIs that are to be retained also should be examined. If the system has not been designed for or applied in the U.S. nuclear industry, there could be significant effort involved in adapting it to the plant's needs.

- What capabilities are supported by the system database, how will it be generated, and how difficult this will be. Modern I&C systems use databases to store information on each parameter that is monitored, each alarm that can be generated, information that is derived or composed from other data points, control and alarm setpoints, and other information needed to support I&C and HSI functions. Experience has shown that developing and validating the database can take considerable effort. If multiple systems with independent databases are to be used, this multiplies the effort. Also, the architecture of the database (fields, size, ability to change, etc.) may affect the ability to implement some desired features.
- How the vendor will work with the plant to address ongoing evolution of the vendor's products and obsolescence of installed versions – this will be a continuing challenge during the migration and over the life of the installed systems, and it should be considered up front in the planning.
- The level of detail and completeness of existing plant functional specifications. Vendor cost estimates are necessarily based on a review of functional specifications. If these specifications have not been meticulously maintained up to date, some functionality may exist in the plant that is not documented in the project specifications and therefore not included in the vendor cost estimates. When this omitted functionality is discovered later in the project, additional costs will be incurred for the changes that were not expected. Also, there is the possibility that this omitted functionality cannot be implemented without major changes to the work completed prior to the discovery.

Getting the answers to some of the questions regarding capability and adaptability may require obtaining prototype equipment and exercising it with operators and design engineers. These and other related issues are discussed further in the sections on endpoint definition (Section 2.2) and migration strategy (Section 2.3).

2.1.9 Scheduling Challenges

There can be some significant challenges to overcome in scheduling major changes to the HSI. These should be recognized and addressed throughout the planning effort, particularly in the development of a migration strategy (Section 2.3).

Some unique scheduling challenges associated with major HSI changes include:

- Scheduling changes to the simulator – making the changes to the simulator at a time that allows for sufficient training of the operators on the new HSI, but still supports training and qualification on the existing HSI until the changes are implemented in the plant. This can be particularly challenging if the simulator supports multiple units. A similar problem can occur in scheduling changes to emergency response facilities and other systems outside the control room when they support multiple units. Section 6.3 provides further guidance.

- Planning for design iteration – development of a new human-system interface involving computer-driven graphic displays for monitoring, task support, alarms, and procedures, requires significant user input and interaction to arrive at an end product that is effective and accepted by the users. Changes should be expected as this interaction takes place during the design and initial development of the system, and some further changes should be expected during implementation and training. The need to accommodate changes that will improve the HSI and its acceptance by the operators must be balanced against the need to hold to defined milestones in the schedule for specification, design, delivery, acceptance and commissioning of the new system. The vendor and the plant's purchasing agents need to work with the project team to communicate the needs and the plan for iterating the design while still controlling the schedule for procurement and acceptance of the new system.

2.1.10 Documentation of the Planning Effort

This guideline does not prescribe how the HSI modernization planning will be documented. Each plant should decide what level of up-front planning will be done based on its particular circumstances, and how it should be documented. In order for the planning effort to have value and to meet the objectives noted earlier, some form of documentation will be necessary in order to communicate the results of the planning to management and other stakeholders. Also, because the purpose of the plan is to guide future modification efforts that may occur years later, it will be important to have sufficient documentation of the plan and its bases so that new personnel involved in future changes will be able to understand and follow the plan. It may make sense for the HSI modernization planning to be documented with the I&C modernization plan, as they are heavily interdependent. However, it is important that the basis for the HSI plan be included along with the specific plans for modifications.

The plans for modernizing the HSI should be considered living documents that are subject to change. Plant conditions, budgets and priorities, and needs will likely change over the time period required to perform the modernization. Also, technology and capabilities of the available equipment will evolve over time. It is important to define a target endpoint and a reasonable plan for achieving it, but it must also be recognized that the plans should change if the goals and objectives, constraints, or technologies that were the basis for the plans change as the modernization progresses. Lessons learned in the early stages of the program also may lead to modifications in the plans for future phases.

2.1.11 Human Factors Engineering

As in any branch of engineering, a disciplined process is important to achieving success with human factors engineering and human-system interface design. However, a process by itself is not enough. Success in a major human-system interface design or modification effort requires a combination of:

- Management commitment – awareness of the need for good human factors engineering, and a willingness to commit resources and time to implement HFE
- People with the skills, knowledge and experience needed to carry out the HFE effort
- A process that provides the necessary discipline and documentation for the effort.

A good process will not be successful if management is not committed to providing the time and budget necessary to carry it out. The best people cannot be effective without management support. And a good team of people with a committed management still need a disciplined process to follow to help them ensure that requirements are met, important considerations are not forgotten, and appropriate documentation is created so that others can later understand the basis for the design and can support plant operation, maintenance and future design modifications.

Application of HFE should be tailored to the needs of the particular modification. The scope of the HFE activities undertaken and the level of documentation should follow a graded approach, in which these are determined based on the risk and importance associated with each change.

Section 2.4 provides guidance on implementing an HFE program as part of the plant's modification process, and establishing a graded approach to HFE.

2.1.12 Licensing Considerations

Planning for regulatory and licensing activities is discussed in Section 2.5, and Section 5 provides additional guidance related to licensing. However, several important management considerations related to licensing should be pointed out here:

- Regulatory acceptance of modern HSIs is not new – although there are significant challenges involved in design and acceptance of digital systems with modern HSIs, the NRC and the nuclear industry have already developed approaches and guidance for regulatory review and acceptance of the new technologies. Modern HSIs were addressed during reviews of the Advanced Light Water Reactor (ALWR) requirements and designs, which formed the basis for the NRC's development of NUREG 0711.
- HSI modernization is addressed in the NRC guidance – the recent revisions to Chapter 18 of NUREG 0800 and NUREG 0711 address modernization of existing plant control rooms and HSIs in addition to new designs. Also, modern digital interfaces are covered in the recent revision to the NRC's detailed HFE review guidelines, NUREG 0700. Section 5 of this document provides more information on regulatory requirements and expectations applicable to HSI modernization.
- The key is in the process – NUREG 0711 describes a process for design and evaluation of a new or modified HSI and what the NRC's expectations are for that process. This is the primary basis on which HSI changes will be reviewed for acceptability (see Section 5.1.2 for additional information on NRC reviews). A good human factors engineering process should meet those expectations. Section 2.4 provides more details on developing an appropriate human factors engineering process to support an HSI modernization program. Section 3.1 discusses integration of the associated HFE activities into the plant's engineering design process.
- A strategy that many plants have adopted is to make changes first to non-safety systems – this allows opportunity to ensure that the necessary processes are in place and to gain experience with the processes and the newer digital technologies before making changes to the safety systems, which carry higher licensing risk. It also allows plants to see which of the new digital hardware and software works well for their crews.

- Developing a human factors engineering program at the planning stage as shown in Figure 2-1, ensuring that it is compliant with the expectations of NUREG 0711, and obtaining NRC review of the program at the earliest opportunity can reduce the amount of licensing effort and risk associated with the downstream modifications. Also, an early look at potential 10 CFR 50.59 issues associated with changes that will affect operator performance can help minimize licensing risk. This is discussed further in Section 2.5.

2.2 Endpoint Definition

2.2.1 Gathering Inputs

2.2.2 Understanding New HSI Technologies and Modern Control Rooms

2.2.3 Key Operational and Design Considerations

2.2.3.1 Workstation Development

2.2.3.2 Operating Crew Issues

2.2.3.3 Restricted or Protected Controls

2.2.3.4 Failure Modes and Backups

2.2.3.5 Compliance with Regulatory Guides

2.2.4 Defining the Endpoint Concept

2.2.4.1 Concept of Operations

2.2.4.2 HSI Design Concepts

2.2.4.3 HSI Failure Management Concepts

2.2.5 Potential Benefits of Control Room Modernization

2.2.5.1 Modernization and Standardization of HSI Equipment

2.2.5.2 Plant Availability

2.2.5.3 Reduced Staffing

2.2.5.4 Personnel Hiring and Training

2.2.5.5 Other Potential Benefits

2.2.6 Costs and Constraints

2.2.7 Comparison of Conventional and Modernized Control Rooms

2.2.8 Worksheets for Development of Endpoint Concept

This section describes how to define a control room “endpoint” – a vision for the control room that will be the end result of the I&C and HSI modernizations and upgrades. Defining the endpoint requires more than just defining the systems and equipment that will be present in the control room, but also the new concept of operations – how the plant will be controlled and operations will be conducted in the modernized control room (see the discussion in Section 2.1). Operation under abnormal conditions needs to be considered, including situations in which failures have degraded the instrumentation and control systems or the human-system interfaces that the operators would normally use to monitor and control the plant. How these degraded I&C/HSI conditions will be managed should be considered as part of defining the control room endpoint.

Figure 2-4 illustrates the activities involved in defining the control room endpoint:

- Identify and gather information on the main inputs or drivers for the HSI modernization. These include items such as the plant's long-terms goals, internal and external constraints and commitments, and the I&C upgrade strategy
- Understand the impact of the new I&C and HSI technologies and the differences between a modern control room and what exists in the plant today
- Recognize and evaluate the major operational and design considerations involved in defining a modernized control room
- Define a control room endpoint concept or vision, having the HSI characteristics that are desired for the plant
- Assess the potential benefits of the HSI modernization
- Evaluate major cost drivers and constraints that affect the endpoint.

Each of these activities is discussed in this section, in the order in which they are listed above.

The double arrows shown in Figure 2-4 are intended to illustrate that the associated activities are interactive and are not performed sequentially. Iteration among these activities should be expected as concepts are developed, operational considerations are evaluated, and potential costs and benefits are assessed.

A multi-disciplinary team is needed to effectively perform these activities and define a long-range vision for the plant control room and HSIs. As discussed in Section 2.1 above, operations involvement is critical. Input and participation from other groups is also very important. When defining the endpoint, plan to involve personnel from the following areas at a minimum (these are not listed in any particular order):

- Operations
- Maintenance
- Training
- Human performance
- I&C design engineering
- Human factors engineering
- Systems engineering
- Procurement
- Licensing

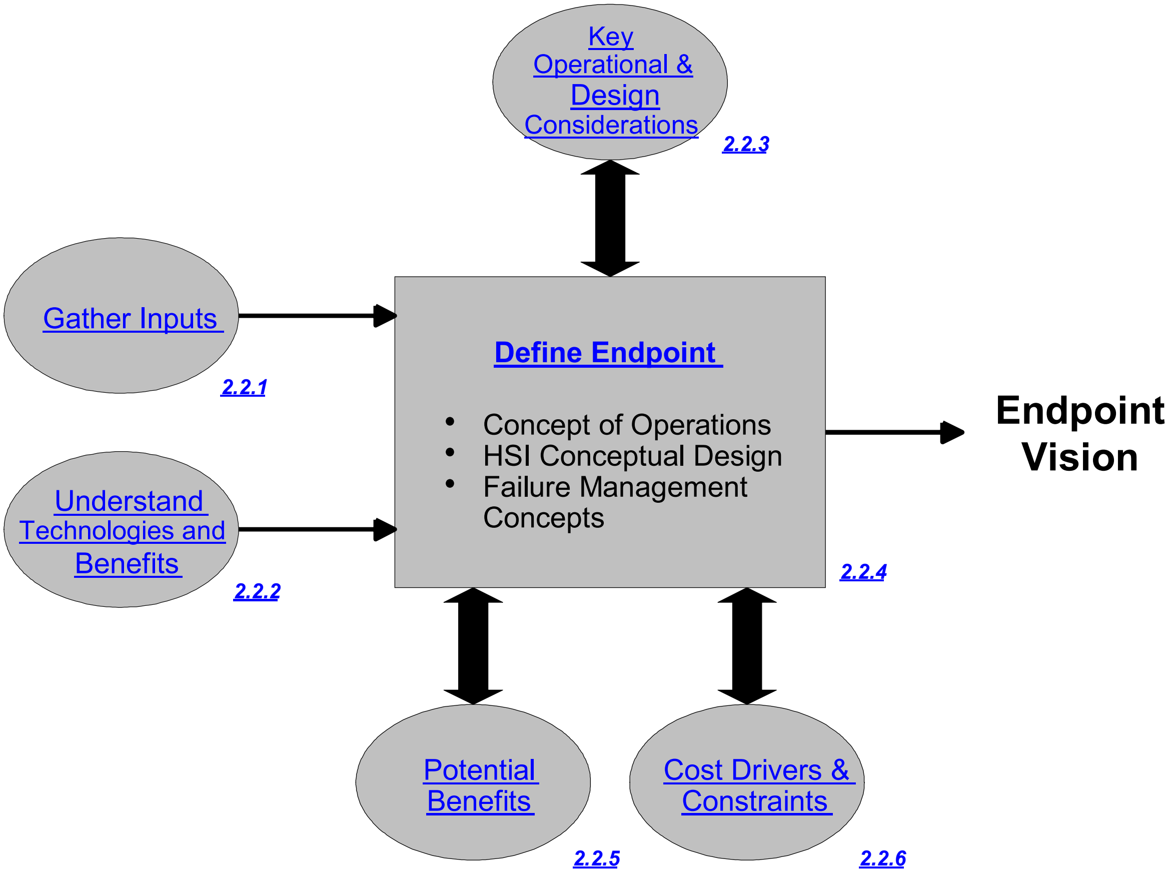


Figure 2-4
Defining a Control Room Endpoint

2.2.1 Gathering Inputs

It is important at the beginning to identify and gather initial information related to the main factors that will drive the endpoint definition. More information can be developed later as the endpoint definition progresses and specific needs are identified. Some of the main drivers of the endpoint definition include:

- Plant long-term goals including any goals related to human performance
- I&C upgrade strategy and initial planning, including I&C architecture, planned changes in functionality (e.g., further automation), and plans for implementing the necessary infrastructure (e.g., distributed control system, communication networks, etc.)
- Operating and maintenance experience, existing operational or human performance problems and opportunities for improvement – this is discussed further in the section on benefits below

- Strengths of the existing control room and other HSIs that should be recognized and maintained or further strengthened in the modernization
- Weaknesses or problems with the existing control room and HSIs (e.g., HSI equipment that has high maintenance burden, equipment abandoned in place, lighting problems)
- Known or expected changes in personnel or their capabilities that should be taken into account in long-range planning (e.g., expected changes in age or experience of operating crews, expected changes in background and experience of new hires)
- Known or expected changes in the plant or utility organization that might affect how operations, engineering, and maintenance activities are conducted, information requirements for various users of I&C/HSI systems, etc.
- Improvements that may be sought in support areas such as equipment monitoring, surveillance testing, logging, administrative controls, limiting conditions of operation (LCO) monitoring, etc., that could lead to requirements or desires that should be reflected in the endpoint design
- Vendor solutions being considered
- Internal or external constraints or commitments (e.g., specific licensing commitments).

2.2.2 Understanding New HSI Technologies and Modern Control Rooms

In order to define a modernized control room endpoint, it is important first to understand what a modern control room looks like, differences in how it is operated compared to existing control rooms, and the potential benefits offered by a modern control room with newer digital technologies. If left to chance, implementation of new I&C and HSI technologies can have a negative impact on the control room and how it is operated. On the other hand, if the control room modernization is a planned effort, and operational and human factors considerations help shape or even drive the modernization rather than be driven by it, then the upgrade to newer technologies can be used to make positive improvements in human performance. Understanding what is possible with modern HSIs is necessary in order to determine how to take advantage of them.

Figure 2-5 provides a representative picture of an existing control room, characterized by relatively long benchboards and vertical panels with discrete controls, indicators, meters, and alarm annunciators. Figure 2-6 gives an artist’s rendition of a modern control room for advanced boiling water reactors, based on designs recently built for new plants in Japan. Figure 2-7 shows a modern control room for a pressurized water reactor plant in France.

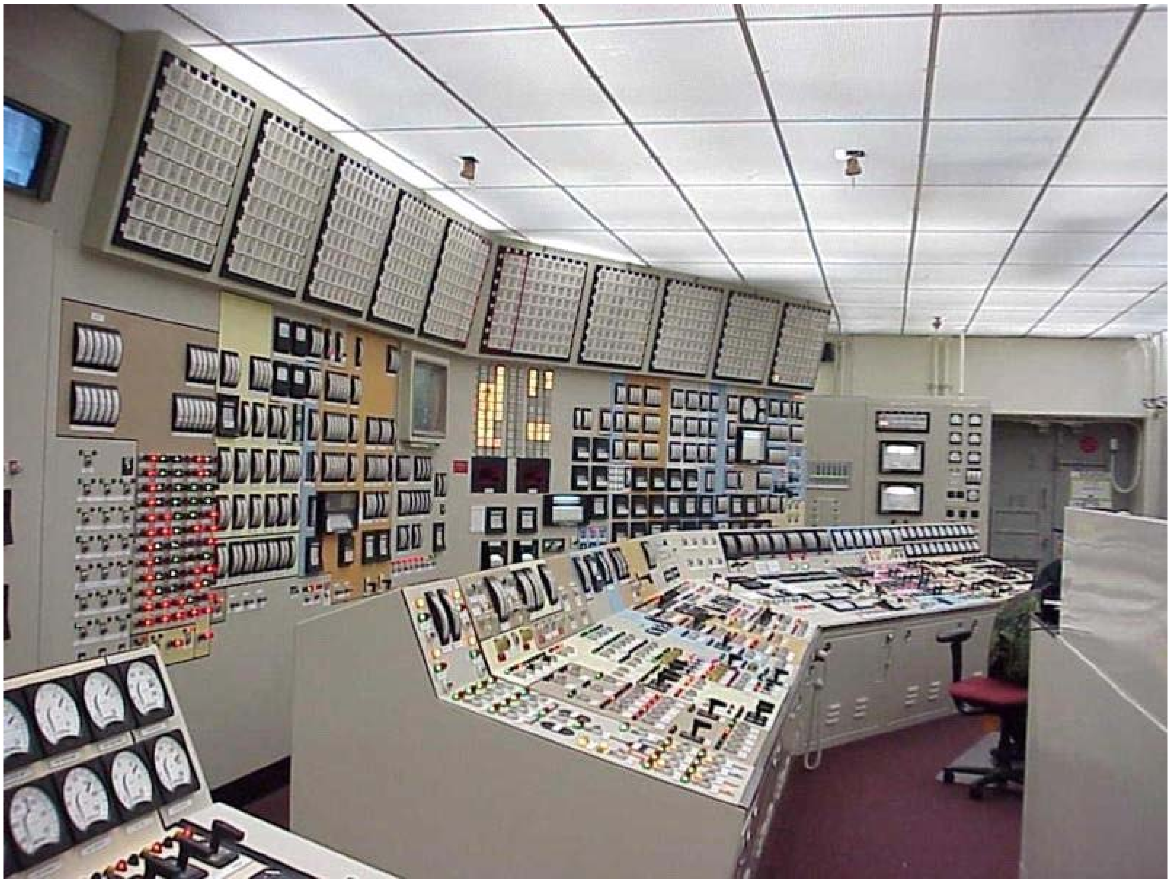


Figure 2-5
Photo of an Existing U.S. Nuclear Power Plant Control Room

Table 2-1 lists important features of a modern, up-to-date control room. This list of features has been drawn from characteristics of control rooms recently built and operated in new plants (outside the U.S.), and control rooms presently being designed for plants to be built in the near future. These features are based on technology that is available today and could be implemented in a modernization program for existing plants. We can consider this a description of what the control room would be like for a plant that has "Fully Modernized I&C and HSI" as illustrated on the map of Figure 2-4.

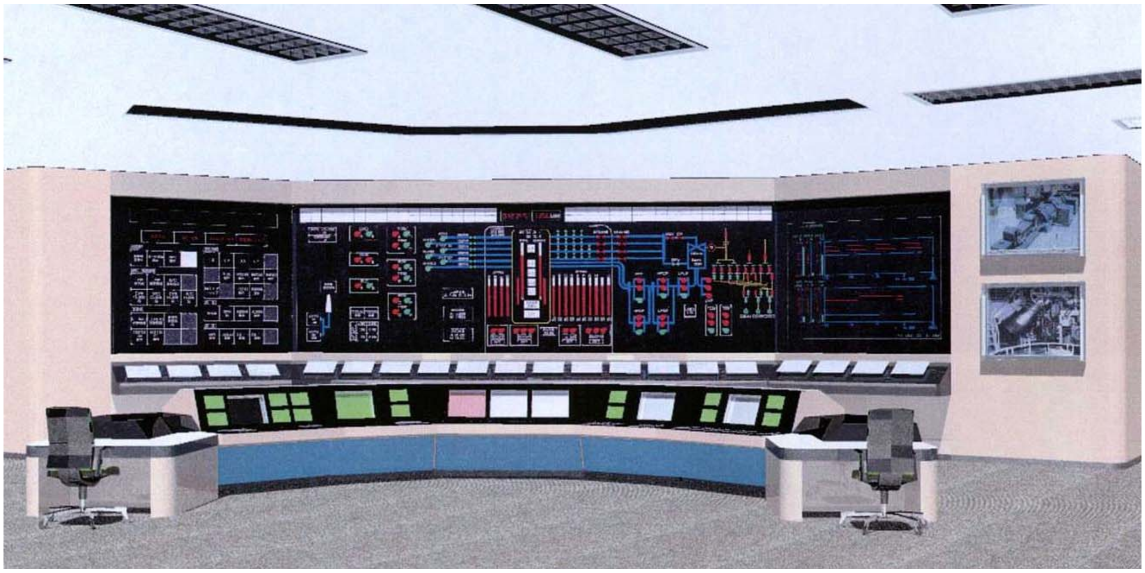


Figure 2-6
Artist's Rendition of a Modern Control Room for Japanese Plants

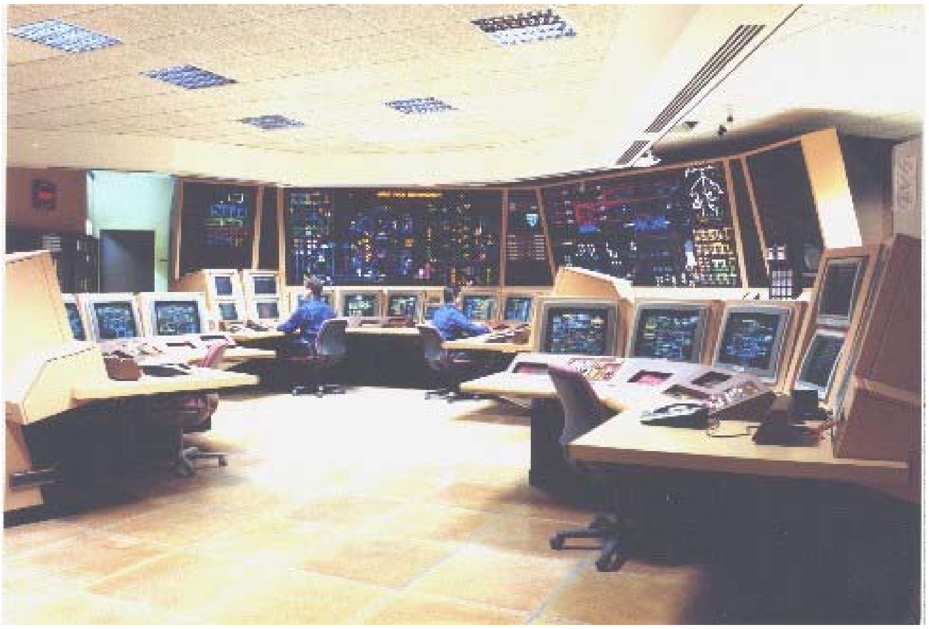


Figure 2-7
Photo of a Modern Control Room Built in France

Note: *In describing this fully modernized control room, we are not suggesting that plants must use this as their target or endpoint or making judgments as to its practicality for any individual plant. It is described here as a means to help readers understand the possibilities, see what technologies and potential benefits might be achievable, and then choose their own endpoint vision based on the plant's particular goals and constraints. This section provides guidance* *on choosing an appropriate endpoint.* ***Section 2.3*** *below discusses how a plant can move toward their chosen endpoint by taking reasonable and practical steps, following a phased "migration path" to the endpoint.*

This modernized control room is described here only as an example to help each plant form a vision of their desired control room endpoint. Each plant should decide how far to go in modernizing based on its own goals, plans, and constraints.

Also, it is important to note that this description of a "fully modernized" control room is based on today's technologies. Technology continues to evolve, and an endpoint envisioned now for plant operation 10 or 20 years hence clearly will change as new developments occur and new benefits can be realized with advancing technology. However, the modernization planning should be based on what is envisioned today (not just what is available today, but also likely or expected developments) and then adjusted as necessary in later years. Planning documents should be living documents, revisited and revised as necessary over time. Newer technologies that come along should not be implemented just because they are new, and the endpoint should not be changed endlessly. However, over the period of time that many plants expect to operate there will be new developments that may offer significant advantages to the plant. In addition, these new developments may make obsolete some of the features originally planned for the endpoint, and thus the endpoint design will have to be changed to accommodate this. Plans should be sufficiently flexible to allow for appropriate updates as time and technologies move forward.

Section 2.2.7 provides more detailed descriptions of the differences between existing and modern control rooms. In particular, information is provided on differences in the concept of operations – how the plant is operated under normal and emergency conditions. It also describes differences in how failures in the I&C and HSI systems and equipment are handled with modern versus conventional control rooms.

It is suggested that readers who are unfamiliar with newer HSI technologies and how modern control rooms are operated use Section 2.2.7 as a tool for gaining more familiarity. In addition, visits to fossil-fueled power plants and other facilities that have modernized their control rooms are highly recommended. Visits to these facilities and discussions with operations, maintenance and engineering personnel can be a very good way to become more familiar with the technologies, understand the benefits that can be achieved, and take advantage of the lessons that have been learned. Finally, it is recommended that the HFE guidelines in Section 4 of this document be reviewed. Guidelines are provided for each of the major elements of a modern HSI (alarms, displays, soft controls, etc.) and each of these begins with an overview of the guidelines. By reading the introduction to Section 4 and then scanning the overview information for each of the sub-sections containing the guidelines, users can become familiar with the basic building blocks and resources that are part of a modern HSI and obtain at least a high-level overview of the design issues involved with each. Of course, the checklists and detailed guidelines that are provided also can be reviewed as necessary to examine each of these in more detail.

Table 2-1
Features of a Fully Modernized Control Room

Workstations	Compact, redundant operator workstations with computer-driven displays and soft control devices provide organized, hierarchical access to alarms, displays, controls and procedures. Each workstation has the capability to perform all main control room functions, but the workstations also support division of tasks between two operators. An additional workstation is provided for use by a supervisor. However, this workstation also can be used as a redundant backup for either of the operator workstations. One or more additional workstations, typically with reduced capability, are provided outside the main control room or operating area for others to access information without distracting the main control room operators. Also, during commissioning and at other times when needed, additional workstations (possibly with reduced capability) can be provided on a temporary basis to support specific evolutions.
Large Display	One or more large display panels, visible to the entire crew, provide a spatially dedicated, continuously available overview of plant status including essential equipment status, values of key process variables, and high-level alarms visible throughout the main control room; these often present information in a plant-level mimic and sometimes include closed-circuit video monitoring of critical plant areas and equipment.
Integrated Soft Control Capability	The soft controls at the workstations, which are non-1E, provide control of both safety-related and nonsafety-related equipment using a single interface. Features are provided in the control and safety systems to ensure that safety functions can be maintained even if the non-1E controls fail.
Automation	Automation of selected functions and tasks, chosen according to a rigorous design and evaluation process, including sequential control actions associated with plant startup, shutdown, and other routine system operations (e.g., testing and maintenance). The automation is implemented in such a way as to keep the operator involved, aware of the status, and ready to back up the automation as necessary.
Computer-Based Procedures	Computer-based procedures provided at the workstations integrate process and equipment information and alarms with procedure steps, and are integrated with the automation features to provide efficient execution of tasks and ready access to information and controls that may be needed.
Intelligent Processing	Intelligent processing of information and alarms and provision of operator aids that help the operators deal with instrument and signal failures, reduce the burden of assimilating and integrating individual readings and data by providing higher-level information to directly support operator tasks, and reduce nuisances and distractions associated with alarms. Access to more detailed information can be obtained by "drilling down" to the level needed.
Failure Management	Redundancy and other fault tolerance features including self-diagnostics, early fault detection, and associated indications and alarms that allow the operators to remain aware of the health of the I&C systems and HSI equipment and deal with degraded conditions gracefully. A small number of controls and displays that are diverse from the computer-driven workstations, selected to meet the regulatory requirements and expectations for defense in depth and diversity and to minimize economic risk associated with equipment failures.

2.2.3 Key Operational and Design Considerations

The following are key operational and design issues that should be considered when defining the endpoint. Plants that have begun developing their modernization programs have found these to be significant challenges or stumbling blocks in their planning efforts.

2.2.3.1 Workstation Development

As described above, most modern control rooms employ seated workstations from which the operators perform most of their tasks in both normal and emergency operations. For existing plants there are a number of challenges involved in determining whether and how to create compact workstations in a room that is presently full of desks and spread-out control boards, panels and cabinets.

In most plants it is not practical to shrink the existing control room down to a small "glass cockpit" from which an operator can monitor and control the entire plant. However, most plants can achieve similar functionality and benefits through a series of modifications to the control room and control panels that create more compact workstations or work areas.

2.2.3.1.1 Example: Converting Desks to Workstations

Figure 2-8 shows an example layout of an existing two-unit control room. Each unit has an operator's desk in addition to control benchboards and vertical panels ("backboards"). The desks have some limited displays driven by the plant computer. Control actions are taken at the stand-up benchboards, which house the controls for the major plant systems. Other panels also are present around the periphery of the room, housing controls and displays for auxiliary and supporting systems.

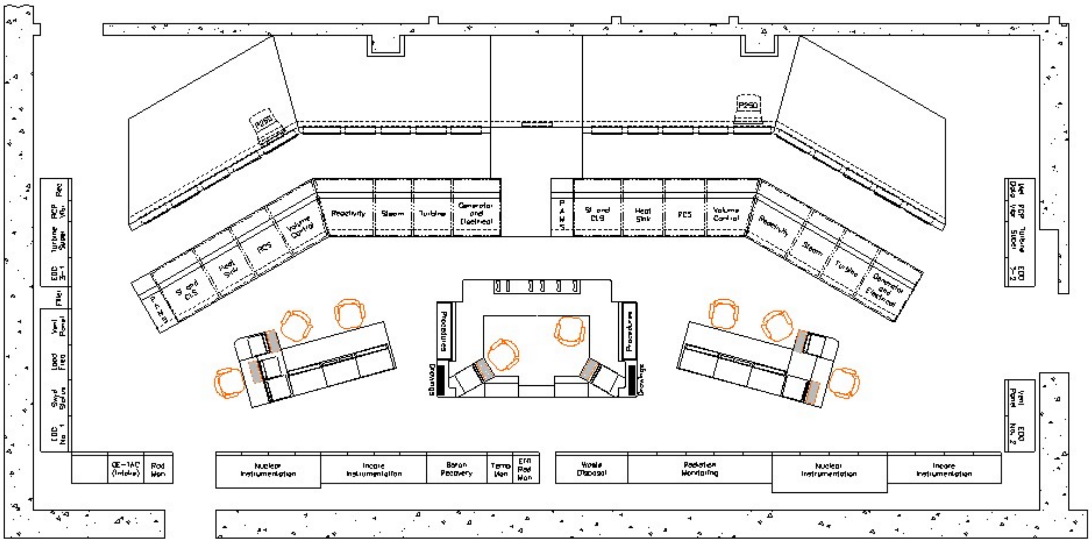


Figure 2-8
Example of an Existing Control Room Layout

A raised area is provided in the center of the room for the unit supervisors. Like the operators' desks, it also provides limited computer-based displays with no control capability.

Figure 2-9 shows a modified layout that illustrates how the operators' desks might be made into operating workstations. This concept adds a raised floor over most of the main operating area to allow for cabling to new, computer-based operator workstations for each unit, plus a supervisor's workstation in the center, driven from a new distributed control system. One or two operators can be seated at each operator workstation, facing toward the benchboards. Monitoring and control of the plant during normal power operation would be conducted from these workstations.

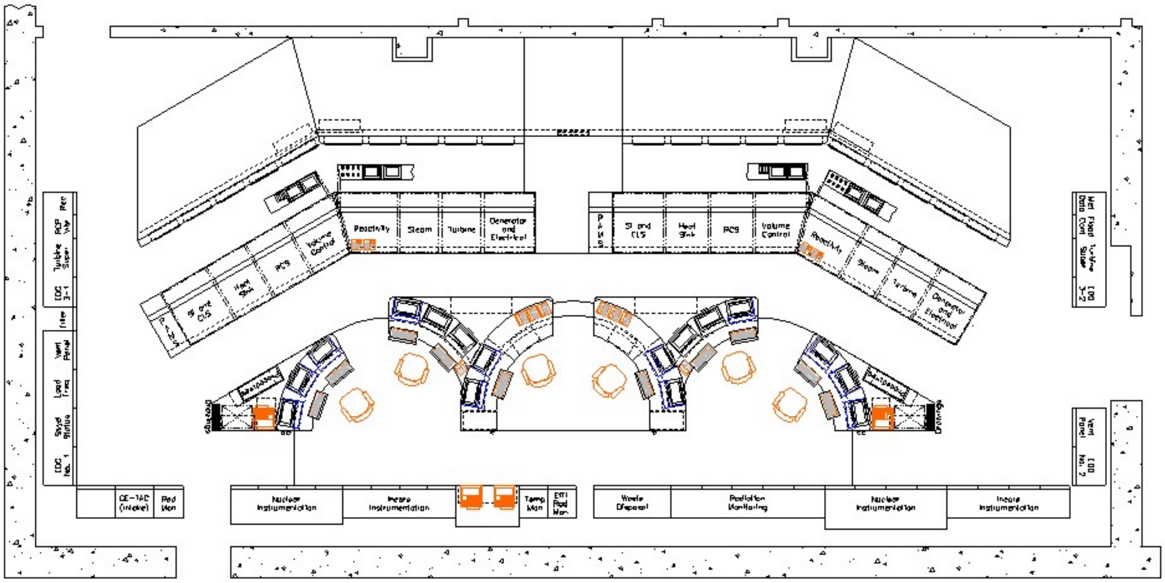


Figure 2-9
Example Concept Showing Operator Desks Converted to Workstations

Space is made on the vertical panels (e.g., by removing and replacing old paper and pen recorders) to allow installation of new large flat panel displays that are visible to the unit operators and supervisors. Figure 2-10 shows a 3D view of this arrangement, with some of the rear panels cut away.

***Note**: These illustrations are provided only as an example of one design concept. There are many options and approaches that can be used. The guidance in this document is intended to assist plants in developing a concept that provides the best solution consistent with their particular goals and constraints.*

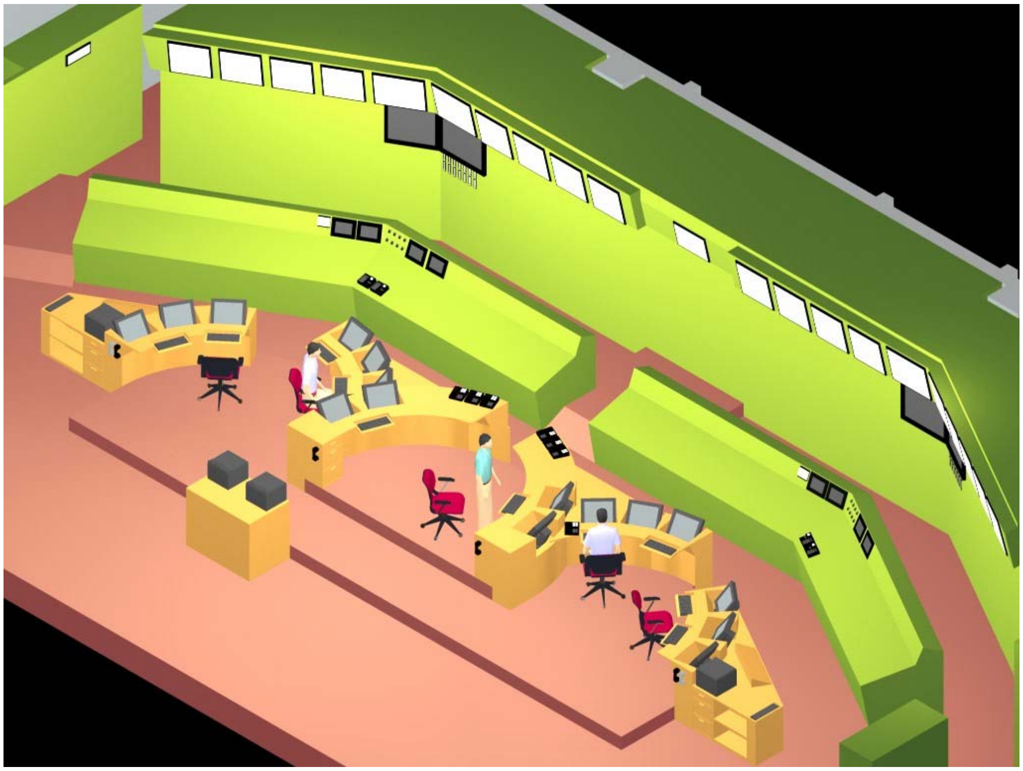


Figure 2-10
3D View of the Concept Shown in the Layout of Figure 2-9
(Benchboard and Vertical Panel Controls and Indicators Not Shown)

This concept could represent an endpoint for a plant that decides to maintain the benchboards as part of the endpoint design. Those controls that are not moved to the new workstations could be maintained at the benchboards (for example, controls that are used less frequently in normal operation, controls dedicated to safety systems, etc. – this would have to be worked out as part of the design). Some or all of these controls could be updated to new soft controls (the figures show some new soft control panels installed on the benchboards as an example of this).

For other plants, this might represent an interim configuration or stopping point along the way to an endpoint that ultimately would remove most or all of the benchboards and provide greater capability at the workstations.

2.2.3.1.2 Hybrid Issues

The configuration shown in Figures 2-9 and 2-10 has controls on both the workstations and on the benchboards. Detailed design of such a hybrid arrangement would require an evaluation of the full range of operator tasks to ensure that they would be adequately supported with this configuration. Note that in this concept, each workstation is split in two parts with an opening in the center to allow access to the benchboards from each workstation. There are other issues associated with this type of hybrid configuration. Section 2.3.4.1 discusses in more detail the identification and evaluation of hybrid HSI issues, including issues associated with interim workstation configurations.

2.2.3.1.3 Workstation Design Considerations

A question that comes up early in workstation design is how many screens or video displays should be provided. This is important even in a conceptual design because of its impact on arrangement and size of the workstation. The answer, of course, ultimately depends on the functions and tasks to be supported by the workstation displays, and other considerations such as how many operators the workstation must support simultaneously. These decisions depend on the overall concept of operations for the control room.

A typical workstation might provide screens to support the following functions:

- Control screens – two screens may be needed to support soft control, depending on the particular system that is chosen (one screen may provide a display from which the component to be controlled is selected, with a separate screen then bringing up the control functions that can be activated for that component).
- Monitoring – at least one screen is needed to support the operator’s monitoring of plant systems and functions. Large display panels visible from the workstation typically provide additional capability to monitor the plant and remain aware of the status of the major plant systems and equipment.
- Alarms – one or more screens may be dedicated to providing alarm information. This may be in addition to higher-level alarms displayed on a large display panel or other alarm displays visible to operators at the workstation.
- Task-based displays – these are displays that are designed to support specific tasks (e.g., starting a feedwater pump or lining up a fluid system).
- Informational displays – displays that can be called up to provide detailed information on the process, systems or equipment (e.g., technical information on a pump or a tank that may be needed in certain situations).
- Procedures – if computer-based procedures are to be provided, a screen may need to be dedicated for this purpose.

To support these functions, recognizing that many of these need to be used or at least displayed simultaneously, typically at least four screens are needed for a full-featured operator workstation. Most workstation designs currently have fewer than ten screens. The number varies depending on the concept of operations – how the operators use the workstations, whether task-based displays and procedures are provided, etc. Also, the particular system implementation affects this – for example, a system that uses multiple windows on a single screen may require fewer physical screens or display units. The guidance in Section 4 addresses workstation, soft control and display system design in more detail.

The use of compact workstations can affect crew coordination and supervision. This is addressed below in the discussion of operating crew issues.

2.2.3.2 Operating Crew Issues

Important considerations related to the operating crew are crew coordination and supervision, and the effect of automation on operator roles and the concept of operations.

2.2.3.2.1 Crew Coordination and Supervision

Because of the tendency for an operator to become focused on detailed information or specific tasks at a compact workstation (the "tunnel effect"), a concern with workstation implementations is maintaining crew awareness of the overall plant situation, and maintaining coordination of crew members. Most modern control room designs employing workstations also include large overview display panels, in part to address this concern. Large overview displays are spatially dedicated (fixed in position), continuously displayed (do not have to be selected or called up), and visible to the entire operating crew. They can aid in crew coordination by providing a common view and awareness of important plant status information. This also may help offset the tunnel effect associated with workstations, although training and a clear division of responsibilities of crew members are critical here. The supervisor should endeavor to keep "the big picture" in mind; the overview display can be an aid in doing so.

Another aspect of crew coordination is the degree to which an operator can remain aware of what other members of the crew are doing, and be prepared to back them up. Related to this is the ability of a supervisor to monitor the actions of crew members. In a conventional control room, operators and supervisors achieve some awareness of what others are doing simply by knowing what section of the control panels they are using or monitoring. For example, if a supervisor directs an operator to take an action related to the feedwater system, he or she can tell whether the operator is working at the feedwater section of the panel or has moved to another location (either in error, or because something else has taken that operator's attention). When an operator uses a compact workstation it can be much more difficult for the supervisor or other members of the crew to monitor or be aware of what the operator is doing.

There are design features that can be considered to address this shortcoming of compact workstations. Large panel displays can help simply because they provide visibility to the entire crew of the status of equipment or plant parameters related to what the operator at the workstation is doing. Some modern control room designs arrange the workstations so that there are sight lines maintained between operators and between the supervisor and the operators, which can be of some help. Other features might be considered such as cues on workstation displays that indicate what displays are being accessed at another workstation or computer-based procedure systems that provide indication of what procedures are being accessed. At this point, the details of such features may not be defined, but the endpoint concept should consider this issue and how it might be addressed.

Section 4.1.3 provides additional guidance related to crew coordination and teamwork.

2.2.3.2.2 Effect of Automation

It is important to recognize the different types of automation that might be implemented in the modernized I&C and control room. Types of automation include:

- Automation of protective actions or protection logic that must be done too quickly to rely on human action – existing plants already incorporate a great deal of this type of automation. Examples are automatic trips of major equipment, and the safety system logic that automatically takes action under accident conditions.
- Continuous control automation – for example, control of water level in the reactor or steam generator, or reactor pressure control. Again, there is a great deal of this type of automation in existing plants.
- Automated sequences of control actions – examples here are automation of sequences of actions to line up a fluid system, automation of sequential actions required during plant startup, and some forms of automated testing. There is little of this type of automation in most existing plants, but new plant designs and some modernization plans include more of this.
- Automation of HSI functions not involving plant or process control actions – examples include automated logs, automatic collection of data from multiple sensors to form higher-level information, automatic cross-checking of variables or sensor readings, automatic display of relevant data when an alarm occurs or a control action is selected, and automatic display of information related to the current procedure step in a computer-based procedure system. These are only a few examples of the types of automation incorporated in varying amounts in modern HSIs.

Section 3.3 provides additional guidance on determining an appropriate level of automation and Section 3.7 discusses designing for automation. Some of the potential benefits of automation are discussed in the section below on modernization benefits. Disadvantages of automation from an operational standpoint are the potential for operators to lose situation awareness as more of the plant processes and the HSI functions are automated, and loss of skills and awareness needed to take actions manually should the automation fail. Also, automated systems often operate in different modes. This introduces the possibility an operator will make an error related to lack of understanding of what mode the automated system is in (often referred to as "mode error"). Measures can be taken in design, evaluation, and training to help address these potential drawbacks.

Introduction of additional automation can necessitate a change in the allocation of tasks and responsibilities among members of the operating crew. This was discussed in Section 2.1, where Figure 2-3 illustrated the change in the operator's role as the HSI is modernized and more automation is introduced. Because the automation takes on tasks previously done by the operating crew, the allocation of remaining tasks should be reconsidered. Also, some of the operator tasks change or are eliminated, and new tasks are created as the role of the operators shifts to a more supervisory role – supervising the automated systems, monitoring their operation, remaining aware of what the automation is doing and when intervention is needed. With better information management and selective automation, operators may have time to perform tasks that are better suited to human performance, such as dealing with unexpected situations and diagnosing problems, while the I&C and HSI systems perform tasks well suited to machines (e.g., low-level, repetitive tasks). See Section 3.3 for guidance on determining appropriate allocation of functions to humans and to automated systems.

2.2.3.3 Restricted or Protected Controls

Some of the controls provided on the panels in existing control rooms have some type of protection (e.g., a hinged cover) or locking function (e.g., keylock) to restrict their use. There are a number of ways in which these types of restrictions can be implemented in a modern computer-based HSI. However, the basis for the existing restrictions needs to be identified in order to choose an appropriate method of implementation. For example, there are several reasons that such restrictions or protective features have been provided for the existing controls. The intent may have been to:

- Protect against inadvertent actuation (simple slips or errors) or provide heightened awareness of the criticality of the control action before it is taken – for example, a protected trip button.
- Protect against action by unauthorized personnel – in most plants, the security associated with access to the control room addresses the authorization issue, and individual controls on the main control boards are not protected for this reason. But local controls might incorporate, or need to incorporate this type of protection.
- Require a second person to agree to or approve the action before it is taken – for example, a control that must be operated with a key that is held by a supervisor.

The basis for some of the existing restricted controls may not be well documented. It may be best to re-evaluate this for controls that presently have some form of protection applied and to determine whether any additional controls need any of these types of protection. Computer-based control systems provide much more flexibility to implement the type of protection that is needed and best fits with the concept of operations in terms of roles and responsibilities of the crew members. For example, for selected controls the system may bring up a warning or require an additional confirmatory action before the control can be actuated. If authorization is needed, passwords might be used. See Section 4.3 for design guidelines related to soft controls.

Note that some critical control actions that are presently protected on the panel may be retained as hard controls for other reasons (e.g., as part of the defense-in-depth and diversity approach).

2.2.3.4 Failure Modes and Backups

Failures or degradation of the instrumentation and controls or human-system interfaces can present significant challenges to the plant operators. Modern digital systems typically combine functions that previously were separated, and integrate data and control capabilities such that failures can lead to more widespread loss of HSI functionality.

There are a number of different I&C and HSI failure situations that should be considered as part of the endpoint definition:

- Failure of a safety system to perform its function – current industry and regulatory guidance for implementation of digital I&C systems requires consideration of the potential for common cause failure of redundant safety systems if common software is used in the redundant elements. A defense-in-depth and diversity evaluation should be performed to address potential software common cause failures. This evaluation typically leads to the need for some diverse backup controls, which may be implemented using hard controls (existing or newly installed).

- Failure of one or more control systems or control loops – for example, failure of an automatic control system, or automatic reversion to manual control.
- Failures of HSI systems or equipment – for example, failure of a monitoring system, large display panel, one or more workstations, or a data network.

Each of these failure situations is discussed below.

2.2.3.4.1 Safety System Failures – Defense in Depth and Diversity

EPRI TR-102348/NEI 01-01 and the Standard Review Plan provide guidance and expectations regarding defense-in-depth and diversity evaluations and determining the need for diverse backups. From an HSI standpoint, it is important that diverse backups be integrated into the design and the concept of operations. The potential for incompatibility of the different controls, the need for training on use of backup controls that are not used normally, and requirements related to their use (e.g., information, or time to take required action) need to be considered. Section 5.2.3 provides additional information related to defense-in-depth and diversity evaluations and their potential impact on the HSI.

See Section 6.4 for a discussion of safety monitoring and control in a modernized control room, including integration of backup controls with other HSIs.

2.2.3.4.2 Control System Failures

The possibility of failure of major control systems needs to be considered as part of the endpoint definition and concept of operations. Important considerations include:

- How the operators will handle the identified failures – actions they should take, manual or other backup capabilities that should be used, whether additional personnel will be required to deal with the situation, etc. Evaluation of the impact of failures on operation and the crew's ability to deal with them may identify the need for changes in the I&C systems or architecture, or HSI capabilities that affect the I&C and control room endpoint designs.
- Potential for new behavior of the plant in response to control system failures needs to be considered and evaluated from an operations standpoint – with more integrated I&C systems, failures may cause multiple control loops or systems to malfunction, creating plant behaviors that have not been evaluated before. The potential for operator confusion due to the new plant behaviors or behavior of the associated instrumentation and information displays needs to be considered.

2.2.3.4.3 HSI Failures

As digital systems combine or integrate functions and rely on more concentrated data sources and information systems, the potential for significant loss of HSI functionality needs to be considered. Partial loss of HSI capability (e.g., loss of an overview display, or loss of one workstation) needs to be addressed as well as potential large-scale failures. Some important considerations when evaluating the effects of such failures include:

- Whether the plant should be shut down due to the loss of HSI capability
- How long the plant can operate with the failed HSI, and what measures would be needed to allow this (e.g., use of backups or extra personnel)
- What actions might be needed in accordance with the plant's emergency plan
- How the operators will know the failure has occurred, and how they will know what is working, what can be trusted, and what should be considered failed or suspect
- What training and procedures will be needed to support operation under these conditions.

In a detailed design each failure mode would be examined in detail and plans for handling them would be developed, possibly with procedures specific to the situation. At this point when defining an endpoint concept, it is important to understand the effects of gross failures that might be present based on the conceptual I&C and HSI designs, and how these would be handled. The results of this evaluation may provide feedback that alters the conceptual designs or the concept of how operations would be conducted.

Many plants are considering implementation of two "platforms" for their modernized I&C – one for safety-related systems, and a second diverse platform for non-safety systems. This provides part of the solution to the defense-in-depth and diversity issue. Also, the availability of two diverse platforms can provide ways of coping with HSI failures. This should be considered when evaluating response to gross HSI failures. Section 6.4 provides additional guidance. It discusses designing for HSI failure situations in the context of overall safety monitoring and control solutions for modernized control rooms. This section should be reviewed when developing a conceptual design of the control room endpoint.

2.2.3.5 Compliance with Regulatory Guides

Most plants today have features in the control room that are intended to comply with specific NRC Regulatory Guides. In particular, plants have post-accident monitoring instrumentation that is in accordance with Reg. Guide 1.97, and bypassed and inoperable status indication in accordance with Reg. Guide 1.47. These guides were written years ago when the instrumentation was mostly analog. With digital systems, there are solutions for post-accident monitoring and bypassed and inoperable status indication that are superior to what could be achieved with the older technologies. Plants should be able to take advantage of these solutions, but will need to determine how to handle compliance with the older regulatory guides. Section 2.5 addresses this further, and more detailed guidance on these and other topics related to safety control and monitoring is given in Section 6.4.

2.2.4 Defining the Endpoint Concept

The endpoint should be defined in three parts:

- Concept of Operations
- HSI Design Concepts
- Failure Management Concepts

Worksheets are provided in Section 2.2.8 that can be used in developing and documenting these concepts. Guidance is provided in Section 2.2.7 describing how the worksheets can be used and examples are given illustrating how to fill them in.

It is important at this point to define a vision of where the control room ultimately might go after all the anticipated upgrades and modernizations are completed. The way to get there most likely is to make incremental changes over time, and this "migration" toward the endpoint is discussed in Section 2.3 below. Interim stopping points along the way to the endpoint will be defined as part of the migration planning and these may become additional, intermediate columns in the worksheets given in the appendix. For now, however, the focus is on defining the final endpoint and how it differs from the current control room.

Because only a concept or vision is being defined here and not a detailed design, the level of analysis that is performed should be just what is needed to adequately define the concept. Formal, detailed analyses need not be performed here, but may be needed later as the actual modifications are developed. Consider automation as an example. Detailed design decisions on what additional functions should be automated may rely on task analysis and evaluation of operator workloads during startup and shutdown. At this point, it may be sufficient to simply interview operators or trainers, observe training evolutions on the simulator, or use other less formal techniques for assessing overall needs and benefits of increased automation.

Although detailed design analyses are not required, it is important to recognize that development of the endpoint design or vision is a form of conceptual design. The endpoint definition activity can benefit from appropriate application of an HFE design process as described in Section 3 of this document. For example, Section 3.2 describes operating experience review. Review of experience with the present control room is an important input to defining the endpoint, as discussed in that section. Section 3.3 addresses function allocation and making decisions on what should be automated. As discussed above, the desired level of automation should be considered as part of defining the endpoint. Section 3.7 provides overall guidance on HSI design, including concept design. Thus, while the effort described here for definition of a vision or endpoint concept for the control room is not a detailed design activity, use of the design process guidance given in Section 3 will help ensure that the endpoint design benefits from application of good human factors engineering design practices.

Finally, as discussed previously, it is important to recognize that the endpoint may need to change later. The plans should be flexible and allow for changes as the modernization program goes forward, because plant conditions may change, budgets and priorities may shift, and technology will evolve during the time required to carry out the modernization. Also, lessons learned in the early phases of the modernization should be reflected in the endpoint definition as appropriate.

2.2.4.1 Concept of Operations

When designing a new plant, the control room can be designed from the ground up, starting essentially with a clean sheet of paper. However, when modernizing an existing control room the starting point is what exists now, its design basis, and how it is operated. To define an endpoint for the modernized control room, it is important to first establish the concepts behind the design and operation of the existing control room.

If more recent documentation is not available, the results of the Detailed Control Room Design Review (DCRDR) performed after the TMI-2 accident might provide some information that would be useful here. It may contain information on the original concept of operations including the makeup of the operating crew, roles and responsibilities, skills and capabilities of reactor operators and equipment or auxiliary operators, and how the operating crew is expected to handle anticipated and unanticipated transients. It may also provide information from previous reviews of the human factors aspects of the control room – for example, overall control room arrangement, relationships and ordering of controls and displays, number of personnel normally in the control room and maximum numbers during situations of augmented manning, use of procedures, and communication among the crew members and with outside personnel.

Worksheet 1 in Section 2.2.8 can be used as a guide for developing the Concept of Operations. It can be used as a worksheet, filling it in, or simply as a checklist of items to consider as part of the Concept of Operations. Note that the items listed are similar to those in Table 2-2 of Section 2.2.7, which describes differences between existing and modernized control rooms. Operational tasks are broken down in more detail in Worksheet 1 than they were in the table.

It will be helpful to identify one or more examples of scenarios for each of the categories in Worksheet 1 (e.g., a startup evolution, or a representative plant upset) to help generate information to be put into the worksheet and to evaluate the endpoint when it is completed.

When developing the Concept of Operations, consider how the flexibility of new computer-based HSIs can affect the assignment of tasks to individual crew members. For example, the current assignment of tasks may have been based in part on limitations related to the fixed locations of controls and displays in the existing control room. Computer-based HSIs allow needed controls and displays to be brought to the operator at a workstation, enabling the design of information displays and control screens that are more compatible with operator functions, possibly allowing a more effective assignment of functions and tasks to individual operators. See Section 4.1.3, Display Functions, in this document for more information that may help stimulate thinking along these lines while developing the new Concept of Operations.

2.2.4.2 HSI Design Concepts

Worksheet 2 in Section 2.2.8 can be used as a guide for developing the HSI design concepts.

This includes concepts for overall control room arrangement, workstations or work areas to be provided for operators and supervisors, overview or large panel display concepts, degree to which soft controls will be implemented (not in detail, but at a scoping level), whether computer-based procedures will be provided, etc. These design concepts should be compatible with the Concept of Operations and the Failure Management Concepts (Worksheets 1 and 3) to ensure a self-consistent endpoint. They should reflect the operational and design considerations discussed above. Potential benefits to be achieved and costs and constraints (discussed below) also should be considered and the design concepts made to reflect them.

Some items that should be considered when developing the endpoint design concepts include:

- Revisit the information obtained on problem areas and strengths of the existing control room. Ensure that the endpoint design concepts address as appropriate the problem areas and needs for improved human performance, and maintain or enhance the strengths of the existing control room.
- The design concepts should provide capability to handle unforeseen conditions, allow for recovery from human error, and provide ways for operators to back each other up. Designers cannot foresee all possible circumstances that the operators will face. The design concepts should reflect the fact that humans do make errors, but they also are able to adapt to unforeseen situations, back up one another and recover from failures or errors. This includes cognitive errors – a mistake in interpreting information or deciding on a course of action. The modern HSI should provide support that will minimize these types of errors, but it also should provide to the extent practical the capability to detect and recover from them if they occur.
- The design concepts should consider which HSIs need to be implemented using qualified equipment. The regulations are clear on the need for qualified HSIs for some tasks credited in the safety analysis, but they are not so clear on what levels of qualification may be needed for HSIs used in other emergency situations. Section 6.4 provides guidance for addressing this and the challenge of integrating qualification requirements with other design requirements such as post-TMI requirements, the need for some fixed-position HSIs, and backups such as those identified in the defense-in-depth and diversity evaluation.

2.2.4.3 HSI Failure Management Concepts

Failure management concepts include methods for dealing with failures or degradation of the instrumentation and control systems or the HSI. I&C failures should be examined for their impact on the HSI and the plant operators. This would include plausible failures of automatic control systems that would automatically revert to manual control or would require the operators to detect the failure and take over manual control. This was discussed previously above. Digital systems often combine control loops and functions in ways that can create the possibility for multiple systems to be affected and new plant behavior that has not previously been addressed. Also, failures of data communication systems and networks should be considered.

Examples of HSI failures include plausible failures of workstation displays, large display panels, alarm systems, and soft controls. Failure of computer-based procedure systems also should be considered if these are part of the endpoint concept. System failures such as failure of monitoring systems, multiplexers, data historian or recording systems, and information systems should be considered.

At this point the design will not be sufficiently developed to allow detailed failure modes and effects analyses. However, at the conceptual and architectural level it is very important to examine the potential for significant failures and to plan for these in the endpoint design concept. This may lead to identification of weaknesses and important requirements that should be fed back to the I&C system designs, or requirements for alternate or backup capabilities that should be built into the HSI concepts. See Section 6.4 for additional guidance on designing for situations in which HSI failures have occurred.

Worksheet 3 in Section 2.2.8 can be used as a guide for developing the HSI failure management concepts.

2.2.5 Potential Benefits of Control Room Modernization

Decisions on how far to go in modernizing the control room and associated human-system interfaces, like decisions on other types of modifications, ultimately boil down to economics. The changes that are made must ensure that plant safety is maintained and the pertinent regulations are met. But there is a wide range of options available to plants for making further improvements and updates to the HSI that can have a beneficial effect on human performance and overall plant availability and productivity. Of course, there are costs and practical constraints associated with making some of these changes. It is difficult to make formal, quantitative cost-benefit analyses of these changes because human performance improvements and the effects of reduced potential for human error are difficult to quantify accurately. However, for most plants the costs and expected benefits of these changes must be evaluated and described so that management can prioritize and make informed decisions about whether and when to implement specific changes.

Therefore, when planning a control room modernization and defining an endpoint vision for the control room, it is important to identify and characterize the types of benefits associated with the modernization. Also, practical constraints affecting the choice among various options available and the costs of implementing the changes need to be assessed at least on a preliminary basis so that the plans are realistic, properly focused, and consistent with management goals and expectations. Potential benefits are described below. Following this, costs and constraints are discussed.

Assessment of potential benefits of control room and HSI modernization should be approached from several directions:

1. Problems – identify any problems, deficiencies or inefficiencies with the existing HSI, human performance problems, and any areas needing improvement. The discussion earlier in this section identified these as inputs for the endpoint definition.
2. Strengths – areas in which the current control room and HSIs offer significant strengths that should be maintained or strengthened in the modernization.
3. Opportunities – identify ways in which the new technologies that will be or could be introduced can provide improvements in the HSI leading to improved human performance, better plant performance or reduced costs. Understanding the new technologies and how a modern control room can provide new capabilities was discussed earlier in this section.

Problem areas can be identified from a number of different sources, including:

- Deficiencies identified in the plant's DCRDR that were not fully corrected at the time. With existing control rooms and control room equipment, it was simply not practical to address some human factors deficiencies or shortcomings of the control room identified in the DCRDR. They may be much more easily corrected or addressed when the I&C systems and control room are upgraded and modernized. Note, however, that the DCRDR was done many years ago. Any information used will need to be checked for validity in today's control room.
- Results of I&C upgrade studies and strategic planning – I&C upgrade planning should include identification of system performance and operational problems, as well as equipment obsolescence issues, and may identify specific HSI problems that should be addressed

- Discussions and interviews with plant operators and trainers regarding overall plant operation, evolutions and activities that represent high workload situations (e.g., during startup and shutdown), tasks that are relatively difficult or error-prone, distractions and nuisances that impact the operators' ability to do their assigned tasks, etc.
- Operating experience reviews, including review of previous plant events, evaluation of situations that involved operator errors, etc. (see Section 3.2 for guidance)
- Review of maintenance experience, including discussions and interviews with plant maintenance and engineering personnel
- Discussions and interviews with the plant's human performance and training groups to identify problem areas, and any initiatives that are planned or already underway to improve human performance that may impact or be impacted by the control room modernization.

Strengths of the existing control room and HSIs also can be identified through discussions and interviews with operators and the human performance and training groups.

Opportunities to make improvements beyond just resolving known problems can be identified from sources such as:

- Experience in fossil plants and other industries where control room modernizations have taken place
- Understanding of the new HSI technologies and the benefits that can be achieved with them – this was discussed earlier in this section. The tables in Section 2.2.7 describe how modern HSI technologies can impact human performance and plant operation.
- Information from vendors on the benefits of their systems and recommended approaches for the HSI, and their experience in implementing updated HSI technologies elsewhere
- Lessons learned from operation of new nuclear power plants overseas that have modern control rooms using the types of technologies and approaches that are being considered for existing U.S. plants
- Examination of the plant's PRA to identify specific places where operator action is critical or a limiting factor, or human action is credited and improvements such as automation or an improved HSI could be beneficial (see Section 5.2.6 for additional guidance on use of the PRA)
- Discussions and interviews with plant operators and the training and human performance groups.

The following are potential benefits that might be achieved by modernization of the main control room in concert with I&C system modernization. These are organized in categories that most directly relate to economics of plant operation. Each plant should determine how these relate to specific goals of the plant or of the owner/operator organization regarding improved plant performance, improved human performance, or other specific financial or economic goals.

2.2.5.1 Modernization and Standardization of HSI Equipment

These items are a subset of the overall benefits related to modernization of the I&C systems. This does not attempt to describe the benefits of overall I&C modernization, but does cover the control room/HSI equipment itself because it is directly related to MCR modernization.

- Reduced maintenance hours due to fewer MCR components (e.g., standard video display replaces many meters and recorders)[1] – standardizing leads to fewer types of installed components which can reduce maintenance costs
- If HSI equipment is standardized, more consistent and compatible human-system interfaces may lead to greater efficiency, fewer errors, and less training burden
- Fewer disruptions to the organization and to operations, and lower costs with up-to-date, reliable HSI equipment
  - With flexible, multi-purpose devices like CRT screens or VDUs, if one unit fails the operator can step to another and get the same information or control capability; when an analog indicator or switch fails, there is much more disruption to operations
  - Getting up-front on the obsolescence curve avoids situations that wreak havoc when a device with no spares fails, causing disruption to the organization and people, higher costs due to the rush to replace, and potential risks to plant operation if the replacement must be done at power
- Reduced cost of future modifications and updates
  - Less need to continually re-interface with older control board equipment (e.g., difficulty in dealing with contact ratings on older switches)
  - Control room equipment can be kept up to date with the I&C equipment, and thus is in synch with vendor offerings that are cost effective, widely used, and subject to less customizing
  - Digital capabilities allow more cost-effective modification of the HSI with less disruption to operations (e.g., changing a screen display versus replacing, moving or adding a meter on the control board).

2.2.5.2 Plant Availability

Higher availability of the plant might result from:

- Shorter time spent in outages due to more efficient HSI and/or more automation, reducing time required to carry out needed actions (see items above)
- Fewer unplanned or extended outages due to fewer human errors that can damage equipment, take equipment off line potentially causing reduced-power operation, or trip the plant off line
- Fewer unplanned or extended outages due to enhanced monitoring and improved situation awareness, allowing operators to take proactive control actions that prevent undesirable situations from developing and affecting plant availability.

[1] It is important not to forget software maintenance that is introduced with digital systems.

2.2.5.3 Reduced Staffing

Manning reduction in general is becoming more important, and will likely increase in importance over time. This is due not only to the desire to reduce costs, but also because of increasing difficulty in obtaining qualified personnel. Experience has shown that I&C modernization can help reduce the number of engineers and maintenance technicians. It may also be possible to reduce operations staffing, or at least reduce the peak workloads that most influence staffing levels and operating crew burden. Size of the operating crew typically has not been reduced in nuclear plants that have implemented modern control rooms, but some plants undergoing modernization are interested in pursuing reduction in the number of auxiliary (local or roving) operators required.

Contributors to reduced staffing burden might include:

- More efficient HSIs leading to reduced operations time required to perform tasks (e.g., providing displays that are designed to support specific tasks like starting a pump or lining up a system, or going through a mode transition, allowing these operations to be done more efficiently).
- Increased automation of data collection and integration, reducing the time the operators spend in gathering or confirming information from various readings and integrating bits of data to create useful information, and reducing likelihood of errors (examples include: automatic comparison of indicators when required; automatic confirmation of a reading; automatically displaying needed information at a workstation where a control action is being taken, avoiding an operator having to move to another location to obtain the needed information; generating a single, validated value of a variable from multiple sensor readings; generating information on readiness of a system or success path from multiple sensor readings and status indications; reducing the need for equipment operators to go find information by providing it in the MCR).
- Greater centralization of monitoring and control capability and responsibility, bringing more of this into the main control room through use of distributed control and information systems, possibly reducing the need for operators to "man" some local or auxiliary control stations in the plant (e.g., sweeping condensate polisher controls into the distributed control system and placing responsibility in the control room, eliminating a local control room/station). [Note: The advantages should be weighed against the possible disadvantages of increasing burden on the MCR operators, and losing the advantage of having operators out near the systems and equipment where they are more likely to be aware of the condition and status of equipment.
- Increased automation of control actions, particularly routine or tedious sequences of actions that can be performed reliably by a digital system with the operator possibly initiating and monitoring or confirming the actions – particularly in times when operator burdens are highest (mode transitions of startup and shutdown, outage activities, etc.); automation can reduce the time taken to perform the required control actions; automation also may essentially eliminate certain types of errors that could be made with manual operation. [Note: Automation can introduce the opportunity for other types of errors associated with the automation itself (e.g., error in interpreting what mode the automated system is in). Also, the operators may have a more difficult time taking over from the automation if training does not ensure they maintain manual operating skills.]

2.2.5.4 Personnel Hiring and Training

Potential benefits of modernized control rooms include:

- Greater ability to attract and retain new talent (operators, engineers and technicians), who tend to be more familiar with and comfortable with computer interfaces and put off by older technologies
- Reduced time spent in familiarizing and training new hires, for the same reason; reduced need for special skills and training associated with operation of the older analog systems and equipment.

2.2.5.5 Other Potential Benefits

These might include:

- Reduction in the number of NRC findings and INPO findings or degraded ratings that can be caused by human errors, thus avoiding the administrative time, management attention and distraction, and other burdens associated with these situations
- Greater ability to maintain a consistent design philosophy and good human factors as modifications are made over time, because the HSI is easier to change without disrupting the basic design philosophy and human factors approach
- Modeling of plant systems and components to enhance monitoring of system operations and improve performance through real-time characterization and optimization of the systems.

2.2.6 Costs and Constraints

When defining the endpoint it is likely that at least a scoping evaluation of costs will be required. The design will only be at a conceptual level, so detailed cost estimates are not appropriate. However, when evaluating options and providing management with a potential target for the modernized control room, it is important to recognize major constraints that may affect the endpoint design, and the main factors that drive the cost.

Table 2-2 lists a number of items that can be significant cost drivers or act as constraints on the final endpoint design. This is by no means an exhaustive list of cost items – it focuses on cost drivers and constraints related to modernizing and implementing new types of human-system interfaces in the control room. Note that some of the items listed as constraints may become costs. For example, HVAC adequacy is a constraint if the plan is to retain the existing system and its capacity. It would become a cost if the decision were made to upgrade the HVAC system.

Table 2-2
Major Cost Drivers and Constraints

Cost Drivers and Constraints Affecting the Endpoint	Discussion
Physical Constraints	
Control room size	The size of the existing control, including ceiling height, sets the envelope within which the modernized control room must be implemented.
Existing console/panel structures	Decisions on whether to maintain, modify or replace existing panel structures affect costs and design constraints. Seismic qualification and the potential need for new seismic analyses should be considered in evaluating these options.
Existing cabling to panels	Some plants have installed raised floors to provide more flexibility in wiring and placement of workstations. Some older wiring may have to be retired in place if it cannot be easily moved or removed. Newer digital I&C and HSI systems make use of multiplexing and networks that minimize the amount of wiring required.
Physical separation	The need to meet physical separation requirements for safety-related equipment, and other fire protection requirements should be considered. If the changes are to come under IEEE 603, new requirements may be introduced as compared to an existing IEEE 279 or pre-279 licensing basis.
Control Room Support Systems	
Lighting	Lighting levels compatible with computer-driven displays need to be considered. Flexibility may be needed in the lighting systems to allow for varying light levels in different locations (e.g., low levels at computer displays, higher levels for conventional indications/controls or for task lighting).
HVAC	Adequacy of ventilation and air conditioning in the control room to handle significant increases in computer equipment needs to be considered.
I&C/HSI System-Related Factors	
I&C architecture and system capabilities	As noted earlier, the ability to modernize the HSI depends on how far the plant will go in modernizing the I&C systems, the architecture that will be used, and basic capabilities planned. Desired HSI features in the endpoint may be easy or hard, inexpensive or costly, depending on the I&C.
Availability of commercial solutions	Ability to use commercial equipment and software/systems versus custom development to accomplish the desired endpoint can be a significant cost driver. If the modernization is to be carried out over a number of years, then the endpoint may be based in part of an expectation of what will be available. More conservative approaches would base the endpoint on what is available now, and plan to update it as technology and vendor/system capabilities improve over time.
Degree to which solutions have been “proven”	The level of experience, breadth of application, and availability of feedback on successful use affect the cost to demonstrate acceptability or provide justification before actual use in the endpoint design.

Table 2-2
Major Cost Drivers and Constraints (Continued)

Cost Drivers and Constraints Affecting the Endpoint	Discussion
Ease of configuration and adaptation	The effort and cost to configure a commercially available system, and if necessary adapt it to the plant's particular needs, should be considered. For example, if the system has not been used in the U.S, it may need to be adapted to meet U.S conventions. In addition, adaptation may be required to meet plant-specific needs for items such as symbols, colors, etc.
Other Factors	
HFE program costs	This includes cost of developing plant-specific HFE guidelines and design practices (e.g., for display design, use of symbols and colors, etc.), providing training, and implementing these as part of the modernization program.
Meeting defense-in-depth and diversity related requirements	There will be costs and design constraints associated with integrating into the endpoint design a minimum set of diverse backup controls and displays to meet defense-in-depth and diversity requirements and expectations on minimum inventory of spatially-dedicated controls/displays (see Section 6.4)
Long-term support costs	Consider the cost of long-term maintenance and support of multiple HSI equipment types and vendors (depending on how much standardization is done) – considering impact on both engineering and maintenance to support the equipment and software. Of course, this should be balanced against the cost of not modernizing.
Transition costs	Costs associated with the transition or migration to the endpoint – these depend on the migration strategy that is chosen and are covered in more detail in the section below on migration planning. They include items such as cost of training including use of mockups/prototypes and simulators, interim configurations and temporary interfacing required during transitions, etc.

2.2.7 Comparison of Conventional and Modernized Control Rooms

This provides more detailed information on the differences between existing conventional control rooms, and modern control rooms employing newer digital instrumentation and control (I&C) and human-system interface (HSI) technologies. It is important to understand these differences when defining an endpoint or vision for the control room that will result from modernizing the I&C and HSIs in an existing plant.

Differences are described in two categories:

- Table 2-3 lists a number of differences in the concept of operations – how the plant is operated in both normal and abnormal or emergency situations.

- Table 2-4 describes differences in failure management – how failures or degradation of the instrumentation and controls or the HSIs are handled by the operating crew.

There are many levels of modernization that can be pursued by existing plants. The characteristics listed here for a modernized control room describe what might be achieved, or the impact that might be experienced with a “fully modernized” control room using current technologies. They intentionally emphasize the contrasts between existing and modernized control rooms, and the improvements and benefits that might be obtained through modernization. The features described here may or may not be included in any particular vendor’s offerings.

2.2.8 Worksheets for Development of Endpoint Concept

The worksheets included here can be used as a guide or a tool for defining and documenting the endpoint control room design concept. Three worksheets are provided, addressing three aspects of the endpoint concept:

1. Concept of Operations Worksheet
2. HSI Design Concepts Worksheet
3. HSI Failure Management Concepts Worksheet

The worksheets are intended to help the project team members organize their thinking as they develop the vision, provide a structure for defining the endpoint concept, and provide a means to document the goals, objectives and bases for the endpoint concept. Typically, the worksheets will be used along with sketches, drawings or computer-aided design renderings that provide visual illustration of the concept.

Note that there is some overlap between the information discussed in Worksheets 1 and 2. This is intentional. The first worksheet addresses the endpoint from an operations perspective – how the plant is operated now, and how operations will be conducted in the modernized control room (see Sections 2.1 and 2.2 for more discussion on Concept of Operations). The second worksheet approaches the problem from an HSI design perspective – how the displays, controls, alarms, and procedures will be modernized. While these worksheets focus on intended operation and use of the HSI systems, Worksheet 3 addresses a third perspective – what happens when there is a failure. It is important that all three of these perspectives be considered when defining the endpoint vision.

The worksheets include columns for documenting characteristics of the existing control room and desired or planned characteristics and features of the modernized, endpoint vision for the control room. The existing control room need only be described to the extent required to show important differences between the modernized control room and what exists today, helping to explain the new features (via comparison to conventional HSIs) and the basis for the changes (e.g., describe weaknesses or shortcomings of the present control room that are specifically addressed with improvements in the endpoint concept).

Note that additional columns can be added for interim configurations that will be produced as the control room migrates toward the endpoint vision – see Section 2.3 for guidance on developing a migration plan and interim configurations that will be produced during the modernization.

Table 2-3
Concept of Operations

	Existing Control Rooms	Example of a Modernized Control Room
How the Control Room Operators		
Monitor the plant process and systems/equipment	• In normal operations, monitoring is largely "by exception" – alarms alert the operators to conditions needing attention – or "by trends" – operators monitor the behavior of important plant parameters over time. • Operators monitor the process primarily through the indications on the control board plus some plant process computer displays (varies among plants). • Operators record some selected parameters or status information on log sheets on a regular basis, e.g., each shift or each day.	• Operation still largely by exception or by trends, but smarter alarms and diagnostics provide early warning of potential problems so action can be taken earlier, and monitoring is improved by integrating individual pieces of data to provide more useful information. • Operators monitor the process using the large overview display panel, plus workstation displays designed to provide both functional (e.g., inventory, flow, availability) and physical (e.g., pump and valve status) views of the process and systems. These displays are designed to assist the operators in identifying unusual trends or changes in status. • Indications and displays provided for monitoring are tailored to the task – overall plant monitoring during normal ops, task-specific displays for evolutions like starting a feed pump or lining up a system, specific information needed when in a particular procedure or accessing a specific control.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
Maintain situation awareness	• Operators scan indicators and meters to determine if variables are within normal bounds, recorders to check trends, alarm tiles to assess health of systems and understand upsets, and SPDS to check safety parameters. They use this information and their own experience to maintain situation awareness. • Operators may create a mental model of the situation by integrating information obtained from the various sources. As experience develops, operators are able to create more accurate and useful mental models to support situation awareness. • Supervisors obtain some limited information from panel displays; however, most information is obtained by oral queries of and responses from the operators at the controls.	• Workstation displays provide high-level overviews of plant status, with data already integrated to provide concise information on the health of systems, system/function availability, safety parameter status, etc. These displays are available to the supervisors and technical staff without any action by the operators at the workstations. • Operator aids use intelligent processing and algorithms to help assess upset situations, diagnose events, and take more effective actions earlier. • Large display panel provides continuous display of high-level plant information to help maintain situation awareness for entire crew. • Workstation displays also provide overview displays and indicators visible even when using a computer-based procedure or soft control screen. • Oral communication among members of the operating crew is still important and used to help maintain awareness and coordinate crew actions. • The process of creating accurate mental models that support situation awareness is facilitated by the relationships and integration provided by the displayed information. This reduces the mental demands on the operators to create accurate mental models, and may make it easier for less experienced operators to create more accurate mental models.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
Are alerted to situations requiring their action	• Annunciators provide visual and aural alerts to off-normal conditions based primarily on individual parameters exceeding setpoints. • In some plants, computer-based alarm systems and/or the plant process computer provides more detailed information on the specific alarm condition. • Alarm response procedures provide information for confirming the alarm condition and, based on other indications specified, help determine what situation caused the alarm. • Actions are also initiated in response to information on plant events or conditions provided by auxiliary operators or supervisors by oral communication or written orders. • Operators often actively search for information and monitor trends depending on the particular problem they are solving or evolution in which they are involved.	• Large display panel annunciates important high-level alarm conditions. • Lower-level alarms are annunciated by system alarms or detailed alarm indications at workstation displays. • Intelligent alarm processing helps prevent nuisance alarms, prioritizes and filters alarms. • Alarm response procedures and aids are provided at the workstations to automatically collect relevant information, help understand the situation causing the alarm, and guide the operator to an appropriate response. • Intelligent “early warning” alarms help detect and alert the operator to degraded or abnormal conditions before they become serious. • Task-based displays, soft control screens, and procedure displays provide relevant information and feedback that helps the operator detect problems immediately during specific operations, before process parameters get out of bounds or equipment trips off line. • Actions are taken in response to written or oral communications as in existing control rooms; however, more information may be provided by computer displays without processing or handling paper communications.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
Diagnose and troubleshoot problems with the plant process, systems and equipment	• Operators use panel indicators, recorders, and data available on the plant process computer, hard copy drawings, procedures, their own experience, and information collected by auxiliary operators outside the MCR to help diagnose problems. • Operators consult with their supervisor or shift technical advisor to identify actions. This is done largely by oral communication and face-to-face communication.	• Workstations provide a variety of displays that can be used to diagnose and troubleshoot problems, including: – Process and system displays (P&ID-like) that provide values of key parameters, status of equipment, system lineup – Plant process overview displays designed to assist operators in assessing the condition of the plant and diagnosing problems (e.g., display depicting thermodynamic conditions) – Equipment displays giving status and key parameters (e.g., vibration, temperature) – Trend displays showing historical trends over different time scales and allowing comparison of different variables on a single screen – Technical data sheets providing design basis information needed when diagnosing and troubleshooting problems. • Supervisors and the shift technical advisor have complete access to all technical data and can provide immediate assistance to the operators without any need to obtain data from them directly.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
Perform control tasks including planned evolutions	• Component control actions are taken using discrete control switches, with feedback obtained from nearby indicators and meters. • Manual control of processes or control loops is accomplished using hard control stations, which may provide limited feedback on control actions; however, feedback often must be obtained from displays that are not located close to the control station. • Sequences of control actions such as for startup and shutdown are taken by following hard-copy procedures and using the interfaces described above. • Supervisors are kept informed of status by oral communications.	• Component control actions are taken using soft controls by selecting the component and the desired control action (e.g., open or close), and then confirming the command; feedback is presented directly on the soft control screen, which also presents related information that helps monitor the effects of the control action and detect problems. • Process control also is accomplished using soft controls by calling up the appropriate control station, selecting the action and confirming it; again, feedback is provided directly on the soft control screen and related task-specific displays. • Planned sequences of control actions are carried out using electronically displayed procedures that indicate each step to be performed, provide information needed to check that prerequisites are satisfied and verify that the actions are proceeding as planned; selected control sequences are automated at operator request, with periodic break points for the operator to verify adequate performance and continue the sequence. • Supervisors are kept informed orally; however, they can also access displays which show precisely where the operator stands in completing a procedure.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
Respond to upsets and emergency situations	• In major upsets, operators enter their Emergency Operating Procedures (symptom-oriented) and follow the prescribed set of initial actions. Later, if they can determine what type of casualty has occurred they may invoke event-specific abnormal operating procedures (event-oriented). • Alarms are typically not used in the early stages of a major upset because the number of alarms is overwhelming and they need to perform immediate actions per the EOPs. • The operators use the controls and indications on the boards to perform actions, determine status, and make decisions (branch points) as prescribed in the EOPs. • When there is time, the alarms and indications are scanned to try to determine the cause of the event, identify any secondary problems that may have occurred, and assess current status of the plant and where it may be headed. • Operators and supervisors determine whether the plant's Emergency Plan must be entered and the action level. • Later, alarm histories, logs and process computer data are examined to further understand the event and determine a recovery strategy, and make necessary reports.	• Operators use the EOPs in the initial stages as before; however, the procedures are accessed through the computer. • Computer-presented EOPs have important parameter and status values inserted at the appropriate points in the text, reducing the time to determine a proper response and helping the operator make decisions at branch points. • Displays designed to support the symptom-oriented approach are accessible to the operators. These displays summarize the status of safety functions and the systems and components needed to perform the safety functions. • Diagnostic aids help the operators diagnose upsets and optimize their response; real-time, on-line plant documentation is available • Operators have available in the main control room a set of controls and displays that provide selected safety functions even if the workstations are not functional. • Supervisors and other plant staff, including those manning the TSC/EOF when activated, have important plant data available for diagnosis without any impact on the operations in the control room. • The supervisors and plant staff can to some degree determine what actions are being taken without interrogation or distraction of the operators. Oral communication is used to supplement this information as needed to maintain coordination. • Notification of regulatory and other authorities can proceed in parallel with operations in the control room. Actual data can be transmitted, where needed, with little potential for incorrect information being provided. • In the case of control room evacuation, a workstation in the emergency or remote shutdown control room can provide much more capability to control the plant than the emergency controls and displays currently provided.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
Take readings and log information	• Operators take readings from displays and manually enter them into log sheets. • Operators keep various operating logs manually and enter events as they occur or when they have the time to make the entries.	• Essential data are recorded continuously; these data and operating information such as equipment lineup changes, start/stop times, and other events are automatically archived. This information is also immediately available outside the control room for review. • Narrative logs are accomplished by keyboard entry, aided by the computer. Data can also be entered by voice commands and notations.
Perform or participate in maintenance and testing of plant systems and equipment	• Operators manually log events and operations. • Test data are recorded either manually or on special test instruments. • Control and tag-out of equipment (‘switching and tagging”) are done using manual methods and physical tags • Maintenance and test operations are coordinated by personal contact in the main control room.	• Operators have available displays that summarize all planned maintenance and testing operations. • Operators are queried for clearance to proceed with maintenance or testing through the computer workstations. Likewise, notification of the completion of maintenance and testing is provided to them and the rest of the plant staff through the workstation interface. • Computer-based operator aids are provided to support equipment “switching and tagging.”
MCR Functions and Responsibilities		
Plant systems and functions for which direct monitoring and control responsibility is in MCR	• Responsibility for monitoring and control of most plant systems and functions resides in the MCR. Controls and displays are provided for this purpose either on the main control boards/panels or on auxiliary or “back” panels. • Some systems and functions are controlled primarily from local stations or local control rooms – e.g., radwaste, off-gas, condensate polishing. Alarms may be provided in the MCR to alert the operators to any problems with these systems, although they are monitored locally.	• Some further centralization of functions is accomplished by bringing the monitoring and control responsibility for selected systems inside the control room, driven primarily by economics and efficiency of operation and maintenance. • This is facilitated by the capabilities of the distributed digital I&C systems and the MCR workstations (new functions can be added relatively easily), and selective automation of control functions. • This centralization is done carefully so as not to over-burden the MCR operators or distract them from their primary responsibilities.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
MCR operator involvement in I&C/HSI system diagnosis, troubleshooting and repair	• Operators are involved in I&C maintenance work only to the extent that it affects or could affect their tasks, their knowledge of the health of the systems, the need for their permission to begin work, etc. • Because a significant amount of I&C equipment and discrete devices is located on the operators' main control panels and other panels and cabinets nearby, the operators sometimes are directly involved with and impacted by I&C troubleshooting, maintenance and repair. • Operators are kept informed of maintenance activities outside the control room by voice communication links. Sometimes these activities result in alarms when equipment or a system is removed from service. Clearing of these alarms is sometimes used to indicate when equipment or a system is restored to service.	• With digital I&C systems, a good bit of the troubleshooting, tuning, and other investigative work by technicians can be done via maintenance workstations that need not be located in the main control room or control area. • Troubleshooting and repair of the I&C hardware is facilitated by self-diagnostics and indicators of failed components, "hot-swap" capability and other features that allow technicians to identify and make repairs with little impact on operations. • Thoughtful definition and processing of alarms on faults, failures and diagnostics of the I&C systems can provide the operators with just the information they need to know the health and operational status of the systems; detailed diagnostic information and alerts can be routed to the maintenance technicians. • Impact on operations resulting from HSI equipment troubleshooting and repair is reduced with multiple redundant workstations, as the operators can shift to another workstation while technicians swap out the faulty or failed workstation components. • Operators are kept informed of maintenance activities outside the control room by voice communication links and by displays that show activities and progress. • Displays show when a component or system is unavailable because of maintenance operations.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
Other functions	• Operators manually communicate with other plant groups, such as security, and outside organizations, such as police, fire, and weather services. • Operators spend time at shift changes bringing the new shift up-to-date on plant status and ongoing activities.	• Operators can communicate with other groups by normal voice communication; however, displays are provided so that summaries of critical information are immediately available to them without activating voice communication systems. • Through the workstation interface the oncoming shift can quickly review the plant status and events without affecting the operations at the workstations. The large display panel also assists in this. This information supplements shift change discussions, which can then focus on meaningful exchanges about plant behavior, unusual events or status information regarding the last shift.
Operating Crew Composition		
Size of operating crew	• Crews typically consist of two operators (one or both of them may be "at the controls") plus a supervisor in the control room. A higher-level supervisor of all plant operations is also on shift, but may not be in the control room. • Additional operators are often available to perform administrative tasks and control personnel access, maintenance, and testing.	• Primary operating crews will be essentially the same; however, sharing of tasks between the operators and supervisors will be facilitated. Operators can divide the workload to match the operations in progress. Similarly, the supervisors can share supervision or back up the operators. • There will be reduced need for direct access to the control room by other than the operating crew. (However, plant practices regarding pre-briefings for planned operational and maintenance evolutions may result in there being little change in control room traffic for these evolutions.)

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
Skills and training of crew	• Training relies heavily on use of a full-scope (replica) simulator, whose availability becomes a limitation on how much and how often training can be performed. • Operators must have skills and training on use of conventional control and display devices primarily (this becomes more difficult as new, especially younger recruits are more familiar with computer interfaces). • Plants have specific criteria regarding operator qualifications including aspects such as physical size and ability, visual acuity, color differentiation, etc., based on current operator tasks and interfaces.	• Training on the full-scope, replica simulator is still needed, but it is facilitated by the workstation-based HSI design. Quite a bit of effective training can be accomplished with an operator using a single workstation connected to the simulator's plant models (or a partial-scope simulator), without tying up the replica simulator facility itself. • Operators must have skills and be trained in the techniques used to manage the computer-based interface (some of this becomes easier as more people are accustomed to computer interfaces in general, but the specifics of the relatively complex NPP interface must be learned through training). • Criteria for operator qualifications must be consistent with assigned tasks and HSI characteristics, which may differ somewhat from current control rooms.
Operating Crew Interaction		
Crew communication, coordination and supervision	• Crew communication is accomplished largely by oral communication. In some control rooms this can involve significant distances. • Quantitative information is transferred to other operators and supervisors orally. This may be subject to errors in transmission or audibility problems in events that involve noise in the control room. • Each operator (and supervisor) knows something about what the others are doing simply by where they are positioned at the boards. However, typically only the operator who is directly in front of a panel section can read indications and parameter values located there, so the capability to check and back up an operator is somewhat limited.	• The operators and their immediate, active supervisor are typically in much closer proximity with compact workstations. • The operators and supervisors can exchange information by accessing the same displays. This avoids the transfer of quantitative information orally. • The large display panel provides a continuous display of high-level information. Also, selected workstation displays can be presented on the large display panel. The entire operating crew is privy to this information in parallel with any other tasks that are in progress, helping the crew's situation awareness, coordination, and teamwork. • It can be more difficult to remain aware of what each operator is doing when full-capability, compact workstations are used. However, features can be developed to help with this (e.g., providing indication of what displays are up at another workstation, or what procedure is being accessed/worked). Also, there is greater ability to check and back up an operator because of the ability to call up the same information at a supervisor's or another operator's workstation, and with the information provided on the large display panel.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
Division of responsibility among crew members	• The division of responsibility among control board operators is often determined essentially by the physical layout of the controls and indications on the boards.	• Division of responsibility can be based on the particular operations in progress and the workloads of the operators. • Increased automation acts essentially like another operator, and thus can affect division of responsibilities and tasks among the human operators.
Interaction with personnel outside the MCR	• Interaction is by voice communication plus some face-to-face contact as auxiliary operators and maintenance personnel are in and out of the control room getting direction and permissions, and reporting on activities in the plant.	• Interaction by voice communication is still used; however, most of the data available to the operators in the control room is also available to other members of the plant staff outside the MCR. The need for communication and interactions directly in the control room is reduced (although plant practices regarding pre-job briefings may result in little impact on control room traffic).
Engineering, Maintenance and Management Functions		
How system engineers monitor their systems' performance, diagnose problems, etc.	• Engineers use logged information and review the contents of logs. • Some plant computer systems can be used by engineers to provide system monitoring and trend information. • Engineers contact the operators directly for specific information not otherwise available to them. This can increase operator workload in logging or performing lengthy procedures to collect engineering data.	• Engineers can access a large amount of the real-time information available to the operators, without entering the control room. • Displays and aids can be designed specifically for system engineers' monitoring tasks.
How maintenance personnel are alerted to I&C/HSI problems, diagnose them, generate work orders, etc. (Note: Also see item above on operator involvement in maintenance.)	• Problems are identified and work requests are often generated by the operators.	• Fault indications and results of self-diagnostics are sent directly to maintenance personnel at their workstations; work orders are generated automatically for certain maintenance and repair actions. • Troubleshooting can be performed in many cases at the maintenance workstation (e.g., querying sensor readings, checking logic to determine possible causes of indications, calling up logs and diagnostic indications). • HSI equipment in the MCR is modular and easily replaceable, facilitating maintenance and repair with minimal disruption of control room operations.

Table 2-3
Concept of Operations (Continued)

	Existing Control Rooms	Example of a Modernized Control Room
How managers obtain plant data and monitor performance	• Managers use logged information and review the contents of logs. They may also direct requests to the operators or their supervisors by voice communication.	• Managers have access to essentially all plant operational or event data. Displays and aids can be provided to facilitate their monitoring needs. Voice communications can be limited to information or questions that are not covered by available displays.

Table 2-4
Failure Management

Characteristic	Existing Control Rooms	Example of a Modernized Control Room
Managing data failures	• Sensor failures are handled individually; operators use alternate or redundant signals if available, or use local instrumentation. • Most failures affect only a single reading or a single control loop.	• Automatic signal validation and signal selection can handle many sensor failures without disrupting automatic operation or the operator's ability to monitor and control. • Displays that integrate multiple sensor readings (e.g., level display that provides access to multiple redundant level indicator readings plus indications from others with different ranges) can aid the operator in interpreting the readings, doing cross-comparisons and making correct decisions. • On the other hand, effects of failures of individual sensors or data values on displays that provide higher-level information from multiple lower-level data sources may not be obvious and need to be considered. • Data quality or integrity indication should be built in for each reading and carried through to each display, calculation or higher-level parameter that depends on the affected reading. • Failures of integrated data sources (e.g., databases) used by the HSI also need to be considered – how they will be detected and what the operators should do in those situations.

Table 2-4
Failure Management (Continued)

Characteristic	Existing Control Rooms	Example of a Modernized Control Room
Managing HSI component failures	• Meter and indicator failures handled individually, using alternate or redundant indications or local instrumentation. • Control device failures also handled individually, falling back to local control of the component if necessary. • Method of dealing with plant computer CRT or workstation failures varies depending on significance to operation and safety, and availability of backups.	• Failures of workstations or portions of a workstation are dealt with through use of another redundant workstation – operators need to be able to detect when a workstation is disabled or malfunctioning and know what other station they will use in this situation, and how they will do this. • When an element of the large display panel fails, the same information typically is available and can be accessed at the workstations until repairs are made.
Managing HSI system failures	• Complete failure of the main annunciator system is rare but has happened – some plants have abnormal operating procedures in place for dealing with this, involving augmented monitoring of key parameters, standing watches, etc. • Monitoring system failures are typically limited in impact because the monitoring system has a narrow purpose (e.g., vibration monitoring) and the systems are not heavily integrated (e.g., individual radiation monitors may still operate in event of a failure). • Plant computer system failures can have significant impact depending on the scope and level of reliance on the system – alternate means of operating in absence of PCS information may be necessary.	• The I&C and HSI systems should be designed such that large-scale failures affecting multiple workstations are extremely unlikely; however, this possibility needs to be considered. • A limited set of diverse backups will be needed to meet regulatory expectations regarding diversity and defense-in-depth; additional diversity may be built in to manage economic risk as well as safety. • Vendor offerings should be scrutinized and system architectures chosen with potential failure modes in mind; most vendors offer two diverse platforms that can be used to manage the risk of large-scale failures. • Operator training and procedures need to reflect the fallback scenarios planned for dealing with large-scale failures.

Table 2-4
Failure Management (Continued)

Characteristic	Existing Control Rooms	Example of a Modernized Control Room
Managing automation failures	• Most automation is closed-loop process control. • Operator is alerted to control failure by alarms indicating the controlled variable is out of bounds. • Manual control capability is used to get the process or variable back under control. • Typically only a single loop is affected by failure.	• Failures of automated process control can have greater impact because multiple control functions are often combined in one processor, board or controller. • The more "integrated" the control, the greater the impact of failure, whereas distribution of loops/functions among controllers, and careful choice of what is combined on a single controller, can lessen the burden when a gross failure occurs. • Operators need to understand the potential effects of failures and be trained to deal with them; if they are not aware of what a control failure can cause, when they see the symptoms they will naturally form other hypotheses about what may be causing the behavior and may take incorrect actions as a result. • Failures of sequential control automation (e.g., automated startup sequences, system lineups) also need to be considered; the operator should be aware of what the automation is doing (e.g., through hold points) and be prepared to take over if it fails. • Critical controls should have fault tolerance features such as redundancy, self-testing, etc., to minimize the likelihood of gross failures; overall life cycle costs may be much lower if more is spent up-front to achieve fault tolerance, preventing situations that can be very difficult for the operators and also making on-line maintenance easier. • Note that even if the automation isn't totally failed, if the operator suspects or mistrusts it, then he or she needs something to fall back to.

The column labeled "Basis/Discussion" can be used to document specific objectives or goals of the endpoint concept and other information related to the basis for the planned changes. Or, it may provide discussion of changes that are likely to occur due to the conversion from analog to digital I&C and HSI technologies (whether intended or not), and how these will be dealt with in the endpoint design (e.g., potential impact on crew coordination and how this is addressed in the design concept). As discussed in the main body of this report, modern technologies can have both positive and negative impacts on the HSI. The challenge to the project team is to implement them in a way that takes maximum advantage of the positive aspects, and minimizes the negative aspects of the technologies.

Examples and suggestions of items to consider are provided in various places in the worksheets (these are shown in italics). These are not complete, and are intended only as examples to help the user understand the purpose and use of the worksheets and how to fill them in. Review of the tables given in Section 2.2.7, comparing conventional and modernized control rooms, may also help in defining the concepts desired for the plant and filling in the worksheets or other documentation the plant chooses to use to capture the endpoint vision.

It is important to remember that these worksheets are developed initially at the conceptual design stage – this is not detailed design. The information will be used to guide the detailed design efforts that occur later, and provide a direction and basis for modifications that, for most plants, will be made over a relatively long period of time. Review the guidance given in Section 3 for HFE design activities, and particularly Section 3.7 on HSI design. The structured approach described in those sections can be applied even at this conceptual design stage. Also, review Section 6.4 for design issues and challenges related to safety monitoring and control in a modernized control room.

The worksheets should be considered as living documents, subject to change as plant goals and priorities change, new problems are identified or lessons learned from early modifications, technologies evolve and new opportunities for improvement are identified. At the same time, the worksheets are intended to help set a direction for the modernization program and provide a means of carrying it through as people and organizations change over time. Capture the original basis for the endpoint design concept in the worksheets when they are first created, ensure that changes proposed in the future are considered in light of the original intent, and update the basis information to reflect any new changes that are incorporated in the endpoint design.

Table 2-5
Worksheet 1: Concept of Operations for the Endpoint Vision

	Existing Control Room	Endpoint Vision	Basis/Discussion
Normal Operation			
Monitor the plant process and systems/equipment, including performance monitoring	*Describe in general terms how operators monitor the process now, assess system performance, etc., sufficient to help explain basis for intended changes at endpoint.*	*Describe briefly any intentions for significant changes in how operators will perform monitoring tasks. For example, will higher-level information be used as opposed to discrete parameter monitoring? High-level overviews (e.g., on top-level workstation display and/or wall panel display)? Is it a goal that more automated equipment monitoring and diagnostics will be done by the system, with alerts to the operator? What about plant performance monitoring?*	*Describe goals and objectives – reduce operator time spent collecting and digesting individual bits of data? Specific goals for certain types of monitoring? Or is the objective to simply maintain equivalent capability to what is provided now? Any goals related to equipment or plant performance monitoring? Any past problems to be corrected?*
Perform or participate in maintenance & testing		*Describe intentions for any significant changes in time spent supporting maintenance and testing (either due to I&C upgrades or related to HSI improvements such as automated test support).*	*Describe any goals in this regard – specific goals for reduction of time spent? Reduction in personnel errors? Any particular evolutions targeted as troublesome now and needing improvement? Describe basis for expecting improvements – where will they come from?*

Table 2-5
Worksheet 1: Concept of Operations for the Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Normal Operation			
Equipment switching and tagging			*Any objectives related to improvements here? Any intent to tie into limiting conditions of operation decision-making or support?*
Take readings and log information		*Will some of this be automated?*	*Specific objectives? Basis for elimination of manual logs? Will operators lose touch if they do not take manual readings? How will this be addressed?*
Accomplish shift turnovers		*Even if no change is intended, describe how change may occur due to the modernization – time spent reviewing displays at workstation, how this will be accommodated, etc.*	
On-shift training			

Table 2-5
Worksheet 1: Concept of Operations for the Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Planned Maneuvers			
Startups and shutdowns		*Describe any significant changes planned for startup and shutdown evolutions, how the operators will accomplish them, what role the operators will play, and how many operators will be required. (Fewer manual control actions? More time to monitor and check for problems, or diagnose abnormal indications? Reduction in peak workloads?)*	*Describe basis for expected changes. Relate the proposed changes to any plant-level goals regarding startup and shutdown, outage time reduction, etc.*
Power level changes, including load following			
Surveillance testing	*Describe any problem areas or burdens on the operators related to surveillance test evolutions, to help explain changes that are proposed for the endpoint concept.*	*Describe significant changes expected in how major plant surveillance tests will be performed, operator roles, burden reduction, etc.*	*Provide basis for expected changes in testing and operator roles (e.g., describe what automation features will be expected to lead to intended reduction in operator time spent on testing).*

Table 2-5
Worksheet 1: Concept of Operations for the Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Abnormal Operation			
Identify and respond to plant equipment failures and other situations requiring operator action		*Describe any changes planned in the operators' use of alarms, expected use of overview displays, and other significant changes in how the operators detect problems and determine actions. Worksheet 2 will describe the alarm system and its features – this is the place to describe the operational implications of planned changes – for example, is it expected that the operators will use alarms during plant upsets? Will greater intelligence in alarm processing allow this, and also allow operators to be given higher-level alerts to developing problems, not just individual parameter alarms? Will this change how the operators monitor or respond to abnormal conditions?*	
Diagnose and troubleshoot problems with the plant process, systems and equipment		*Is it intended that operators will use specific displays or aids to assist them in diagnosis or troubleshooting? Any automation that will allow operators to work at a higher level, not having to deal with low-level information?*	

Table 2-5
Worksheet 1: Concept of Operations for the Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Abnormal Operation			
Respond to plant transients and upsets			
Respond to accidents using emergency operating procedures		*Describe any differences in how emergency operations will be conducted, and EOPs will be used.*	*Provide a description of the basis for the changes including any improvements that are intended and why they can be expected.*
Maintain situation awareness		*Describe concepts regarding how operators will maintain situation awareness in the modernized control room, and how this will differ from the current control room.*	*Discuss the basis for the planned concept and how situation awareness will be maintained or improved (describe goals for improvement). Address the potential drawbacks of computer-based systems and seated workstations regarding impact on situation awareness and how this is addressed.*
Handle compliance with tech spec conditions			
Monitor and control the plant under conditions of degraded or failed I&C/HIS	See Worksheet 3	See Worksheet 3	See Worksheet 3
Monitor and control the plant when the main control room must be evacuated		*Note any planned changes in use of the remote or auxiliary shutdown panel.*	

Table 2-5
Worksheet 1: Concept of Operations for the Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
MCR Functions and Responsibilities			
Plant systems and functions for which direct monitoring and control responsibility is in MCR	*A brief, high-level description should suffice here, with specifics given only as needed to help explain differences in the endpoint design concept.*	*Describe any plans related to centralizing functions, bringing some responsibilities into the MCR that presently reside outside. Discuss impact on operators in various plant operating modes.*	*Discuss basis for the planned change and objectives that are to be met. Discuss potential for increased burden on MCR operators, and potential loss of information and awareness due to not having as much presence out in the plant – discuss how this is addressed.*
Plant systems and functions given oversight in MCR but controlled outside the MCR		*Describe any changes in level of automation for these functions and the impact on operations.*	*Discuss basis for the change – what goal is to be achieved.*
MCR operator involvement in I&C/HSI system diagnosis, troubleshooting and repair			
Operating Crew Composition			
Number of reactor operators, senior reactor operators, and auxiliary or equipment operators on shift		*Note any planned changes here.*	*Describe basis for making the change (what is to be accomplished and why), and basis for acceptability (e.g., address burden on the remaining crew members if staffing is to be reduced).*

Table 2-5
Worksheet 1: Concept of Operations for the Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Operating Crew Composition			
Skills, education and training of reactor operators, senior reactor operators, and auxiliary or equipment operators			
Operating Crew Interaction			
Division of responsibility among crew members		*Describe how this is expected to change in the modernized control room, considering roles of automation, more efficient HSIs, etc.*	
Crew communication and coordination			*Address the potential for crew communication and coordination to be degraded if a compact workstation design is used in the endpoint, and how this will be addressed.*
Crew supervision			
Interaction between MCR operators and AO's		*Describe any intentions regarding use of new information systems to share information between MCR and outside operators.*	

Table 2-5
Worksheet 1: Concept of Operations for the Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Operating Crew Interaction			
Interaction between MCR operators and maintenance			
Interaction between MCR operators and engineering			
Maintenance, Engineering and Management			
Maintenance personnel are alerted to I&C/HSI problems, diagnose them, generate work orders, etc.		*Describe intentions for handling low-level diagnostic alarms, fault indications, etc. from the new digital systems. Will these be sent directly to a maintenance work order system? Will operators be alerted to these and be expected to take any action?*	
System engineers monitor their systems' performance, diagnose problems, etc.		*Any improvements planned related to the Maintenance Rule?*	
I&C engineers perform configuration changes and modifications to I&C/HSI			*Describe basis for the chosen approach. Address minimization of errors at the interface and potential for such errors to cause system failures.*
Managers obtain plant data and monitor performance			

Table 2-6
Worksheet 2: HSI Design Concepts for Endpoint Vision

	Existing Control Room	Endpoint Vision	Basis/Discussion
Information Display			
Architecture/arrangement and types of information displays provided, including: • Degree of conversion of discrete indicators and meters to computer-based information displays • Method of displaying trend information • Recording of historical data • Plant/process overview information display • Display of detailed data on systems and equipment including individual sensors		*Describe overall concept for information display and degree of modernization planned, including:* • *Any fundamental changes in the type and structure of information displays (e.g., functional displays, system-oriented displays similar to P&IDs, task-based displays, higher-level information displays)* • *Provision of spatially-dedicated indications and displays, in addition to computer-driven displays* • *How information presently displayed on recorders will be handled (trends, historical data)* • *Overview displays (e.g., large display panel, overview displays on workstations?)* • *Access to detailed information*	
Method of handling safety system status indication (W) and bypassed and inoperable status indication (BISI)			

Table 2-6
Worksheet 2: HSI Design Concepts for Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Alarms			
Architecture of alarm information presentation, including: • Different levels of alarm information (e.g., plant level, system level, component level) • Different priorities of alarms • Groupings of alarm information (e.g., by system, function, operator areas of responsibility) • Display of diagnostic or other information to support responding to alarms, including alarm response procedures		*Describe overall alarm presentation concept, including how and where different levels of alarm information will be presented, how alarm priorities will be handled, and presentation/automation of alarm response procedures.*	
Alarm processing, including: • Level of integration of data to form higher-level alarms • Alarm logic, filtering, suppression, reduction		*Describe any changes in overall alarm processing concepts.*	*Describe goals and basis for alarm processing concept (e.g., goals for alarm reduction during upsets, fewer alarms active during shutdown)*

Table 2-6
Worksheet 2: HSI Design Concepts for Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Controls			
Overall concept and architecture for controls, including: • Degree of implementation of soft controls • Spatially dedicated controls • Diverse backup controls		*Describe concept for controls, including overall approach for soft versus hard controls, spatially dedicated controls, diverse backups, etc.*	
Degree to which control actions are automated (e.g., sequences of control actions automated, startup sequences, system line-ups, etc.)		*Describe control automation approach.*	*Discuss basis for automation – objectives, basis for deciding what to automate, etc.*
Degree to which safety related and non-safety related controls are integrated (e.g., ability to control safety related equipment using the same non-safety workstations that are used for normal operation)			

Table 2-6
Worksheet 2: HSI Design Concepts for Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Procedures			
Degree of implementation of computer-based procedures, and method of presentation and use		*Describe overall approach to procedures – access, presentation, use, and any associated automation.*	
Computerized Operator Support Systems (COSS)			
Degree to which COSS are implemented in control room			
Integration of Displays, Alarms, Controls and/or Procedures			
Level of integration of displays, controls, alarms, and procedures		*Describe overall approach regarding degree of integration. Does the concept include presentation of alarm information on process/system monitoring displays? Integration of live information display with procedures? Access to controls from procedures?*	
Control Area Arrangement			
Degree of consolidation of monitoring and control capability at one or more locations (e.g., workstations) in the control room		*Describe approach regarding work areas or workstations. Will desks be converted to seated workstations? Retain benchboards, vertical panels? Create work areas at panels rather than seated workstations?*	

Table 2-6
Worksheet 2: HSI Design Concepts for Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
HSI Equipment Standardization			
Degree to which control room HSI equipment (user interface including hardware and software) is made consistent or standardized	*Consider the number of different types used now and the impact on maintenance and on operator burden and training.*		
Maintenance, Engineering and Management Interfaces			
Degree of support provided for maintenance personnel			
Degree of support provided for system engineers to monitor system and equipment performance, diagnose problems, etc.			
Support for I&C engineers to perform configuration changes and modifications to I&C/HSI			
Degree of support for managers to obtain plant data and monitor performance			

Table 2-7
Worksheet 3: HSI Failure Management Concepts for Endpoint Vision

	Existing Control Room	Endpoint Vision	Basis/Discussion
Data and Information Failures			
Instrument/sensor failures	*How detected?* *How handled?* *Procedure used?*	*How detected?* *How handled?* *Need procedure?*	
Multiplexer/communication link failures	*How detected?* *How handled?* *Procedure used?*	*How detected?* *How handled?* *Need procedure?*	
Data storage/database failures or corruption		*How detected?* *How handled?* *Need procedure?*	
HSI Component Failures			
Display device failures including individual meters, indicators, CRTs, panel displays	*How detected?* *How handled?* *Procedure used?*	*How detected?* *How handled?* *Need procedure?*	
Recording/logging device failures (including historian)	*How detected?* *How handled?* *Procedure used?*	*How detected?* *How handled?* *Need procedure?*	

Table 2-7
Worksheet 3: HSI Failure Management Concepts for Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
Control device failures including individual control switches, controllers, manual/auto stations, and dedicated soft control panels	*How detected?* *How handled?* *Procedure used?*	*How detected?* *How handled?* *Need procedure?*	
Workstation failures including processor, overall workstation failure		*How detected?* *How handled?* *Need procedure?*	
Alarm/annunciator system failures including gross failure, failure to update (lock-up), display failure, audible failure	*How detected?* *How handled?* *Procedure used?*	*How detected?* *How handled?* *Need procedure?*	
Monitoring and display system failures	*How detected?* *How handled?* *Procedure used?*	*How detected?* *How handled?* *Need procedure?*	
Large-scale failure of component control capability	*How detected?* *How handled?* *Procedure used?*	*How detected?* *How handled?* *Need procedure?*	

Table 2-7
Worksheet 3: HSI Failure Management Concepts for Endpoint Vision (Continued)

	Existing Control Room	Endpoint Vision	Basis/Discussion
HSI System Failures			
Large-scale integrated system failures affecting multiple workstations, display and control capability		*How detected?* *How handled?* *Need procedure?*	
Automation Failures			
Failures of process control automation	*How detected?* *How handled?* *Procedure used?*	*How detected?* *How handled?* *Need procedure?*	
Failures of sequential control action automation (e.g., automated startup sequences, etc.)		*How detected?* *How handled?* *Need procedure?*	
Automation Failures			
Failure of other automatic features the operators may rely on (e.g., automatic thermal limits monitoring, automated tech spec condition monitoring, other operator aids)		*How detected?* *How handled?* *Need procedure?*	

2.3 Migration Strategy

2.3.1 Gathering Inputs

2.3.2 Guidelines for HSI Migration

2.3.3 Planning and Evaluating the HSI Transitions at Each Migration Step

2.3.3.1 Migration of the Control Panels

2.3.3.2 Migration toward Operator Workstations

2.3.3.3 Migration of Functionality and Concept of Operations

2.3.3.4 Size and Number of Steps in Migration

2.3.4 Ensuring Adequacy of Interim Hybrid HSIs

2.3.4.1 Hybrid HSI Issues

2.3.4.2 Evaluation of HSI Effectiveness

2.3.5 Conceptual Design of HSI Changes

2.3.6 Evaluating Costs and Minimizing Project Risk

2.3.6.1 Costs and Constraints Affecting the Migration Plan

2.3.6.2 Minimizing Project Risk

2.3.7 Licensing Evaluations

This section provides guidance on development of a “migration strategy” for the main control room and other human-system interfaces. A migration strategy defines the specific steps that will be taken to modernize the HSI as the various stages of I&C modifications are undertaken, with the ultimate goal of reaching the endpoint “vision” for the HSI defined in Section 2.2 above. This includes changes in functionality such as automation, and changes in procedures and training as well as physical changes to the HSIs.

Although the prioritization and ordering of changes to be made at each step in the program will be driven in large part by the I&C upgrade plan, there typically is some flexibility in how the HSI upgrades are scheduled. Also, operational and human factors considerations may lead to a different ordering or prioritization of the changes.

For example, some plants have delayed making changes to the control boards or panels during their earliest upgrades, choosing to change primarily the I&C equipment “behind the boards” and leave the interface largely the same. This allows the plant to gain experience with digital equipment qualification, installation and maintenance before taking on the other human factors and operational aspects of modernizing.

On the other hand, plants may choose to accelerate some HSI changes to begin familiarizing the operators with newer interfaces gradually. For example, some discrete indicators, meters, and recorders on a control panel might be replaced with a video display unit even before the associated I&C systems have been fully converted to digital, if this is seen as beneficial in starting the migration toward digital interfaces. Soft controls might be implemented for a non-critical system at an early stage of the upgrades to gain experience with the new HSI before more widespread implementation of soft control.

Other plants may pursue a more aggressive implementation of HSI changes to avoid having to deal with many interim configurations and begin to reap the benefits of a modern HSI in a shorter timeframe.

Advantages and disadvantages of these different approaches are discussed in this section.

Figure 2-11 illustrates the migration planning process and some important inputs and considerations involved in the development of a migration plan:

- Gathering **inputs** that will be needed to develop the migration plan
- Applying human factors engineering **guidelines** or principles that should be followed in planning and implementing the migration
- Planning and evaluating the HSI **transitions** – planning the migration steps to allow sufficient time and training to ensure that operators and other users become familiar with the changes and comfortable with the new technologies being introduced, and to minimize the likelihood of human error
- Ensuring **effectiveness of hybrid HSIs** produced at each stopping point – at each step, the modifications must result in an HSI that is acceptable for operation until the next step is taken, even though this may involve interim, “non-ideal” designs and hybrid interfaces. (In fact, each interim HSI should be designed to be acceptable for operation indefinitely. Circumstances and priorities at the plant could change later, causing the next set of modifications to be delayed and requiring operation with the interim configuration for an indefinite period of time.)
- Developing **conceptual designs** of the individual HSI changes to be made during migration
- Evaluating **costs** and minimizing project risks
- Performing **licensing evaluations** and minimizing licensing risk.

Each of these is discussed in this section, in the order in which they are listed above.

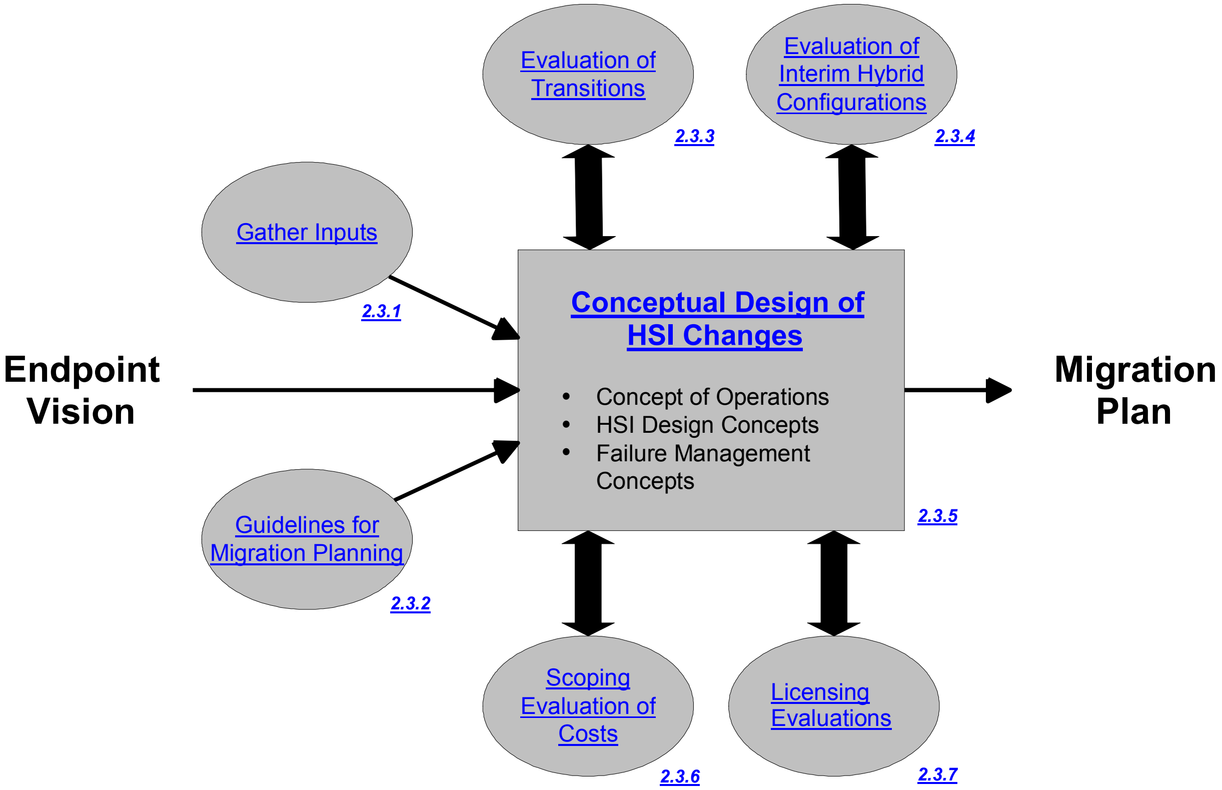

Evaluation of Transitions
2.3.3
Evaluation of Interim Hybrid Configurations
2.3.4
Gather Inputs
2.3.1
Conceptual Design of HSI Changes
• Concept of Operations
• HSI Design Concepts
• Failure Management Concepts
2.3.5
Endpoint Vision
Migration Plan
Guidelines for Migration Planning
2.3.2
Scoping Evaluation of Costs
2.3.6
Licensing Evaluations
2.3.7

Figure 2-11
HSI Migration Planning

2.3.1 Gathering Inputs

It is important at the beginning to identify and gather initial information that will be needed to develop the migration plan. More information can be developed later as the migration planning progresses and more specific needs are identified.

The inputs and drivers that were listed in Section 2.2 for endpoint definition also apply to migration planning. These are repeated below:

- Plant long-term goals including any goals related to human performance
- I&C upgrade strategy and initial planning, including I&C architecture, planned changes in functionality (e.g., further automation), and plans for implementing the necessary infrastructure (e.g., distributed control system, communication networks)
- Operating and maintenance experience, existing operational or human performance problems and opportunities for improvement – this is discussed in more detail in Section 2.2
- Strengths of the existing control room and other HSIs that should be recognized and maintained or further strengthened in the modernization

- Weaknesses or problems with the existing control room and HSIs (e.g., HSI equipment that has high maintenance burden, equipment abandoned in place, lighting problems)
- Known or expected changes in personnel or their capabilities that should be taken into account in long-range planning (e.g., expected changes in age or experience of operating crews, expected changes in background and experience of new hires)
- Known or expected changes in the plant or utility organization that might affect how operations, engineering, and maintenance activities are conducted, information requirements for various users of I&C/HSI systems, etc.
- Improvements that may be sought in support areas such as equipment monitoring, surveillance testing, logging, administrative controls, limiting conditions of operation (LCO) monitoring, etc., that could lead to requirements or desires that should be reflected in the endpoint design
- Vendor solutions being considered
- Internal or external constraints or commitments (e.g., specific licensing commitments).

In addition to these, other inputs and driving factors for the migration plan include:

- Outage plans – schedule, durations, other activities planned during outages that could impact or be impacted by the HSI changes
- Resource constraints – availability of personnel to support the full extent of the changes, including engineering, operations, maintenance, training, etc.

Both of these are discussed further in the section below on costs and constraints affecting the migration plan.

2.3.2 Guidelines for HSI Migration

Table 2-8 lists a number of guidelines or principles that should be followed in planning and carrying out the various steps involved in modernizing the main control room and other HSIs, procedures and training. These are focused particularly on the issues associated with hybrid interfaces involving both the older analog style interfaces and those employing more modern, digital technologies.

Consider these guidelines when developing the initial migration plan. Then revisit each of them when the plan is completed, and again as each phase is implemented.

Table 2-8
Guidelines for HSI Migration

1.	Plan the extent and pace of the HSI modifications, and the associated training and procedure changes, such that the operators and other users will have opportunity to become sufficiently familiar with the new technologies and new interfaces, and can be expected to perform adequately during and after each step of the migration.
2.	Ensure that changes to the training simulator are properly scheduled and coordinated so that the operators can maintain their proficiency and qualification as each change is made. This may include the need to support qualification on both the old and new interfaces, particularly if the simulator supports multiple units. (See Section 6.3.)
3.	Ensure that the impact of each step-wise change on control room operations (Concept of Operations) is evaluated, well-understood, accepted by the Operations staff, reflected in the procedures, and consistent with other changes being made to the I&C and plant systems before operation begins with the new HSI.
4.	Ensure that potential failure modes and degraded conditions of the I&C and HSI are appropriately addressed in the design, training, procedures, and Concept of Operations as each step change is made. (See Section 6.4 for guidance on designing for conditions of failed or degraded HSIs.)
5.	Ensure that sufficient HSI equipment is provided to enable operators to adequately monitor and control the plant and maintain plant safety during and following each HSI transition. If necessary, temporary HSI equipment or other necessary support (e.g., additional operational staff) may be used. (See Section 6.4 for guidance on safety monitoring and control design.)
6.	Ensure that issues associated specifically with hybrid HSIs are identified and adequately managed at each step in the migration (examples of these are given in the section below on evaluation of interim hybrid configurations).
7.	Apply appropriate human factors engineering design and verification and validation (V&V) processes to ensure that each interim configuration is adequate to support plant operation – not only until the next planned step, but for an indefinite period of time (the next modification planned could later be postponed). (See Section 3.8.)
8.	Ensure that the impact on the plant's licensing basis at each step is evaluated, is consistent with the licensing plan, and meets applicable regulatory requirements. (See Section 5.)
9.	Ensure that an appropriate monitoring program is in place at each step to detect and correct any problems that may arise once the interim configuration becomes operational. (See Section 3.9.)

2.3.3 Planning and Evaluating the HSI Transitions at Each Migration Step

There are many different approaches that can be taken to modernize the HSI as I&C modifications and upgrades are made. Guidance is given below on several aspects of planning for the HSI migration steps and transitions:

- How the control panels and associated controls, displays and alarms will be changed over time – by system, by panel, etc.
- How the functional and operational characteristics of the control room will be changed

- The size and number of steps to be taken to migrate to the endpoint – for example, concentrating many of the changes in a few outages, or spreading them out over many outages.

2.3.3.1 Migration of the Control Panels

In planning the migration of the control panels or control boards toward the chosen endpoint, there are several approaches that can be considered. Note that no one of these will be used exclusively – a realistic plan for migration of the HSI over time will involve many or all of these methods:

- Migrate by I&C system – as the instrumentation and control systems are updated, also update the associated HSI (controls, displays, alarms, etc.) for that I&C system. Note that this does not necessarily correspond to plant systems or functions. The "I&C system" may be one or more cabinets full of analog circuit cards that serve various functions for a portion, but not all, of one or more plant systems. Updating the HSI driven by the analog controls in these cabinets would not modernize the other portions of the HSI for the affected plant system (e.g., component controls such as pump and valve controls, indicators or recorders driven by instrumentation that does not go through the analog cabinets).
- Migrate by plant system or function – for example, upgrade all of the HSI for the feedwater system, or for a function such as reactivity control or inventory control
- Migrate by physical location in the control room or plant – modernize the controls, displays, and alarms on a location by location, or panel section by panel section basis
- Migrate by HSI element – modernize the displays in one or more steps, modernize the alarms, modernize the controls, and so forth, across systems and across the control boards or panels. Although this is not practical on a large scale, it can be followed for some portions of the control room changes.
- Advantages and disadvantages of these approaches are noted in Table 2-9 below. These should be considered when defining the HSI migration strategy.

Any temporary HSI equipment or administrative controls that may be needed during the transitions also should be identified. Examples include temporary alarms needed during transitions that take the primary alarm system out of service, and temporary indications or augmented operator surveillances needed while monitoring systems are being replaced.

Temporary communications may also be required. It is important that any temporary HSIs are developed and evaluated using an appropriate human factors engineering process, verifying that the operators can perform the required tasks satisfactorily during the transitions. This is particularly important when changes are made at power, but also can be needed during an outage when some level of monitoring is still required (e.g., moving fuel, fuel storage pool, radiation monitoring). Use the guidance given in Section 3 for HFE design and analysis activities.

Table 2-9
Advantages and Disadvantages of Different Migration Approaches for Control Panels/Boards

Migrate By	Advantages	Disadvantages
I&C system (e.g., upgrade the feedwater control system, or all the analog controls within an I&C cabinet)	Most logical fit with the I&C upgrade needs and upgrade plans based on I&C obsolescence. Can provide a good fit with operations and operator tasks if the system is somewhat stand-alone and the tasks that are impacted are just those associated with that system. (However, see discussion at right for cases when tasks cross over into other systems.)	Inconsistency within a panel section – a hybrid work area is created if the controls and displays associated with the I&C system being upgraded are interspersed with controls and displays for other systems. Inconsistency within functions and tasks – although a task may primarily involve the I&C system that is being upgraded, it also may involve use of some controls and displays of other systems. Also, some HSI elements for the affected plant system (e.g., component controls) may not be upgraded if they are not driven by the I&C that is being replaced. As a result, tasks require use of hybrid HSI elements. Similarly, tasks related primarily to other systems may occasionally require use of the controls and displays for the upgraded system. This requires evaluation to ensure that use of the new HSI equipment along with conventional interfaces for the non-upgraded systems will provide acceptable performance.
Plant system or function (e.g., upgrade all the HSI for the feedwater system, or for reactivity control or inventory control)	May provide the best fit to operations and operator tasks. Facilitates implementation of features such as function-oriented and task-based displays, task automation, etc.	Inconsistency within a panel section if the panels are not organized by plant system/function (although the change may be consistent with demarcation lines on the panel) Greater impact on I&C upgrade plans – changes may affect more than one system in order to create a truly functional upgrade
Physical location (e.g., by panel section)	Can be more straightforward and less confusing to the operators, as it is very clear which parts of the HSI are using the new technologies and which are not. Also may have advantages for installation, as the changes are localized to a defined portion of the panel/control room.	Inconsistency within functions and tasks – if the panel sections do not map strictly to specific systems or functions, then operator functions and tasks will necessarily involve use of hybrid HSIs as the actions required cross over multiple panel sections.

Table 2-9
Advantages and Disadvantages of Different Migration Approaches for Control Panels/Boards (Continued)

Migrate By	Advantages	Disadvantages
HSI element (e.g., alarms, displays, etc.)	This may be the most straightforward for the operators to assimilate, as it is very clear what has been upgraded and there are no hybrid issues within the HSI element (displays, alarms, controls, etc.) being changed.	May not be practical to implement on a large scale for elements other than the main annunciators. The change involves multiple systems and many tasks, so the impact on operations is widespread. Inconsistency in overall design approach – differences in design approach may be introduced among HSI elements (e.g., implementing a new alarm system that organizes the alarm information in a way that is different from how the controls and displays are organized). These would need to be addressed in familiarization and training, and task verification.

2.3.3.2 Migration Toward Operator Workstations

If the endpoint calls for operation from more compact workstations[2] or work areas, then migration of existing operator desks in addition to the benchboards and panels needs to be addressed.

If the work areas are to be created at the existing panels or benchboards, then the information in the table above related to panel migration applies. Another option is to transition the existing operator desks, or other work areas separate from the boards, into workstations for monitoring and control. An example of this was described in Section 2.2.

Workstations can be implemented initially for control of non-critical systems. Large display panels can be installed in parallel, with most of the conventional controls remaining on the benchboards. This allows the operating crews to become familiar with both the large displays and the workstations, before they must be used for critical plant systems.

2.3.3.3 Migration of Functionality and Concept of Operations

In addition to the migration of the physical control panels and individual HSI resources such as controls, displays, and alarms, it is important to consider how the functionality of the HSI will be changed over time to reach the desired endpoint. Section 2.1 above discussed changes in the functional characteristics of the control room that may be part of the modernization, such as

[2] In the computer industry the term "workstation" is often used to refer to a single computer (e.g., an engineering workstation). Here we use the term to refer to a work place from which the operator can monitor and control the plant. This typically involves multiple computer-driven information displays and other HSI elements such as control input devices, alarm displays, etc.

increased automation and a higher level of intelligence built into the HSI. If these are part of the chosen endpoint, consider how they will be phased in as the HSI migrates toward the final design.

Acceptance by the operators of the new functionality should be considered here. In some cases a smoother transition may be obtained with less training burden if the interface itself is changed first (e.g., changing from conventional controls to a new soft control system), and then additional functionality (e.g., automation of control actions) is introduced later after operators become familiar with the new interface.

More generally, the overall Concept of Operations must evolve along with the control panels and HSI functionality as the HSI migrates toward the endpoint. This was illustrated in Figure 2-3. The migration plan should include planning for:

- Migration of operator roles and responsibilities
- Changes in how normal and emergency operations are conducted in the control room
- Changes in how the operating crew will deal with failures or degradation of the I&C or the HSI itself, at each step
- Corresponding procedure changes (normal operations, emergency operating procedures, alarm response procedures, etc.).

2.3.3.4 Size and Number of Steps in Migration

This section discusses different approaches that can be taken in defining steps or phases of HSI migration, and considerations involved in selecting the specific approach for phasing the changes, including:

- Making the changes in a large number of steps that are small in scope
- Concentrating the changes in one or a few large modifications, possibly during an extended outage
- Making some of the changes with the plant at power (non-outage changes)
- Retaining some of the old interfaces for a period of time, allowing parallel operation of the old and new HSIs.

Table 2-10 below identifies advantages and disadvantages of each of these aspects of phased HSI changes. These should be considered when developing the migration plan. Of course, the potential disadvantages also should be specifically addressed in design and evaluation of the modifications. More detailed guidance on design and evaluation methods is provided in Section 3. Also, note that NUREG 0711 provides guidance related to stepwise implementation of HSI changes (see Table 12-1 in NUREG 0711).

Table 2-10
Phased Implementation of HSI Changes

Phasing Aspect	Advantages	Disadvantages
Many small modifications	Minimum disruption to plant operations related to each change Least impact on available resources (engineering, operations, training, maintenance) Easier for users to assimilate the changes individually	Many interim, hybrid configurations leads to greater likelihood of inconsistency in the HSI Potential for greater burden on operators in the long run due to the HSI continually changing Smaller changes are less obvious to the user – may require extra measures to make the differences clear and avoid negative transfer of training Potential for unexpected interactions as many small changes are made
One or very few large modifications	Can avoid inconsistencies and non-ideal designs associated with interim configurations – produce a more optimum configuration in a single design Reduced cost of evaluation, development of procedures, and training on interim configurations	Greater impact on plant operations and available resources Large training burden as operators must become familiar and proficient with a significantly different HSI Greater difficulty in scheduling simulator modifications to support training and qualification on the new HSIs, while maintaining qualification on the old HSIs prior to completing the change Cost of lost production due to extended outage(s)
Modifications made at power	Can significantly shorten the overall schedule – time to reach the endpoint Allows changes to be made when there are fewer conflicts with other activities such as maintenance or repair activities, and there are fewer alarms due to maintenance or systems out of service Reduces impact on outages and outage resources – lessened risk of extending an outage. For some systems that must remain operational during shutdowns, there may be lower risk to replace them at power.	Risk to plant availability (e.g., risk of plant trip or need to reduce power) Need for temporary procedures and special training to handle transition during power operation

Table 2-10
Phased Implementation of HSI Changes (Continued)

Phasing Aspect	Advantages	Disadvantages
Overlapping – use of parallel (old and new) HSIs for a period of time	Any problems with the new HSI can be identified and resolved while the old HSI is still in place and can act as a backup Users can become familiar with the new HSI while the old one is still available for use (particularly in an emergency, when a user may prefer to revert to a familiar interface)	Inconsistencies and differences in behavior between the old and new HSIs, while both are present and being used, may be more of a problem than if the old is simply replaced with the new Space limitations, clutter, and potential distraction associated with two sets of HSIs

This table addresses issues associated with the size and number of migration steps. Another aspect of phasing the implementation of HSI changes is which systems are changed first, and which come later. As discussed in Section 2.1 and in the section below on Licensing Evaluations, one strategy often followed is to make changes to non-safety systems first, and make safety-related changes later after some experience has been gained. This can help minimize safety and licensing risks.

2.3.4 Ensuring Adequacy of Interim Hybrid HSIs

It is very important to ensure that the interim HSI design that is produced at each stage, coupled with appropriate procedures and training, adequately supports operator tasks and the overall concept of operations as it evolves. This should be ensured even when the interim configuration involves non-ideal designs and hybrid configurations brought about by a step-wise progression toward the endpoint.

2.3.4.1 Hybrid HSI Issues

This section identifies a number of hybrid HSI issues that should be addressed when designing and evaluating interim HSI configurations. These issues relate to potential human performance problems associated with a human-system interface employing a mixture of older, typically analog equipment and more modern, digital equipment and systems. The same issues will need to be addressed as part of detailed design of the HSIs (using the guidance given in Sections 3 and 4), in regulatory and licensing activities (see Section 5.2.1.2), and in development or modification of training programs (see Section 6.3).

Note that many of these issues are not new, as existing plants have dealt with a mix of analog and digital technologies for some time. For example, in many plants the operators currently work with a combination of analog and digital or computer-driven displays for monitoring plant variables, including Safety Parameter Display Systems (SPDS) and Post-Accident Monitoring Systems (PAMS), see Section 6.4. Plant computers provide graphical displays that are used under normal and emergency conditions along with conventional meters and indicators.

However, as plants further modernize their control rooms over time there will be a significant increase in the number of digital HSIs that will be used and thus hybrid issues will be more pronounced, particularly as digital controls (e.g., soft controls at workstations) are introduced alongside conventional controls.

Note that these are just some of the issues that may arise with control rooms containing hybrid HSIs. It is important that the project team:

- Specifically identify the hybrid issues that need to be addressed at each step in the migration
- Assess the risks associated with them – likelihood of a problem resulting from the hybrid situation, and potential consequences to plant safety and availability, and
- Determine how they will be addressed.

This may affect planning of the activities involved in the modifications, and in some cases it could lead to changes in the designs to accommodate specific hybrid HSI concerns.

Also note that in addition to these issues, which relate to potential differences between older analog and newer digital HSIs, there are other aspects of HSI design that also can introduce differences in the interfaces the operators use – for example, use of both qualified and non-qualified HSIs (see Section 6.4.3.4). These should be considered along with the hybrid analog-digital issues discussed here.

High-level issues related to overall plant operation are described first, followed by specific issues related to individual hybrid HSI elements.

2.3.4.1.1 Hybrid Issues Related to Overall Plant Operation

HFE evaluations should address the potential impact of hybrid HSIs on operator tasks, and how this might affect plant safety. For example, the following hybrid issues or concerns should be addressed:

- Inconsistencies in design or operation between different systems (e.g., one still analog, the other converted to digital) or between different sections of the interface, when these must be used together or alternately to perform operator tasks, such as:
  - Carrying out abnormal and emergency operating procedures – where in these procedures must the operators transition across the technology interface (i.e., move from analog to digital or vice-versa), what confusion or errors or delays might occur at these transitions, and what would be the impact on plant safety? How is this addressed in the HFE evaluations?
  - Assessing the state of the plant, its systems, and the status of the critical safety functions – is there a mix of technologies that must be used here? Does this impact operator performance, and has this been addressed in the HFE evaluations?
  - Operator actions credited in the licensing basis – are there transitions across technologies that must be made to carry out these tasks? If so, what errors or delays might be imposed by this, and how has this been addressed in the HFE evaluations?

  - Other risk-important operator actions or tasks, such as those identified as risk significant in the PRA – what transitions between interface technologies are involved in these tasks, and has this been addressed in the HFE evaluations? See Section 5.2.6 for guidance on use of the PRA to identify risk-important human actions, and assessing impact on the PRA of the control room changes being made.

- Increased training burden to allow operators to remain proficient with old interfaces that are retained, while gaining proficiency on the newer ones being installed – sufficient resources and time must be available to ensure that this training is accomplished effectively. If it is not, there is risk that operators may lose their proficiency with older interfaces they use infrequently, or there may be insufficient time or attention paid to training and familiarization on the new interfaces, either of which could lead to errors. See Section 6.3 for a more detailed discussion of training issues associated with digital I&C and HSI upgrades.

- Compromises in design to accommodate old and new technologies – for example, attempts to set lighting levels high enough to make remaining analog gauges readable but not too high for recently installed CRT or flat panel displays.

2.3.4.1.2 Specific Issues Associated with Hybrid HSI Elements

At a more detailed level, there are a number of specific issues or concerns related to different aspects of hybrid HSI designs. For example, hybrid issues need to be examined for the following types of hybrid HSI elements:

- Duplicated indications – both analog and digital indications of the same variable
- Duplicated controls – both analog and digital controls provided for the same function
- Control tasks that require use of analog and digital controls at different steps in the same task
- Deactivated controls and/or indications (those left in place but non-functional)
- System/functional groupings of controls and indications in hybrid designs
- Differences in level of automation between analog and digital implementations
- Hybrid alarm systems, or different implementations of alarms between analog and digital systems
- Hybrid procedure implementations – some procedures converted to computer-based format but others not
- Differences in failure modes between analog and digital HSIs

Table 2-11 lists examples of hybrid issues or concerns for each of these HSI elements. These are examples only – it is important for the design team to identify hybrid issues applicable to the plant-specific design at each step in the modernization program and to ensure that they are adequately addressed.

Table 2-11
Specific Hybrid Issues for Individual HSI Elements

Hybrid Issues for Individual HSI Elements
Duplicated (analog and digital) indications • Are the same values shown on each? How will potential differences in displayed values be handled by the operators? Which one will they trust to be correct? • Will there be differences in accuracy of the two indications, or perceived accuracy and potential confusion (e.g., a digital indication with several significant digits appearing to be more accurate than an analog meter reading, but in fact based on a wider-range or less accurate instrument) • Are both types of indication referenced in the procedures?
Duplicated (analog and digital) controls • Differences in how the controls operate, including potentially subtle differences such as range of control, rate of change, etc. • Differences in how auto/manual controls are used, how bumpless transfer is accomplished, indications used when operating the controls (e.g., demand, actual) • Are both types of control referenced in the procedures?
Control tasks that require use of analog and digital controls at different steps • How smooth are the transitions between use of one type of control at one step, and another type at the following step? • Are there subtle differences in how the controls operate (e.g., analog and digital controllers with auto/manual stations that on the surface appear to perform similar functions, but the details of their operation reveal differences in behavior between the analog and digital devices)? • Will there be extra mental workload during transitions due to the need to focus on the differences between the controls? • If an operator were to become confused as to which type of control is being used at any given step, what types of errors would be most likely to occur and what would the consequences be? How would such errors be detected and corrected?
Deactivated (left in place but non-functional) controls and/or indications • How might these interfere with task performance? • What is the potential for an operator to mistake one of these for an active control or indication, particularly in stressful or high-workload situations? What errors might be made, and what would the potential consequences be?
System/functional grouping of controls and indications • Will the benefits obtained from system/functional groupings of controls and indications that were implemented post-TMI be lost or degraded with a hybrid arrangement? • Are the groupings of controls and indications on new digital HSIs compatible with the groupings of the remaining analog controls and indicators? • If controls related to a single system or function are split between two different locations (e.g., some control actions can be taken at a workstation while others must still be performed at the control boards), is there potential for operator confusion as to where an action can be taken? Could this lead to delays that impact task performance?

Table 2-11
Specific Hybrid Issues for Individual HSI Elements (Continued)

Hybrid Issues for Individual HSI Elements
Differences in information presentation • Are there differences in how information is arranged on new computer-driven displays as compared to the way similar information is presented on control boards that are retained? • Are there differences in coding used for digital versus analog information presentations (e.g., different use of symbols or colors)?
Differences in level of automation • If some systems/functions have been upgraded but others have not, could differences in the level of automation of the systems/functions lead to confusion or errors (e.g., if some steps in a sequence of control actions are automated with the new digital implementation for a given component or function, but these steps must be performed manually for a very similar component or function that has not been upgraded to digital)? • What types of errors might occur, how would they be detected and corrected, and what would be the consequences of such errors?
Hybrid alarm systems • Are there differences in how alarms are defined and generated for new digital systems as compared to alarms for existing systems? • Are there alarms generated by new digital systems that are not presented on the main alarm system (e.g., overhead annunciators)? Are any of these at the same level of importance as the main alarms? How will the operators integrate these alarms when responding to plant events or upsets? • Are the prioritization of alarms and the methods for indicating alarm priority consistent among the various alarm implementations? • Are the annunciation sequences different between analog and digital alarm implementations (e.g., different behavior of incoming versus clearing alarms, momentary alarms, flash rates, etc.)? • Are the alarm controls (e.g., for silence, acknowledge, reset, and test) consistent among the various alarm implementations? • Will the addition of new digital systems result in additional alarms requiring separate acknowledgment? Will the operators be burdened by having to take multiple actions to acknowledge all the alarms and silence audible indications during plant upsets?
Hybrid procedure implementations • If some procedures have been converted to computer-based procedures, but others have not, how smooth will the transitions be between the two types of procedures? • How might this affect task performance?
Differences in failure modes • Are there differences in the behavior of digital versus analog devices when power is lost to the device? When the input signal is lost or off-scale? • Have functions been combined as part of the digital upgrade? If so, will the consequences of failure of the new equipment (e.g., failure of a card, module, or communication link) be more severe or otherwise different as compared to failures of the remaining analog equipment? • Will the indications the operators receive when these types of failures occur be different for the digital implementation than for the analog? Is there potential for operator confusion or errors to result from these differences?

2.3.4.2 Evaluation of HSI Effectiveness

It is important to remember that each interim configuration produced during migration is a design in itself, which should undergo appropriate HFE evaluation. Human factors verification and validation techniques should be applied to ensure effectiveness of each configuration. Section 3 provides more detailed guidance on HFE evaluations and analyses including human factors verification and validation.

Training of operators on the new interfaces provides an additional opportunity for validation of the interim designs. Human performance evaluations can be made to see if the goals of the modifications are being achieved, to identify any unexpected human performance issues, and to specifically evaluate hybrid issues associated with the interim designs.

Finally, the migration planning should include plans for monitoring the initial phase of startup after each modification step to ensure that:

- Operational and maintenance problems that arise with the new systems and HSIs are identified and addressed
- Personnel are sufficiently familiar with the new systems and HSIs to adequately support operations and maintenance
- Any negative "transfer of training" from the old removed HSIs to the corresponding new HSIs is identified and addressed
- No new problems are created due to the new HSIs or performance of tasks using the remaining old HSIs and new HSIs
- Any unexpected negative effects on crew coordination, interaction and teamwork are identified and addressed
- Lessons learned from this phase are reflected as appropriate in the plans for the next phase.

Section 3.9 provides guidance on monitoring of changes after they have been placed in service.

2.3.5 Conceptual Design of HSI Changes

The migration plan should identify conceptually the HSI changes that will be made at each step. These conceptual designs should cover the same areas that were addressed when the endpoint concepts were developed (see Section 2.2):

- Concept of Operations – the changes will show how the Concept of Operations will evolve from the way the plant is presently operated and the crew organized, through each successive change until the new endpoint Concept of Operations is achieved
- HSI Design Concepts – this describes the changes that will be made to the physical and functional characteristics of the HSI
- Failure Management Concepts – methods for handling situations in which there are failures of the I&C or HSI systems should be identified for each step in the migration path.

The guidance given here does not prescribe how the migration plan and interim HSI configurations should be documented. The worksheets presented in Section 2.2.8 for endpoint definition can be used also as a tool for developing and documenting the migration plan and the intermediate HSI concepts, by filling in the appropriate information for each step in the migration (add intermediate columns to the worksheets as needed). However, each plant should determine the appropriate form of documentation to fit its particular needs and practices. What is important is having a well thought-out plan, communicating it to the relevant stakeholders and reviewers to ensure it meets the plant's needs, and providing sufficient documentation to allow future modification teams to understand the plan, its implications for each set of modifications, and its bases – why the particular changes were chosen for each step.

Use the guidance given in Section 3 for HFE design and analysis activities that can be applied as appropriate in developing intermediate HSI configurations. In particular, Section 3.7 provides guidance on HSI design activities that can be applied when developing the conceptual designs.

Again, the migration plan is likely to change. Iterations in design, problems with delivery or installation, changes in management goals, budgets and priorities, and lessons learned in the early phases all can lead to the need for changes in the plan. Flexibility and contingency planning are important. This is discussed further in the guidance below on minimizing project risk.

2.3.6 Evaluating Costs and Minimizing Project Risk

2.3.6.1 Costs and Constraints Affecting the Migration Plan

Table 2-12 lists a number of cost drivers and constraints that should be considered when developing the HSI migration plan.

2.3.6.2 Minimizing Project Risk

The cost drivers and constraints listed in the table above also represent areas of potential project risk – that is, risk that the project is stopped or canceled, is delayed in schedule, extends the outage in order to complete installation or exceeds the budgeted costs. Contingency plans play an important role in minimizing project risk. Contingency plans might be considered for situations in which some or all of the new interface cannot be implemented in the planned timeframe – for example, if the vendor discovers that the customization required will take longer than originally expected, or early familiarization and training show problem areas that will take further development, changes to the interface, or more extensive training evolutions. The plan may define contingencies for handling delays, or how and when the modification could fall back to the existing HSI or use another solution if required.

Table 2-12
Major Cost Drivers and Constraints

Cost Drivers and Constraints Affecting the Migration Plan	Discussion
Physical Constraints	
Interim space constraints	If the control room is small and the boards already crowded, new HSI equipment can be added only when existing equipment is removed or consolidated. This can be a challenge in the early stages of the modernization until significant consolidation can be done to create space.
Time and Resources Available	
Outage constraints	Outage schedule, length of upcoming outages, other activities that will be ongoing during the outages, etc.
Non-outage work constraints	Restrictions on how much can be done at power as opposed to in an outage
Budget constraints	Budget constraints obviously affect how much can be accomplished at each step.
Availability of personnel	Availability of qualified personnel to design, develop, evaluate and implement each set of changes, including engineering, operations and maintenance. Costs of any outside support personnel that will be needed should be considered.
Project team turnover	Turnover of personnel on the project team over time should be considered. Appropriate plans, guidelines, and documentation should be developed so that the ability to complete the later phases of the migration does not depend entirely on the same personnel being available to the team. Management attention to this issue early in the program may help ensure longer-term availability of key people and minimize turnover. Any planned or probable changes in plant organization also should be considered.
Control Room Support Systems	
Lighting	The endpoint design may call for changes to the control room lighting to properly support the endpoint design concept. Plans for intermediate lighting system upgrades (if any) need to be considered in the migration plan – lighting changes and HSI modifications may need to be coordinated to support interim configurations. Capability to adjust lighting levels in specific areas should be considered – building this flexibility into the system early may save having to make incremental modifications in later phases.
HVAC	Similar to lighting – plans and schedules for HVAC changes need to be considered.

Table 2-12
Major Cost Drivers and Constraints (Continued)

Cost Drivers and Constraints Affecting the Migration Plan	Discussion
I&C/HSI System-Related Factors	
I&C architecture and system capabilities	Migration/phasing of the I&C systems and I&C architecture changes, and capability to support the desired HSI at each step in the control room migration need to be considered.
Interfacing to existing equipment	If early modifications upgrade only the I&C "behind the boards," leaving the existing HSI largely the same, the costs associated with required interfaces and temporary input/output (I/O) equipment, which later will be removed, need to be considered.
Interfaces to support parallel HSIs	If the old HSI is to be left in place for a period of time in parallel with the new one (e.g., to allow operators to become familiar with the new interface while having the old one available), temporary interfaces or I/O equipment or other interim configurations may be required.
Adapting or modifying available systems	Consider the potential cost of adapting or modifying the vendors' standard, proven solutions (including software, libraries, etc.) to meet the plant's specific needs for interim configurations.
Database development	Modern I&C systems use databases to store information on each parameter that is monitored, each alarm that can be generated, information that is derived or composed from other data points, control and alarm setpoints, and other information needed to support I&C and HSI functions. The cost to develop/modify and verify the database for each step needs to be considered. Experience has shown that this can be very labor intensive, particularly if there are multiple databases.
Procedures and Training	
Evaluating new HSIs and gaining acceptance	Consider the costs associated with efforts to familiarize the operators and other users with the changes, the new technologies, new ways of accomplishing tasks, and new skills and strategies needed to operate effectively at each step. This may include costs of procuring and configuring prototypes of the new HSI equipment and systems, building mockups, vendor-supplied training, etc.

Table 2-12
Major Cost Drivers and Constraints (Continued)

Cost Drivers and Constraints Affecting the Migration Plan	Discussion
Procedures and Training	
New or modified procedures	The cost of modifying or developing new procedures, and adapting or "porting" existing procedures to a computer-based procedure format (if applicable), need to be considered.
Impact on training	Consider impact on training and the ability to conduct the required training in the planned timeframe. This includes consideration of the need and cost for a second simulator (possibly a part-task simulator) to allow training on the new system while keeping operators current on the existing MCR until the change is made. A desktop or PC-based simulation of the interface might be used if available for the system, instead of or in addition to a part-task simulator. In addition, costs to upgrade the full-scope training simulator at each step need to be considered.
Other Factors	
Impact on drawings, etc.	Impact on drawings and other documentation, and the resources needed to make the necessary changes need to be considered.
Maintaining the licensing basis including diversity and defense-in-depth	Maintaining compliance with the plant's licensing basis, including the approach to diversity and defense-in-depth, and maintaining controls and displays that may be identified as backups for postulated failures of the protection systems. Early evaluation of this issue can avoid a situation in which controls that prove to be needed as backups in later phases were removed as part of modifications made in an earlier phase.
Licensing, regulatory review and acceptance	Costs associated with any required regulatory reviews, licensing submittals, etc. need to be considered for each step. This should be considered when developing the licensing strategy for the overall migration and endpoint design.

Requirements of the plant's purchasing or procurement process need to be considered when developing the migration plan. Design, development, installation and startup of a new human-system interface typically involve iteration. Changes will be identified as issues become apparent during the design and development of the interface, and as users begin to work with prototype and actual equipment. Project and purchasing milestones need to be defined in a way that allows for these types of changes. Milestone and deliverable requirements on the supplier that are unnecessarily rigid can inhibit making changes that will facilitate user acceptance and potentially improve human performance. On the other hand, there must be control over the project schedule, deliverables, and supplier performance. This needs to be worked out when developing the HSI modification plans and specifications, and should include involvement by those responsible for purchasing as well as project management, engineering, operations, maintenance, and training.

The plan needs to provide appropriate project controls but recognize the need for iterative design and refinement to arrive at an effective interface reflecting operator input and acceptance.

If the planned changes to the HSI are extensive, the effort, cost and scheduling difficulty associated with operator training and making changes to the plant simulator should not be underestimated. Maintaining operator qualification on the current control room, and conducting training on the new modified control room sufficiently early to ensure proficiency and qualification, can represent a significant scheduling challenge. This is particularly true for multi-unit plants where the simulator supports more than one unit. Considering these issues early in the development of the HSI migration plans will help minimize project risk. Section 6.3 provides guidance in this area.

It is important to gain a full understanding of the capabilities and limitations of the I&C and HSI equipment and systems that will be used. Experience has shown that it is difficult to determine this fully in the early stages of the project, and there can be surprises later that represent risks to the project. Consider the following items as ways to address this, depending on the extent and criticality of the planned modifications, and the particular vendor and systems being considered:

- Obtain a prototype of the planned HSI system or equipment (e.g., a single DCS workstation and associated development tools) early in the project. Use it to gain a better understanding of the system, its capabilities and limitations, and difficulties or hard spots that may be encountered in configuring the system for the plant's particular needs.
- Use the prototype and/or a suitable part-task simulator to familiarize operators and other users with the equipment, its configuration and operation, and how it will be used to perform actual tasks at the plant. Procedure walk-throughs or limited task analyses might be performed using the prototype in order to verify that the desired capabilities can be realized. These techniques also can be used to obtain input and feedback from the operators during the design phase. See Section 6.3 for further discussion on use of simulation to support both training and design.
- Build a full-size mockup of the modified control room, panels, workstations, desks, etc. The prototype equipment can be integrated into this mockup. A full-size mockup can be very effective in supporting evaluation of overall control room arrangement, line-of-sight issues, personnel locations and access during various evolutions, laydown space, crew coordination, etc. It also may prove useful later to support training on the new HSI.
- Communicate closely with the vendor or supplier. Use the actual equipment and the prototype evaluations as a tool to improve communications, helping the vendor to better understand the plant's specific needs, and the plant to better understand the system's "out-of-the-box" capabilities and limitations.

Continued evolution of commercial I&C and HSI products needs to be considered when developing the migration plans. For example, a prototype that is obtained early in the project may be obsolete before the first changes are installed in the plant. Plans should be developed to evaluate updates and revisions to the commercial products and determine whether and how to incorporate these into the modifications.

Responsibilities and plans for developing the databases required by the I&C system to support the needed HSI functions should be addressed early in the development of the migration plan. This was listed as one of the cost drivers in the table above, but it is worthy of some additional emphasis. The effort to define and develop this database should not be under-estimated. Also, capabilities that are planned for a future phase may need to be built into the database in the beginning (e.g., extra fields to allow for operator-defined or mode-dependent setpoints). If this is not considered up front, there is a risk that significantly greater effort will be needed later to modify the database.

2.3.7 Licensing Evaluations

Section 2.1.12 identified a number of licensing considerations related to HSI modernization. These should be considered when developing the HSI migration plan.

As discussed in Section 2.1.12, an approach that helps limit licensing risk is to make changes first to non-safety systems, gain experience with the process and new digital equipment and HSIs, then make changes to the safety-related systems. Note that the I&C equipment and some aspects of the HSI for non-safety systems may be quite different from that used for safety-related systems, so some of the experience gained with the equipment itself may not transfer readily to the safety systems. However, experience with the design, evaluation, implementation and operation of newer digital systems in non-safety applications can be very helpful in reducing risk associated with safety-related upgrades that are accomplished later. Consider this when developing the migration strategy.

Section 2.5 provides more information on planning for licensing and regulatory activities, and Section 5 addresses licensing in general as it relates to control room and HSI modernization.

2.4 Human Factors Program Planning

2.4.1 HFE Program Elements

2.4.1.1 General HFE Program Goals and Scope

2.4.1.2 HFE Responsibilities

2.4.1.3 HFE Procedures

2.4.1.4 HFE Issues Tracking

2.4.1.5 Style Guide

2.4.2 A Graded Approach to HFE

2.4.2.1 Introduction

2.4.2.2 Approach

2.4.2.3 Establishing the Risk Significance of a Modification

2.4.2.4 Adjustment Based on Secondary Factors

2.4.2.5 Establishing the Scope of the HFE Activities Based on Assigned Grade and Applicability

2.4.3 Sources of Additional Information

2.4.4 Appendix – Example of HFE Procedure for Modifications

This section provides guidance on planning and management of HFE in the design of HSIs in support of plant modifications. The guidance applies to a broad range of modifications to HSIs and other changes that affect human performance. Changes at plants will range from the replacement of a few obsolete components with digital devices, to major replacement of entire systems, control boards, or interface types. These changes are likely to be made over a number of years and may eventually result in a much more advanced control room. Some of these changes will have substantial impact on the ways that operators and maintainers interact with plant systems and react to plant changes. Existing HFE programs have proven to be adequate to address relatively modest modifications to HSIs, and should continue to be effective for those kinds of changes. However, with larger, more comprehensive and potentially more risk significant I&C and control room modifications being planned and implemented, many plants will need to adapt their HFE process to deal with the increasingly significant and complex digital I&C systems and HSI available to support plant life extensions.

Section 2.4.1 describes the features of an HFE program that should be in place to support the HFE aspects of more significant upgrades. These HFE program features should be a part of the plant’s engineering design and modification processes to define the way in which HFE activities will be performed to support the development, design, evaluation, and modification of HSIs. The purpose of the HFE program is to identify organizational responsibilities for HFE, to establish a means to define, describe, and specify required activities, and to establish the procedures that govern the performance of those activities.

Section 2.4.2 provides a methodology for grading an individual modification, identifying the HFE design activities appropriate for a given modification, and tailoring the scope of the HFE activities. Throughout its lifetime, a control room will undergo many modifications, some of which will be minor and some of which will be substantial; some changes will affect HSIs for protection systems and some will affect HSIs for non-safety systems. The human factors activities that should be performed for a minor or relatively simple change are considerably different from those required for a complex, substantial change or one that affects highly risk-significant systems or tasks. This section provides an approach for tailoring the scope of HFE activities to the specific features, scope, complexity and importance of the individual modification. Additional guidance on grading each of the individual HFE activities is provided in Section 3.

The HFE program described in this section is not intended to be separate from an organization’s existing modification process. The HFE program should be used to supplement and should be integrated into the plant’s normal design and change processes.

Section 3.1 provides more information on existing HFE programs and provides guidance on HFE planning for individual modifications.

2.4.1 HFE Program Elements

The purpose of having an HFE Program is to ensure that:

- HFE has been integrated into the plant design, evaluation, and change process

- Design products (e.g., new or modified HSIs, procedures, and training) support safe, efficient, and reliable performance of operation, maintenance, test, inspection, and surveillance tasks
- The design process and products reflect human factors principles and satisfy the applicable regulatory requirements regarding HFE

To accomplish these objectives, the plant should have an HFE program implemented by designated personnel. Personnel responsible for developing, establishing, managing, controlling, and implementing the HFE Program should be identified. The HFE Program should include the following elements:

- General HFE Program Goals and Scope
- HFE Responsibilities
- HFE Procedures
- HFE Issues Tracking

These elements are described in the following subsections.

2.4.1.1 General HFE Program Goals and Scope

The goals and objectives of the HFE program should be determined and documented. The remainder of the HFE program should be structured around these goals. Several general HFE design goals that should be included in the HFE program are:

- Personnel tasks can be accomplished within time and performance criteria
- The HSIs, procedures, staffing/qualifications, training and management and organizational support will support a high degree of situation awareness
- The plant design and allocation of functions will support operator vigilance and acceptable workload levels, i.e., to minimize periods of operator underload and overload
- The operator interfaces will minimize operator error and will provide for error detection and recovery capability

Additional features of well-designed HSIs are described in detail in Section 4 and Section 6.

The HFE program goals may be documented along with the other goals for the I&C modernization program and for individual design modifications.

The scope of the HFE program should also be established. This includes the locations and systems subject to the HFE program and the HSIs, procedures, training, and personnel that will be impacted by the changes. Applying the HFE program at an appropriate graded level to any system, equipment, or facility, that will be used by personnel to interface with the plant is strongly recommended.

2.4.1.2 HFE Responsibilities

For the purpose of this document, the plant personnel who have the responsibility for planning and carrying out HFE activities are referred to here as “HFE Personnel. HFE personnel should be responsible for:

- Development of HFE plans and procedures
- Oversight and review of HFE design, development, test, and evaluation activities
- Initiation, recommendation, and provision of solutions through designated channels for problems identified in the implementation of the HFE activities
- Verification of the implementation of recommendations resulting from HFE activities
- Assurance that HFE activities comply with the HFE plans and procedures
- Scheduling of HFE activities and milestones in coordination with other modification activities
- Documenting the HFE activities and results

The organizational and functional relationships, reporting relationships, and lines of communication should be identified and described. In general, HFE personnel should have the authority and organizational placement to ensure that all of the activities in their areas of responsibility are accomplished and to identify problems in the implementation of the design. There should also be the authority for HFE personnel to control further processing, delivery, installation, or use of design products until the satisfactory disposition of a nonconformance, deficiency, or unsatisfactory condition has been resolved.

Additional HFE resources and expertise beyond those present on-staff may be needed to support modifications that have significant human factors impact. Note that major changes to the HFE personnel over the course of a modernization project can waste effort and cause the project(s) to lose focus.

2.4.1.3 HFE Procedures

The plant’s design and change processes should include a screening mechanism to determine when design changes affect HSIs or otherwise impact human performance and thus require the application of HFE activities. Appendix of Section 3.1 provides an example of a checklist that could be used in the modification process to determine the applicability of HFE to the modification. To ensure that good human factors design principles are consistently applied, there should be a formalized HFE procedure or set of procedures. In addition, the HFE standards and design guidelines that the plant will follow should be identified.

Procedures should be in place to control and document the process through which the HFE personnel will carry out their responsibilities. The procedures should address the following:

- Assigning HFE activities based on expertise needed

- Establishing the training requirements for and maintaining the qualification of HFE Personnel
- Making management decisions regarding HFE activities
- Governing the performance of HFE activities
- Review of design products

The HFE procedures should also address the following:

- The methods to be used to verify and document that needed HFE activities have been performed. This might be accomplished, for example, by using a form or forms to document decisions on which activities are needed and that they have been performed satisfactorily
- The inputs to the HFE program from other plant activities (i.e., from non-HFE related activities), and the outputs from the HFE program to other plant activities
- The iterative nature of the HFE design and evaluation process
- The HFE implementation plan and associated milestones. The schedule of activities in the project plan for a design or modification should include a schedule of HFE tasks showing relationships between HFE elements and activities, products, and reviews as they relate to the overall project schedule. Additional guidance on development of an HFE implementation plan is provided in Section 3.1
- The required documentation of HFE activities and results

There are no specific requirements with respect to where this information should be documented, or how the information should be documented, as long as it is documented such that it can be retrieved for verification or used to evaluate future plant modifications. The Appendix in Section 2.4.4 provides an example procedure.

2.4.1.4 HFE Issues Tracking

The design team should keep track of human factors issues that are identified throughout the design process and need to be addressed at a later date (e.g., information obtained from the operating experience review, or any design alternatives that have not been completely evaluated or validated). The purpose of the system is to keep track of and document open issues, the activities to be performed to address those issues and achieve an acceptable design, and the final resolution of each issue. HFE issue tracking procedures should address who has the responsibilities of issue logging, tracking, resolution, and resolution acceptance.

A separate system need not be created to track HFE issues if the plant already has an existing system that can adequately perform the HFE issue tracking function (logging, documenting the required details, ensuring timely resolution, etc.), If a new system is needed, it may be as simple as maintaining an open issue log as part of the modification project administration.

A distinction should be made between the more global HFE issues associated with HFE issues tracking and the individual Human Engineering Discrepancies (HEDs) identified as part of HFE Verification and Validation as described in Section 3.8. The HEDs are usually design discrepancies associated with individual HSI features. Depending on the scope and complexity of the modification, the sheer volume of HEDs and their nature could be overwhelming and inappropriate for tracking within the normal plant tracking systems, and a separate HED tracking system should be implemented as described in Section 3.8.

2.4.1.5 Style Guide

Although it is more of a technical document than an HFE program feature, it is important to recognize that a plant-specific style guide should be an essential element of a plant's management of HFE. It provides detailed specifications or rules that describe the characteristics and functions of a specific plant's HSI, such as the overall control room layout, display screen organization, the way system features and functions are presented to users, establishing coding conventions for HSIs, and navigational features and functions. For details on style guides, see Section 3.7.

2.4.2 A Graded Approach to HFE

2.4.2.1 Introduction

Once a modification has been "screened in" for HFE (see Section 3.1) and the HFE procedure(s) (see Section 2.4.1.3) has been invoked, the scope of HFE activities should be determined. This section describes a graded approach to tailoring the HFE activities for an individual modification. Throughout its lifetime, a control room will undergo many modifications, some of which will be minor and others, which will be substantial; some changes will affect tasks and HSIs for protection systems and others will affect tasks and HSIs for simple non-safety systems. The scope of human factors activities that should be performed for a minor or relatively simple change is likely to be considerably different from what is needed for a substantial or highly complex change, or one that affects risk-significant systems or tasks. The scope of the HFE design activities that should be undertaken for a given modification should be tailored based on the nature of the risk significance and complexity of the change. The graded approach concepts described in this section are consistent with NRC expectations as described in NUREG-1764 and NUREG-0800, Chapter 18. For a more detailed discussion on the licensing and regulatory issues related to HFE, see Section 5.

The primary factors that should influence the determination of risk significance are nuclear safety risk, operational risk, and personnel safety risk.

Even for the most significant modifications, there are additional, secondary risk factors that should be used in the determination of risk significance. These secondary risk factors are complexity and uncertainty. See Section 2.4.2.4 for a discussion on secondary risk factors.

The primary benefit of applying a graded approach to HFE with respect to control room modifications is the elimination of unnecessary work with the assurance that all necessary HSI design activities are still completed. This helps ensure that resources available for the modification are directed towards areas where they provide the greatest value in terms of ensuring plant and personnel safety and economic operation. A graded approach also benefits those reviewing human factors-related work (e.g., the NRC) by helping these reviews to identify and, thus, focus on the most critical activities.

2.4.2.2 Approach

A suggested approach for grading HFE activities for individual modifications is presented in this section. It represents a practical method using documented analysis and engineering judgment; it is intended to ensure value-added HFE activities for a wide range of HSI modifications.

The recommended level of the HFE activities is determined by considering risk to the public, plant personnel, and commercial stability based on the three primary drivers:

- Nuclear safety risk significance
- Operational significance (importance to power production), and risk to investment (major component damage)
- Personnel safety hazard

These primary drivers are used to assign a risk significance (high, moderate, or low) to a modification, which is then used to define three corresponding levels of activity for each of the HFE design and evaluation activities described in detail in the graded approach sections of Sections 3.2 through 3.9.

Even after the overall level of the HFE activities is established, the scope of many of the design and evaluation activities can be further refined based on the specific issues and topics discussed in detail in Sections 3.2 through 3.9. These considerations will help establish and document which HFE activities are applicable and important for the specific modification.

If a plant already has a grading approach defined for the digital I&C aspects of modifications, coordinate the application of grading HFE activities with the existing grading system, as appropriate.

2.4.2.3 Establishing the Risk Significance of a Modification

This activity assesses the nuclear safety risk significance, commercial risk (risk of loss of power production or major equipment damage), and personnel hazard associated with the modification as drivers to determine an appropriate level of HFE activities. One of three levels is assigned based on each of these three drivers. These levels are then used to establish an appropriate scope for each of HFE activities based on the guidance given in Section 3 for each activity. The levels are defined as follows:

- Level 1 – High Risk
- Level 2 – Moderate Risk
- Level 3 – Low Risk

2.4.2.3.1 Nuclear Safety Risk Assessment

Plant modifications can result in various degrees of impact on the nuclear safety risk. A larger potential impact warrants a greater level of HFE activity. The primary focus for nuclear safety significance for HFE is on the impact of the changes to Human Actions (HA). Assessment of nuclear safety risk can be made using one of the following two approaches: assessment based on a PRA analysis conducted specifically to assess the effect of the modification or assessment based on the risk significance of affected systems derived from the existing PRA.

Determine Nuclear Risk Significance Based on Modification-Specific PRA

For a given plant modification or series of modifications, the nuclear safety risk should be determined using the plant PRA and the risk screening methods described in the subsequent paragraphs of this section. This has the benefit of using the already developed plant PRA model and of involving the risk analysts in supporting the grading of the modification activities. The output of this step will be a placement of the modification into one of three risk importance levels, as shown in Table 2-13.

Table 2-13
Grading Modifications Based on Nuclear Safety Risk Significance

Benchmark for the Systems Involved in the Modification	Nuclear Safety Risk Significance
Red	High
Yellow or White	Moderate
Green	Low

The risk screening methodology of NUREG-1764, “Guidance for the Review of Changes to Human Actions,” was developed to determine the appropriate level of regulatory review for HFE activities. It involves four steps. This method first estimates the change in risk associated with a modifications based on changes in Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). The second step of the method is an especially useful input for determining the scope of HFE to be applied. The risk importance of the human actions impacted by the modification is determined using risk-importance measures such as Risk Achievement Worth. This step proposes quantitative criteria that can be used for assigning high, moderate, or low risk significance. The third step is qualitative and provides a means to make necessary adjustments in the quantitatively determined risk levels. The fourth step integrates the first three steps to determine the appropriate level of HFE review.

If possible, the modification should be evaluated for its impact on human actions as they are already used in the PRA model. Early in the modification process, if specific human actions and tasks have not yet been defined and entered into the PRA model, it may be expeditious (and conservative) to use these concepts to evaluate the failure risk of the entire modification (equipment and human actions), similar to the screening process described in NUREG-0800, Chapter 18. That is, it is proposed that the four steps in the NUREG-1764 process be used to assign a high, moderate or lower risk level to the modification. Later in Section 3.4, individual human tasks will be defined and evaluated separately. See Section 5.2.6 for more information on NUREG-1764 and the use of PRA in HFE activities.

Determination of Nuclear Risk Significance Based on the Risk Significance of Affected Systems

The risk significance of the plant modification can be bounded without use of a modification-specific PRA analysis by considering the risk significance of the affected plant systems. The risk significance for these systems in a nuclear facility can be obtained from the plant's updated Probabilistic Risk Assessment (PRA). Systems can be divided into three risk levels (high, medium, or low).

This information, represented in summary form as a color code for each system, can also be extracted from the NRC plant-specific, risk-informed inspection notebooks and Table 1 of the related benchmarking reports. A similar qualitative approach is used for risk-screening changes to human actions in NUREG-1764, section 2.4, "Screening Process for Non-risk-informed Change Requests."

Once the risk importance information on a system level is identified, the classification grade for the modification can be determined as summarized in Table 2-13. Specifically, systems that benchmark as Red should be considered to have high risk significance. Those that benchmark as Yellow or White should be considered as having moderate risk significance. Green benchmarks would be considered to have lower risk significance. If multiple systems are affected, a conservative approach is to use the system with the highest risk significance.

One may also treat a large modification with different levels of HFE activity for different systems depending on the risk significance of each system. Further refinement may be appropriate, e.g., if the affected system may be very risk significant but personnel tasks involved are not. Engineering judgment may be used to assist in this assessment. In this manner, a preliminary high risk level based on the system risk importance may be reduced to a moderate or low risk importance based on the actual tasks or operator activities being affected by the modification. It is important to document the basis for such engineering judgments as they determine the scope of the HFE activities. Use of grading on a task level is discussed further in Section 3.4.5.

The output of this section is the determination of the modification's risk (high, moderate, or low) based on nuclear risk significance, determined either quantitatively or qualitatively.

2.4.2.3.2 Risk to Power Production and Investment

Commercial risk associated with the modification should also influence the level of recommended HFE activities. Human error may have the potential for causing a plant trip, a reduction in efficiency, a reduction in power production, a reduction in plant stability, or damage to major plant equipment (such as the main generator). If the potential for a plant trip exists, then an assignment of a high commercial risk is recommended. If the worst that can result from human errors is a reduction in plant performance or equivalent loss caused by damage to major equipment, then a moderate commercial risk determination is recommended. A plant may want to establish financial limits (e.g., $100K as the boundary between moderate and low) for the investment protection related to possible equipment damage and then use these to assign levels of HFE activities, as well.

As discussed above for the nuclear safety risk assessment, if it is not practical to assess the potential for the modification to result in a plant trip or a reduction in plant performance or equivalent equipment damage, this assessment can be bounded at the system level. That is, assess whether the system being modified can result in a plant trip, a reduction in plant performance, or major equipment damage and assign a high or moderate risk significance grade, respectively. A detailed analysis of tasks using the guidance in Section 3.4 will result in a clearer understanding of the tasks affected by the modification.

All other commercial risk consequences should be assigned a low commercial risk significance.

As with safety risk assessment, document the basis for assigning a specific risk significance level.

Risk of Hazard to Plant Personnel

The third risk factor is the potential for personnel hazard. If errors in using the modified system can result in death, serious injury or significant radiation exposure (above plant limits to workers), a high risk significance determination is recommended. If such errors can result in no more than mild injury or radiation exposures within plant allowed limits, then a moderate risk determination is recommended.

For all other less severe potential personnel consequences, a low risk determination is recommended.

Combined Risk Assessment

Table 2-14 presents the combined levels of nuclear safety risk significance, commercial risk, and risk to personnel safety involved in the modification.

When a combination of factors (nuclear safety risk, commercial risk and personnel risk) is considered, a conservative assessment of the level of HFE activity can be obtained using the highest grading level entered on the table.

Table 2-14
Grading Modifications Based on Nuclear Safety Risk Significance, Risk to Power Production and Personnel Safety

Nuclear Safety Risk Significance	Commercial Risk Significance	Personnel Safety Risk	Level of HFE Activities Recommended
High	Plant Trip	Death, serious injury, or significant exposure	Level 1
Moderate	Reduction in plant performance or equivalent major equipment damage	Risk of mild injury or exposure	Level 2
Low	Other	No Personnel Hazard	Level 3

For example, a modification with a moderate safety risk importance, with a potential plant trip, but no personnel hazard would be assigned a Level 1 for HFE activity because the potential for plant trip necessitates the highest level of activity for the modification.

2.4.2.4 Adjustment Based on Secondary Factors

Once the initial grade is assigned based on the combined risk assessment, the secondary risk factors listed below should be considered and the grade for a modification should be changed from Level 2 to Level 1 or from Level 3 to Level 2, as appropriate. The secondary factors should not be used to change the grade of a modification from a Level 1 to a Level 2 or from a Level 2 to a Level 3. The secondary risk factors are:

- Complexity
  - of the modification or portion of the modification
  - of the technology
  - of the technical features of the system
  - of the change to the concept of operations or operating procedures
- Uncertainty
  - Similarity between new and old HSIs
  - Level of industry experience with the vendor equipment in similar applications
  - Level of experience of plant personnel with the replacement I&C/HSI system
  - Completeness of existing HFE documentation for the system being modified
  - Knowledge gap between vendor personnel and utility personnel

The secondary factors have also been considered in the methodology subsections of the HFE design and evaluation elements in Section 3 to tailor the scope of HFE activities to the nature of the modification.

2.4.2.5 Establishing the Scope of the HFE Activities Based on Assigned Grade and Applicability

A modification that is assigned a high risk significance and thus a Level 1 for HFE, will require consideration of the full scope of HFE activities as described in Section 3 of this guideline. Modifications with an assigned moderate or low risk significance, and thus a Level 2 or Level 3 for HFE activities, will require increasingly less detailed HFE activities as described in the Graded Approach subsections in Section 3. Additional information regarding typical HFE activities as part of the normal plant modification process is provided in Section 3.1.

2.4.3 Sources of Additional Information

NUREG-0711, Human Factors Engineering Program Review Model, Revision 1.

NUREG 0800, Chapter 13, “Conduct of Operations,” Revision 1/2 (varies) Draft.

NUREG 0800, Chapter 18, “Human Factors Engineering,” Revision 1 Draft.

Interim Human Factors Guidance for Hybrid Control Rooms and Digital I&C Systems, EPRI July 2003. 1003696.

IEC 964, Design for Control Rooms of Nuclear Power Plants, 1989.

ISO 11064, Ergonomic Design of Control Centers.

NUREG-0700, Human-System Interface Design 2.

Code of Federal Regulations, Title 10, Chapter I, Section 50.54, “Conditions of License.”

2.4.4 Appendix – Example of HFE Procedure for Modifications

This appendix provides a generic example of a plant design procedure for implementing Human Factors Engineering as part of the design and modification process at a plant. It does not represent a procedure from any specific plant.

The intent of this example is to provide a starting point for plants to use to develop a procedure for HFE. Many of the terms, names of organizations, responsibility assignments, etc., are for example only and will vary for individual plants. Each plant’s procedure should use its own terminology and be in accordance with its organizational structure.

Text in italics indicates areas in the procedure where plants need to insert their terminology or specific features or where an arbitrary choice was made by the authors. For example, in Section 3, Responsibility, "Modification Engineering" and "Modification Engineering/I&C Engineering" have been used in the example procedure to illustrate the hierarchical nature of responsibility, where a plant department (in this case "Modification Engineering") and a group within that department ("I&C Engineering") have different levels of responsibility.

Example Human Factors Engineering Procedure

1. Purpose

The purpose of this document is to apply Human Factors Engineering (HFE) principles to the design and implementation of modifications, minor modifications, and plant changes that affect Human System Interfaces (HSIs) and the other human factors aspects of the plant, including procedures, training, tasks and task design, task allocation, and automation. The purpose of the application HFE is to help ensure that the HFE aspects of the plant are well designed and to improve overall plant operations, reliability, and safety. The application of HFE is also to ensure that modifications that have the potential to adversely affect user performance are designed so that the design minimizes and mitigates any negative affects and unintended consequences of the modification. That is, to realize the benefits on digital I&C and HSI technology.

2. Applicability

This procedure is applicable to the Main Control Room (MCR), the Remote Shutdown Room (RSR), the Remote Shutdown Panel (RSP), and the plant locations containing the transfer devices associated with the transfer of control from the MCR to the RSR. This procedure should also be applied to changes that affect plant personnel interfaces in other locations.

The application of accepted HFE principles to all areas where personnel interact with the plant is good engineering practice. Engineering personnel should confer with the Operations and Maintenance Departments to identify and document the applicability of HFE to all modification projects.

It is the intent of this procedure to appropriately apply and document the HFE process where necessary, while avoiding unnecessary work and documentation. The use of a graded approach to ensure that the scope of the HFE design activities that are undertaken for a given modification is tailored based on the nature of the nuclear risk significance, risk to personnel safety, and importance to power production and equipment protection of the change.

This document provides the description of the organization responsible for HFE, the qualifications for HFE reviewers, the steps in the HFE review process, and HFE documentation requirements.

The Purpose and Applicability sections are intended only to serve as an example. Individual utilities will define these issues in their own procedure.

3. General HFE Principles

The potential interactions between the system and the operators, system engineers, and technicians should be considered in all aspects of plant changes that affect human-system interfaces or human actions.

Human factors should be integrated into the plant change process at various levels, from project management to end user. It is imperative that the end users of the system participate in the design process, as they can provide unique insights into the actual use of the system.

Where appropriate to the complexity of the change to the operator interface, the use of a multi-disciplinary design team is recommended. As a minimum, a modification design team should include personnel familiar with each aspect of the system(s) being modified.

Each modification should be carefully evaluated to ensure that it does not have negative implications on other plant HSIs, whether existing or planned. The design basis should be fully documented.

4. Responsibility

This section summarizes the responsibilities of plant personnel for HFE by providing an overview of the responsibility, authority, placement within the organization and composition of the HFE.

For the purpose of this procedure, *HFE Personnel* are the plant personnel who have responsibility for HFE. The term does not include the managers of design engineering, modification engineering, systems engineering, operations, maintenance, procedures, training, etc. that are responsible for the personnel and their activities that perform HFE activities or use the products of HFE. HFE Personnel are the engineers, designers, HFE experts, control room team members (Ops, Training, Maintenance, etc.), and others that perform, support, review, approve, or use the products of HFE activities. HFE Personnel are responsible for planning, analysis, design, evaluation, review, and acceptance of modifications to HSIs and the other Human Factors aspects of the plant, which includes automation, procedures, training, tasks and task design, task allocation, etc.

The following personnel and organizations have specific responsibilities for the HFE aspects of design changes as indicated:

Modification Engineering is responsible for reviewing modifications and any other plant changes that affect operator interfaces, for providing feedback to various design teams, and for integrating and coordinating resources.

Modification Engineering/I&C Engineering is responsible for ensuring the application of Human Factors Engineering in the design modification process.

The *Supervisor, Modification Engineering* is responsible for ensuring that are adequate numbers of suitable plant personnel qualified per Section 3 of this procedure to perform HFE activities as required and to verify the qualifications of contractor personnel, if necessary. The supervisor is responsible for identifying personnel and ensuring that they obtain the necessary training and experience to be designated to perform HFE activities.

The *Lead Modification Engineer (LME)* is responsible for a change package or new design that requires the application of HFE. These changes can be those implemented through the modification process or other plant changes as initiated by: (*indicate plant-specific standards, manuals and procedures that regulate modification and plant change processes*). The LME or qualified designee is also responsible for performing:

- HFE portion of the design modification documentation package;
- Operational Experience Review (see Section 7.1 of this procedure);
- Functional Requirements Analysis and Function Allocation (see Section 7.2 of this procedure);
- Task Analysis, alternately, task analysis can be assigned to Operations Personnel or HFE personnel (see below), with the assistance of HFE experts, as needed (see Section 7.3 of this procedure);
- Human Error Analysis (see Section 7.4 of this procedure)

The LME can perform the functions of HFE Specialist (see below) upon having met the requirements as outlined in the HFE Specialist Qualification Card *(These qualification requirements will normally be defined uniquely at each individual plant).* If the LME is not qualified to perform any of these functions, the LME is responsible for allocating responsibility to a qualified party.

The qualified *HFE Specialist* is responsible for working with the LME to plan HFE activities, document the planned HFE activities in the Conceptual Design Document (CDD), ensure completion of the HFE activities, verify the adequacy of the design, and approve the final HFE documentation using the process defined in this procedure. This includes supporting the LME to keep the HFE work scope current in the project plan, updating the HF style guide, and revising the concept of operations document, as necessary. The Modification Engineering Group is the owner of this job function.

A qualified *HFE Verifier* is responsible for independent review when required. *(Reference Section 2.4.2 and Section 3.8 of EPRI 1008122, Human Factors Guidance for Control Room and Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance.)* A qualified HFE Verifier should have the same qualification level as the HFE Specialist but be independent from the HFE Specialist.

The *Control Room Design Review (CRDR) Team* (or some similar organization that has been defined as having the integrated responsibility for managing and controlling the plant HSI modernization strategy and for achieving the modernization *endpoint* vision) is responsible for performing high-level review and direction-setting functions, such as review and approval of design options. The CRDR Team is also responsible for establishing the schedule for the reviews and determining the applicability of the HFE Process steps. The LMEs for major digital modifications should be included in the CRDR Team. Other members of the CRDR Team should consist of “stakeholders” (i.e., representatives of departments that are involved in a particular modification), including representatives of Modification or Systems Engineering, Operations, Maintenance and Training Personnel.

5. Qualification

A qualified HFE Specialist or Verifier should have a level of engineering or design experience involving the application or review of HFE requirements or resolution of HFE problems appropriate for the scope of reviews performed, and should have completed formal training in the HFE process and guidance. The Supervisor of Modification Engineering will identify those personnel who meet the qualification requirements and will maintain a list of qualified personnel. Qualification requirements are listed in *a plant specific definition of the requirements that need to be met to perform the functions of HFE Specialist or HFE Verifier. (Reference Section 2.4.1 of EPRI 1008122, Human Factors Guidance for Control Room and Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance.)*

6. HFE Process for Plant Changes and Modifications

Plant changes and modifications to existing designs vary greatly as to their effect on the user interfaces and/or user tasks. *(Reference Section 3.1 of EPRI 1008122, Human Factors Guidance for Control Room and Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance.)*

6.1 Entry Conditions

HFE activities are required for plant changes initiated using appropriate Engineering Procedures *(indicate plant-specific standards/manuals/procedures that control the plant change process)*, or for additional plant changes identified through answering the questions of the *Modification Checklist (Reference Section 3.1 of EPRI 1008122, Human Factors Guidance for Control Room and Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance.)*

6.2 Reserving Control Board Space

Modification Engineering or Systems Engineering shall reserve any required control board space *(indicate plant-specific standards/ manuals/ procedures that regulate reservation control board space)*. The intent is to show reserved control board spaces or upcoming HSI configurations clearly with associated notes that provide traceability to the expected plant change package. As an alternative, any plant change package that “creates” open panel space or “spares” any HSI interfaces (minor modification or modification) can annotate the associated configuration documents where there is an intent to reserve that space or interface for a future plant change.

6.3 HFE Activities

Each of the HFE analysis, design, and V&V activities defined and described in Section 7 through Section 11 of this procedure should be considered for applicability for all modifications that have screened-in using the checklist in Section 6.1. The applicability of the HFE activity depends on the nature of the modification and the scope and detail required for each activity depends on the risk significance of the modification and the affected human tasks according to the grade level assigned. *(Reference Section 2.4.2 of EPRI 1008122, Human Factors Guidance for Control Room and Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance.)*

Sections 7 though 11 of this procedure provide guidance and requirements for the application of each HFE activity. *(Reference Section 3.2 through Section 3.9 of EPRI 1008122, Human Factors Guidance for Control Room and Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance.)*

Where a plant change affecting HSIs or the Human Factors portions of the plant is being made outside the modification process, appropriate HFE activities shall also be performed and documented; list any additional documentation requirements and indicate the source of the requirement.

Section 10 of this procedure defines the necessary documentation that should be included in the HFE portion of the design modification documentation package.

HFE requirements and design criteria derived from the plant styles guide, the HFE analysis, or other approved sources hall be defined, and the plant change shall be evaluated for conformance to those criteria. It shall contain adequate documentation to describe what was done and to confirm that the final design is acceptable. The objective of the process is to confirm the HFE adequacy of the design prior to approval of the change package. Any HFE deviations discovered during development of the design change must be resolved or justified, and the acceptability must be documented, prior to issue of the change package.

For the following sections, use the guidance provided in Sections 3.2 through 3.9 of EPRI 1008122, Human Factors Guidance for Control Room and Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance to develop the procedural requirements.

7. Design Analyses

7.1 Operating Experience Review (Section 3.2)

7.2 Function Analysis and Allocation (Section 3.3)

7.3 Task Analysis (Section 3.4)

7.4 Human Error Analysis (Section 3.6)

8. Detailed Design Processes (Sections 3.5 and 3.7)

9. Verification and Validation (Section 3.8)

10. Documentation

11. In-Service Monitoring (Section 3.9)

12. References

EPRI 1008122, Human Factors Guidance for Control Room and Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance.

2.5 Planning for Regulatory and Licensing Activities

2.5.1 Frequently Asked Questions

2.5.2 Planning for Licensing Activities

2.5.3 Sources of Additional Information

Up-front planning can reduce the cost of activities related to regulatory compliance and can minimize licensing risk. Section 2.1.12 introduced several considerations related to licensing that the project management team should be aware of at the planning stage. This section provides further guidance on planning for licensing activities specifically related to the HFE aspects of I&C, control room and HSI modernization.

At the planning stage it is important to have a good overview of the potential licensing impacts of the changes that will be made over the course of the modernization program, and the possible interactions with NRC on human factors and human performance issues related to the modernization. Section 2.5.1 below provides an overview by addressing a set of frequently asked questions related to regulatory and licensing activities. Following that, Section 2.5.2 discusses actions that can be taken at the planning stage to help minimize the overall cost and risk associated with those activities.

Section 5 contains more detailed guidance on licensing that can be used throughout the upgrade process.

2.5.1 Frequently Asked Questions

The following is a set of questions that are often asked by utility personnel related to licensing and regulatory compliance. Brief answers are given along with references to more detailed guidance. These questions and answers can be used to gain a quick overview of licensing-related issues. They also serve as an introduction to the guidance provided in Section 5.

The questions below and the guidance in Section 5 address both regulatory requirements and NRC expectations. Regulatory requirements are contained in the Code of Federal Regulations (CFR). NRC expectations can be inferred from the review criteria used by NRC reviewers (NUREG-0800) and other guidelines published by the NRC (e.g., regulatory guides).

1. *Is there a special licensing process or procedure that applies when making changes to the plant that may impact human performance?*

No. Changes that impact human performance, such as changes to the level of plant automation, changes to personnel tasks, and changes to HSIs are like any other plant modification – they are governed by 10 CFR 50.59. The 50.59 regulation allows licensees to determine whether a change requires a license amendment and thus needs prior NRC review and approval, or the change can be implemented within the current licensing basis (no amendment and no prior review required).

2. What are the primary regulatory requirements and guidelines that are applicable to the *human-system interface* and *human factors engineering*?

The only regulatory requirements (i.e., regulations that are law) that directly address the HSI are the General Design Criteria (GDCs) in 10 CFR 50 Appendix A, and the post-TMI requirements in 10 CFR 50.34(f). GDC 13 states the basic requirement for instrumentation and controls, and GDC 19 states the requirement for a control room and an alternate shutdown capability outside the control room. 10 CFR 50 Appendix R adds additional requirements related to alternate or remote shutdown. 10 CFR 50.34(f) added the requirement that the control room design reflect "state-of-the-art" human factors principles, and it required features such as safety parameter displays, post-accident monitoring, and bypassed and inoperable status of safety systems based on lessons learned from the TMI-2 accident. All of these requirements are stated at a relatively high level. However, there are a number of more specific guidelines and NRC review criteria that plants should be aware of, as they indicate what the NRC's expectations are regarding human factors engineering and changes affecting the HSIs and human performance. Regulatory requirements and expectations are described in more detail in Section 5.1. It is recommended that the information in that section be reviewed as part of the planning effort.

3. *What about my plant's Detailed Control Room Design Review (DCRDR) performed after TMI? Will I need to revisit that as part of licensing the modifications?*

DCRDRs were performed after the TMI-2 accident to identify and correct human factors deficiencies in the control rooms at that time. They were closed out after that effort was completed, and there is no requirement to keep DCRDRs themselves up to date when making HSI changes. In part, this is because NRC expected utilities to incorporate HFE into the plant modification process so that changes are made in a way that maintains or improves the HFE basis for the control room established at the time of the DCRDR. The DCRDR documentation may provide information useful to the project team when making changes to modernize the control room, but it need not be "re-opened" as part of licensing. Plants are expected to follow a modification program that includes application of appropriate HFE principles and processes, and to use 10 CFR 50.59 to determine when NRC review of a change is required. Section 2.4 provides guidance on implementing an HFE program. Section 3.1 and Section 3.7 provide more detailed guidance on incorporating HFE into the design process and using plant-specific design criteria and style guides when designing or modifying HSIs. Guidance on the HFE aspects of 10 CFR 50.59 evaluations is given in Section 5.3.

4. *Will control room modernization require re-licensing of the operators?*

No. Operator licensing is governed by 10 CFR 55. Licensees are required to provide adequate training and maintain qualifications of the operators as changes are made to the plant, control room, or other HSIs. This is done now when small changes are made to the control room from time to time. Major control room changes made as part of a modernization program can have a much greater impact on training and qualification exams. However, there is no "re-licensing threshold." The same requirements apply as for any other change that affects operator training and qualification – these must be kept up to date with the control room so that the operators are always satisfactorily trained and qualified on the plant they are operating and the training program retains its accreditation by INPO and approval by NRC.

Providing adequate familiarization and training on the modified control room, while still maintaining qualification on the existing control room prior to the modifications, is a challenge that increases with the scope of the change. If the modifications require changes to operating procedures, the need to maintain and train on separate sets of procedures complicates the training and qualification efforts. The difficulty is increased even further for multi-unit plants that are served by a single, shared simulator.

Purchasing a second full-scope simulator to allow parallel training on both the old and new configurations is an option, but it is an expensive one. On the other hand, there are engineering objectives that also can be served by having a separate simulator, such as evaluation of design options, conducting proof of concept tests, etc. Other methods besides a second full-scope simulator can be used to address both the training challenge and the engineering needs, including use of mockups, prototypes, partial-scope simulators, stand-alone workstations, and other types of computer-based simulations. Modifications needed to the full-scope training simulator and the need for other simulation and training devices should be considered when planning the upgrades. Section 6.3 provides further guidance on training considerations and use of simulation.

5. *How do I evaluate plant modifications impacting personnel performance in the context of 10 CFR 50.59? When will NRC review be required?*

A 10 CFR 50.59 evaluation typically is performed for the overall modification, including both I&C and HFE aspects. Reg. Guide 1.187, NEI 96-07, and TR-102348/NEI 01-01 provide guidance for this evaluation. Additional guidance that supplements these guidelines is given in Section 5.3. It should be expected that significant HSI changes will screen in (i.e., require that a 50.59 evaluation be performed), but the evaluations may conclude that the modifications do not require prior review and approval. Individual changes to the HSI made as part of modernization typically will be designed such that they improve human performance – most will not increase the probability or consequences of accidents or malfunctions, nor create new accidents or malfunctions with different results. It is important that the bases for such judgments be documented as part of the 50.59 evaluation.

The I&C changes themselves may require changes to the Technical Specifications and thus require a license amendment. One of the advantages of digital I&C upgrades is the potential lengthening of surveillance intervals or reduction in the number and type of surveillances, which could affect Tech Specs. In any case, NRC will expect to review major upgrades to the reactor trip system (RTS) or engineered safety features actuation system (ESFAS). See TR-102348 and its endorsement by NRC in RIS 2002-22. Also, some HSI changes could require a license amendment per 50.59 if they present the possibility of new malfunctions (with new results) not previously analyzed – some examples are given in Section 5.3. The failure analysis performed for the modification should include consideration of plausible HSI failures and potential human errors associated with use of the HSI.

It is important to remember that a major control room modification, or the accumulation of many individual changes made as part of a modernization program, can impact the way in which the operators interact with each other and with the plant (the Concept of Operations). It is recommended that such changes be discussed with the NRC early in the project even if a license amendment is not strictly required per 10 CFR 50.59. This can significantly reduce licensing risk and the costs associated with potential NRC interactions. Also, an early look at 10 CFR 50.59

during the planning stage of the modifications is recommended to uncover any significant issues that may arise and deal with them earlier rather than later when they can be more difficult to resolve.

6. *What about I&C changes that do not physically alter the HSI?*

Even when a change to an I&C system does not physically change the HSI, it still may affect operator performance. For example, an I&C change that significantly alters the time response or sensitivity of a control system can affect operator performance when manually operating the system. Changes to plant equipment can do the same thing (e.g., replacing a valve with one that opens significantly faster or slower than the previous one). If such a change significantly affects an operator action credited in the UFSAR, such that the criteria of 10 CFR 50.59 are not satisfied, then the change will require a license amendment and review by the NRC. The NRC staff has developed guidance recently for review of changes affecting credited human actions (NUREG-1764). The guidance uses a risk-informed approach consistent with Reg. Guide 1.174 (regardless of whether the plant's submittal is risk-based or deterministic). This is discussed further in Section 5.3 and Section 5.4.

7. *If a license amendment is required for a modification, what should the license amendment request (LAR) submittal contain related to HFE?*

See Section 5.4 for guidance on information that can be provided or referenced in the submittal to help streamline the NRC review of a license amendment related to changes potentially affecting human performance. The guidance is based on the HFE program review elements that are presented in Chapter 18 of NUREG-0800 and described in more detail in NUREG-0711.

8. *Are there any special licensing requirements or issues that should be addressed related to "hybrid" human-system interfaces?*

There are no special regulatory requirements for hybrid interfaces. A good HFE design process should address hybrid HSI issues along with other human factors considerations in the design. However, hybrid aspects of the control room are likely to be of concern to the NRC in any reviews or audits of the changes, and therefore receive particular scrutiny. It is a good idea to identify and evaluate hybrid HSI issues as part of the design process, and to be prepared to address these with the NRC. Section 2.3.4.1 describes potential hybrid HSI issues that should be considered during design and evaluation of the modifications. Section 5.2.1.2 provides guidance on addressing hybrid issues in the context of licensing.

9. *What about the control room design requirements that the NRC imposed on new plants as part of design certification reviews? If I do significant modernization of my existing control room, will I need to meet those requirements as well?*

No, but you should be prepared to address the NRC concerns that were at the root of those requirements to the extent that they may apply to the proposed changes.

During the reviews for design certification of Advanced Light Water Reactor (ALWR) designs, the NRC expressed concerns regarding the potential effects of common mode failures in the protection and control systems, which were essentially all digital computer-based and used identical software in multiple redundant trains. This led to an expectation, described in SRP Chapter 7, Branch Technical Position (BTP) 19, that a set of controls and displays be provided for manual system-level actuation of critical safety functions. As stated in BTP 19, this was intended to apply only to new plants and not to modernization of existing plants.

NRC reviewed the HFE aspects of the designs as well. For example, they were concerned about the possibility that many or all of the controls provided for the operators might be implemented as "soft controls" and thus could be located on displays that must be retrieved (see Section 4.3 for a more detailed discussion of soft controls). Based on their concerns, and because the ALWR designs were described at a relatively high level without details on any specific implementation, the NRC required that the designers provide in the final designs a "minimum inventory" of fixed-position controls, displays and alarms. This is not a requirement for modernization of existing plants, but the issue is likely to be considered by NRC in their review using NUREG-0800 and NUREG-0711. The guidance given in Section 4.3 should be followed to ensure that appropriate choices are made regarding soft versus hard controls, and retrievable versus spatially dedicated controls.

See Section 5.2.5 for guidance on addressing these issues in licensing. Section 6.4 contains more detailed guidance for addressing them in design.

10. What about the post-TMI requirements and commitments made to old regulatory guides such as 1.47 and 1.97, which were written primarily around older analog instrumentation?

After the TMI-2 accident, a number of requirements were established for instrumentation and display capabilities related to monitoring plant safety status during normal operation and after an accident. This includes post-accident monitoring instrumentation (Reg. Guide 1.97) and safety parameter display systems or SPDS (NUREG-0737 Supplement 1). Other related requirements include monitoring the status of bypassed and inoperable portions of the plant protection system (Reg. Guide 1.47), and manual initiation of protective actions (Reg. Guide 1.62). The need for these monitoring and control capabilities still exists, but with the upgrade to digital instrumentation and modern human-system interfaces, more modern solutions are available that can meet these needs more effectively and were not envisioned when the regulatory guidance was originally developed. Guidance on meeting the intent of the original requirements while employing updated solutions as part of modernization is given in Section 5.2.5, with additional detail provided in Section 6.4.

11. What about backup controls and displays that result from a defense-in-depth & diversity evaluation, and the hybrid HSI issues they present? Will they result in prior review being required per 10 CFR 50.59?

Branch Technical Position (BTP) 19 in Chapter 7 of the SRP describes NRC expectations regarding a defense-in-depth & diversity evaluation to be performed for digital upgrades to the reactor trip and/or engineered safety features actuation systems (RTS/ESFAS). The evaluation is intended to address vulnerability associated with common mode or common cause failures owing to problems with software used in redundant trains. In the past this evaluation typically has led to identification of a handful of manual controls and displays that would be used by the operators to mitigate the design basis events described in the SAR, if such a common mode failure were to occur.

Risk-based approaches also can be used to address potential common cause failures and determine what backups may be needed. A recent industry effort led by EPRI and NEI has developed guidance for applying risk-informed approaches that are alternatives to the deterministic BTP-19 method.

Regardless of the method used it is important to remember that common cause failures due to software are considered a beyond design basis concern and the defense-in-depth and diversity evaluation should be addressed as part of the design process, using best-estimate assumptions (see EPRI TR-102348/NEI 01-01 and EPRI 1002835). The answer to the second part of the question (regarding prior NRC review) is "no" – the need to do the defense-in-depth & diversity evaluation and any backups that are identified for mitigation do not in themselves result in prior NRC review being required. As discussed above, the criteria in 10 CFR 50.59 should be used to determine when a license amendment and NRC review are required.

12. What issues need to be addressed related to the impact on remote shutdown?

Modernization of the main control room does not affect the requirement for an alternate or remote shutdown capability as defined in 10 CFR 50 Appendix A (GDC 19) and Appendix R, "Alternative and Dedicated Shutdown Capability." These require that equipment be provided outside the control room to achieve prompt hot shutdown and maintain a safe condition during hot shutdown with potential capability for subsequent cold shutdown. This requirement still applies. However, there are some design considerations that arise when modernizing the control room. For example:

Impact on the transfer capability needs to be addressed (transfer switches are typically provided to transfer selected controls from the main control room to the alternate shutdown location).

- Impact of consolidation and centralization should be addressed – if some local control panels or stations are to be eliminated by bringing these functions into the main control room, the impact on the remote shutdown procedure should be evaluated. Some local actions are typically relied upon in situations in which the control room must be evacuated.
- The degree of modernization, if any, of the remote shutdown panel or other HSI should be addressed as part of the modernization program. Obsolescence of the remote shutdown panel equipment may be an issue just as it is in the main control room. Also, the human factors issues associated with operators having to use an older style interface at the remote shutdown location after they become familiar with and regularly use a more modern interface in the upgraded control room should be addressed. A major modernization program may offer an opportunity to design and install a remote shutdown station that has an interface similar to the main control room interfaces, and which could provide much greater capability than existing remote shutdown panels.
- The extent to which the remote shutdown station will be relied upon as a backup to any of the main control room HSIs in case of their failure should be determined. The requirement for remote shutdown comes not from concerns about HSI equipment failures, but rather situations involving the need to evacuate the control room should it become uninhabitable. However, the remote shutdown panel does represent an alternate means of performing some monitoring and control functions, and thus could be considered when examining how the operators will deal with failures of HSI capabilities in the main control room. Of course, this

can be impacted by the degree to which the remote shutdown panel is upgraded along with the control room – for example, it could be affected by the same failures that degrade the control room HSIs.

13. What about our site's Emergency Plan –could it be affected?

Possibly. I&C and HSI upgrades may introduce new failure modes that, depending on the system architecture, could cause greater loss of alarms, monitoring or control capability than were considered previously. Plant Emergency Action Level declarations typically include criteria related to loss of control room alarms and loss of monitoring capability (e.g., see NUREG-0654 Appendix 1 for the pertinent NRC guidelines). The potential impact of new I&C and HSI failure modes on Emergency Action Level declarations should be evaluated early so that these can be considered when developing the overall I&C and HSI design concepts.

Additionally, as with the remote shutdown station discussed in question 12, implementation of new computer-based displays in the main control room will make implementation of similar displays in the Technical Support Center (TSC) and Emergency Operations Facility (EOF) relatively easy.

14. Do I need to be concerned about the effect of modernization on my PRA?

Yes. Plant changes can affect risk-important human actions that have been analyzed in the plant's probabilistic risk assessment (PRA). For example, changes in automation or the introduction of new HSI technologies can introduce new types of errors that may not have been considered previously in the PRA, or may affect assumptions made in the previous analyses. Also, new HSIs may change human error probabilities (HEPs) for some operator actions (HEPs will probably be reduced, but not necessarily so). In fact, key risk-important actions should be addressed specifically during the design process to identify opportunities to improve human performance and thereby lower HEPs and plant risk. Guidance is given in Section 5.2.6.

15. Will the NRC accept the use of risk-based approaches to determine what activities and analyses should be performed in demonstrating adequacy of human factors –can we use a graded approach based on risk?

Yes. In fact, the NRC encourages use of risk-based approaches and has provided guidance for their use in licensing submittals – see Reg. Guide 1.174 and NUREG 1764. Section 2.4 provides guidance on implementation of graded approaches and consideration of risk in the HFE design process. Section 5.4 discusses the licensing aspects and information that should be contained in related submittals.

2.5.2 Planning for Licensing Activities

There are a number of actions that can be taken at the planning stage to help minimize the cost and risk associated with licensing and regulatory compliance. Here are some recommendations:

- Involve licensing personnel up-front as part of the planning and then throughout the project. (See Section 2.2 for additional guidance on the makeup of the project team.)

- Ensure that the plant procedure for 10 CFR 50.59 evaluations is up to date, consistent with the guidance in EPRI TR-102348/NEI 01-01 and Reg. Guide 1.187, and includes human factors considerations and effects on human actions credited in the plant's licensing basis. Ensure that plans for failure analysis of the systems to be installed include consideration of HSI failures and potential human errors (see the EPRI/NEI guideline, the information provided in Section 2.2.3.4, and Section 5.2.2 for guidance). Note that consideration of system failure modes should begin at the planning and conceptual design stage, when the overall system architecture and endpoint concept are being developed and evaluated. As noted above, an early look at failure modes and 10 CFR 50.59 can help identify any significant issues at a time when they can be more easily dealt with.

- Ensure that the 10 CFR 50.59 evaluation procedure includes consideration of the cumulative effects of modifications. A series of small changes made over time can have an impact on operations that may not be obvious from an evaluation of any individual change by itself. This should be considered when developing the migration plan. See Section 5.3 for more guidance.

- Look for opportunities to obtain early NRC review and concurrence with the plant's HFE program – the sooner the better. Early review and approval of the program and associated design process documents and style guides can make subsequent reviews easier and less risky.

- Be prepared to show how the plant's HFE program and processes map to the NRC expectations as described in Chapter 18 of the SRP (NUREG-0800) and in more detail in NUREG-0711. Section 2.4 provides guidance on establishing or updating an HFE program as part of the plant's modification process. For a major modernization program, some of the required HFE activities to be carried out by the project team may need procedures that go beyond the normal modification process. The team should be prepared to describe how all of these activities, taken together, meet regulatory requirements and expectations. Section 5.4 provides more guidance.

- For major modernization programs, talk to the NRC early and often. As noted above, it is recommended that major changes affecting the plant's overall concept of operations be discussed with NRC. Experience has shown that communication with the NRC staff can help reduce licensing risk and costs. Topics that might be covered in the early discussions include:
  - Scope of the modernizations being planned
  - Plant expectations regarding submittals that may be required (e.g., results of early look at 10 CFR 50.59)
  - Planned schedule for any submittals and associated reviews to ensure sufficient time is allowed for these in the modification schedule
  - Identification of issues or areas of NRC concern regarding the proposed design or the planned design process.

2.5.3 Sources of Additional Information

Note: The references to regulatory documents given here were the current revisions at the time of this writing. Users of this guidance should consult the latest versions of the regulatory documents, which may have been updated since this was published.

10 CFR 50 Appendix A. General Design Criteria for Nuclear Power Plants, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

10 CFR 50 Appendix R. Alternative and Dedicated Shutdown Capability, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

10 CFR 50.34(f). Contents of applications; technical information; Additional TMI-related requirements, Code of Federal Regulations Title 10, Part 50.34, U.S. Nuclear Regulatory Commission, Washington, DC.

10 CFR 50.59. Changes, Tests and Experiments, Code of Federal Regulations Title 10, Part 50.59, U.S. Nuclear Regulatory Commission, Washington, DC: 2000.

10 CFR 55. Operators' Licenses, Code of Federal Regulations Title 10, Part 55, U.S. Nuclear Regulatory Commission, Washington, DC.

EPRI TR-102348 Revision 1 – NEI 01-01. *Guideline on Licensing Digital Upgrades: A Revision* of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule, EPRI, Palo Alto, CA: 2002. 1002833.

Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades, EPRI, Palo Alto, CA: 2004. EPRI 1002835.

NEI 96-07 Revision 1. Guidelines for 10 CFR 50.59 Implementation, Nuclear Energy Institute, Washington, DC: November 2000.

NUREG-0654 (FEMA-REP-1) Rev. 1. Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, Appendix 1, Emergency Action Level Guidelines for Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, DC.

NUREG-0700 Revision 2. Human-System Interface Design Review Guidelines, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

NUREG-0711 Revision 2. Human Factors Engineering Program Review Model, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

NUREG-0737 Supplement 1. Clarification of TMI Action Plan Requirements – Requirements for Emergency Response Capability, U.S. Nuclear Regulatory Commission, Washington, DC: January 1983.

NUREG-0800. Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

NUREG-1764. Guidance for the Review of Changes to Human Actions, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

Regulatory Guide 1.47. Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, U.S. Nuclear Regulatory Commission, Washington, DC: 1973.

Regulatory Guide 1.62. Manual Initiation of Protective Actions, U.S. Nuclear Regulatory Commission, Washington, DC: 1973.

Regulatory Guide 1.187. Guidance for Implementation of 10 CFR 50.59 Changes, Tests, Experiments, U.S. Nuclear Regulatory Commission, Washington, DC: November 2000.

Regulatory Guide 1.97 Revision 3. Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident, U.S. Nuclear Regulatory Commission, Washington, DC: 1983.

Regulatory Guide 1.174 Revision 1. An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, U.S. Nuclear Regulatory Commission, Washington, DC: April 2002.

RIS 2002-22. NRC Regulatory Issue Summary 2002-22, Use of EPRI/NEI Joint Task Force Report, 'Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,' U.S. Nuclear Regulatory Commission, Washington, DC: November 2002.

3
HFE DESIGN, ANALYSES, AND TOOLS

This section describes the HFE activities and analyses that should be performed as part of the design process (see Figure 3-1). The section begins with a discussion of how HFE fits into the overall design process (see Section 3.1) along with the main considerations for planning HFE activities for individual modifications. The subsequent sections describe each HFE activity in terms of its objectives, methods, use of results, grading, and documentation. The scope of each HFE activity is graded into three levels reflecting the application of the overall grading approach determined in Section 2.4 for each HFE activity. The last section presents information on methods to collect information from users and test and evaluation tools and techniques. Where appropriate, references are provided to sources of additional information. A brief overview of each HFE activity is shown in Figure 3-1 and summarized in the subsequent paragraphs.

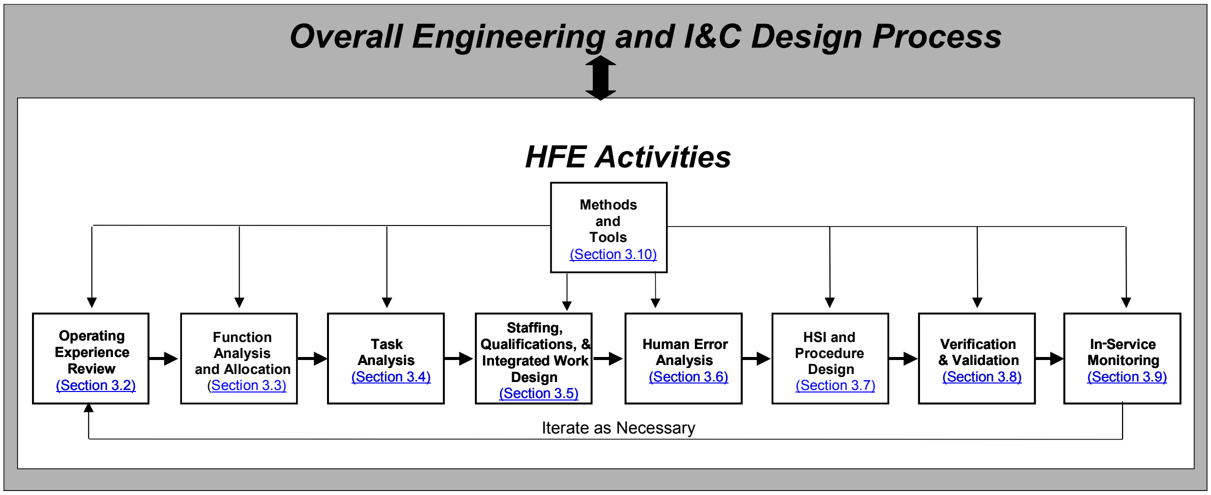

Overall Engineering and I&C Design Process
HFE Activities
Methods and Tools (Section 3.10)
Operating Experience Review (Section 3.2)
Function Analysis and Allocation (Section 3.3)
Task Analysis (Section 3.4)
Staffing, Qualifications, & Integrated Work Design (Section 3.5)
Human Error Analysis (Section 3.6)
HSI and Procedure Design (Section 3.7)
Verification & Validation (Section 3.8)
In-Service Monitoring (Section 3.9)
Iterate as Necessary

Figure 3-1
HFE Activities

Operating Experience Review (OER)

Changes made to personnel tasks and HSIs should be made with a thorough understanding of the strengths and weaknesses of the existing design and the new design and technology that will be used once the modification is complete. Gaining this understanding is the purpose of conducting an OER. The goal is to understand (1) current work practices so the potential impact of planned changes can be assessed, (2) operational problems and issues in current designs that may be addressed in the modernization program, and (3) relevant industry experience with candidate technological approaches to system and HSI technology and specific candidate supplier solutions.

After identifying the functions, tasks, and HSIs that will be impacted by the modification, both plant specific and industry experience is sought. A variety of data sources can be used, including: available documentation; interviews; talkthroughs and walkthroughs with personnel; and interactions with other facilities and organizations.

The next step is to classify OER items. Since OER information is useful only if it is available to the members of the design team who can make use of the information, it is desirable to classify the information according to design topics for which it is relevant. Finally, items are prioritized based on their importance.

Two things that are often overlooked are emphasized as part of the OER methodology. First, the methodology emphasizes the identification of positive as well as negative experiences. Second, the methodology emphasizes the identification of collateral effects. These two factors consider tasks that might be impacted by a modification that are not directly part of the modification. They include: (1) unintended consequences – tasks that are inadvertently hampered by changes that are made; and (2) targets of opportunity – opportunities to positively impact tasks not directly involved in the modifications but which share resources with modified tasks.

Function Analysis and Allocation

The term function allocation, as used here, simply refers to the allocation of responsibility for conducting an activity to plant personnel, to automatic systems, or to some combination of the two. The allocation is made on the basis of a function analysis to determine what is required to perform the function. Using the results of the function analysis, responsibility is allocated in a way that best ensures overall accomplishment of the function. With respect to modernization programs, the main focus is on how functions are changed rather than the creation of new functions.

The objective of this analysis is to specify the roles and responsibilities of plant personnel in the performance of plant functions and tasks (F/Ts), and how F/Ts may be changed as a result of the modification. The methodology (1) evaluates F/Ts that may be impacted by the modifications; (2) evaluates the suitability of full automation, partial automation, and manual F/T performance; and (3) identifies the design consequences. This analysis leads to four possible outcomes: Full F/T automation, partial F/T automation, manual F/T performance, and manual F/T performance with task support.

Task Analysis

Task analysis is the analysis of functions that have been assigned to plant personnel in order to specify the requirements for successful task performance. The tasks personnel perform are a primary consideration in designing the HSI, procedures, and training that are provided to plant personnel.

The method presented combines features of several approaches to task analysis and is intended to be sufficient for most task analysis needs in plant modernization programs. The first task analysis activity is to select tasks to analyze. Once accomplished, tasks need to be described and then the requirements for performance identified. Task descriptions provide information about the task, such as its purpose, its relationship to other tasks (e.g., performed in sequence or in parallel), the time it takes, etc. Task requirements are the resources that must be available to perform the task, e.g., the information and controls required. Finally, in addition to task requirements, personnel may require specific knowledge, skills, and abilities (KSAs) in order to perform the task. KSAs are identified as well.

Staffing, Qualifications, and Integrated Work Design

The purpose of this activity is to guide the assessment of the staffing levels and personnel qualifications associated with a modification. In particular, the analysis is intended to accomplish the following: (1) allocate new tasks to crewmembers, (2) evaluate whether shifts in task assignments should be made, (3) evaluate whether the new and modified tasks impact other personnel responsibilities when they are considered in an integrated fashion, and (4) evaluate whether plant changes drive new job qualifications. The methodology uses a combination of analysis and walkthrough techniques.

Human Error Analysis

The purpose of this activity is to evaluate the potential for human error in plant operation and maintenance and to define the circumstances surrounding an error specifically enough so that means for reducing or coping with the error can be identified. The analysis largely rests on qualitative methods. Analysis of potential human errors should be undertaken throughout the design process, since it can help prevent or minimize the likelihood of errors; i.e., an effort can be made to minimize critical errors through design of the HSIs, procedures, and training or through changes in plant automation. The design can also focus on making the system "error tolerant" by providing support for error detection and recovery in case errors do occur.

Human-System Interface and Procedure Design

The objective of this activity is to develop HSIs and procedures that (1) reflect the plant's functional and physical design, (2) meet personnel task requirements, (3) exhibit the general characteristics of a well-designed HSI, and (4) are easy to use and learn.

The HSI design process begins with information developed in formulation of the endpoint definition and the HFE analyses that specify changes to human functions (automation), new and modified tasks and the requirements for their performance, and the expected allocation of work to various crewmembers. Using that input, a concept design(s) is (are) developed that reflect these inputs. Once a concept design is selected, the detailed design of the HSIs can be accomplished. The design is developed using the detailed HSI guidance that is provided in different parts of the document (Sections 4 and 6). As with any modification, the new HSIs must be integrated into their locations (e.g., main control room or local control stations) along with existing equipment. Finally, procedures have to be developed and/or modified to reflect plant changes. At any point along the way, various types of tests and evaluations can be performed to collect needed information, obtain user feedback, resolve design options, or evaluate performance with the new HSIs.

HFE Verification and Validation (V&V)

HFE V&V is conducted to ensure the HSI is well designed, easy to use, and meets performance requirements. This includes three evaluations:

- HSI Task Support Verification is an evaluation to verify that the HSI supports personnel task requirements as defined by task analyses
- HFE Design Verification is an evaluation to verify that the HSI is designed to accommodate human capabilities and limitations as reflected in HFE guidelines
- Integrated System Validation is an evaluation using performance-based tests to determine whether an integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and acceptably supports safe and economical operation of the plant

These evaluations identify potential design problems that should be assessed for importance and corrected if necessary.

In-Service Monitoring

A common lesson learned from plants that have completed major digital I&C and HSI modernization programs is that once the new systems are used on a "day-to-day" basis, additional issues will arise. Examples include an incorrect label on a process display, an HSI function that behaves differently on the simulator than in the control room, and a change in the way a task is performed creating unanticipated difficulties. Treating these types of issues in a formal program can help to systematically identify and address issues, rather than depending upon anecdotal information and ad hoc fixes.

Methods and Tools for Collecting Information from Users

Information from users is an essential part of all HFE activities. It is used to support system or equipment design. The design team may wish to resolve a tradeoff (for example, whether to use touch screen or mouse input), obtain design information (for example, determine the meaning of a set of icons), or to try out a new approach (for example, web-like monitoring and control of remote equipment). Information from users also supports performing evaluations, for example, to evaluate whether the design meets performance requirements. Test and evaluation methods range from activities as simple as interviewing operators about how they perform their tasks to measuring task performance and workload as part of full-mission simulator test scenarios.

The methods presented in this section include interviews, surveys, walkthrough, and tests and evaluations using simulators. Since the same methods are used for many different HFE activities, the decision was made to discuss the details of those methods in one place, rather than repeating them in each section in which they were used.

How to Use Section 3

The HFE activities presented in Section 3 are oriented to modernization programs of significant scope or new design involving digital technology and computer-based interfaces. When the guidance is used for less extensive modifications, not all the HFE activities described will necessarily apply. For example, if operator tasks and HSIs are not substantially changed, then the elements of function allocation (Section 3.3) and task analysis (Section 3.4) may not be applicable.

The first step in using Section 3 is to become familiar with the subsections and the HFE activities, their purpose, and the methodologies suggested. The methods described in Section 3 should be compared with the plant's existing HFE procedures, if any. Note that these methods reflect the expectation that the modifications involve digital technology and computer-based interfaces. Existing plant procedures may be oriented to conventional technology only. Also, some HFE procedures may exist outside of engineering, in departments such as training. For example, training departments often conduct task analyses to provide input to training program development.

Once a comparison is completed, a new procedure should be developed, or the existing one modified, to use or adapt the methods presented in this section.

The methods presented in this section are complete methodologies, i.e., they can be used when no existing HFE design information and analyses are available. However, in many applications, information already exists. For example, the existing, validated operating procedures are an importance source of information about operator tasks and, depending on the scope of the modification, the grade level assigned to the modification (see Section 2.4.2), and, the nature of the changes to existing tasks, little additional analysis may be needed.

HFE activities should begin with an identification of what information already exists. Where that information is current, accurate, and sufficiently detailed, it should be used and the analysis should focus only on what additional information is needed.

In those circumstances where little information already exists, the HFE analyses should be conducted as described in this section to provide the needed design input.

3.1 Implementing HFE in the Design Process for Individual Modifications

3.1.1 Introduction
3.1.2 Design Process Steps
3.1.3 Basic Application of HFE in Design Processes
3.1.3.1 Project Planning/Design Concept
3.1.3.2 Requirements
3.1.3.3 Design
3.1.3.4 Implementation
3.1.3.5 Testing
3.1.3.6 Operational Support
3.1.4 Planning for HFE Activities in Individual Modifications
3.1.4.1 Develop Plan and Preliminary Conceptual Design

3.1.4.2 Designate the Personnel Responsible for HFE
3.1.4.3 Assess Impact on Concept of Operations
3.1.4.4 Identify HSIs to be Upgraded
3.1.4.5 Determine HSI Design Concepts
3.1.4.6 Identify Scope of HFE Design Activities
3.1.4.7 Identify Test and Evaluation Tools and Techniques for HFE Activities
3.1.4.8 Determine Cost of HFE Activities
3.1.4.9 Determine Schedule of HFE Activities
3.1.4.10 Consider Endpoint and Overall I&C/HSI Migration Strategy
3.1.4.11 Documentation and Licensing
3.1.5 Appendix – Example HFE-Related Portion of Modification Checklist

3.1.1 Introduction

Nuclear plant utilities use documented design procedures to govern changes and modifications. A structured design process provides a means to trace requirements from the early stages of design through the final design and to verify and validate its adequacy. In addition to ensuring that the final design can be used effectively, a structured design process can identify and correct design flaws and errors, thus reducing the impact on cost and schedule.

As was discussed in Section 1, HFE should be fully integrated into the overall plant engineering process to ensure timely and complete interaction with other engineering activities. Implementing HFE from the earliest stages of design helps ensure that a design considers impacts on all affected HSIs, and plant modifications do not create human performance problems. HFE is an essential engineering activity/discipline complementing the traditional I&C Engineering, Mechanical Engineering, or Electrical Engineering. HFE should be implemented as a part of the existing plant modification process. This section provides the following:

- A description of the design process,
- The elements of a basic HFE program and ways in which designers currently apply HFE-related activities in the design process, and
- Guidance on planning for HFE activities in individual modifications.

3.1.2 Design Process Steps

The basic steps common to the majority of engineering design processes are listed below:

- Project planning/design concept development
- Requirements definition
- Design development
- Design implementation
- Acceptance testing
- Support during operation and maintenance

The major activities associated with the design process for a generic digital I&C modification are provided in Figure 3-2. The figure is not intended to show the full scope of modification activities; only major activities are provided. Figure 3-3 shows how HFE is being applied to existing design modification processes.

3.1.3 Basic Application of HFE in Design Processes

Applying HFE to a design process is not intended to create a new and complicated set of activities. Most plants have basic screening steps to determine if HFE is involved or required for specific modifications and HFE programs in place that are appropriate for modifications that are graded as Level 3 per the graded approach described in Section 2.4.2. The following features are common to many of these programs:

- A commitment by management to include HFE reviews as a part of the change process to ensure modifications will maintain affected control spaces in a state at least as representative of accepted HFE principles as was established following the completion of the DCRDR; this commitment is often a formal licensing commitment.
- Qualification requirements and HFE training to establish a required minimum “level of competence” for design engineers performing HFE activities.
- The identification of the design engineering, modification engineering, or other organization managers that have responsibility to implement required HFE activities.
- A method in the design modification process to identify when HFE activities are required.
- A procedure to govern the implementation of HFE in the design modification process and to manage the HFE program.
- A style guide that specifies plant-specific HSI conventions and design criteria based on accepted HFE guidelines.
- A requirement in the design and modification process that documents that the required HFE activities have been performed.

In addition, many plants routinely perform activities in the design modification process that in reality are HFE activities but may not be recognized or documented as such. These activities, which implement the basic HFE program outlined above, are discussed below. Figure 3-2 shows where in the existing design modification process these activities typically occur.

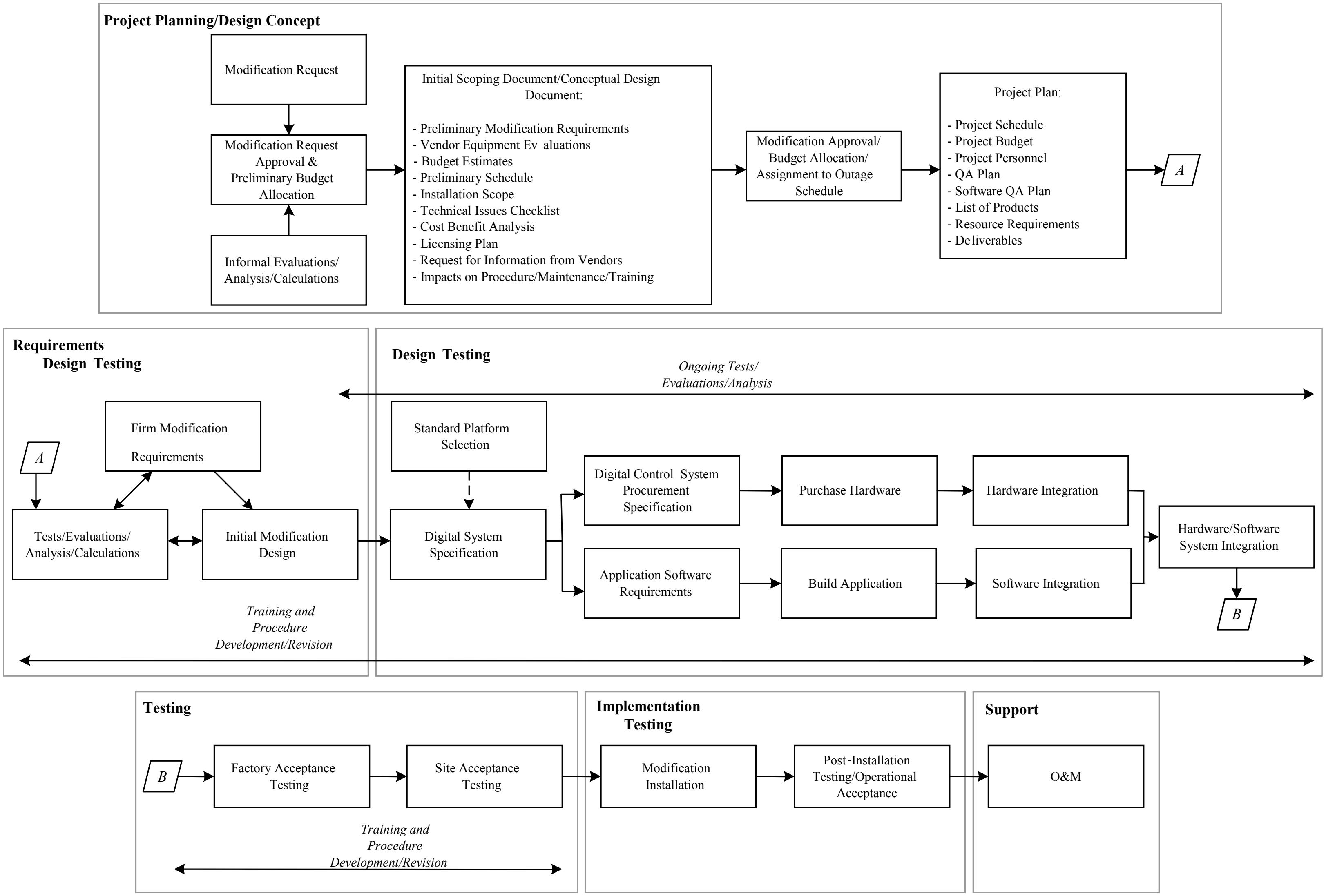

Project Planning/Design Concept
Modification Request
Modification Request Approval & Preliminary Budget Allocation
Informal Evaluations/ Analysis/Calculations
Initial Scoping Document/Conceptual Design Document:
- Preliminary Modification Requirements
- Vendor Equipment Ev aluations
- Budget Estimates
- Preliminary Schedule
- Installation Scope
- Technical Issues Checklist
- Cost Benefit Analysis
- Licensing Plan
- Request for Information from Vendors
- Impacts on Procedure/Maintenance/Training
Modification Approval/ Budget Allocation/ Assignment to Outage Schedule
Project Plan:
- Project Schedule
- Project Budget
- Project Personnel
- QA Plan
- Software QA Plan
- List of Products
- Resource Requirements
- De liverables
A
Requirements Design Testing
A
Firm Modification Requirements
Tests/Evaluations/ Analysis/Calculations
Initial Modification Design
Training and Procedure Development/Revision
Design Testing
Ongoing Tests/ Evaluations/Analysis
Standard Platform Selection
Digital System Specification
Digital Control System Procurement Specification
Application Software Requirements
Purchase Hardware
Build Application
Hardware Integration
Software Integration
Hardware/Software System Integration
B
Testing
B
Factory Acceptance Testing
Site Acceptance Testing
Training and Procedure Development/Revision
Implementation Testing
Modification Installation
Post-Installation Testing/Operational Acceptance
Support
O&M

Figure 3-2
Elements of a Generic Digital I&C Modification

3.1.3.1 Project Planning/Design Concept

HFE is addressed in the Project Planning phase when the need for new or revised procedures and training and maintenance activities due to the modification is identified and included in the Initial Scoping Document/Conceptual Design Document (ISD) and the modification Project Plan. Because procedures, training, and maintenance activities affect the way personnel interact with systems, addressing impacts on each is an HFE activity. Including these activities in the Project Plan for the modification is a part of establishing an HFE Plan, even though it may not be labeled as such.

Basic HFE programs for design modifications often include a checklist to determine the impact of a modification on HSIs in the control room (i.e., to determine whether HSI modifications are involved and the HFE expertise and activities that may be required). An example of such a checklist is provided in the Appendix. Checklist answers are inputs to the initial conceptual design document and to the modification project plan (i.e., to the project budget, schedule, activities, etc.).

Often a modification will result from problem reports that involve an affected HSI. Thus the Operating Experience Review is an input to the Modification Request in the Project Planning phase.

3.1.3.2 Requirements

Plants perform a number of activities as part of defining modification requirements that are essentially simplified forms of HFE analysis. For example, function and task allocation is performed when design requirements for a modification intentionally retain or change the existing allocation of functions to an HSI based on favorable or unfavorable attributes of the existing HSI. A simple form of task analysis is performed when procedures are used to identify how a design modification will affect current personnel tasks, and a form of Operating Experience Review is performed when input regarding design considerations is obtained from plant Operations personnel and/or problem reports involving affected HSIs. The results of these activities form the basis for the design requirements.

3.1.3.3 Design

HFE is addressed in the design phase of a modification when a plant HFE style guide or similar document, such as one developed from this guidance document, is used to guide design activities. HFE is also addressed in the design phase when procedures or the training program are revised or developed due to a modification.

3.1.3.4 Implementation

The decision regarding how to install a modification (during one outage, during multiple outages, during plant operation, etc.) is a part of the control room migration strategy, addressed during the Project Planning phase of a modification.

3.1.3.5 Testing

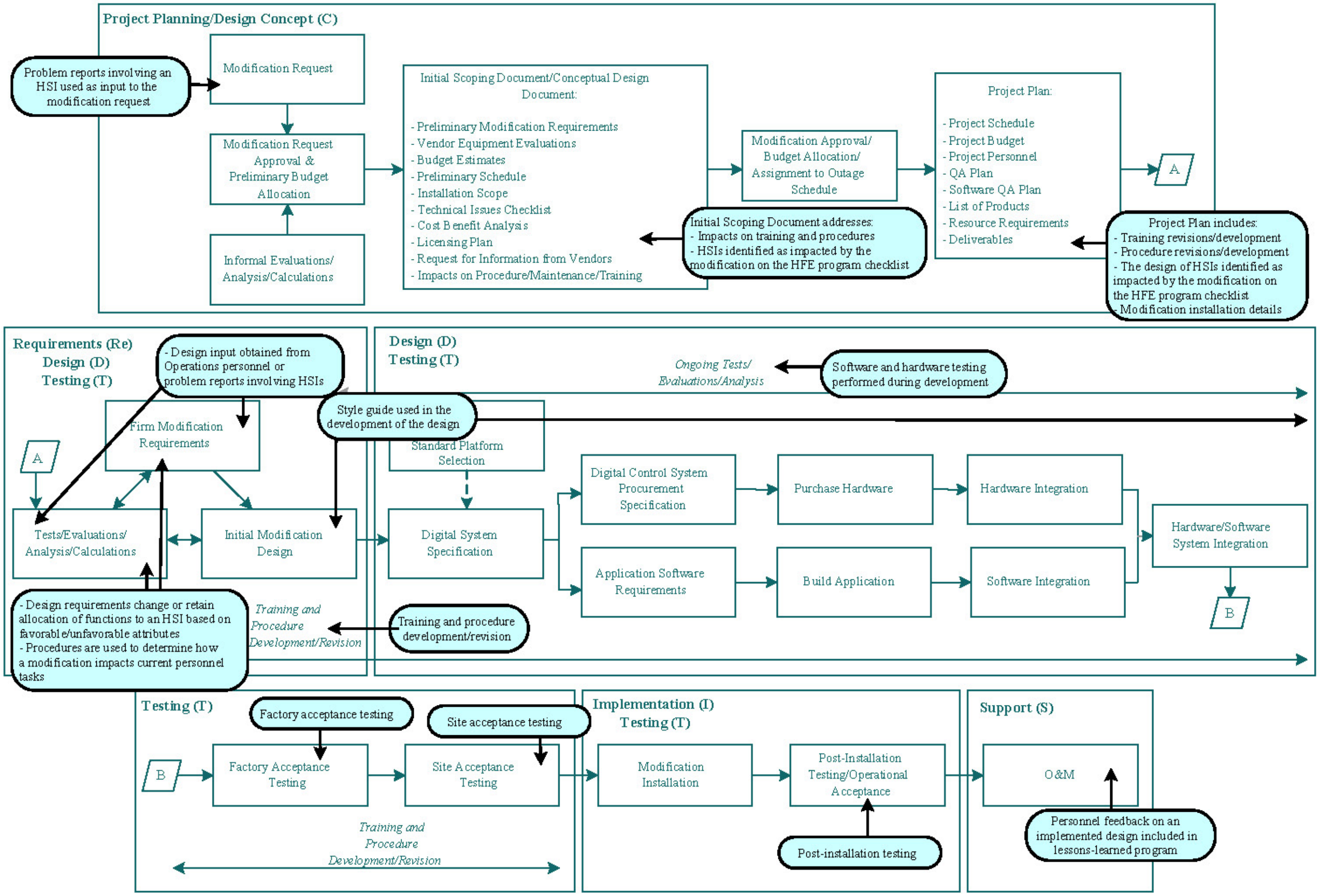
The following testing activities are performed in parallel with or after the completion of modification design activities:

- Testing of software and hardware during development (i.e., before installation in the plant)
- Factory acceptance testing of the modification
- Site acceptance testing of the modification
- Post installation testing of the modification

This testing typically includes functional tests of the HSI and ensures that users can perform the necessary tasks satisfactorily with the modified system.

3.1.3.6 Operational Support

Lessons learned or similar program feedback obtained from personnel regarding any problems associated with a new design after its implementation is a form of in-service monitoring.


Project Planning/Design Concept (C)
Problem reports involving an HSI used as input to the modification request
Modification Request
Modification Request Approval & Preliminary Budget Allocation
Informal Evaluations/ Analysis/Calculations
Initial Scoping Document/Conceptual Design Document:
- Preliminary Modification Requirements
- Vendor Equipment Evaluations
- Budget Estimates
- Preliminary Schedule
- Installation Scope
- Technical Issues Checklist
- Cost Benefit Analysis
- Licensing Plan
- Request for Information from Vendors
- Impacts on Procedure/Maintenance/Training
Modification Approval/ Budget Allocation/ Assignment to Outage Schedule
Initial Scoping Document addresses:
- Impacts on training and procedures
- HSIs identified as impacted by the modification on the HFE program checklist
Project Plan:
- Project Schedule
- Project Budget
- Project Personnel
- QA Plan
- Software QA Plan
- List of Products
- Resource Requirements
- Deliverables
A
Project Plan includes:
- Training revisions/development
- Procedure revisions/development
- The design of HSIs identified as impacted by the modification on the HFE program checklist
- Modification installation details
Requirements (Re)
Design (D)
Testing (T)
- Design input obtained from Operations personnel or problem reports involving HSIs
Firm Modification Requirements
A
Tests/Evaluations/ Analysis/Calculations
Initial Modification Design
- Design requirements change or retain allocation of functions to an HSI based on favorable/unfavorable attributes
- Procedures are used to determine how a modification impacts current personnel tasks
Training and Procedure Development/Revision
Design (D)
Testing (T)
Ongoing Tests/ Evaluations/Analysis
Software and hardware testing performed during development
Style guide used in the development of the design
Standard Platform Selection
Digital System Specification
Digital Control System Procurement Specification
Purchase Hardware
Hardware Integration
Application Software Requirements
Build Application
Software Integration
Hardware/Software System Integration
B
Training and procedure development/revision
Testing (T)
Factory acceptance testing
Site acceptance testing
B
Factory Acceptance Testing
Site Acceptance Testing
Training and Procedure Development/Revision
Implementation (I)
Testing (T)
Modification Installation
Post-Installation Testing/Operational Acceptance
Post-installation testing
Support (S)
O&M
Personnel feedback on an implemented design included in lessons-learned program

*The highlighted information in the figure indicates activities that are currently being performed by plants that, although maybe not recognized or documented as so, are HFE activities performed during the design modification process.

Figure 3-3
Basic HFE Activities Performed in the Design Modification Process

3.1.4 Planning for HFE Activities in Individual Modifications

This section describes and provides guidance for planning for the HFE analysis, design, V&V, and implementation of individual plant modifications. These modifications may involve the replacement of older pen and paper, strip-chart recorders with modern digital recorders with VDUs and RS232 serial communications, or they may involve more complex modifications (e.g., replacement of an electro-hydraulic turbine control system) or several related modifications during a single outage.

At this point in the modification process, there should be a defined endpoint vision (see Section 2.2) and a strategy for migrating from the original plant configuration to that endpoint (see Section 2.3). Some steps may have already been taken to reach the endpoint, and there may be many more to come. Regardless of whether it will be in use for one cycle or the remainder of the plant's life, the design should incorporate proper HFE if it will be used to operate the plant.

The implementation details for the human factors-related activities should be included in the project plan for the modification and should not be confused with the generic procedures that apply to all modifications. Implementation plans should include the goals and scope of the modification; an updated list of the HFE modification personnel involved and their responsibilities; a description of the procedures that will be invoked and how the HFE activities will be tailored to the specific modification; and the schedule for planning, analysis, design, verification and validation (V&V), procurement, installation, training, etc. This plan should be part of the overall project plan for the modification. The portions of the project plan that address HFE should document which HFE activities are applicable, and the scope or nature of the activities to be undertaken in each case based on a graded approach and based on the scope and nature of the modification. An initial assessment of the scope of HFE activities should be performed and documented as early as possible in the conceptual design phase. An abbreviated application of the graded approach described in Section 2.4.2 could be used for the conceptual design phase definition of HFE activities. A more comprehensive application of the graded approach should be used to determine the detailed scope of HFE activities for the modification.

Details of HFE activities should be included in the integrated budget, schedule, and implementation plan for the modification (see Section 2.4.1.1). A modification plan is used to integrate activities, coordinate the efforts of plant personnel and contractors, and ensure that resources will be available when needed to support each activity. Table 3-1 provides a partial listing of modification activities and the associated HFE activities that should be defined in the HFE portion of the project plan for an individual modification.

After the activities are defined and integrated into the plan, the planning team can assign responsibilities and allocate resources to ensure that the modification will be performed on time and within the prescribed budget.

During the planning for a modification, some level of function analysis and allocation (see Section 3.3) should be performed to define the performance requirements for new equipment, such as response times and information availability. The scope of the analysis should include all functions for which the existing equipment is used and for which the new equipment will be used.

In most modification projects, the major high-level functions and their requirements may not change substantially. However, some modifications may change the allocation of functions between human and machine. These types of changes can have broad effects on crew coordination, procedures, training, and the amount of information needed at the workstation. Functional requirements analysis ensures that all functional requirements that must be met after the change is implemented are identified. While this analysis does not reach the level of detail needed to specify components, it is needed to perform a task analysis (see Section 3.4) and to develop V&V criteria (see Section 3.8). It can also be used to identify changes in the operators' responsibilities for a given function.

Note that it is very important to pay particular attention to modifications that affect functions that are identified as important to nuclear and personnel safety and plant availability or that change the allocation of those functions.

Table 3-1
HF Planning Activities

Modification Activity	HFE Design Activity to be Integrated with the Modification Activity
Scope and Purpose of the Modification	OER to identify need, scope and purpose HSI interim design and relationship to the migration strategy
Modification Plan	HFE Plan
Designation of modification personnel	Designation of HFE personnel
Roles of modification personnel	Roles of HFE personnel
List of systems and equipment to be upgraded	List of HSIs (associated with those systems and equipment) to be upgraded, added, or removed
Determination of the modification activities to be performed	Determination of the HFE design activities and HSI upgrade activities to be performed
Schedule with work breakdown structure	Integration of HFE activities and identification of HFE hold points
Overall modification cost	Cost associated with performance of the HFE activities and HSI upgrades

3.1.4.1 Develop Plan and Preliminary Conceptual Design

As soon as an approved modification is identified as requiring the application of HFE as part of the modification design activities, one or more qualified human factors engineers should be assigned to perform the preliminary HFE planning and conceptual design. As recommended earlier, HFE planning should be a component of the overall modification project plan. It will include the preliminary identification of HFE activities, a schedule for those activities integrated with the modification schedule, and the resource requirements for the HFE activities including whether specialized expertise will be required. The initial human factors evaluation of the modification will also include a certain amount of operating experience review (Section 3.2) that, at a minimum, identifies any problem reports written against the affected systems and HSI, any operator "workarounds," and any outstanding HEDs that were not resolved as part of the original DCRDR.

3.1.4.2 Designate the Personnel Responsible for HFE

Designate HFE personnel at the same time personnel are designated for other modification activities. This should occur before any significant design process activities are performed. The roles of the HFE project participants should also be determined at this time. The primary roles of the HFE personnel are as follows:

- Perform modification planning and conceptual design for HFE related activities (see Section 3.1.4.1)
- Perform HFE analyses
- Support HSI design and perform periodic reviews of HSI design work to ensure the appropriate application of HFE
- Perform HFE V&V activities

Modification staffing should account for iterations in the design that will result from HFE V&V activities.

3.1.4.3 Assess Impact on Concept of Operations

Assessing how a modification will affect the overall concept of plant operation is an important activity in the planning phase. Through this assessment, planners can determine the effect on the staff size, roles, and responsibilities; the level of automation; and the design of the control room. The assessment will ultimately determine the existing HSIs that will need to be modified or deleted and any new HSI that need to be added because of the overall modification. Therefore, this activity should be performed in conjunction with or prior to determining the scope of modification activities.

3.1.4.4 Identify HSIs to be Upgraded

Ensure that the HSIs to be upgraded, deleted, or added are considered and appropriately included in the list of systems and equipment to be upgraded by the modification. This step involves identification of the displays, controls, alarms, procedures, and training that will require modification, or must be newly installed, to support the overall modification. Ensure that the identified HSI and associated requirements are included in the procurement specification for the control system.

3.1.4.5 Determine HSI Design Concepts

Determine the overall HSI design concepts at the same time the overall modification design concepts are determined. The endpoint vision for the control room should be considered. Design concepts for each stage of the modification should be developed. Ensure that the design concepts for the HSI are included in the procurement specification for the control system. It is important to evaluate the potential system suppliers for their ability to provide HSI with the features that support the design requirements for the specific modification and that are consistent with plant conventions and the endpoint vision. This activity should be performed after the HSIs to be upgraded have been determined, but before the scope of HFE design activities is determined.

3.1.4.6 Identify Scope of HFE Design Activities

Determine the scope of HFE design activities that will be required to support the modification – not only for the HSIs that will be upgraded, but also for the systems and other equipment that will be modified, deleted, or added. This step should be performed when the scope of activities for the overall modification are determined. Section 2.4.2 discusses a graded approach to determining the activities and level of effort of each activity that must be performed. Use this graded approach method during the planning stage. Determining the scope of all modification activities, not just HFE activities, to be performed for a modification is an important step in the planning phase. It is an input to the overall modification schedule and the overall cost of the modification. Specific items to consider in addition to the HSI include the impact of the modification on the plant's PRA/HRA (Human Reliability Analysis), as well as implications associated with changes to procedures and training.

3.1.4.7 Identify Test and Evaluation Tools and Techniques for HFE Activities

Determine the tools and techniques (e.g., mockups, prototypes, and "walkthrough / talkthroughs") needed for HFE activities along with those tools needed for the overall modification. See Section 3.10 for more discussion and details on HFE tools and techniques used to perform tests and evaluations. This activity cannot be performed until the scope of HFE activities to be performed has been established. Results will affect the cost and schedule of the modification. Performing this step early in the modification process is important to ensure that any materials that must be purchased are received in time.

3.1.4.8 Determine Cost of HFE Activities

Include the costs associated with upgrading the HSIs and performing the HFE design activities in the overall modification cost. The scope of the HFE activities and HSI upgrades associated with the modification are inputs to this activity. Note that costs associated with iterations in the design as a result of V&V activities should be addressed.

The inclusion of HFE activity costs is an important step in the planning phase of a modification. If the costs of HSI upgrades and HFE design activities are not included as a part of the overall modification cost, the activities likely will not be performed. The result will be, at best, simple HFE reviews of completed design. Similar to quality, human factors cannot be reviewed into the design at the end of a design process.

3.1.4.9 Determine Schedule of HFE Activities

Include the HFE activities and HSI design activities in the overall modification schedule. Similar to developing the overall modification cost, the scope of the HFE activities and HSI upgrades associated with the modification are inputs to this activity. The schedule should include adequate activity durations to account for iterations in the design that will result from HFE V&V activities. Including HFE activities in the overall modification schedule is critical – if the activities are not scheduled, they will likely be omitted from the modification.

3.1.4.10 Consider Endpoint and Overall I&C/HSI Migration Strategy

As the scope of the modification and the HFE design activities is being determined and scheduled, any lessons learned from previous modifications associated with I&C and HSI modernization should be evaluated for applicability. It is also important to ensure the modification is consistent with the goals and expectations within the overall facility I&C/HSI modernization strategy that was developed according to the guidance in Sections 2.2 and 2.3. If applicable, any prerequisites or limitations that were identified in the original modernization plan should be evaluated. This step involves determining the implications of other modifications (previously installed, concurrent of planned) on features, resources, and schedule for this modification and the implications of this modification on the same aspects of other modifications. Conflicts must be resolved, and consideration should be given to activities that can be performed in parallel, as well as tools and resources that can be shared between various modifications.

In addition, at this time, the implications of the interim HSI design defined by the completion of this step in the overall migration strategy should be addressed. It is important that each return to service configuration provide users with a complete and well-designed set of HSI. Always consider the possibility that priorities and budgets may be changed and what were originally expected to be short-term interim configurations may have to be used for unexpected long periods.

3.1.4.11 Documentation and Licensing

Documentation for HFE activities should be based on the scope of the HFE activities and the grade assigned the modification per the graded approach. The discussions of specific HFE activities in the subsequent sections in Section 3 provide recommendations for documentation.

The guidance found in Section 5.3, 10 CFR 50.59 Evaluations and Section 5.4, Licensing Submittals should be considered to determine the impacts of the modification on the facility license and associated evaluation, documentation, and submittal requirements.

3.1.5 Appendix – Example HFE-Related Portion of Modification Checklist

		Yes	No
1. Does this change involve the modification, movement, non-identical replacement, addition, deletion, or deactivation of the following components?			
	a) Switches (thumbwheels, pots, etc.)		
	b) Meters		
	c) Recorders		
	d) Hand-Auto/Manual Stations		
	e) Indicating Lights		
	f) Computers affecting HSIs (hardware, software, displays)		
	g) Alarms/Alarm Inputs		
	h) Desks, Consoles, or Equipment Cabinets		
	i) Component Power Disconnected		
	k) Video Display Unit or other computer display		
	l) Controls		
	m) Operator aids		
2. Does this change involve the modification, movement, addition, or deletion of:			
	a) Legends		
	b) Labels		
	c) Annunciator Windows		
	d) Demarcation/Mimics		
3. Does this change involve the modification, addition, or deletion of a set point?			
4. Will this modification cause changes to operating procedures or other information commonly used by the operator?			
5. Does this change modify the function of any control loop, e.g., implements automation of a previously manual control function, affects the response time or other requirements for task performance, or assigns a new task to an operator?			
6. Does this change affect Main Control Room or Remote Shutdown Facility lighting, acoustics, noise level, voice communications, HVAC, or access control?			
7. Does this change affect Operator Training Aids (simulator, mock-up, etc.)?			
8. Does the change otherwise affect an operator's tasks or performance requirements?			
If the answer to any of the questions above is 'Yes', then an HFE Specialist should be assigned, and the procedure that governs the application of HFE for modifications and changes should be followed.			

3.2 Operating Experience Review

3.2.1 Introduction
3.2.2 Design Process Steps
3.2.3 Basic Application of HFE in Design Processes
3.2.3.1 Inputs
3.2.3.2 Identify the Functions, Tasks, and HSIs Impacted by the Modification
3.2.3.3 Review Plant-Specific Experience
3.2.3.4 Review Relevant Industry Experience
3.2.3.5 OER Item Classification
3.2.3.6 Operational Support
3.2.4 Documentation
3.2.5 Grading the OER Effort
3.2.6 Use of the Results
3.2.7 Appendix – HFE-Related Issues Arising in Plant Modernization Programs

3.2.1 Introduction

The purpose of this section is to provide guidance on how operating experience can be used to support the HFE design of a particular modification. It discusses the topics to be addressed, the methods and data to analyze, documentation, and the application of the information developed.

Vendors and utilities typically have programs in place to gather operating experience and develop lesson learned to support design improvements and to help avoid operations and maintenance problems. The difference between such general efforts and the OER described in this section is the restricted scope and focus that is specifically oriented toward providing input to digital I&C and control room upgrades.

The lessons learned from previous experience, both at the plant being upgraded as well as at other plants that underwent similar modifications, can help ensure that existing problems are addressed, and that positive approaches are incorporated into the modifications while past problems are avoided. The information developed as part of OER has broad application to many HFE design activities that are performed as part of the modification (see Section 3.2.6).

Evaluation of operating experience also can help a utility develop overall plans for the modernization program and the desired endpoint vision, and it will help utility personnel become familiar with new technologies that may not currently be available in their plant. OER in support of modernization planning is discussed in Section 2.

3.2.2 Design Process Steps

The objective of an OER is to identify and analyze:

- Current work practices so that the potential impact of planned changes can be assessed

- Operational problems and issues in current designs that may be addressed in the upgrade project
- Relevant industry experience with candidate technological approaches to system and HSI design and technology

Uses of the results of OER are discussed in Section 3.2.6.

3.2.3 Basic Application of HFE in Design Processes

The complete methodology described here is for a Level 1 analysis. For recommendations on grading the methodology, see Section 3.3.5.

The scope of topics that can be addressed in OER is illustrated in Table 3-2. The general approach to obtaining and using information on these topics consists of five activities as shown in Figure 3-4. Each of these activities is discussed below. A variety of data sources are used for OER, including:

- available documentation
- interviews and walkthroughs with personnel
- interactions with other facilities, organizations, and vendors.

Two things are emphasized as parts of the OER methodology that are not typically thought of in OER. First, the methodology emphasizes the identification of positive as well as negative experiences. Second, the methodology emphasizes the identification of collateral effects that are beyond the specific scope of the modernization project (e.g., opportunities to make additional improvements that may not have been identified in the planning for the modification but the OER shows could provide substantial benefit). The use of such information is described below.

3.2.3.1 Inputs

The main input for OER is the activities conducted as part of endpoint vision planning (see Section 2). As part of that activity, an initial OER was performed and initial concepts of the type of operation and control room envisioned were developed. In addition, a utility's processes for obtaining authorization and funding for a modification usually requires a business case to be made. That preliminary activity will typically occur long before the actual design process starts. Usually the modification request documentation will require a specific enumeration of the known problems the modification is intended to mitigate and a preliminary cost/benefit analysis to justify the modification implementation. Any such details available from the initial modification package evaluation should be treated as OER material. This information serves as an initial starting place for the OER analysis described in this section.

Table 3-2
Scope of OER

Modernization Activity	Topic Classification
Planning	Endpoint vision
	Concept of operations
	Migration strategy
Design Process	Approaches and techniques
	Design Tools
	Test and evaluation
	Design implementation
	HFE verification and validation (V&V)
Licensing	Safety evaluations
	HFE adequacy demonstration
Personnel Role	Automation
	Work practices and task design
	Staffing, qualification, and task allocation to crewmembers
	Teamwork, crew coordination,
	Communication and peer checking
	Supervision
	Task location, e.g., main control room vs. local actions
	Training
HSI Design	Alarm system design
	Display and information design
	Control design
	Operator aids and support systems
	Procedures design
	Control room layout and environment

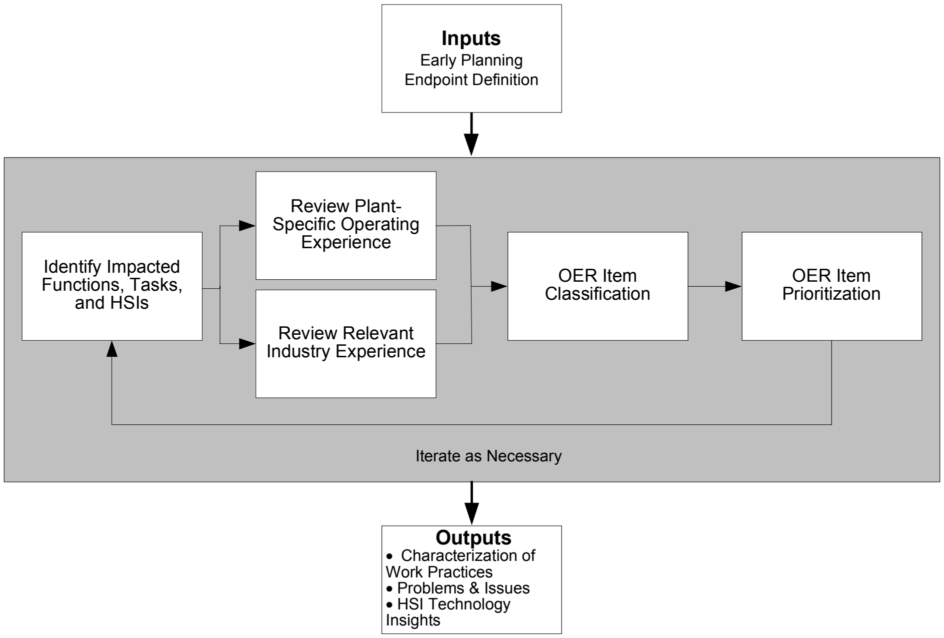

Inputs
Early Planning
Endpoint Definition
Identify Impacted Functions, Tasks, and HSIs
Review Plant-Specific Operating Experience
Review Relevant Industry Experience
OER Item Classification
OER Item Prioritization
Iterate as Necessary
Outputs
• Characterization of Work Practices
• Problems & Issues
• HSI Technology Insights

Figure 3-4
Overview of Operating Experience Review

3.2.3.2 Identify the Functions, Tasks, and HSIs Impacted by the Modification

In order to screen operating experience so the review can focus on the modification, the first step is to identify the functions, tasks, and HSIs that will be impacted. This can be accomplished by evaluating the plant systems being replaced and identifying the higher-level functions that are impacted, personnel tasks involving those systems, and their HSIs. HSIs include not only the individual displays, controls and procedures used for monitoring and controlling the affected systems, but also the panels on which they are located. In addition, all affected tasks and HSIs should be identified:

- Both maintenance and operations tasks and HSI should be considered
- Tasks and HSIs in the main control room and outside the control room should be considered

This information can be assembled into a list of impacted functions, tasks, and HSIs that will be used to focus the remaining activities on the experience that is relevant to the plant modification.

3.2.3.3 Review Plant-Specific Experience

One of the main purposes of the OER is to identify plant experience relevant to the scope of the upgrade (identified in the previous section). This will include both documented and undocumented sources.

3.2.3.3.1 Documented Operating Experience

Documented operating experience is available from many sources, including event reports and systems such as the plant's corrective action program. These sources should be reviewed to identify any aspects or items that are relevant to the systems being modified. While the focus of this discussion is on HFE information, the review may be expanded if desired to identify information useful for other aspects of the modification design as well.

3.2.3.3.2 Personnel Interviews and Walkthroughs

Not all of the relevant operating experience is available through documented sources. To supplement this information, interviews and walkthroughs should be conducted with operations, maintenance, and training personnel familiar with the systems and tasks affected by the modification. The purpose of these interviews is to understand current work practices and to identify positive and negative feature of the current design. Also, if a similar HSI has been implemented for a different function or system, its operating experience and potential applicability for the current modernization effort should be determined from interviews and walkthroughs. Developing an understanding as to how functions and tasks are performed and how HSIs are used in support of performance is important in determining the impact of changes on work practices. Experience has shown that personnel often perform tasks and use HSIs in ways that are different from what is described in documentation and the way designers anticipated. An example is provided in the Example 3-1 below.

Example 3-1 Example of the Unanticipated Use of HSI Technology
In early applications of new alarm technology, the "old-fashioned" annunciator tiles were replaced with alarm message lists presented on VDUs. The new alarm systems were unsuccessful because the designers failed to appreciate how much the old alarm system was used for high-level plant status assessment. Operators could quickly scan the alarm tiles and see which functions and systems were OK and which were not. This could not be accomplished with the message lists because only a small number of alarms could be seen at any one time (the message list had to be scrolled to see other alarms) and the alarms had no spatial dedication. Thus the strong pattern recognition that operators had developed with the older alarm system was lost.

It is best to ask personnel about their experiences from two perspectives: task-oriented and HSI oriented. The methodology for each of these is discussed in Section 3.10.2.4. In all cases, it is essential to follow the guidelines for interacting with personnel provided in Table 3-20.

Task-Oriented Interviews and Walkthroughs

In applying the task-oriented approach, the interviewer should focus on the tasks that will be impacted by the modification. Information is gained by walking through tasks with personnel, such as walking through a procedure with an operator. Personnel should be asked to verbalize their thought process so that their actions can be understood. As the tasks are being described, ask the personnel to identify any especially positive or negative features of the tasks or the HSI (including procedures). Personnel should be asked to think of past experiences and any difficulties they have encountered. Personnel should also be asked about any aids that could potentially improve performance, efficiency, and safety.

Personnel should be asked for the root cause of the problems identified and any suggestions they have for improving the design. Note that such information should only be treated as a suggestion since:

- the issue may be unique to one individual
- the individual may not accurately identify the root cause
- the suggested improvement may not reflect the capabilities of the new systems being designed – other solutions may be more appropriate
- the impact of the problem must be assessed and evaluated against cost-benefit criteria and the impact of the specific problem must be compared with the overall expected benefit of the proposed modification.

Examples of the types of information that can be obtained are illustrated in Example 3-2.

Another source of information on deficiencies of the current design is the presence of "workarounds" in the workplace. These are "temporary" additions to the workplace made by personnel who perform a task. They are usually used to provide important reminders or information needed for task performance that is not readily available in the design. The "Level of Automation" item in Example 3-2 provides an example of a workaround.

Example 3-2 Two Examples of Items Identified in an Operating Experience Review

Area of Design	Example Item
1. Alarm Design	The alarm system can be misleading during transients. For example, diesel generator (DG) trips are restricted during emergencies. If a non-emergency trip comes in, the DG will not trip, but the "DG TRIP" alarm still rings. This occurs because the DG TRIP alarm is set off by any of 17 trip signals; while, in emergencies, only 3 conditions (e.g., diesel engine overspeed) will trip the diesel. Yet, if any of the remaining 14 signals occur, those trip alarms still come in.
2. Level of Automation	Reactor coolant pump seal leak off return isolation – Under loss of seal injection and thermal barrier cooling, operators are required to manually isolate the seal within one minute. This prompted management to place a large sign on the control panel to remind operators to take this action when indicated. Failure to do so could lead to seal degradation, possibly escalating to a seal loss of coolant accident. Operators suggested that automation of the task of seal isolation should be explored.

Note: These are two example items from an OER conducted at a multi-unit US plant using task walkthroughs and interviews with shift crews totaling 14 operators and supervisors.

HSI-Oriented Interviews and Walkthroughs

In the HSI-oriented approach, personnel are specifically asked about their experiences in using the HSIs. The interview, instead of centering on specific tasks, focuses on HSI resources, e.g.,

- alarms
- displays (including detailed aspects such as labeling, abbreviations, acronyms, coding)
- controls
- procedures (including technical correctness, format, and usability)
- job performance aids
- control room layout
- local control stations

The interviewer asks personnel about their experience with each of the HSI resources. Again, positive and troublesome aspects of the HSIs should be identified along with personnel evaluation of root causes and suggestions for improvements. This also provides an opportunity to obtain input on experiences personnel have with digital systems, generally.

Changes to control panels may impact other tasks, which are not the focus of the modification, either positively or negatively. During any interviews and walkthroughs, it is a good practice to also look for these "collateral" impacts. They include:

- Unintended consequences – tasks that are inadvertently hampered by changes that are made, e.g., changes made to a control panel may make doing other tasks more difficult
- Targets of opportunity – opportunities to positively impact tasks not directly involved with the modifications but which share resources with modified tasks

It might be possible for example, to improve a collateral task by relocating information that is currently located elsewhere in the control room and requires another operator to access to a new panel-mounted VDU. Thus, an opportunity may exist to address additional operating difficulties that are not directly related to the planned upgrades. Interviewed personnel can often identify such opportunities.

While this is a major focus in a later HFE activity (see Section 3.5 on Integrated Task Demands), OER provides an opportunity to examine these collateral effects very early in the process. It is also an opportunity to identify tasks that are risk-important and for which errors might have serious consequences. The OER should identify tasks that have been prone to errors in the past. These tasks should receive special attention during the design of the user interface to lessen the probability of error.

To summarize:

For task-oriented interviews and walkthroughs, be sure to:

- include operations, maintenance, and training personnel
- focus on the tasks that will be impacted by the modification
- discuss current work practices
- identify positive and negative feature of the current design
- ask personnel to verbalize their thought process
- ask personnel to identify especially positive or negative features of the tasks or the HSI (including procedures)
- ask about past experiences and any difficulties they have encountered
- ask about any aids that could potentially improve performance, efficiency, and safety
- ask for a root cause and suggestions for improvement for any negative features identified
- look for “workarounds” personnel use
- ask about potential “collateral” impacts, both unintended consequences and targets of opportunity

For HSI-oriented interviews and walkthroughs, be sure to:

- include operations, maintenance, and training personnel
- focus on the tasks that will be impacted by the modification
- ask about the experience in using the HSIs, including,
  - alarms
  - displays (including detailed aspects such as labeling, abbreviations, acronyms, coding)
  - controls
  - procedures (including technical correctness, format, and usability)

  - job performance aids
  - control room layout
  - local control stations
- ask about positive and troublesome aspects of the HSIs
- ask for a root cause and suggestions for improvement for any negative features identified
- ask about potential "collateral" impacts, both unintended consequences and targets of opportunity

3.2.3.4 Review Relevant Industry Experience

While OER related to the plant being modified is vital, the experience available in the nuclear industry in general is also a valuable source of information. This experience can provide lessons learned from modifications at other plants and facilities involving systems or HSI technologies that are similar to those under consideration for the upgrade.

Several sources of information should be evaluated:

- General Relevant Nuclear Industry Issues
- Relevant Operating Experience at Other Facilities
- Open Literature

The Appendix identifies some general HFE-related issues that have been observed in plants that have modernized.

3.2.3.4.1 General Relevant Nuclear Industry Issues

General issues addressing both safety and non-safety related experience of the commercial nuclear industry have been identified by organizations such as INPO, NRC and vendors. For example, in the area of safety related issues, NUREG/CR-6400 (Higgins and Nasta, 1996) provides a categorization of safety issues as follows:

- unresolved safety issues/generic safety issues
- TMI issues
- NRC generic letters and information notices
- low power and shutdown operations

Additional issues can be obtained from INPO's SEE-IN Program, the NRC's HFIS, and Owners' Groups. These issues should be reviewed to identify any that may be applicable to the types of plant changes to be made from the standpoint of I&C and HSI modernization. Some of these issues may be new to the plant being upgraded because they are associated with the new technologies being employed.

3.2.3.4.2 Relevant Operating Experience at Other Facilities

Where the modification incorporates technology that has not been used in the current plant, additional information on operational experience with similar systems in similar or comparable plants may need to be evaluated. In addition to design similarity, operating experience related to new technological approaches being considered in the current design should be evaluated. For example, if touch screen interfaces are planned, HFE issues associated with their use in actual plants can be obtained. Although plants obviously vary in their culture and practices, operating experience that indicates a feature has been problematic at another plant should be carefully analyzed before implementing that feature in the plant.

Perhaps the best way to obtain such information is by contacting other facilities. At a minimum, informed individuals at the other facilities can be “interviewed” and asked about their experiences. It would be even better to visit the facilities. This provides an opportunity for plant operators and maintainers to see the new systems first hand and discuss the benefits, drawbacks, and lessons learned directly with their counterparts at the other plants. Given the needs of the OER, non-nuclear facilities may be suitable, e.g., to enable operators whose experience has been primarily in an analog control room to see what screen-based monitoring and control is like. Many fossil power plants have upgraded to digital technologies that may be similar to those being considered.

This approach can be particularly effective in supporting the development of an endpoint vision when a utility is anticipating an upgrade with completely new technology, such as when a predominantly analog plant is upgrading with digital technology.

Topics to address in such contacts with other plants could include:

- Extent to which the technology has been implemented, and amount/duration of experience that has been gained
- Project management and coordination of contractors and subcontractors for the modification
- Design features and functions of the new systems and HSIs
- Operational and maintenance tasks and their importance to safety and economic plant operation
- Procedures impact and experience in their development and use
- Training and training facility issues
- Migration planning and implementation and familiarization of personnel
- Impact of automation and task changes on crew performance
- In-service monitoring and human performance results obtained
- Impact on maintenance and experience in maintaining the new system
- Overall scheduling of all activities
- Lessons learned and plans for future implementations of the technology

3.2.3.4.3 Open Literature

Another source of information is papers and reports available in the open literature. This is especially important when information from other facilities is not readily available. There are many sources of nuclear industry information related to large modernization programs that can provide applicable lessons learned. Some of these sources include:

- IAEA Reports and proceedings
- OECD/NEA Reports and proceedings
- ANS Transactions and proceedings
- IEEE Transactions and proceedings
- EPRI Reports
- DOE Reports
- NRC Reports
- Trade publications such as Nuclear Plant Journal

While utilities may not need to do an exhaustive literature search of these and other sources, a limited and focused search to identify literature directly related to the utility's modernization project is likely to provide information on lessons learned without a great deal of effort.

3.2.3.5 OER Item Classification

OER information is useful only if it is available to the appropriate personnel responsible for HFE. Since OER information can be relevant to many different parts of the organization, it is desirable to classify the information according to design topics for which it is relevant. Since at this stage, it may not be clear how an OER item should be addressed, the item should be included into to all relevant topics. This will help to ensure that the appropriate individuals on the design team can locate information of importance to their efforts.

General topics for classification include those listed in Table 3-2. For any given modification, there may be unique topics that should be added to the list or these topics may be further broken down, e.g., into the individual systems being upgraded.

3.2.3.6 Operational Support

In addition to classification of the design relevance of OER items, each should be prioritized based on its importance to the design effort. A qualitative evaluation of each item is recommended in terms of its direct relationship to the modernization project and its importance (see Figure 3-5).

With respect to relevance, some items will be directly related to the modernization program while others may not be. Those that are not can be identified as Priority 3. These are low priority for the modernization program and do not need to be addressed. It might be worth documenting Priority 3 items so they can be reevaluated in light of future changes.

Those items that are directly relevant should be evaluated in terms of their overall importance with respect to plant and personnel performance. Those that are significantly linked to production or safety goals and functions should be evaluated at Priority 1 and the others as Priority 2. Priority 1 items contain information that should be addressed in the design effort and a check on their resolution might be built into V&V activities. Priority 2 items may be addressed, (e.g. to provide improved consistency and to avoid cumulative effects of individual non-significant items) but the information is not deemed to be essential.

As an example, Example 3-2 provided two examples of items identified in an actual OER. The second example, modification of the RCP seal leak off return isolation under loss of seal injection and thermal barrier cooling, would should be considered a Priority 1 item because failure to do so can lead to seal degradation, possibly escalating to a seal loss of coolant accident. This event has a reasonable likelihood of leading to significant equipment damage.

The first example in Example 3-2 pertaining to alarm system design is probably a Priority 2 item. It certainly would be desirable to improve the DG trip alarm but failure to do so is not as likely to lead to problems as the RCP item. Operators do not have to take rapid action and can easily verify DG operation.

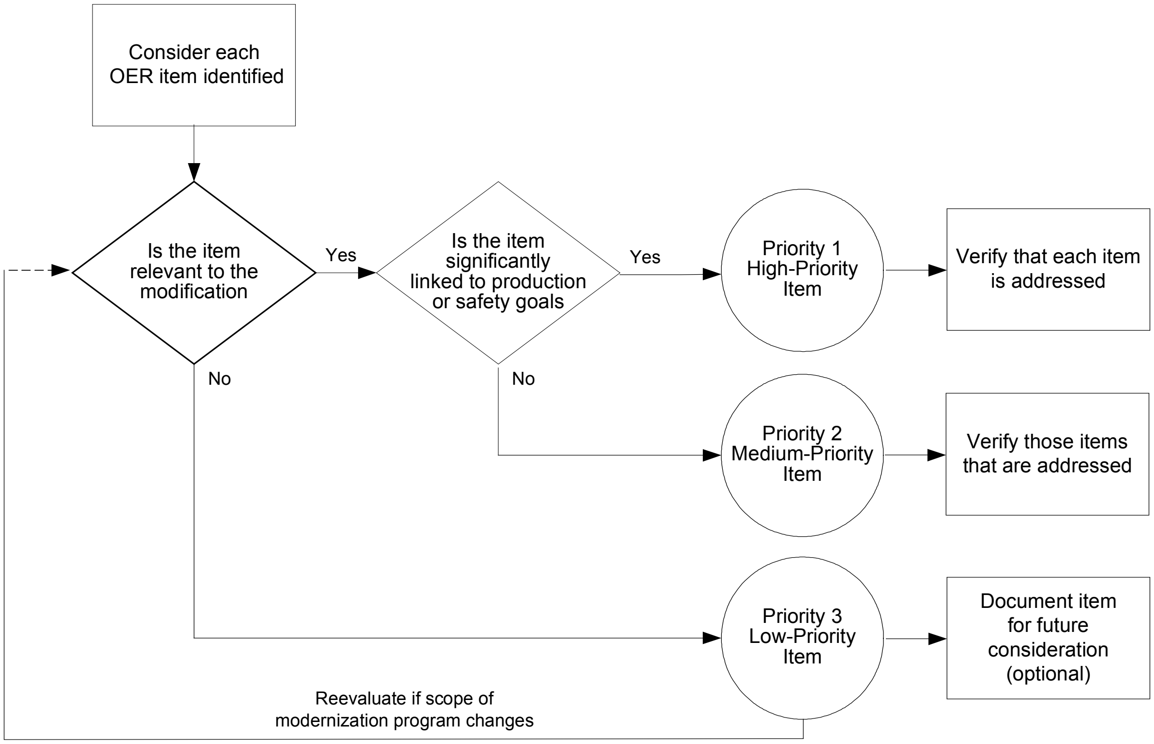
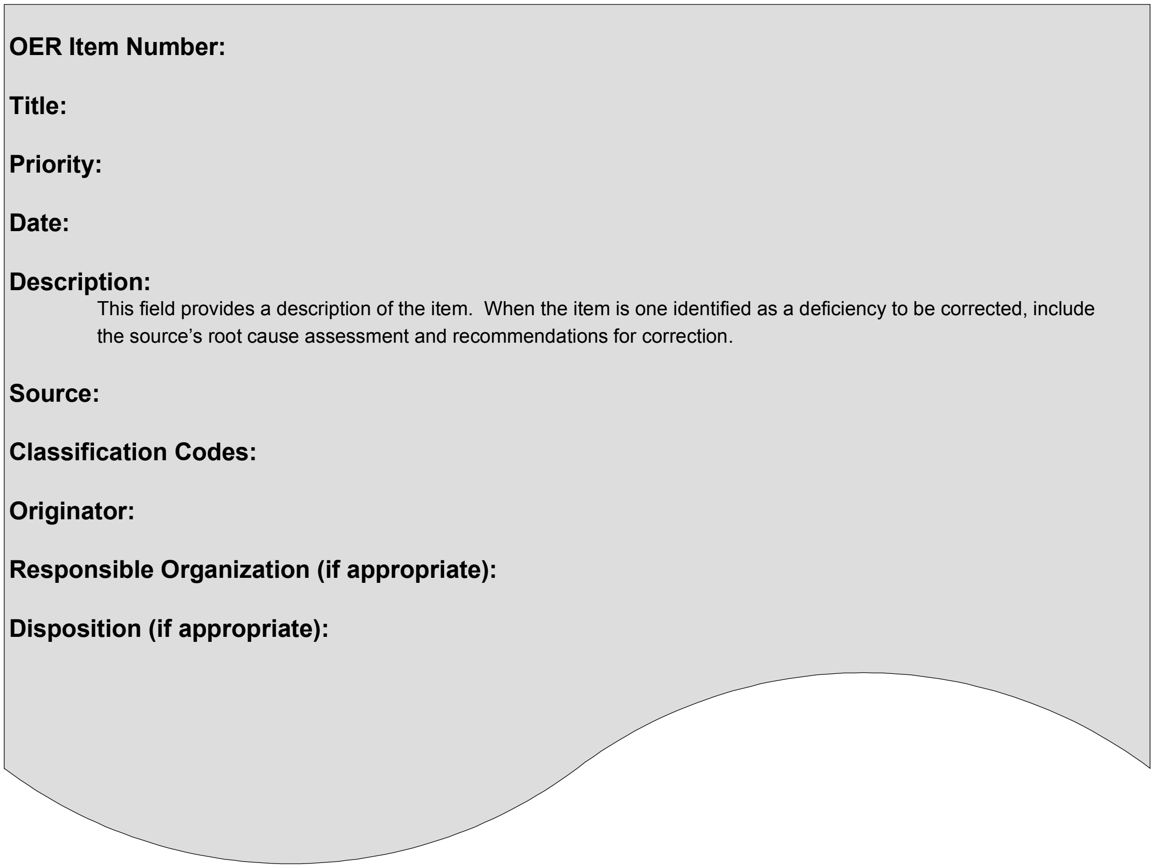

Consider each OER item identified
Is the item relevant to the modification
Yes
No
Is the item significantly linked to production or safety goals
Yes
No
Priority 1 High-Priority Item
Verify that each item is addressed
Priority 2 Medium-Priority Item
Verify those items that are addressed
Priority 3 Low-Priority Item
Document item for future consideration (optional)
Reevaluate if scope of modernization program changes

Figure 3-5
Prioritization of Operating Experience Review Items

3.2.4 Documentation

Individual OER findings having relevance to operations and design should be documented. Figure 3-6 illustrates suggested documentation fields of an OER item. To ensure maximum usefulness of the information, OER results must be accessible to members of the design team engaged in the relevant activities. As noted above, this is supported by a good topic classification scheme. The other important consideration is documentation of OER findings in a manner that makes the findings accessible. Thus in addition to traditional paper documentation, the more important findings might be considered for inclusion in a tracking system and text searchable database. This is especially useful for items that reflect design deficiencies that should be addressed as part of the modernization process. Each design function or organization should be made aware of the relevant OER information.

For a major upgrade, the results of the OER should used to identify the general functions and requirements that are expected in the final design of the automation, HSI, and procedures. Additional, more detailed documents on each specific aspects of design (e.g., soft controls, displays, alarms, control room layout) can be developed as warranted based on the scope of the plant modification. The documents should first, identify the operating needs based on the OER and the expected requirements stemming from the operating needs. OER documents will be used to support preparation of the related technical specifications.



OER Item Number:

Title:

Priority:

Date:

Description:

This field provides a description of the item. When the item is one identified as a deficiency to be corrected, include the source's root cause assessment and recommendations for correction.

Source:

Classification Codes:

Originator:

Responsible Organization (if appropriate):

Disposition (if appropriate):

Figure 3-6
Documentation of OER Items

3.2.5 Grading the OER Effort

Section 2.4.2, A Graded Approach to HFE, introduces the concept that the level of HFE effort for a modification should be based on the nature of the risk significance and complexity of the change. A methodology is provided to establish a grade for a modification in one of three levels: Level 1 – high risk, Level 2 – moderate risk, or Level 3 – low risk. The methodology presented in this section corresponds to a Level 1 effort. Modification programs engaged in Level 2 or Level 3 activities, may consider streamlining the methodology in the following manner. For all levels, aspects of the complete Level 1 methodology that may be useful to a particular utility's specific modification could also be included where clear benefits would be obtained.

For Level 2 projects, the OER should focus on HSI-driven OER (not the functional and task-analysis parts), and should include both in-plant and industry input. The methodology is summarized in Table 3-3. In addition, the results should be documented as discussed in Section 3.2.4.

Table 3-3
Level 2 OER Methodology

Methodology Section	Level 2 OER Activity
3.2.3.1 Inputs	include all
3.2.3.2 Identify the Functions, Tasks, and HSIs Impacted by the Modification	include HSIs only
3.2.3.3 Review Plant-Specific Experience	include only documented operating experience, HSI-oriented interviews and walkthroughs
3.2.3.4 Review Relevant Industry Experience	include only "Relevant Operating Experience at Other facilities"
3.2.3.5 OER Item Classification	omit
3.2.3.6 OER Item Prioritization	omit

For Level 3 OER, OER information can be obtained from the plant's corrective action and lessons learned database. However, if the design team thinks there are circumstances that such information is too limited, consider supplementing that information with interviews with personnel that focus directly on the HFE aspects of the plant that are being modified.

3.2.6 Use of the Results

As noted earlier, OER information has broad application in a plant modernization program. Table 3-4 illustrates some of its uses within the context of endpoint definition and the other HFE activities. Beyond this, based on OER, positive credit can be taken for technologies that have successful operating histories at the plant, other nuclear plants, or in a different industry. In addition, OER information can be used to support the preparation of technical requirement.

Table 3-4
Use of OER Information

HFE Analysis Topic	OER Contribution
Endpoint Vision Planning	• Identify desired changes to operation or maintenance • Identify general control room design concept
Function Analysis and Allocation	• Identify a need for allocation modifications • Identify a basis for initial requirements • Identify a basis for initial allocations
Task Analysis, Human Reliability Analysis, and Staffing/Qualifications	• Identify risk-important human actions and errors • Identify problematic operations and tasks • Identify staffing shortfalls
Human-System Interface, Procedures, and Training Development	• Identify potential design issues • Identify potential design solutions • Identify proven technology
Human Factors Verification and Validation	• Identify tasks to be evaluated • Identify events and scenarios to use • Identify performance measures

3.2.7 Appendix –HFE-Related Issues Arising in Plant Modernization Programs

This appendix is identifies issues that have been found in plant modernization programs when HFE has not been appropriately addressed. The issues are listed in Table 3-5. They are presented for two purposes. First, information on issues that have arisen at other plants that have modernized can help utilities who are just beginning an I&C modernization program be better prepared. The second reason is to emphasize that the guidance provided in this document can help utilities to minimize or avoid the issues and, thus better achieve the potential benefits of the modernization.

Table 3-5
HFE-Related Issues Found in Plant Modernization Programs

Impact on Individual and Team Performance
- Plant personnel may not at first favor new technology, but will eventually - The impact of modifications on personnel is not always obvious - New technology can be poorly designed from the user’s standpoint - Computer-based HSIs can add to overall complexity - New technology has unanticipated consequences - Personnel do not always use HSIs in the way designers expect
Organizational and Programmatic Considerations
- Knowledge gaps early in a modification project can be problematic - Plant personnel involvement in the modernization process increases over time and is often more than expected - The original endpoint vision is often not achieved - Computer-based systems may change staffing, training, and procedure requirements - Coordination of plant modifications with ongoing training and operational demands is a challenge

Impact on Individual and Team Performance

Plant personnel may not at first favor new technology, but will eventually – Many control rooms have remained relatively unchanged, except for minor improvements and modifications, for decades. Over the years, through training and experience, crewmembers develop expert knowledge and skills for monitoring and operating the plant with the HSIs provided. When new technology is initially introduced, it is not always embraced by plant personnel. When faced with the prospect of significant changes, many crewmembers are reluctant to change. However, experience has shown that after training with the new HSIs and an initial period of familiarization, operators generally do not want to return to the old technology. The transition to the new technology is facilitated when operator input is sought and utilized in the design of new HSIs.

The impact of modifications on personnel is not always obvious – While some changes in the plant have relatively obvious effects, such as the creation of new tasks that have to be performed, other changes are more subtle. For example, at a high level a task may be unchanged, e.g., the operator has to align a system in a certain way. But at a more detailed level, the way the task is performed may be very different, e.g., a series of displays have to be retrieved from a computer system and the operator has to use on-screen “soft controls” to change the status of the equipment. To crewmembers accustomed to manipulating switches on a control board, this new type of operation is very different. Perhaps more significantly, the new systems may result in modified task demands, e.g., operators may have to manipulate a valve control differently when implemented using a digital system if the rate at which the valve is commanded to open or close is different from the existing implementation. Thus personnel tasks can be changed by plant modifications in subtle ways.

New technology can be poorly designed from the user’s standpoint – There is a common tendency to equate new technology with better design. However, this is not necessarily the case. Some relatively common examples are:

- personnel may experience data overload with digital systems (too much data and too many alarms)
- poor organization of information can make some operational tasks more difficult
- greater cognitive workload and time, which may be required to work with and manage the computer-based interfaces, can distract personnel from plant monitoring and control tasks

Computer-based HSIs can add to overall complexity – Computer-based systems add to the overall complexity of the plant. As the computer-based systems incorporate more automation and intelligence, the complexity factor may increase. Crews can have difficulty understanding what the computer system is doing, in part because the behavior of computer-based systems, if not designed properly, is often not sufficiently observable and the capability to make inquiries is inadequate. Further, computerized systems can make mistakes. Therefore, personnel must know the appropriate uses and limitations of the new HSIs.

New technology has unanticipated consequences – New computer-based technology can have unanticipated consequences for team and individual performance. In one example where a computer-based procedure system was introduced, the new HSIs unexpectedly altered the roles and responsibilities of crewmembers and the way they worked as a team.[1]

Personnel do not always use HSIs in the way designers expect – Plant personnel adopt numerous strategies to create workarounds and aids to correct for limitations in designs. As an example, computer-based control rooms are designed with vast amounts of data, available through hundreds and sometimes thousands of displays, and viewed by the operator through a limited number of display devices. Designers expect that operators will use the flexibility of the computer-based interfaces to access many of these displays and configure the HSI in such a way that it is ideally tailored to the unique demands of the current situation. However, because of the workload involved, operators frequently do not follow this strategy. Instead, they configure their HSI as a fixed and spatially dedicated interface and use that configuration for a variety of situations that might arise.

Organizational and Programmatic Considerations

Knowledge gaps early in a modification project can be problematic – The initial knowledge gap between a utility in the beginning stages of an I&C/HSI modernization program and their vendor/supplier can be significant and problematic. Misunderstandings can arise between utility expectations and the vendor interpretations of what the utility wants. As the utility gains knowledge and familiarity with the new technology, they frequently recognize that modifications to their plans are needed, often at additional time and cost.

One important consequence of this is that their "endpoint vision" (their vision of what the control room and HSIs will be like once all modifications are completed) changes. Utility expectations often start out quite modest, e.g., wishing to minimally impact the control room by making small-scale "replacements in kind." However, as their familiarization with the technology increases and they become more aware of what beneficial functionality can be readily introduced into the control room, e.g., alarm reduction techniques, powerful information processing and display approaches, and computerized procedures, the endpoint vision changes and becomes more ambitious. Of course, changing the endpoint vision can be challenging for vendors who must modify their design approach.

Plant personnel involvement in the modernization process increases over time and is often more than expected – At the beginning of the modernization process, utilities sometimes expect a "turnkey" process. That is, following the selection of a vendor/supplier, the vendor will design and install the new systems with minimal involvement of utility personnel. However, they quickly learn that modernization is not a turnkey process. Instead, as time goes on, the demands for utility personnel involvement increase. While this is a natural result of adapting vendor approaches to the unique plant design and operational practices of a specific plant, it is often not fully anticipated. A changing endpoint vision is a contributing factor as well; utilities begin to identify modifications to the new systems they would like to have to better meet their needs.

[1] For more information about this plant's experience, see 3.5, Staffing, Qualifications, and Integrated Work Design and specifically Example 3-4, Example of the Impact of Technology on Teamwork.

The original endpoint vision is often not achieved – Extensive digital I&C modernization programs often take many years to complete. Over time, circumstances may arise that make it necessary to cut back on the extent of the endpoint vision. This possibility emphasizes the importance of having an adaptable plan or “migration strategy” that leaves the plant in an acceptable configuration after each individual modification is completed.

Computer-based systems may change training requirements – Operation of the HSI is often a skill that is learned on the job and typically little attention is devoted to it in formal training. However, with computer-based HSIs there is a greater training burden because, with added HSI functionality, there is more to know about how data is processed, how system modes affect user inputs, and what strategies are needed to manage the interface (e.g., information access, navigation, and workstation configuration). In fact, one of the most common complaints of operators following the introduction of computer-based interfaces is that they received little training in the proper use of the functionality of the new HSIs; hence, operators evolve their own strategies. Thus, well-planned training in the design and use of HSIs is necessary.

Coordination of plant modifications with ongoing training and operational demands is a challenge – Coordination of design activities, i.e., implementation of upgrades, simulator modifications, and ongoing training, is a significant challenge. The challenge is even greater at multi-unit sites where some of the details of the upgrade design and the upgrade schedule are different between plants.

3.3 Function Analysis and Allocation

3.3.1 Introduction

3.3.1.1 Overview of Function Analysis and Allocation

3.3.1.2 The Changing Concept of Automation

3.3.1.3 Application to Plant Modifications

3.3.2 Objective

3.3.3 Methodology

3.3.3.1 Inputs

3.3.3.2 Identify Changes to Functions and Allocations

3.3.3.3 Conduct Function Analysis

3.3.3.4 Conduct F/T Allocation Evaluation

3.3.3.5 Evaluate Overall Personnel Role

3.3.3.6 Verify F/T Allocations

3.3.4 Documentation

3.3.5 Grading the Function Analysis and Allocation Effort

3.3.6 Use of the Results

The primary purpose of the analyses described in this section is to allocate functions to automatic systems, plant personnel, or to some combination of the two. The allocation is based on a function analysis and considers the general design implications of how functions were allocated.

The term function allocation as used here simply refers to the allocation of responsibility for conducting an activity to plant personnel, to automatic systems, or to some combination of the two. The allocation is made on the basis of a function analysis, determining what is required to perform the function. Using the results of the function analysis, responsibility is allocated in a way that best ensures overall accomplishment of the function.[2]

With respect to plant modernization programs, much of the focus is on changes that are made to how functions are performed as a result of new design goals, new plant systems, and new capabilities offered by digital I&C systems and HSIs. In this section, we will discuss how these changes should be detected and considered in the design.

3.3.1 Introduction

This introduction provides a brief general overview of function analysis and allocation, followed by a discussion of its application to plant modernization programs.

3.3.1.1 Overview of Function Analysis and Allocation

A function is a process or activity that is required to achieve a desired goal. The term function can refer to very high-level plant functions, such as critical safety functions, or merely the functioning of an individual piece of equipment, such as a valve or a wall-panel information display system. Examples of high-level functions are reactivity control, containment integrity and Reactor Coolant System (RCS) water mass inventory control. Thus, functions are essentially hierarchical. Plants have a natural hierarchical structure of functions, processes, systems, and components. Figure 3-7 provides a simple illustration of the functions associated with a mission to supply power to the grid (see Section 4.2 of this document and O'Hara, et al. (2003) for a detailed discussion of this concept). Functional decomposition and analysis for commercial nuclear plants is addressed in many documents, most notably IEC Standard 61839 (IEC 2000).

High-level functions can be described without reference to specific plant systems or to the level of human/machine intervention that is required to accomplish the function. High-level functions are usually accomplished through some combination of lower-level system actuations such as reactor trip, safety injection, or accumulators, and may require human action. Often plant systems are used in combination to achieve a higher-level function. Human involvement may be needed at any or all levels of this functional structure.

[2] There are two other "allocations" that are important to the HFE aspects of the plant: allocation of tasks to individual crewmembers and allocation of tasks to physical locations, e.g., the control room or a local station. Those two aspects of allocation are addressed in Sections 3.5 and 3.7 respectively.

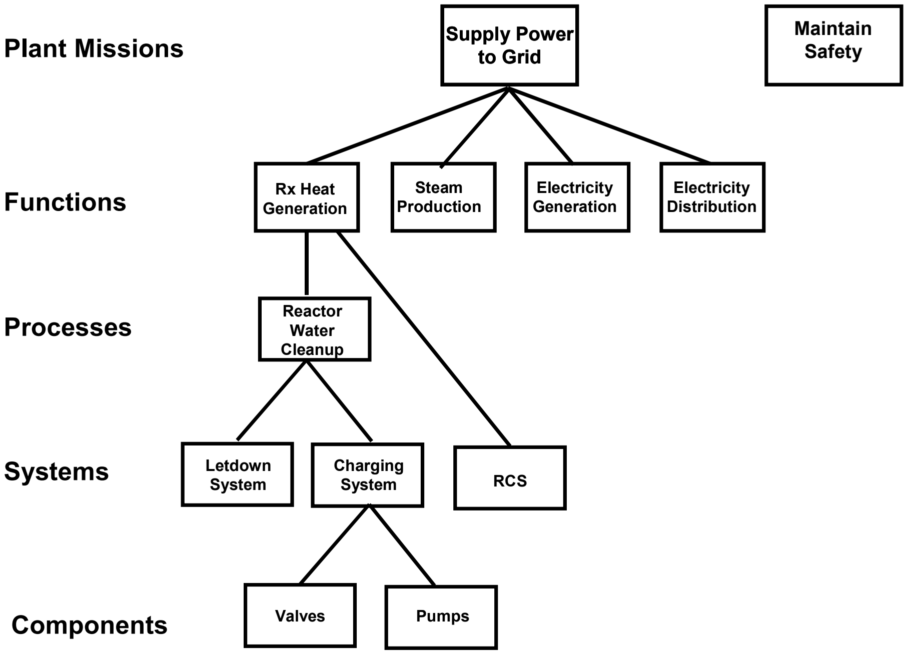


Figure 3-7
High-Level Functions of a Nuclear Plant

As functions are analyzed, their requirements become better defined. At some point, those functions or parts of a function are assigned to the available resources, which include hardware, software, and human elements. The overall purpose of function analysis and allocation is to ensure that functional requirements are sufficiently defined and analyzed so that the allocation of functions to human and machine resources can take advantage of human strengths and avoid human limitations; i.e., to make use of automation and human capabilities in a way that maximizes overall function accomplishment. The term “automation” is used broadly to include automation of a function, process, system, component or supporting level (e.g., automatically capturing data needed for archival purposes rather than entering by hand) (Section 3.3.1.2, The Changing Concept of Automation, has a detailed discussion of this topic).

Decisions about automation shape the role of personnel in plant operations, defining the specific responsibilities personnel will have in accomplishing plant functions and the activities they will perform. How these responsibilities are defined impacts several aspects of human performance. Since human performance is essential to the overall plant performance, design decisions that have a negative impact on human performance can ultimately compromise plant performance. The most significant negative impacts on human performance associated with automation are:

- *Loss of situation awareness* – greater degrees of automation are often associated with a loss of situation awareness, or at least greater difficulty in gaining situation awareness.
- *Loss of vigilance due to trust and complacency* – when personnel come to trust the automation, they can become complacent and less vigilant in monitoring its performance. Personnel will thus become less likely to intervene when they should.

- *Workload extremes* – greater automation is often associated with lower workload (sometimes to the point of boredom) when the automation is functioning properly and periods of extreme workload when the automation fails and personnel must intervene
- *Degradation of Skills* – since automatic systems are usually reliable, human performance of the function is rare and personnel skills for performing the actions may be poor.

Thus, changes to the role of plant personnel introduced by new systems should be carefully considered.

3.3.1.2 The Changing Concept of Automation

In many older plants, the allocation of function process was fairly simple. Functions were either automated (i.e., controlled automatically) or manually performed by plant personnel. However, as computers have become more involved in process control, the nature of automation has changed. Two issues: varying degrees of automation and automation beyond controls are discussed below.

3.3.1.2.1 Varying Degrees of Automation

With modern computer and control technology automation is no longer "all or none." A process function does not have to be either automatic or manual. It can be both. Greater integration of human and automatic processes in the same control activity helps minimize the negative effects on human performance discussed above and provides a more flexible application of automation. This takes several forms. For example, control of a process can be shared. A process sequence is broken up into discrete chunks and the chunks are automated. However, transition from one chunk to the next requires human intervention. The startup process in one of the advanced light water reactor designs is an example of this type of approach. A similar application is when a control sequence can be partially automated, but human intervention is needed to provide information not available to the automatic controller.

Another type of automation is dynamic allocation. In this case, a function can be performed by either automatic systems or by humans. The decision as to who controls the function is made dynamically based on situational considerations, such as the overall workload of personnel.

3.3.1.2.2 Automation Beyond Controls

Historically "automation" has meant automating a control function or process. However, computer-based systems offer the opportunity to provide "intelligence" in the HSIs themselves to "automate" cognitive activities typically performed as part of the decision-making by plant personnel.

In this context, the term "agents" is often used to generically refer to who/what is performing an activity; i.e., agents are entities that do things. Figure 3-8 illustrates the generic activities an agent must perform so that functions can be achieved. The agent must monitor the plant to detect conditions indicating that a function has to be performed. The agent must assess the situation and plan a response. Once the response plan is established, the agent implements the plan by sending control signals to actuators. The agent must also monitor the function to determine that the function is being accomplished and to replan if it is not. Finally the agent must decide when the function has been satisfactorily achieved.

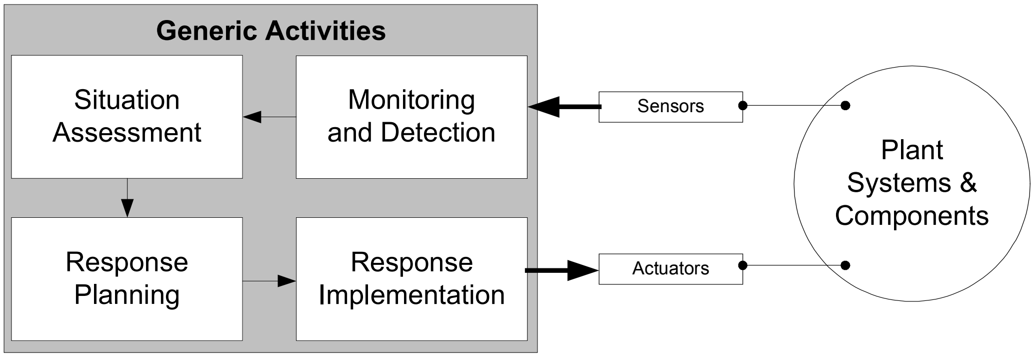


Figure 3-8
Generic Activities Performed by Agents

Human or machine agents can perform any or all of these activities. Figure 3-9 provides some examples of various levels of human and automatic responsibilities for process control as well as for the generic activities shown above.

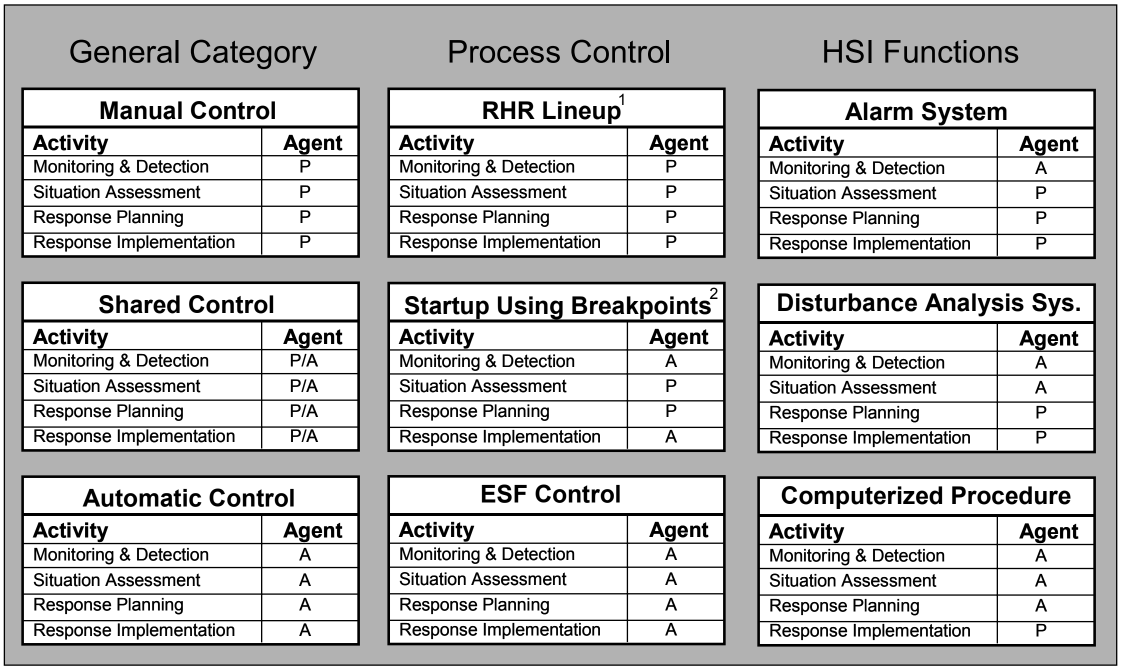
An "alarm system," for example, is an automated monitoring system that alerts operators via visual and/or auditory displays when parameters deviate from specified limits or set points. However, as more and more functionality is given to HSIs, they evolve toward automatic systems. For example, the only difference between a typical computer-based procedure and an automatic process system is the control. The procedure can monitor, assess, and plan a response (essentially a paper procedure is a response plan strategy). Most computer-based procedures (CBP) stop at that. If a CBP is also given the means to initiate control signals, it becomes an automatic system.

Some additional examples include:

- Calculation of time to boiling of the primary coolant for a PWR and presentation on a display (when plant conditions warrant)
- Automatic calculation of time to trip for trip variables
- Automatic display selection whereby the system indicates that there are situationally relevant displays to look at, such as through a special icon, and the operator then can opt to accept them or not

When all of these activities are completely accomplished by plant personnel, the function is said to be "manual." When all of these activities are completely accomplished by machine agents, the function is said to be "automated." When both human and machine agents are involved, the function is "shared."

As discussed earlier, functions are hierarchical. The analysis of functions and their allocation is also hierarchical. When focusing on the human role accomplishing functions, break human actions down into tasks to be performed. While a function may be primarily a human responsibility, some of the more detailed tasks may be automated. Thus, we will apply the allocation concept to both functions and tasks. The allocation process (deciding what is automated and what is not) can be performed iteratively as the design becomes more detailed. While this type of analysis is called function allocation, in reality the allocation can be at the level of an entire function or the tasks that are performed to accomplish the function. To simplify the language, this text uses the acronym F/T.



General Category

Manual Control

Activity	Agent
Monitoring & Detection	P
Situation Assessment	P
Response Planning	P
Response Implementation	P

Shared Control

Activity	Agent
Monitoring & Detection	P/A
Situation Assessment	P/A
Response Planning	P/A
Response Implementation	P/A

Automatic Control

Activity	Agent
Monitoring & Detection	A
Situation Assessment	A
Response Planning	A
Response Implementation	A

Process Control

RHR Lineup[1]

Activity	Agent
Monitoring & Detection	P
Situation Assessment	P
Response Planning	P
Response Implementation	P

Startup Using Breakpoints[2]

Activity	Agent
Monitoring & Detection	A
Situation Assessment	P
Response Planning	P
Response Implementation	A

ESF Control

Activity	Agent
Monitoring & Detection	A
Situation Assessment	A
Response Planning	A
Response Implementation	A

HSI Functions

Alarm System

Activity	Agent
Monitoring & Detection	A
Situation Assessment	P
Response Planning	P
Response Implementation	P

Disturbance Analysis Sys.

Activity	Agent
Monitoring & Detection	A
Situation Assessment	A
Response Planning	P
Response Implementation	P

Computerized Procedure

Activity	Agent
Monitoring & Detection	A
Situation Assessment	A
Response Planning	A
Response Implementation	P

Note: "P" means personnel perform the activity and "A" means the task is automatic

[1] In a BWR during suppression pool cooling mode

[2] In the ABWR, breakpoint logic is used for partial automatic startup

Figure 3-9
Examples of Allocations

3.3.1.3 Application to Plant Modifications

With respect to plant modernization, the main focus of function analysis is on changes to the way functions are accomplished. High-level plant functions are seldom changed, however, modernization programs often change plant systems and HSIs in ways that alter the role of personnel, for example, by automating activities previously performed by operators. The automation can involve an entire process control sequence or it can be applied to the generic activities involved in decision-making.

Most often these changes are a deliberate and intended consequence of the modification. Some modifications make minimal changes to the level of automation and the allocation of F/Ts. However, even when an overall change in the level of automation is not an explicit goal of the modernization project, the specific F/Ts of the operator or technician may be changed. In all cases, however, the designer must ensure that if the F/T allocations are changed, these changes are recognized and their impact on performance analyzed.

When allocation of F/Ts is considered for plant changes, comparing to the baseline or existing design simplifies the analysis. Unlike completely new designs, the allocation process is not started from scratch.

3.3.2 Objective

The objective of this analysis is to specify the roles and responsibilities of plant personnel performing plant functions and tasks, and how those roles may change as a result of the planned modification. The methodology:

- evaluates F/Ts that may be impacted, both deliberately or inadvertently, by the changes made to plant systems as part of the plant modernization project
- evaluates the suitability of full automation, partial automation, and manual F/T performance
- identifies the design consequences of allocation decisions
- provides a basis for allocation decisions

3.3.3 Methodology

An overview of the analysis is shown in Figure 3-10. The complete methodology is for a Level 1 analysis. For recommendations on grading the methodology, see Section 3.3.5. The analysis is performed iteratively as the design evolves. At first, allocations may be qualitatively performed for higher-level functions and later more quantitative assessments are made for the detailed tasks, as discussed below.

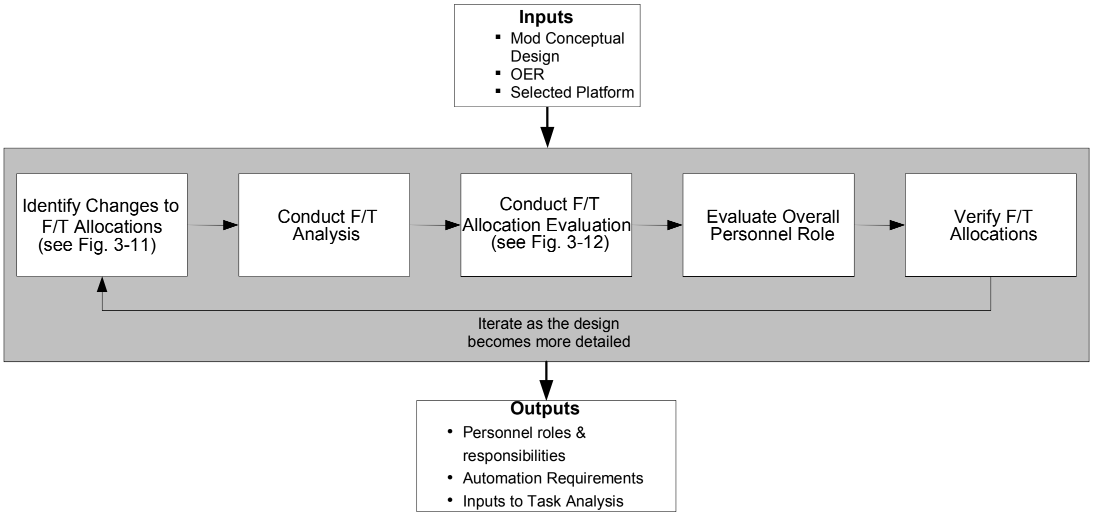

Inputs
▪ Mod Conceptual Design
▪ OER
▪ Selected Platform
Identify Changes to F/T Allocations (see Fig. 3-11)
Conduct F/T Analysis
Conduct F/T Allocation Evaluation (see Fig. 3-12)
Evaluate Overall Personnel Role
Verify F/T Allocations
Iterate as the design becomes more detailed
Outputs
• Personnel roles & responsibilities
• Automation Requirements
• Inputs to Task Analysis

Figure 3-10
Overview of Function Analysis and Allocation

3.3.3.1 Inputs

The conceptual design for the modification is a key input to this analysis. The concept design describes what performance is expected of the systems being modified. OER results conducted subsequent to the modification authorization may have identified opportunities for automation to be addressed in the design. Finally, the selected platform is a key consideration. Specific vendor platforms include a specific approach to automation. The consistency of this approach to that identified in the concept design or the OER needs to be evaluated.

3.3.3.2 Identify Changes to Functions and Allocations

As part of OER (see Section 3.2), the functions, tasks, and HSIs involved in the plant modification are generally identified. In this analysis, these changes to functions and tasks are examined in greater detail.

Changing functions and the level of automaton may be one of the design goals of the plant modification. In that case, the input mainly comes from the modification conceptual design, the overall endpoint vision, or from the review of operating experience. The utility’s endpoint vision and the specific goals for the current modification may include objectives that might be achieved by changes to automation, e.g.:

- to increase some aspect of efficiency or productivity (e.g. to reduce system start-up time)
- to reduce or eliminate the opportunity for human error, although use of automation may result in increased opportunity for other kinds of human error
- to change staffing responsibilities, e.g., to perform normal control room operations with a single operator
- to reduce overall staffing

Another driver is the review of OER. The OER may have identified difficult or troublesome operations that can be addressed by changing the way functions are performed or allocated, e.g., by introducing additional automation. Similarly, the OER may have identified some troublesome aspects of an automated system that could be addressed by increasing the level of human involvement in the F/T accomplishment. An example is when there are situations where the decision to initiate an automatic sequence cannot be made solely on information available to the automatic control system. The OER may have indicated that an automatic sequence was incorrectly initiated on past occasions. One solution may be to build a hold at some point in the automatic process to allow time for an operator to control whether the sequence proceeds based on information not available to the automatic system.

The OER may also identify difficult, time-consuming, and/or error-prone evaluations or mental calculations that users must make that should be automated.

A third input comes at the time a supplier is chosen for a plant modification. Vendor products include an allocation of functions that is not readily modified as an integral imbedded part of the design. A vendor’s product may not provide all of the allocations that were specified in the endpoint vision or OER and they may inadvertently change automation in ways not part of the endpoint vision or OER results.

A comparison of the vendor design and the desired changes in allocation can have three possible results:

- Functions and allocations are changed in accordance with desired changes
- Desired function and allocation changes are not accomplished
- Functions and allocations are changed that were not identified as desired (including any additional tasks necessitated by the design change that were not performed in the old design).

These results should be analyzed to determine their acceptability.

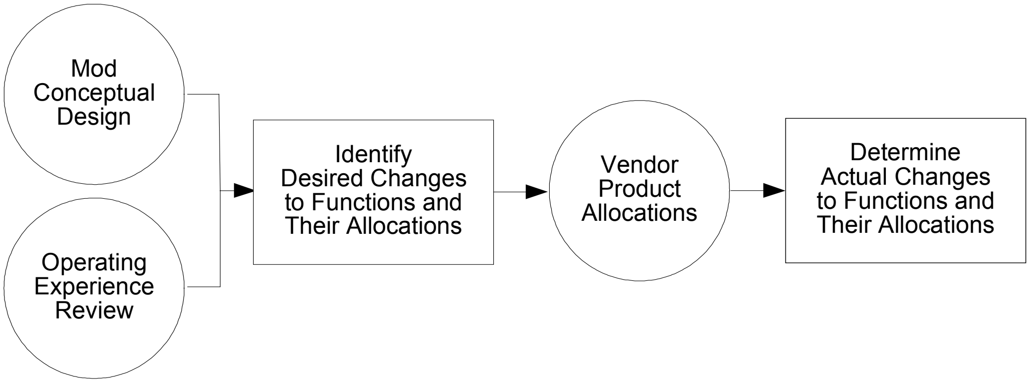

Mod Conceptual Design
Operating Experience Review
Identify Desired Changes to Functions and Their Allocations
Vendor Product Allocations
Determine Actual Changes to Functions and Their Allocations

Figure 3-11
Identify Changes to F/T Allocations

3.3.3.3 Conduct Function Analysis

In this step, the impact of plant modifications on functional requirements and performance is assessed and the F/Ts are characterized. Function analysis is the identification of those functions that must be performed to satisfy the plant's goals and objectives at any level in the functional hierarchy. It is conducted to:

- Determine the objectives, performance requirements, and constraints of the design
- Define the activities that must be accomplished to meet the objectives and required performance
- Define the relationships between functions and plant processes (e.g., plant configurations or success paths) responsible for performing the function
- Provide a framework for understanding the role of agents (whether personnel or machine) for controlling plant processes

Function characterization includes:

- Purpose of the function
- Cues indicating that the function is required

- Cues indicating that the function is available (the systems/means of performing the function that are available)
- Actions needed to perform the function
- Time and performance requirements and constraints for performing the function
- Information that indicates the function is operating (the system/means of performing the function are operating, e.g., flow indication)
- Information that indicates the function is achieving its purpose (e.g., reactor vessel level returning to normal)
- Information that indicates that operation of the function can or should be terminated
- Potential failures of the function and alternative means for function attainment
- Cues to identify each of the postulated failures

The level of description of these elements of the characterization begins at a general level and becomes better defined as the design details emerge. For example, the term "information" may mean the identification of some triggering event when a function is described at a high level, but later it can mean some parameter (or set of parameters) that more precisely define the event.

3.3.3.4 Conduct F/T Allocation Evaluation

The changes in allocation should be evaluated to make sure they are suitable. The focus at this point is on the changes that were made; however, the next section considers the impact of those changes on the overall functions and tasks that personnel perform.[3]

The process for analyzing F/T allocations is shown in Figure 3-12. As the whole function analysis and allocation process is iterative, this analysis can begin at the earliest stages of the modification planning. Allocations can be refined or tweaked as more information about performance is known and evaluations are conducted.

Each of the proposed changes in allocation should be evaluated using the flow diagram in Figure 3-12.[4] Consider first whether an allocation is mandatory; e.g., required by regulatory requirements. If it is, ensure that the function allocation is consistent with the requirements.

For those that are not mandatory, determine whether the F/T is automatic or not. If it is automatic, an evaluation should be performed as to whether there is some need for human involvement. The following are typical reasons for human involvement in an otherwise automatic task:

- There are situations where circumstances could make the automatic response inappropriate and it is difficult to build these considerations into the control logic, e.g., if the information for one of the signaling conditions to prevent an automatic sequence is not available to the system or highly subjective decisions are required.

[3] The assumption made is that the F/T allocations of the old design are acceptable unless identified as requiring a change during the OER.

[4] There are certain F/Ts for which there is no compelling reason to allocate either to human or machine agents. In that case, the allocation can be kept as assigned, unless later evaluations identify reasons to change.

- It is desirable to keep personnel “in the loop” in the event that they have to take over control
- It is important to keep personnel involved to support their other F/T responsibilities
- As a deliberate activity to require attention and effort in order to preclude boredom

In all such cases, the added human involvement should not defeat the purpose of the automation due to the demands on personnel related to F/T requirements and characteristics (discussed below).

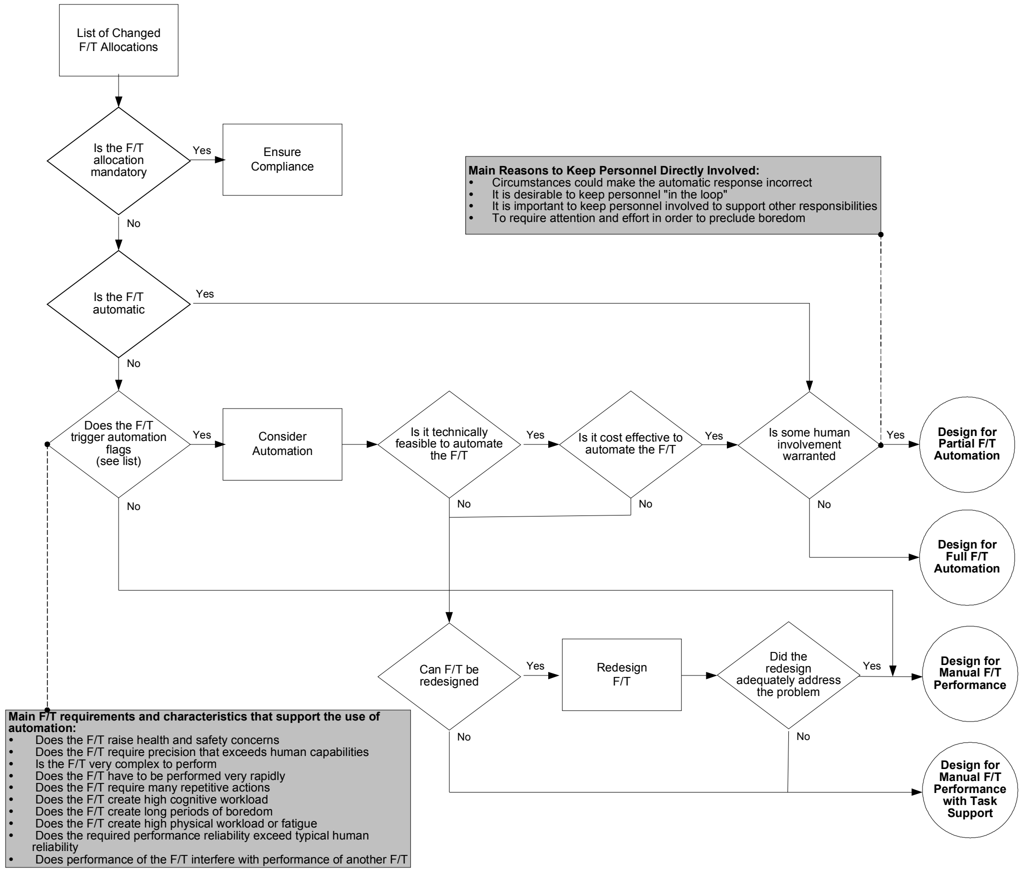

List of Changed F/T Allocations
Is the F/T allocation mandatory
Yes
Ensure Compliance
No
Main Reasons to Keep Personnel Directly Involved:
• Circumstances could make the automatic response incorrect
• It is desirable to keep personnel "in the loop"
• It is important to keep personnel involved to support other responsibilities
• To require attention and effort in order to preclude boredom
Is the F/T automatic
Yes
No
Does the F/T trigger automation flags (see list)
Yes
Consider Automation
Is it technically feasible to automate the F/T
Yes
Is it cost effective to automate the F/T
Yes
Is some human involvement warranted
Yes
Design for Partial F/T Automation
No
No
No
No
Design for Full F/T Automation
Can F/T be redesigned
Yes
Redesign F/T
Did the redesign adequately address the problem
Yes
Design for Manual F/T Performance
No
No
Design for Manual F/T Performance with Task Support
Main F/T requirements and characteristics that support the use of automation:
• Does the F/T raise health and safety concerns
• Does the F/T require precision that exceeds human capabilities
• Is the F/T very complex to perform
• Does the F/T have to be performed very rapidly
• Does the F/T require many repetitive actions
• Does the F/T create high cognitive workload
• Does the F/T create long periods of boredom
• Does the F/T create high physical workload or fatigue
• Does the required performance reliability exceed typical human reliability
• Does performance of the F/T interfere with performance of another F/T

Figure 3-12
F/T Allocation Analysis

If none of these reasons exists, then full automation is suggested. Note that this does not mean personnel will not have to be aware of the automatic actions (see design implications below). If some human involvement is warranted, then some of the basic activities needed to perform the F/T should be designed for partial automation. An example of this presented earlier is the need to keep operators aware of status of startup systems in the design of the advanced light water reactor startup.

If the change in allocation is a manual action, evaluate if any F/T requirements and characteristics raise concerns over the suitability of the task for personnel. Specifically, automation should be considered for any F/Ts having these requirements and characteristics:

- *The F/T raises health and safety concerns* – F/Ts that are associated with risks to the health and safety of personnel are candidates for automation.
- *The F/T requires precision that exceeds human capabilities* – F/Ts may require a degree of precision that is too great for human performance.
- *The F/T is very complex to perform* – Some tasks can be complex for personnel to perform, yet very easy for computers to perform. Solving complex Boolean logic is one example of such a task.
- *The F/T has to be performed very rapidly* – F/Ts that require actions to be performed very rapidly (within a few seconds) are candidates for automation.
- *The F/T requires many repetitive actions* – When many repetitive actions are required, such actions can produce fatigue and boredom that can negatively impact human performance.
- *The F/T creates high cognitive workload* – even though a task is not complex, it can still be very cognitively demanding, e.g., it may require attention to too many details simultaneously or may rely very heavily on memory for a great deal of information.
- *The F/T creates long periods of boredom* – Human performance not only suffers from high workload, it can suffer from too little workload as well. Tasks that create long periods of boredom are not well suited to human performance.
- *The F/T creates high physical workload or fatigue* – just as F/Ts can be cognitively demanding, they can be physically demanding as well. Personnel performance of such a F/T will become worse under those conditions.
- *The required performance reliability exceeds typical human reliability* – As with equipment, any human action is subject to error. In a plant PRA, this error probability may be represented as an human error probability (HEP). If the risk of F/T failure is unacceptably high when performed by personnel, then automation should be considered. For example, using human reliability analysis (HRA), if the HEP for the human action is estimated to be 10-2 and that value leads to unacceptable risk, then automation should be considered.
- *Performance of the F/T interferes with performance of another F/T* – Sometimes, while manual performance of a F/T may seem warranted, performance of the new F/T may interfere with another F/T that needs to be performed at about the same time.

It must be determined whether it is technically feasible to automate the task; and if so, whether it is cost effective. Automating a F/T may be a relatively simple matter of adding already existing functionality to a vendor's design. In other cases, it may be technically feasible, but require an extensive development effort and thus not be cost effective relative to the impact of human performance issues.

If automation is a possibility, then the desirability of maintaining some level of human involvement should be evaluated (as is discussed above).

There are other cases where it is not possible to automate. In this case, F/T redesign should be considered, i.e., alternative means to accomplish the F/T that can eliminate or reduce the undesirable F/T requirements and characteristics. A redesign could involve:

- Modifying performance requirements by making system changes
- Modifying the way in which a F/T is performed, e.g., changing the task sequence
- Increasing the staffing available to perform the task

If efforts to redesign the F/T are successful, then manual performance may be acceptable. If the F/T requirements and characteristics cannot be redesigned and automation is not possible, then enhanced task support may be used (such as very detailed task procedures or computerized operator support systems).

This analysis leads to four possible outcomes: Full F/T automation, partial F/T automation, manual F/T performance, and manual F/T performance with task support. The design implications of each are discussed in 3.7.3.2.2, Special Design Considerations (see Design for Differing Levels of Automation).

3.3.3.5 Evaluate Overall Personnel Role

The previous discussions focused on changes to allocations that were either intentional or “inherited” as part of a selected platform. It is important to evaluate whether any of these new allocations impact other F/Ts personnel are responsible for. This was done within the context of the F/T assignment (see “Does performance of the F/T interfere with performance of another F/T” above). The following considers all other F/Ts.

While these other F/Ts are not directly impacted by the plant modifications, they may inadvertently be impacted by the changes that are made. For example, a new system may require a new manual task to be performed that makes it impossible for an operator to do a task typically performed at the same time. Another example is when a previously manual task is automated; operators may no longer have the information needed to perform a second task, if that information was derived as a consequence of manually performing the first task. The impact on the second task is an unintended consequence of changes made to the operator’s overall F/T allocation.

This type of evaluation is best made with the support of operators and maintainers whose tasks are being impacted.

Once identified, the F/T impact on staffing, HSIs, procedures, and training can be addressed (as these evaluations are addressed in later sections).

3.3.3.6 Verify F/T Allocations

Verification of the acceptability of the changes in F/T allocation is an ongoing process. While initially qualitative evaluations are necessary such as the allocation bases discussed here, allocation acceptability is continuously evaluated as part of later design activities. As noted, the entire process is iterative.

Task analysis is the process of defining the detailed requirements for human performance of allocated F/Ts. As part of the analysis, it may become apparent that some of the assumptions made during function allocation were incorrect and the allocation decision should be reevaluated.

For example, it may be found that much less time is available than originally thought or that an activity takes longer than expected. Such findings can lead to reallocations or other design solutions such as shifting F/T responsibility to another crewmember.

As the design becomes yet more detailed and mockups, simulators, and other tools become available, it may be possible to walk through F/Ts to evaluate the allocations (see Section 3.10 for a discussion of testing approaches). Again the evaluations should consider the overall role of personnel including:

- human responsibilities vs. automatic system responsibilities
- allocation of tasks to individual crewmembers
- coordination of the team

The ultimate criterion is that the integrated human-system performance is acceptable (see Section 3.9).

3.3.4 Documentation

The results of the function allocation should be documented, including:

- the changes in allocation introduced by the new systems
- the basis for such allocations
- the verification of the acceptability of the allocations

This documentation should be maintained for future reference both as the detailed design unfolds and as further plant modifications are considered throughout the life of the plant design.

3.3.5 Grading the Function Analysis and Allocation Effort

Section 2.4.2, A Graded Approach to HFE, introduces the concept that the level of HFE effort for a modification should be based on the nature of the risk significance and complexity of the change. A methodology is provided to establish a grade for a modification in one of three levels: Level 1 – high risk, Level 2 – moderate risk, or Level 3 – low risk. The methodology presented in this section corresponds to a Level 1 effort. Modification programs engaged in Level 2 or Level 3 activities, may consider streamlining the methodology in the following manner. For all levels, aspects of the complete Level 1 methodology that may be useful to a particular utility's specific modification could also be included where clear benefits would be obtained.

For Level 2 programs, it is recommended that the analysis be streamlined as shown in Figure 3-13. Following identification of changes, the allocation evaluation can be limited to those changes that are a significant departure from current practices and/or identified by personnel as potentially problematic. For verification, it is sufficient to conduct a walkdown with affected personnel.

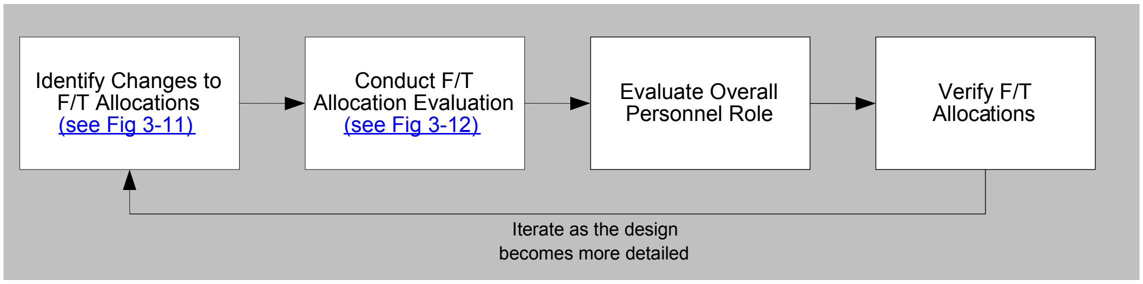

Identify Changes to F/T Allocations (see Fig 3-11)
Conduct F/T Allocation Evaluation (see Fig 3-12)
Evaluate Overall Personnel Role
Verify F/T Allocations
Iterate as the design becomes more detailed

Figure 3-13
F/T Allocation Analysis

It is recommended that for Level 3 analyses, changes to allocations should be identified and documented and personnel impacted should review these changes to determine their acceptability. The personnel review should include the direct change on the F/T itself as well as any changes in their overall responsibilities and workload.

3.3.6 Use of the Results

The main use of the results is that the personnel role in F/T performance is identified thus those activities to be performed by personnel can be analyzed in greater detail to reveal their task requirements (see Section 3.4, Task Analysis). Personnel responsibilities include monitoring of automatic systems.

The analysis also identifies the design implications for F/T performance. This information is used in HSI, procedure, and training design to ensure that adequate task support is available.

3.4 Task Analysis

3.4.1 Introduction

3.4.2 Objectives

3.4.3 Methodology

- 3.4.3.1 Inputs
- 3.4.3.2 Select Tasks to Analyze
- 3.4.3.3 Develop High-Level Task Descriptions
- 3.4.3.4 Develop Detailed Task Descriptions
- 3.4.3.5 Identify Task Requirements

3.4.4 Documentation

3.4.5 Establishing the Task Risk Level and Grading the Task Analysis Effort

- 3.4.5.1 Establishing the Task Risk Level
- 3.4.5.2 Grading the Task Analysis Effort

3.4.6 Use of the Results

3.4.1 Introduction

Task analysis is the analysis of functions that have been assigned to plant personnel in order to specify the requirements for successful performance. The actions personnel must do to accomplish their functions are called "tasks." Generally, the term "task" is used to refer to a group of activities that have a common purpose. The requirements developed in task analysis are a primary consideration in designing the HSI, procedures, and training that are provided to plant personnel.

Task analysis is actually a family of techniques. A single technique is not adequate for all situations because tasks can be very different from one another. Some tasks are sequential and well defined, like starting a system. Other tasks are ill defined and not sequential, like fault-detection and troubleshooting. Different task analysis methods are better suited to different tasks. For example, *Link Analysis* (LA) is a method of analyzing the layout of equipment and consoles based on task demands. *Operational Sequence Analysis* (OSA) is a method of examining the detailed behavioral aspects of tasks that are fairly well defined and sequential. *Hierarchical Task Analysis* (HTA) is a method of decomposing higher-level functions to the information and controls that personnel need to perform their tasks. *Cognitive Task Analysis* (CTA) is a method for analyses focusing on the thought process in addition to the physical actions best suited to examining tasks that are very ill defined and very dependent on the expertise of the user. Diagnosis is an example of the type of task that can be analyzed using CTA methods. In combination, these methods provide powerful tools for identifying task requirements. A comparison of these techniques is provided in Table 3-6.

However, these are only four of many techniques.[5] For the reader wishing a more complete discussion of various types of task analysis, see Kirwan and Ainsworth et al. (1992), Shraagen et al. (2000), and Vicente (1999). For published task analyses of commercial nuclear plant tasks, see Burgy et al. (1983).

The method described below combines features of several of these approaches. This method is intended to be sufficient for most task analysis needs in plant modernization programs.

3.4.2 Objectives

The objectives of task analysis are to evaluate personnel tasks in sufficient detail to identify the requirements for task performance, e.g., the alarms, information, controls, procedures, and training needed to perform the tasks. Uses of the task analysis results are discussed in Section 3.4.6.

[5] Kirwan and Ainsworth (1992), for example, list over 40 tasks analysis techniques. While many are highly related to each other, there are many different approaches. Those methods illustrated in Table 3-6 are the most common and important techniques.

Table 3-6
Comparison of Task Analysis Techniques

Method	When to Use	Product	Use of Results	Level of HFE Expertise Needed
Link Analysis	When you want to know the sequence with which HSIs are used or panels are accessed	Information on sequence of HSI and panel use. The transition from one HSI/panel to the next is called a "link."	To organize HSIs on panels or in computer displays.	Low
Operational Sequence Analysis	When tasks are fairly well known. This analysis is similar to Link Analysis, but addresses a much broader range of task factors such as communications.	An operational sequence diagram describing the sequence of tasks to be performed, often with a timeline. The diagrams can show multi-person interactions and automatic actions. HSI and other requirements for task performance and their interrelationships are included in the diagram.	Design of HSIs, procedures, training, job design, and staffing.	Medium
Hierarchical Task Analysis	When the detailed tasks that need to be performed to accomplish higher-level functions and tasks are not well defined.	Detailed task descriptions that define the tasks to be performed, their relationship to functions and higher-level tasks, and HSI and other requirements for task performance.	Design of HSIs, procedures, training, job design, and staffing.	Medium
Cognitive Task Analysis	To determine how cognitive tasks, such as situation assessment, are performed by experienced personnel.	Detailed description of how cognitive tasks are performed and what is required to accomplish them.	Design of HSIs to support cognitive tasks and to develop operator aids based on the knowledge of experts (e.g., expert systems).	High

3.4.3 Methodology

An overview of the process is presented in Figure 3-14. The complete methodology is for a Level 1 analysis. For recommendations on grading the methodology, see Section 3.4.5. In addition to the specific grading recommendations provided, the effort associated with conducting this HFE activity also depends on whether the same or similar analysis has been conducted in association with earlier modifications. The design team should typically start with prior analyses and modify or extend them as appropriate for the current modification. In some cases, even if the modification is Level 1, the availability of prior analyses may result in little new effort required for the current modification. Thus, when conducting this or any HFE activity, the team should ensure that the results of any relevant prior analyses are examined and applied as appropriate.

As illustrated, the methodology is divided into three major steps. The first is to *Select Tasks to Analyze*. The purpose of this step is to identify where detailed task information will be beneficial to the design (see Section 3.4.6 on the many uses of task analysis results). Once the tasks are selected, the next major step is to *Develop High-Level Task Descriptions*. Task descriptions provide information about the task, such as its purpose, its relationship to other tasks (e.g., performed in sequence or in parallel), the time it takes, etc. Using the high-level descriptions, *Detailed Task Descriptions* are developed by decomposing the tasks into detailed steps. The final step is to *Identify Task Requirements*. Task Requirements are the resources that must be available to perform the task, e.g., the information and controls required.

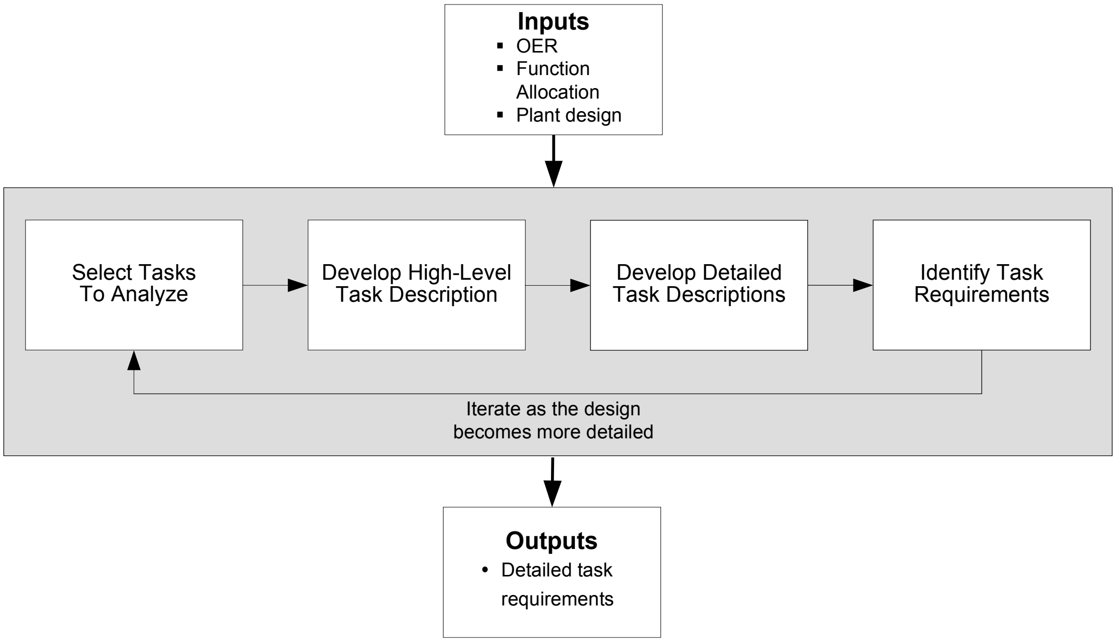

Inputs
▪ OER
▪ Function Allocation
▪ Plant design
Select Tasks To Analyze
Develop High-Level Task Description
Develop Detailed Task Descriptions
Identify Task Requirements
Iterate as the design becomes more detailed
Outputs
• Detailed task requirements

Figure 3-14
Overview of Task Analysis

3.4.3.1 Inputs

The main inputs to task analysis are the OER, function allocation, and plant design information. The OER provides information about which tasks are impacted by the modifications, which tasks have been problematic in the past, and which tasks might be targets of opportunity for improvements. The function allocation analysis identified tasks associated with the modification that are new or modified due to changes in the level of automation. Detailed plant design (systems, components, and the existing, verified plant procedures) information is needed to properly describe the tasks.

3.4.3.2 Select Tasks to Analyze

The first step is to create an inventory of tasks that are new or significantly changed. This is done by comparing how tasks are performed with the modified systems as opposed to the existing systems. While the modified task requirements may not be known in detail, an assessment can be made at a high level; detailed analysis for selected tasks will be performed later. At this point, the main goal is to see where things have changed sufficiently that some form of task analysis may be warranted.

The ways in which tasks can change include:

- The task is no longer performed because it is unnecessary with the new system
- The task is no longer performed by personnel because it is automated
- The task is new
- The way the task is performed is significantly different
- The task demands are significantly different, e.g., less time is available
- The task is performed in a similar way, but the HSIs and/or procedures are modified

As part of the OER the functions, tasks, and HSIs that are impacted by the modernization program were identified (see Section 3.2.3.1). Additional identification of personnel tasks may have resulted from the function analysis. This information should be used to identify the list of tasks that should be analyzed. Included in this inventory should be tasks that were difficult and could be improved by the modification even though that is not the modification's main purpose (see Section 3.2.3.2 related to targets of opportunity). If such an analysis to identify targets of opportunity was not performed during OER, it should be performed at this point.

Vendor and engineering personnel can develop the task list, but it should be evaluated for correctness by operations and maintenance personnel who are familiar with current practices.

Each of the tasks in this list should be subjected to some form of task analysis. Section 3.4.5 discusses how to grade the task analysis, based initially on the grade established for the modification as described in Section 2.4.2 and then on the nature of the task itself. The sub-sections below describe the activities that should be performed for a Level 1 (high importance) task analysis. Use of less formal and less rigorous forms of task analysis for Level 2 and Level 3 tasks is described in Section 3.4.5.

3.4.3.3 Develop High-Level Task Descriptions

Once the tasks to analyze are selected, the actual task analysis is a matter of developing a high-level task description and decomposing a high-level description to a level of detail precise enough to identify the requirements for performance. Thus, task analysis is a continuation of the process of hierarchical decomposition that began in function analysis (see Section 3.3).

The basic elements of a task description are provided in Table 3-7. It is acceptable if the initial description is missing some of this information since it can be added once the task is analyzed in detail and/or the design matures sufficiently to make such information available.

Table 3-7
Task Description Elements

Element	Description	Crewmember's Perspective
Purpose	The reason a task is performed (usually to accomplish a function or higher-level element in a functional decomposition).	Why do I perform this task?
Task Initiation	The plant conditions, events, or situations that indicate that it is time to perform the task	When do I do this task? What tells me it is time to do it?
Preconditions	The initial conditions that must be met before a task can be undertaken (including role of interlocks)	How do I know it is OK to start?
Instructions/ Decisions	The general approach to how the task should be performed, including include the decisions and actions that need to be taken. (May involve procedures)	How do I accomplish the task; what steps do I have to take?
Cautions/Warnings	Cautions and warnings related to task performance	Are there any cautions or pitfalls I need to be aware of?
Information	Specific plant or other information needed to perform the task and obtain feedback on progress (May involve procedures)	What information do I need for each step; e.g., what "function, system, equipment" is involved and what do I need to know about it, e.g., status (open/closed) or parameter value (flow rate, temp)? How do I know things are proceeding satisfactorily?
Alarms	Any alarms related to the task or task step that may impact the user's ability to perform the task or may alter the actions the user should take	What abnormal conditions might I need to be alerted to at each step?
Controls	Specific control actions that need to be performed and the controls that should be used to take the actions	What controls do I need to take the necessary actions at each step?
Time	The time constraints, if any, on task performance: time available for the action and time required to do it	How much time do I have for each step?
Failures[1]	Things that can go wrong, identifying cues and alternative actions	What can go wrong? How do I know that it has gone wrong? What needs to be done if something is wrong?
Task Termination	The plant conditions, events, or situations that indicate that it is time to stop the task	How do I know when to stop performing the task?

[1] The analysis of human errors that can contribute to failures is addressed in Section 3.6.

The actual starting point for the analysis depends on what information is already available. The HFE analyst should determine what information already exists for the selected tasks. Task analysis information may be available from the following sources:

- an existing verified plant procedure
- an analysis of the task from a previous activity
- an analysis of a similar task from a previous activity
- an analysis of the task from a similar plant
- an analysis of the task from vendor design efforts or vendor manuals

If prior analyses are available, they should be modified to reflect the current design. However, sometimes little task analysis data is available and it has to be developed as part of the modification project effort. Information to develop the task description can come from a variety of sources, such as:

- Review of existing documentation
  - supplier documentation
  - existing procedures
  - manuals
  - training materials
- Knowledgeable personnel from the design team
- Subject matter experts
- Onsite or offsite personnel who perform the task
- Walk-throughs and talk-throughs (see Section 3.10 for a discussion of these methods)
- Tests and evaluations (see Section 3.10 for a discussion of these methods)

Often a combination of these information sources is used. The sources of information that are more readily available can be used to lay out the scope of the tasks. The more resource-intensive sources can be used as a last resort or reserved for those tasks of particular interest, for example, mission critical tasks, safety critical tasks, and tasks associated with new functionality, such as those graded as Level 1 per Section 3.4.5.

3.4.3.4 Develop Detailed Task Descriptions

Developing detailed task descriptions involves the following steps:

- Decompose the task from high-level to low-level descriptions
- Evaluate the completeness of the task decomposition
- Identify the relationship between elements at each level
- Develop a timeline if time-criticality or workload problems are suspected
- Identify additional considerations as needed

Each of these is discussed below.

3.4.3.4.1 Decompose the Task from High-Level to Low-Level Descriptions

Starting with the high-level task descriptions, the tasks are broken into detailed steps, i.e., the steps that have to be performed to accomplish the task (see Figure 3-15). The steps can be further broken into activities. Activities are the lowest level of analysis and describe behaviors such as “monitor the water level” and “close the valve.”

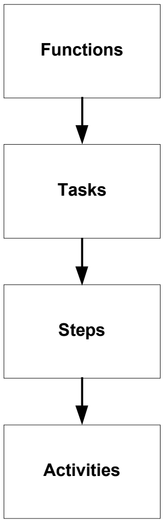


Figure 3-15
Hierarchical Levels of Analysis

There can be many levels depending on the complexity of the task. The essential thing is that they are hierarchical. Higher-level descriptions can be decomposed into lower and more precise levels of description. Tasks are decomposed sufficiently to identify the requirements for their performance. In much of the discussion below, the term “task element” refers to the collection of items at any one level, whether it is a task, a step, or an activity.

As a simple illustration of task decomposition, consider the task of starting a system. This task is decomposed into a number of activities that must be performed. See the startup task decomposition shown in Figure 3-16.

In this example, the hierarchical relationship between the levels is shown through a numbering scheme that relates lower-level and upper-level elements. Thus, all decomposition elements under Task 1 are numbered beginning with “1” and that convention follows as one proceeds down the hierarchy. If a Task 2 were shown, all its elements would begin with the number 2.

As required, decompose the task even further than is shown in Figure 3-16. For instance, Activity 1.1.2, Open Valve B, may involve a number of discrete actions. The analyst should decompose the tasks until the level is reached where the specific HSI requirements can be identified.

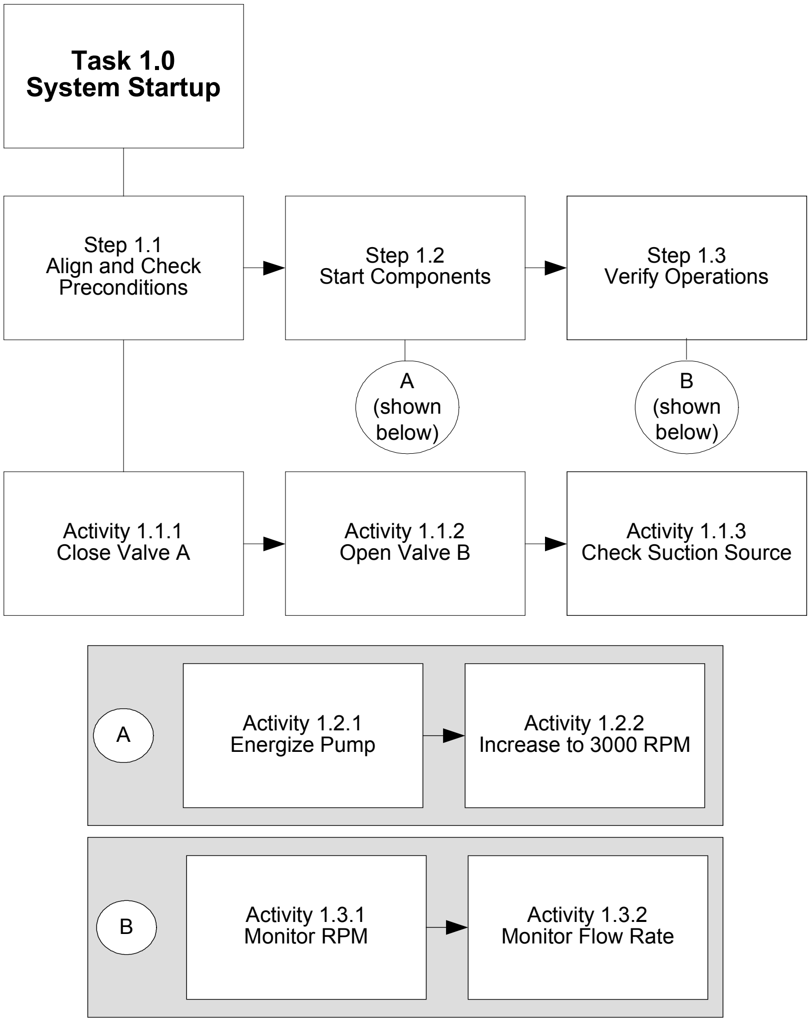


Figure 3-16
System Start-Up Task Decomposition

3.4.3.4.2 Evaluate the Completeness of the Task Decomposition

When task decomposition is completed, it is important to make sure that each set of elements at a lower level completely describes the higher-level box. This evaluation involves two questions:

- Is there anything missing (can the higher-level element be achieved with only the lower-elements listed)?
- Is there anything in the lower-level task description that is not needed?

One good way to answer these questions is to hold discussions with users (operators or maintainers) and step through the task decomposition with them. If the tasks are completely new, then this can be accomplished with the help of system designers and engineers.

3.4.3.4.3 Identify the Relationship between Elements at Each Level

Once the task decomposition has been verified, the relationship between task elements at each level should be identified. This is because the elements at each level are related, but they may be related in different ways. For example, for some tasks, each step must be completed before the next one can be started. That is, the steps are performed serially. For other tasks, the steps may be started or stopped based on external criteria, such as a plant condition that is achieved. For other tasks, there may be steps that have to be or can be performed in parallel. Table 3-8 describes the ways in which elements can be related.

3.4.3.4.4 Develop a Timeline

While the time to perform each task element is part of its description (see Table 3-8), the plant response time between task elements and the relationship between task elements, as discussed above, impact overall task time. A task timeline can be created that accounts for these factors. While the creation of a timeline is always useful for looking at allocation of tasks to crewmembers, it is only essential when there is some concern about the successful completion of a task within some defined timing criterion, e.g., based on requirements established from thermodynamic analyses. The timeline should identify tasks that overlap in time possibly creating an overload situation.

3.4.3.4.5 Identify Additional Considerations as Needed

As indicated in the introduction, task analysis has many applications. As the design becomes more detailed, additional considerations can be identified in the task description to provide a basis to evaluate the function allocation or the allocation of tasks to individual crewmembers, or to evaluate the HSI. These additional considerations relate to workload and HSIs:

- *Workload* – assign an anticipated workload to task elements at an appropriate level (not necessarily for each task element, but at a level where workload assessments are meaningful, e.g., low, medium, or high). This can help to determine what task elements are difficult and may suggest which should be automated or allocated to other crewmembers. The assignment can be based on information obtained from personnel responsible for task performance or from other subject matter experts. Lacking this type of input, the HFE analyst may also assign workload values to tasks by evaluating the detailed task requirements.
- *HSIs* – To help in evaluating HSIs it is beneficial to identify the specific HSIs used for each task element and their location. First, identify the control capabilities required and parameters to be evaluated. As the analyses evolve, identify desired formats and characteristics for the controls and displays needed. Using this information, an assessment of the layout (or organization) of the HSIs can be made along with the secondary tasks associated with task performance, e.g., alarm management, navigation, and display retrieval.

Table 3-8
Possible Relationships Between Task Elements

Relationship	Description	Example
Simple Linear Sequence	A series of elements that are performed sequentially, so that completion of each element acts as the cue to initiate the next one.	Do 1, then 2
Constrained Linear Sequence	A linear sequence of elements in which the start of the next element depends not only on completion of the previous element but upon certain other conditions being met, e.g., a parameter reaches a specific value and a specific system state in achieved, such as when a valve closes. It could also include activities of coworkers, such as waiting until an AO gets to a specific location in the plant.	Do 1, then when pressure falls to 100 psi, do 2
Unordered List	In an unordered list the only requirement is that a number of elements have to be undertaken, but the person is free to perform them in any order that is appropriate at the time. (While there may not be a necessary order, there may be a preferred order, e.g., a sequence that saves time).	Do 1, 2 and 3 in any order
Conditional Branching	The selection of which element to undertake next is based upon the conditions that pertain (which might include the success of a previous action).	If there are no alarms, Do 1, otherwise do 2
Condition Attainment Looping	A sequence of elements is continued until a condition is met.	Do 1, then 2 and repeat until the X stabilizes
Continual Looping	A task element (or set of elements) is repeated at appropriate times. Continual looping of elements may be accomplished intermittently in parallel with other tasks.	Do 1, then 2 and repeat at least once every 5 minutes
Concurrent Elements	Task elements that need to be carried out at the same time.	Do 1 while doing 2.
Continuous monitoring-conditional branching	A potential event/situation not part of the task being performed which will require stopping the task to deal with it.	Continuously monitor A; if at any time B occurs, cease the task at hand and perform A

3.4.3.5 Identify Task Requirements

Once the task is decomposed to a sufficient level of detail, the specific requirements for personnel to properly perform the task should be identified. The categories of task requirements are identified in Table 3-9. These requirements are a major input to HSI, procedure, and training design. All of the items listed in Table 3-9 are typically not needed in every task analysis.

Table 3-9
General Task Requirements Considerations

Categories of Requirements	Example
Information Requirements	• Parameter values (units, precision, and accuracy) • Display format (analog format device, numerical readout, binary status indicator) • Parameter trends (e.g., rate of change, direction of change) • Parameter limits (e.g., normal ranges, hi/lo alarm limits) • System or equipment state (e.g., operating state, availability) • Feedback required to indicate adequacy of task performance • Task-related alarms
Decision-making Requirements	• Evaluations to be performed by user • Criteria for making decision • Risks associated with making a wrong decision
Response Requirements	• Type of action to be taken • Time available and temporal constraints • Accuracy needed • Frequency • Reach and movements needed to take an action • Alternate means of accomplishing the action (e.g., backup controls)
Communication Requirements	• Personnel communication (such as for trouble shooting or when multiple users work on the system)
Workload	• Physical, cognitive, overlap of tasks (serial vs. parallel tasks)
Task Support Requirements	• Special and protective clothing • Special tools • Job aids or reference materials required
Workplace Factors	• Workspace envelope required by action taken • Typical and extreme environmental conditions, such as lighting, temp, noise

To illustrate the specification of task requirements, following from the example provided in Figure 3-16, the requirements for the task elements are summarized in Table 3-10 for information, controls, and alarms.

Table 3-10
Task Requirements for System Start-Up

Task	Information	Control	Alarm
1.1.1 – close valve A	position	throttle control	power loss
1.1.2 – open valve B	position	throttle control	power loss
1.1.3 – check suction source	tank level	none	low level
1.2.1 – start the pump	pump status indication	pump start control	bearing temp
1.2.2 – bring to 3000 RPM	impeller speed	pump speed control	bearing temp
1.3.1 – monitor RPM	pump status indication	none	power loss, trip
	pump speed		high/low RPM
1.3.1 – monitor flow rate	pump flow (gpm)	none	high/low flow

Each of these can be further specified. For example, for tank level, one would consider:

- what precisely needs to be known (present value, trend, etc.)
- how should level be quantified
- what is the degree of precision needed
- what is the needed range
- the set points and other significant limits on performance

During HSI design for the task, information at higher levels, such as indications of overall function performance, may be identified as well (following the guidance in Section 4.1.3). The analysis may also include other indications of performance beyond those simple indications identified above. For example, vibration indication and alarms may help personnel anticipate a problem prior to failure.

Another consideration with respect to this example is that the task decomposition was carried down to the component and parameter level. In fact, the operator may monitor and control at higher levels in the hierarchy if, for example, automatic alignments are implemented in the digital system.

3.4.4 Documentation

When the task analysis makes use of existing analyses and documentation, such as an established and verified procedure, little additional documentation may be needed. In this situation, the changes from the previous documentation should be identified.

When the tasks are new or significantly modified, the documentation should identify the tasks and their requirements. These requirements reflect the information, controls, etc., that the HSIs must provide to the user, so they can perform their tasks. For any task analysis, it can be beneficial to retain the intermediate documentation products and information developed in deriving the task requirements (e.g., the kinds of information developed per Tables 3-7 and 3-8). If changes are made in later stages of HFE activity (i.e., during Staffing Analysis, Human Error Analysis, HSI Design, etc.) or in future modifications, the task analysis may need to be revised. It will be easier to evaluate the impact of these changes or to modify the task analysis if the intermediate documentation is kept. However, for a Level 1 task analysis, retaining the intermediate documentation products is particularly appropriate in order to demonstrate an adequate degree of rigor, which can be subject to specific review.

3.4.5 Establishing the Task Risk Level and Grading the Task Analysis Effort

Section 2.4.2, A Graded Approach to HFE, introduces the concept that the level of HFE effort for a modification should be based on the nature of the risk significance and complexity of the change. A methodology is provided to establish a grade for a modification in one of three levels: Level 1 – high risk, Level 2 – moderate risk, or Level 3 – low risk.

3.4.5.1 Establishing the Task Risk Level

3.4.5.1.1 Tasks for Level 1 Modifications

The grade for the overall modification may have been assigned a Level 1 because of the importance of the system at an early point in the modification process before fully developed information regarding the resulting tasks and their individual importance was available. Once the individual tasks have been defined in detail, it may become clear that not all of the tasks may be Level 1 in importance. Therefore, the candidate task list developed in Section 3.4.3.2 should be evaluated to determine the importance of the tasks. Tasks associated with a modification that has been graded Level 1 with any of the following characteristics should be identified as Level 1 tasks and selected for task analysis using the complete methodology described in Section 3.4.3:

- Dangerous – can result in death, serious injury or significant radiation exposure
- Important to nuclear safety – High nuclear safety risk significance
- Important to overall plant productivity – Can result in a plant trip or can result in significant damage to important equipment
- Important to system availability or equipment protection (this should be used judiciously and only for tasks that could notably impact important systems and components)
- Demanding or difficult to perform based on:
    - Past experience (OER)
    - The judgment of plant personnel (operators or maintainers) who will have to perform the task
    - Function analyses indicating the task is demanding for personnel but will not be automated (see Section 3.3)

All other tasks identified for a Level 1 modification that meet the Level 2 criteria in Section 2.4.2 (i.e. where potential errors have a nuclear safety risk potential corresponding to the Level 2 criteria, or can result in some reduction in plant power production or equivalent loss resulting from damage to equipment or can cause mild personnel injury or radiation exposure) should be considered Level 2 tasks and should be analyzed according to the Level 2 approach described below. With adequate justification, low risk tasks can be analyzed using the Level 3 approach described below.

3.4.5.1.2 Tasks for Level 2 Modifications

Tasks for Level 2 modifications should also be evaluated to identify those that meet the Level 2 criteria in Section 2.4.2 (i.e. where potential errors have a nuclear safety risk potential corresponding to the Level 2 criteria, or can result in some reduction of plant power production or equivalent loss resulting from damage to equipment or can cause mild personnel injury or radiation exposure). Level 2 tasks that are identified as demanding or difficult to perform should be upgraded and analyzed as Level 1 tasks. All other tasks for a Level 2 modification should be analyzed as Level 3 tasks as described below.

3.4.5.1.3 Tasks for Level 3 Modifications

Level 3 tasks that are identified as demanding or difficult to perform should be upgraded and analyzed as Level 2 tasks. All other tasks for a Level 3 modification should be analyzed using the Level 3 task analysis methodology described below.

Note that it is possible for a task for a Level 2 modification to meet the criteria for a Level 1 task or for a task for a Level 3 modification to meet the criteria for a Level 2 task. In such cases, the tasks should be analyzed using the Level 1 or Level 2 methodology, as appropriate.

3.4.5.2 Grading the Task Analysis Effort

Tasks for Level 2 and Level 3 modifications should be analyzed using the methodology for task analysis as described in Section 3.4.3 but with less formality and using less rigorous methods. This approach is recommended to promote greater efficiency while still ensuring that all modified or new tasks are analyzed and the necessary information is developed and used for HSI design and procedure development.

The following are examples of how the task analysis methodology described in Section 3.4.3 could be applied for Level 2 and Level 3 tasks:

- *Level 2 Tasks* – Use the tables in 3.4.3 as checklists to structure the analysis, filling them out (as checklists so there is a record of the analysis steps). This approach would ensure that all of the elements of a task analysis have been addressed, but it does not require performing detailed analyses except where warranted. It also does not require detailed analysis descriptions to be developed, thus lessening the documentation burden. Task requirements should still be defined as the end product, and these should still be used as input to HSI design and procedure development. However, this should be straightforward for changes to existing tasks since the existing procedures would be used as inputs to avoid having to re-create the task steps, etc. This approach could be taken jointly by the procedure writer and an HFE engineer, working with the design engineers and one or more operators. This approach relies more on experience and engineering judgment and less on detailed analysis, as compared to Level 1.

- *Level 3 Tasks* – Knowledgeable personnel (modification engineers, systems engineers, operators, maintenance personnel, procedure writers, etc.) supported by walkthroughs/talkthroughs should use the methodology for task analysis described in Section 3.4.3 as an aid. The procedure writer would use the information in 3.4.3 as an aid when developing the new or modified procedure, but would not fill out checklists or write down detailed task descriptions. The new or revised procedure becomes the documentation. The conceptual design for the HSI should be developed by the modification design engineers working with the procedure writer as the procedure is developed. See Section 3.8 for a description of how a Level 3 Task Support Verification might be performed.

3.4.6 Use of the Results

Task analysis provides detailed information about what is needed to perform tasks. This information has many uses in subsequent analyses, including: staffing, error analysis, HSI and procedure design, training, and V&V.

The results of task analysis are used as one of the major inputs to the staffing analyses addressed in Section 3.5. Based on the task requirements, tasks are assigned to personnel and staffing levels are examined. For modifications to existing plants, it is unlikely that Operations staffing levels will change as a result of the HSI modifications, particularly since the staffing levels are tied closely to regulatory requirements. However, assignment of tasks among the crew members may well change as discussed in Section 3.5.

The detailed task descriptions developed in task analysis are used to initiate an evaluation of the types of human errors that can result when personnel perform tasks individually or in groups (see Section 3.6).

The task requirements are also a significant input to HSI design, perhaps even more so when designing computer-based HSIs as compared with analog HSIs. This is because of the high-degree of freedom that exists with computer-based HSIs to design the alarms, displays, and controls to be much more task-specific. This is discussed in Section 3.7 and again in Section 4.1.3 where task requirements are used directly to develop task-based displays. However, even when the displays are not task-based, the task information is used to determine what should be displayed and how information should be grouped. For example, using the task element relationships can indicate how information should be grouped and how users will need the information in sequence. This is extremely important. When the HSI does not present information in a manner that is consistent with the task demands, user performance suffers. A good task analysis can help prevent this type of problem.

Task requirements and sequence information are key inputs to procedure design. In fact, draft procedures can be written directly from the task analysis documentation when new tasks are created. For modifications, the initial task analyses usually start from the established, verified procedures used with the existing system. Vendor component procedures also may be used as a starting point for analysis of tasks using those components. Finally, as discussed in Section 3.4.5, for Level 3 (low importance) tasks the task analysis may be performed in conjunction with the development of new or modified procedures.

Ultimately, whether the design meets the task requirements is verified in "Task Support Verification" (see Section 3.8).

Task analysis information is also an important input to trainers since the analysis identifies what skills and training users need to perform the tasks. For a new plant design, the skills, knowledge and abilities identified from the task analysis would be reflected in personnel selection/hiring and to initially develop the training program. For modifications to existing plants, changes needed to the existing training program should be defined based on results of the task analysis, and this should reflect unique considerations related to digital I&C/HSI upgrades as described in Section 6.3.

3.5 Staffing, Qualifications, and Integrated Work Design

- 3.5.1 Introduction
- 3.5.2 Design Process Steps
- 3.5.3 Methodology
  - 3.5.3.1 Inputs
  - 3.5.3.2 Assign Tasks to Crewmembers
  - 3.5.3.3 Evaluate Integrated Task Demands and Staffing Levels
  - 3.5.3.4 Evaluate Teamwork
  - 3.5.3.5 Evaluate Staff Qualifications
- 3.5.4 Documentation
- 3.5.5 Grading the Staffing Analysis Effort
- 3.5.6 Use of the Results

3.5.1 Introduction

Plants are operated and maintained by crews of individuals, including both shift personnel and normal daytime workers (those working a typical "8-to-4" 40 hour work week). Each crewmember e.g., shift supervisor, reactor operator, and maintenance technician, has a unique set of responsibilities. In this context, responsibilities refers to the complete set of tasks that the crewmember is expected to perform. To accomplish human functions, crewmembers interact with each other and with plant systems and components. Plants "staff" each shift to a certain level based on the need to accomplish all personnel tasks within a reasonable workload level. More extensive upgrades may have impacts on the number of personnel needed to staff the plant.

As part of a modernization project, new tasks are created, other tasks no longer need to be performed, and others are changed as a result of the new systems and HSIs. These tasks were identified as part of the operating experience review and function analysis, and a subset of those tasks were evaluated using task analysis. The main purpose of this section is to consider the allocation of these tasks to individual crewmembers, the impact of those tasks on their other responsibilities (called a collateral effect, see Section 3.2.3.2), and the impact of these changes on the crew's functioning as a team. Qualifications may also be affected by any change that requires personnel to have different knowledge, skills, or abilities than those they currently possess. Major upgrades such as migrating to an all sitdown "soft control" operations might also permit relaxation of some physical standards. For example, operators might be subject to different visual requirements, especially relating to color vision, in order to operate the screens, and, theoretically, a wheelchair-bound operator could now control the plant, assuming all of the required tasks not involving the sitdown workstation could be performed.

Staffing analyses are important for operations and maintenance personnel. In fact, the latter may be more significantly impacted by digital I&C upgrades because their tasks are often changed to a greater degree. For example, it is likely that testing and calibration of new systems will not be the 'hands-on' tasks that they formerly were. These activities are likely to be automated to a great extent. Other tasks may be performed from computer-based workstations in contrast to directly interacting with field equipment.

3.5.2 Design Process Steps

The objectives of this section are to:

- allocate new tasks to crewmembers
- evaluate whether shifts in task assignments should be made
- evaluate whether the new and modified tasks impact other personnel responsibilities when they are considered in an integrated fashion
- evaluate whether changes in tasks and responsibilities require new job qualifications
- evaluate whether changes in staffing levels are needed
- evaluate whether changes in personnel selection/ physical standards are needed

Uses of the results of staffing analyses are discussed in Section 3.5.6.

3.5.3 Methodology

The process for carrying out this assessment is illustrated in Figure 3-17. The complete methodology is for a Level 1 analysis. For recommendations on grading the methodology, see Section 3.5.5. In addition to the specific grading recommendations provided, the effort associated with conducting this HFE activity is also based on whether the same or similar analysis has been conducted in association with earlier modifications. The design team should typically start with prior analyses and modify or extend them as appropriate for the current modification. In some cases, even if the modification is Level 1, the availability of prior analyses may result in little new effort required for the current modification. Thus, when conducting this or any HFE activity, the team should ensure that the results of any relevant prior analyses are examined and applied as appropriate.

The process is essentially a building block approach. Tasks are first allocated to crewmembers. Then the impact of the new tasks on the crewmember's existing tasks is considered. At that point some adjustments in task allocation may be considered. In more significant modifications, actual changes in staffing levels may be identified at this stage. Then the effect of the changes on the crewmembers work as a team is considered. Changes in teamwork may be recommended based on changes in crewmember task responsibilities (and based on changes in technology used to accomplish those tasks). Finally, implications for staff qualifications are considered.

In the discussion to follow uses operations staff as examples. The same analyses should be performed for maintenance personnel as well.

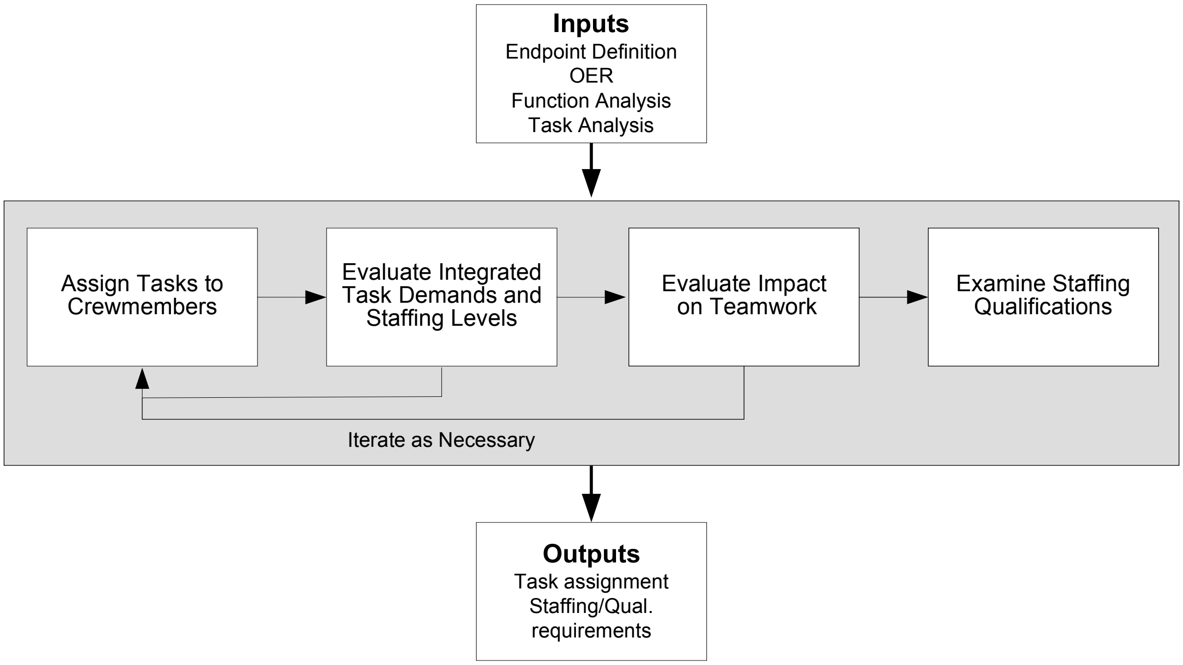

Inputs
Endpoint Definition
OER
Function Analysis
Task Analysis
Assign Tasks to Crewmembers
Evaluate Integrated Task Demands and Staffing Levels
Evaluate Impact on Teamwork
Examine Staffing Qualifications
Iterate as Necessary
Outputs
Task assignment
Staffing/Qual. requirements

Figure 3-17
Evaluation of Staffing and Qualifications Considerations

3.5.3.1 Inputs

The staffing analysis is based on inputs from the endpoint definition (especially considerations of concept of operations), operating experience review, function analysis and allocation, and task analysis.

3.5.3.2 Assign Tasks to Crewmembers

As part of the OER, function analysis, and task analysis, the tasks that are impacted by the modernization program were identified and analyzed. These tasks need to be assigned to individual crewmembers.[6]

Many of these tasks may have been analyzed with particular crewmembers in mind. However, especially for new tasks, a determination of who should perform the task will have to be made. The main considerations in assigning tasks are the general areas of responsibility defined by current plant practices (workload is also important and will be addressed in the next subsection). With respect to general areas of responsibility, the initial assignment of new tasks should be consistent with current practices. For example, if operating practices divide operator responsibilities into reactor operations and balance of plant operations, then new tasks involving the reactor side of the plant should be assigned to the crewmember engaged in reactor operations.

It is important from a human performance standpoint, to keep the task responsibilities of crewmembers related to each other. Assigning tasks on the basis of their relationship to general areas of responsibility supports situation assessment and awareness. When a crewmember works on related tasks, it is easier to maintain focus on the area of responsibility. Conversely, when a crewmember is assigned an ad hoc group of unrelated tasks, the demands associated with shifting attention between them detracts from maintaining situation awareness and the ability to properly monitor status and detect situations deviating from where they should be.

3.5.3.3 Evaluate Integrated Task Demands and Staffing Levels

In the introduction, crewmember responsibilities were defined as the complete set of tasks that the crewmember is expected to perform. The focus of this next analysis is to examine the impact of task assignments on these responsibilities. The key considerations involve workload and collateral effects, i.e., impacts of task changes on other tasks that are part of a crewmember’s responsibilities but were not the focus of the modification.

As a result of the task changes resulting from the modification, crewmember workload may have significantly changed. Several tasks may have been eliminated for one crewmember, while for another crewmember several new tasks may have been created. This might occur, for example, when the modification to BOP systems greatly increases the level of automation, thus reducing BOP workload. However, subtler changes to plant operations lead to increased indication, increased monitoring responsibility, and less time to respond for the reactor operators. Therefore, it may be necessary to assess workload and revise the assignment of tasks to personnel in order to balance workload more evenly (see Example 3-3).

Note that the old divisions of responsibility may have reflected characteristics of the control room, e.g., layout of control panels. With computer-based interfaces, much greater freedom may exist to share information or bring information to any workstation. Thus new technology can make it possible to provide more flexible lines of responsibility.

[6] There is a great deal of variation in the degree to which utilities formalize divisions of responsibilities between individual crewmembers. However, even if a utility does not formalize responsibilities, it is important to consider the conduct of new tasks by the crew and whether such formalization is warranted.

With respect to collateral effects, all the changes discussed above can have impacts on the other responsibilities the crewmembers have, thus when looking at integrated task demands, it is necessary to consider all of a crewmembers responsibilities and not just those directly related to the modification.

Example 3-3 Modified Turbine Control Responsibility at One PWR

A PWR has a well defined division of responsibilities in the control room based on systems and panels. Their existing practice is that, because of its immediate impact on reactivity, control of the main turbines at power rests with the Reactor Operator (RO), not the Balance of Plant (BOP) Operator, as is often the case. Turbine system startup, shutdown, and turbine auxiliary systems, however, are under the control of the BOP Operator (or an additional third licensed operator brought in for scheduled plant start ups or shut downs). The plant is installing a digital upgrade to main turbine controls and auxiliaries that migrates those controls and displays to a sit down workstation with soft controls. No other similar modifications are presently in progress for the primary or other systems. The new workstation will be on the BOP operator's desk, and the Supervisor will have a back up workstation, but no workstation is planned for the RO. Therefore, the plant has decided to change their concept of operations and give all operational responsibility for the main turbines to the BOP Operator.

The evaluation of integrated task demands can use several methodologies. First, a table-top assessment can be made by talking through the tasks (see Section 3.10 for a discussion of general methodology). To perform the evaluation, the designer can talk through scenarios of plant evolutions that involve the modified tasks with operations and training experts. Task descriptions and detailed analyses should be available to support the evaluation. The experts should consider all the tasks that each crewmember has to perform and the overall time available and workload created. This will help to pinpoint times when workload may be high or when an unanticipated consequence arises. This process may be facilitated by having the experts walk though the scenarios in the control room, the simulator, or using mockups or prototypes.

For tasks that are more uncertain or when a more realistic evaluation is needed, they can be performed in a simulated environment using a full scope simulator with selected scenarios (normal, abnormal, and accident). This will allow the sensitivity of the prior analyses to assumptions about task times and about operators' scheduling of required actions to be assessed; individual variation in the responses of personnel to demands posed by the pacing of plant processes can also be assessed. It will also reveal, to the extent possible before modifications are put into service, any unforeseen collateral effects of the modifications (i.e., effects on tasks not directly affected by the modifications). For these reasons, it can be beneficial to have simulation capability that reflects the plant modifications very early in the design process.

One of the consequences of these evaluations may be that following the modifications, all personnel tasks and responsibilities can be accomplished with fewer staff. This situation may arise following a significant change toward greater automation or efficiency improvements in the way tasks are performed. The reduction in staff may be either to on-shift or to daytime workers. For modifications to the current fleet of NPPs, it is not envisioned that there would be changes to the licensed control room staff as defined in 10 CFR 50.54 (i) through (m). For new advanced plants, some changes to these staffing regulations are expected (see NUREG-6838 for guidance on addressing the licensing aspects of this type of staffing change.)

Less likely but also possible is a required increase in staffing. This might occur due to the addition of significantly new monitoring capabilities, e.g., new security systems added in response to increased threat levels.

3.5.3.4 Evaluate Teamwork

NPP crews work as teams. Behaviors that are typically identified as important elements of teamwork include having common and coordinated goals, maintaining shared situation awareness, engaging in open communication, and cooperative planning. Successful teams monitor the status of others, back each other up, actively identify errors, and question improper procedures. Any shift in the allocation of individual tasks or a change in the overall responsibilities of individual crewmembers can impact teamwork. Thus this potential effect should be evaluated using operations and training experts, following the evaluation of integrated task demands.

Another important consideration is the new HSI technology. An often unintended and unanticipated impact of technology is its effect on crewmember's responsibilities and team processes. The effect stems from the opportunity that digital I&C systems and computer-based HSIs provide to automate monitoring, decision-making, and control activities that previously were performed by crewmembers. This can affect the structure and dynamics of the team as a whole. It can affect the amount and kinds of information available to each crewmember, the communication pattern among crewmembers, and the situation awareness of the different crewmembers. This is in part because, in a control room environment, key information is distributed among crewmembers. The quality of decision-making depends on the ability of everyone of the team to be aware of important control actions about to be taken and to evaluate the appropriateness of the actions based on each crewmember's knowledge and perspective. This is significant because a large part of nuclear plant personnel efforts involve working as a team and providing checks against error. Therefore, reliable performance depends on the team's communications and interactions. An example of how technology can impact teamwork is presented in Example 3-4.

Thus the effect of the modifications on teamwork should not only examine shifts in task assignment, but the impact of technology on the integration of tasks across crewmembers. These evaluations can be made using walkthroughs and simulator exercises with entire crews. Of course, the effects of technology may be examined iteratively as the details of the detailed HSI design become known.

Example 3-4 Example of the Impact of Technology on Teamwork
As part of one utility's digital I&C upgrade, a computer-based EOP system was installed. Prior to the upgrade, EOP use was an activity that involved the entire control room crew. The supervisor read the procedure and made decisions at each step as to how to proceed. The operators retrieved the needed data for each procedure step and communicated it to the supervisor. At the supervisor's instruction, they would take any required actions. This required a lot communication and coordination.

The CBP significantly changed this activity. It performed many of the tasks that the crewmembers did, including:

- *Retrieving data and assessing its quality*

- *Resolving step logic*
- *Keeping track of location in the procedure*
- *Keeping track of steps of continuous applicability*
- *Assessing cautions, critical safety function status trees, and fold-out page criteria.*

As a result, workload was greatly reduced and procedure use became a one-person activity. The operators were far less engaged in EOP use, except to take occasional control actions. The operators felt they were out of the loop, lost situation awareness of EOP activities, and were not sure what to do. Team cohesiveness lessened at a critical time (when plant circumstances require EOP use).

The situation was addressed by the operations and training departments. The roles and responsibilities of the individual crewmembers were redefined and steps to foster teamwork were put in place. First, operators were to manage alarms and check key parameters on their side of the plant (reactor and BOP). Then specific stop points were added into the procedure where the supervisor updated the operators on the procedure status and the crew shared their assessments and informed the supervisor of key findings. Because the shift supervisor and operators worked more independently and attended to separate sources of information, this provided the opportunity to keep each other informed and to ensure a common understanding between crewmembers. It also provided better situation awareness for each of the individual crewmembers, thus providing more people who were actively involved in evaluating plant status and who could provide valuable input at critical times. EOP training was then used to reinforce this new approach to emergency management.

3.5.3.5 Evaluate Staff Qualifications

Following the evaluations of integrated task performance and teamwork (and any changes that may have been implemented as a result of the evaluations), an evaluation should be made of whether any changes in staff qualifications are necessary. Personnel may require specific knowledge, skills, and abilities (KSAs) in order to perform their assigned task. The staffing and task analyses should be reviewed by members of the training department to determine whether any new training needs to be developed in order for personnel to perform the task. New KSA that are identified should be addressed in personnel training programs.

Qualification may not only be impacted by task assignments, but may also be impacted by the technology used for the modifications. For example, a modification that includes advanced high-level displays may require balance-of-plant operators to have a more advanced understanding of thermodynamics. Similarly, when sophisticated automation techniques are introduced, the nature of the operators' role changes from a 'hands-on' activity to a monitoring role, which may require greater familiarity with sensor technology and programming logic. Any impact on qualifications of changes to technology should be identified as well.

As discussed in the introduction, personnel physical qualifications and selection criteria could potentially be affected by the technology or final HSI configurations.

3.5.4 Documentation

The results of the evaluation of staffing, qualifications, and integrated work design should be documented to include:

The allocation of tasks to crewmembers, including any changes in task assignments that may have been made to make tasks more efficient or to reduce workload

- Any changes to how teamwork is supported
- Any changes to personnel qualifications that are necessary
- Any changes in required staffing levels
- The methodology used to conduct the evaluation and its results

3.5.5 Grading the Staffing Analysis Effort

Section 2.4.2, A Graded Approach to HFE, introduces the concept that the level of HFE effort for a modification should be based on the nature of the risk significance and complexity of the change. A methodology is provided to establish a grade for a modification in one of three levels: Level 1 – high risk, Level 2 – moderate risk, or Level 3 – low risk. The methodology presented in this section corresponds to a Level 1 effort. Modification programs engaged in Level 2 or Level 3 activities, may consider streamlining the methodology in the following manner.

It is recommended that for Level 2 and Level 3modofications, each of the basic steps in the methodology should be performed; however, evaluations can be limited to obtaining a review by affected personnel that the assignments and impacts are acceptable. If the review uncovers a concern, that specific topic can be addressed in more detail.

3.5.6 Use of the Results

The results of these analyses are used in the following ways:

- Input is provided to the analysis of human error
- Input is provided to the HSI and procedure design to so that they can reflect the task assignments to individual crewmembers
- Input is provided to training personnel, so that they can develop appropriate training objectives and programs to support task performance and to meet the necessary job qualifications
- If the analyses suggest staffing reductions are possible (or increases needed), these may have licensing implications. In that case, input should be provided to licensing analyses (see Section 5).

3.6 Human Error Analysis

3.6.1 Introduction
3.6.2 Objectives
3.6.3 Methodology
3.6.3.1 Inputs
3.6.3.2 Select Tasks
3.6.3.3 Augment Task Descriptions
3.6.3.4 Identify Potential Errors
3.6.3.5 Consider Implications for HRA/PRA
3.6.4 Documentation
3.6.5 Grading the Human Error Analysis Effort
3.6.6 Use of the Results

The purpose of this section is to provide guidance for evaluating the impact of a modification on human errors related to plant operations or maintenance. It provides a basis for developing improvements to the design to mitigate or eliminate potential human errors.

3.6.1 Introduction

Evaluating the potential for erroneous personnel actions that may affect plant operations or safety is essential to achieving the design goal of providing effective HSIs, procedures, and training. Analysis of potential human errors should continue throughout all phases of the design process: the Operating Experience Review should help identify sources of potential error in the past with previous designs and configurations, automation of high error-prone or unacceptable error consequence activities is a major objective of the function allocation, and the task analyses should include analyses of potential errors. The detailed design of the HSI should focus on methods to prevent or minimize human errors and making the system "error tolerant" by providing for error detection and recovery from errors that can have serious consequences. Both the development of operational and maintenance and testing procedures, and the system training should consider how to prevent errors, include confirmatory steps to recognize when errors have occurred, and include how to recover from expected errors that have happened. One of the major goals of the Verification and Validation process is to assure that the design and implementation have, in fact, minimized the error-likely configurations. As a practical matter, the informal analysis and development of error mitigations will never end, simply because humans will always commit new, previously unanticipated errors throughout the life of the plant, often fostering later modifications in the life cycle.

Within this global error-mitigating perspective, the formal analyses that are performed as part of plant probabilistic risk analyses (PRA) may be required as part of the plant licensing basis. The PRA's can cover a wide continuum of specificity and detail. Most tend to be hardware-oriented or at global system levels of detail. It is highly desirable, however, that such analyses consider the probabilities of successful human performance and the probabilities of human errors, which is called Human Reliability Analysis (HRA). In this context, human errors are typically analyzed for the purpose of estimating their probabilities, so that human actions can be taken into account in risk assessment. During the design process, there is less concern with quantification than with identifying potential human errors and reducing their likelihood and their consequences.

This section is concerned with evaluation of potential human errors as part of the design process and does not address quantitative HRA. Nevertheless, it should be recognized that a digital upgrade or modification might impact existing plant risk analyses (e.g., PRA). At the later stages of the implementation, formal risk analyses may require modeling of new or modified human actions, quantification of the associated human error probabilities, and integration of these analyses into the PRA. Thus, while this section focuses on evaluation of potential errors to support the design, the results of the human error analysis can provide input for making any necessary changes there. (See Section 5.2.6 for more discussion of this in the context of licensing).

3.6.2 Objectives

The objective of this analysis is to identify errors having potentially significant consequences. When identified early enough in the design process, effective means for mitigating these errors can be introduced. It is assumed that quantification of error probabilities and of the likelihoods of plant events is not required (i.e., the result of this analysis is not to create or modify an HRA).

Uses of the results of human error analyses are discussed in Section 3.6.6.

3.6.3 Methodology

The process for analyzing human errors is provided below, and illustrated in Figure 3-18. The complete methodology is for a Level 1 analysis. For recommendations on grading the methodology, see Section 3.6.5. In addition to the specific grading recommendations provided, the effort associated with conducting this HFE activity is also based on whether the same or similar analysis has been conducted in association with earlier modifications. The design team should typically start with prior analyses and modify or extend them as appropriate for the current modification. In some cases, even if the modification is Level 1, the availability of prior analyses may result in little new effort required for the current modification. Thus, when conducting this or any HFE activity, the team should ensure that the results of any relevant prior analyses are examined and applied as appropriate.

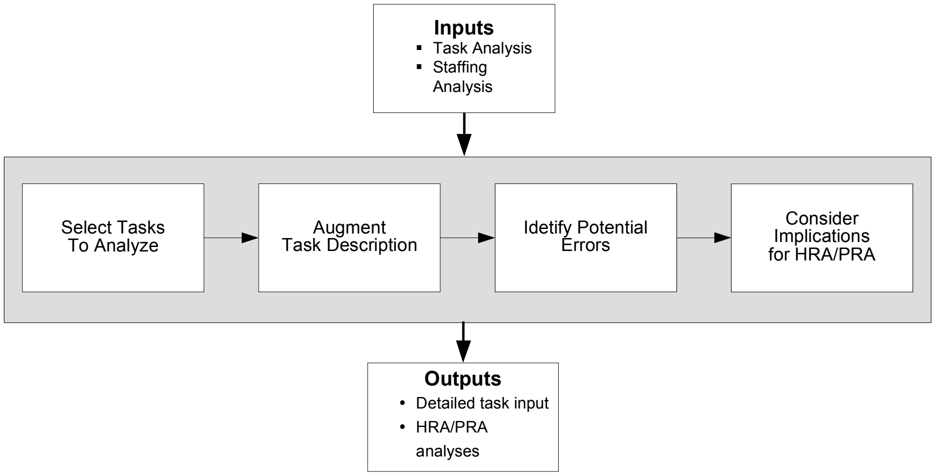


Figure 3-18
Human Error Analysis Process

The initial steps, described at the task level (rather than individual actions), are intended to characterize tasks in enough detail to decide whether/which errors might be expected to occur during the tasks and whether they will have significant consequences. For this analysis, only the tasks selected in Section 3.4 should be considered, i.e., those corresponding to a Level 1 or Level 2 analysis or those tasks designated as “Demanding or Difficult to Perform”. Errors considered significant are analyzed in detail (the later part of the process). This further analysis concentrates on the subtasks and individual actions associated with the error. Breakdowns of tasks to this level will typically have been done as part of the task analysis; if detailed breakdowns are not available, they will be developed as part of this analysis. The aim of this analysis is to define the circumstances surrounding an error so that means for reducing the error can be identified.

3.6.3.1 Inputs

Human error analysis uses information developed in other analyses (e.g., task analysis and staffing analysis) to identify human actions and action sequences in which human errors may occur. It can only be done when the tasks and contexts (especially changes to tasks or circumstances associated with the upgrade) are well defined, which implies that the task analysis and staffing analysis have been completed and the HSI design is defined enough to support these analyses. However, it should be recognized that these analysis are iterative, and aspects of the design may not be fully specified when the initial analyses are done.

3.6.3.2 Select Tasks

When analyzing complex systems, comprehensive consideration of all personnel actions is not feasible; it is typically necessary to develop screening criteria and, for new designs, to select tasks or human actions to be analyzed from the full set of tasks across the entire design. However, for a system upgrade or modification, the identification of key tasks to be included in the human error analysis can be limited to those systems, interfaces, tasks, or actions that are affected by the modification, which should already have been identified by the task analysis process (see Section 3.4). This selection should have already been accomplished as a Section 3.4 activity for a Level 1, Level 2, or Level 3 analysis.

For a Level 1 analysis, additional tasks should be identified (based on operating experience and previous risk analysis) that will also be evaluated for human error potential. The task analysis should already include tasks related to the modification known to have caused problems and identified high-risk tasks. This additional activity is to identify any tasks that may not have been addressed in the task analysis but that might be indirectly affected by the modification. For example, the system failure analysis may identify specific errors or types of errors that are important from a system standpoint but were not identified in a task context (see Section 5.2.2.). Such tasks should be analyzed to the level described in Section 3.4 to allow the error analysis.

3.6.3.3 Augment Task Descriptions

The activities in this section are recommended for a Level 1 analysis.

Descriptions of the tasks for which errors will be analyzed should be augmented with details concerning how error might occur, circumstances that predispose toward (or mitigate against) errors, and pertinent characteristics of the HSI.

Augmenting the task descriptions will require subject matter experts; at a minimum, personnel who are expected to perform the tasks should be consulted. Table 3-11 contains sample questions that can be asked of personnel in the course of reviewing or talking through the task to be analyzed.

Table 3-11
Sample Questions for Human Error Analysis

- Are there any adverse reasonable and credible conditions, occurring either coincidentally with the event or in a casual relationship to it (e.g. a loss of power occurring at the same time as, and possible as a result of, a storm), which could affect the level of performance significantly?
- How stressful do you think the scenario would be for the operating team? Have you been in any events like this one, or in any other emergencies/abnormalities? Would you anticipate this being more or less stressful?
- What do you believe would be the most credible way in which this task could fail?
- Can you think of any errors or unintended actions that could delay the task's completion or jeopardize it entirely?
- Are there any problems if this task is interrupted prior to completion?
- Are there any steps in performing the task that may be confusing, and in which errors may occur?
- Is adequate and understandable information available at each step of the task to support decision-making and selection of appropriate response actions?
- Is access to any control, or possible confusion between different controls, a possible problem that could cause an error?

Since the HSI design details have a major influence on error, personnel should be questioned about their use of HSIs to carry out the task. Those soliciting this information should keep in mind that personnel might take interfaces for granted; they may routinely 'work around' existing deficiencies, or may uncritically accept new interfaces as better. Several examples of aspects of HSIs that can predispose toward error are identified in Table 3-12. Features that protect against error include those that:

- Prevent actions from being omitted from a sequence (e.g., making the final action of a sequence unavailable until all of the other actions have been performed)
- Prevent certain sequences from being carried out or certain states from being reached using interlocks (e.g., by making an action unavailable unless necessary preconditions exist)
- Make certain high consequence actions harder to perform or make them involve extra actions (e.g., make explicit confirmation of certain actions required)
- Allow the user to carry out actions but limit the effect that they can have on the controlled process (e.g., by blocking erroneous inputs that would result in damage to equipment)[7]

Consult any available results of testing of the pertinent interfaces or prototypes, particularly for new or modified HSIs.

Table 3-12
Interface Characteristics that can Induce Errors

Appearance

- Do displays or control panels look cluttered?
- Is it difficult to find important information and controls?

Complexity

- Are complex command sequences, manipulations of data, complex calculations, or perceptual or mental operations necessary?
- Will users find it hard to understand or predict what the effects of carrying out commands or actions will be? Is close attention to unimportant details required?
- Do actions have complex side effects?

Discriminability

- Do different controls look or feel the same?
- Are data that mean different things displayed in visually indistinguishable ways?

Consistency

- Are similar tasks carried out in different ways?
- Are similar data displayed in different formats for no apparent reason, e.g., to optimize information presentation for task-related purposes?

Transparency

- Is the function and method of activation of controls hard to determine from their appearance?
- Does the representation of data fail to make apparent the ways in which they can be manipulated?

Modes

- Does the system have different modes in which the same input has different effects and/or the same displayed data has a different meaning?
- Does the interface lack clear indications of the currently active mode?
- Can the mode change automatically (i.e., other than at the users request)?

Note: A "yes" answer to each question indicates an interface characteristic that can induce error.

[7] The industry has on-deign approaches to help support such actions (actions whose consequences may be severe), such as the STAR method where another person verifies the action before it is performed.

3.6.3.4 Identify Potential Errors

The activities in this section are recommended for a Level 1 analysis.

Once the human error considerations have been added to the selected tasks descriptions, they should be reviewed to explicitly identify potential errors and changes to the task that might reduce the likelihood of errors or mitigate their consequences. Table 3-13 identifies circumstances that might predispose personnel to make errors (Table 3-13 is long so it is located at the end of this section).[8] The table prompts the analyst to consider the general reason for an error occurring for each task (see the first row of the table). Various reasons are given in the shaded rows in the remainder of the table. The analyst should consider more specific possible causes (given on the left side of the rows directly below) for any reasons judged to be likely sources of failure of the task. For each of these causes, related design features are listed (directly to the right of the causes in the table) that should be considered in the design. These features are meant only to illustrate possible approaches. Designing for error prevention and tolerance is discussed in Section 3.7.3.4.4.

The table is not comprehensive. If the task description or error considerations suggest potential reasons for error or related design features not in the table, the analyst should add to the table as needed.

3.6.3.5 Consider Implications for HRA/PRA

Potential impact on the plant's PRA should be considered for Level 1, Level 2 or Level 3 modifications.

A determination should be made as to whether the modification introduces new human actions that, although not included in the existing HRA, might nevertheless affect systems modeled in the PRA. Effects of the modification on assumptions made for human actions already included in the HRA should also be considered. If the modifications affect systems involved in the PRA, personnel responsible for evaluating or carrying out PRA/HRA changes should be informed of how the systems are impacted and how the operator actions that may be involved have changed.

3.6.4 Documentation

The human error analysis will identify potential errors and related design features for the selected tasks. This information should be added to the high-level description of each task (see Section 3.4.3.3); if the high-level descriptions a have been developed in tabular form (as shown in Table 3-6), the description of the error will be entered under "Failures". If potential errors have been identified for a large number of tasks (as in an extensive modification) it may also be useful to record the error causes and related design features in a table or spreadsheet so that they can be sorted. Grouping tasks with similar causes for potential error or design features to be considered may allow the results to be used more effectively during detailed design.

[8] The table is an abbreviated version of a much more elaborate human error identification method proposed by Kirwan (1994).

3.6.5 Grading the Human Error Analysis Effort

Section 2.4.2, A Graded Approach to HFE, introduced the concept that the level of HFE effort for a modification should be based on the nature of the risk significance and complexity of the change. A methodology was provided to establish a grade for a modification into one of three levels: Level 1 – high risk, Level 2 – moderate risk, or Level 3 – low risk. The methodology presented in this section corresponds to a Level 1 effort. Modification programs engaged in Level 2 or 3 activities, may consider streamlining the methodology in the following manner. Aspects of the complete Level 1 methodology that may be useful to a particular utility's specific modification may be included were benefits would be obtained.

For Level 2 programs, it is recommended that the tasks for which error analysis is to be performed be selected based on the criteria in Section 3.4. The possible errors in those tasks should be evaluated by relevant members of the design team, including personnel performing those tasks, those knowledgeable in the design of the systems involved, and HP and training personnel.

No formal human error analysis (as described here) is recommended for Level 3 analyses, except as follows: If a task that is modeled in the existing plant PRA is affected by the modification and thus the reliability numbers in the existing plant PRA may be affected, an error analysis of that task may be required. In any case, as part of task analysis, the analyst should always consider what can go wrong and include that information in the results of the analysis.

3.6.6 Use of the Results

As indicated above, the principal use of the analysis of human error is to help designers and subject matter experts 'design-out' error, beginning early in the design process. Accordingly, the results are an input to HSI and Procedure Design (Section 3.7) and to training as well. Anticipating and designing against potential errors allows the effects of error to be reduced (e.g., by blocking erroneous action, help in identifying the occurrence of the error, aiding recovery, or limiting consequences). The analysis can also reveal 'upstream' opportunities to improve performance and thereby prevent errors; see the discussion of error-tolerant design in Section 3.7.3.4.4.

As mentioned earlier, task modifications for preventing or mitigating error should be re-evaluated to ensure that issues have been addressed and that no new error vulnerabilities have been introduced; i.e., the human error analysis is part of an iterative process. The results of the error analysis should also be fed back into the system failure analysis. The information developed in the analysis may also be of use in later formal risk analyses.

Table 3-13
Human Error Identification

If an error were to occur involving the task, is it likely to be the result of misdiagnosis or misinterpretation, possibly due to a misperception of signals or expectations; the complexity of the situation itself; a failure to notice special circumstances?	
Possible Causes	**Design Features to Consider**
personnel prematurely interpret the situation	• fault diagnosis training • procedures • crew composition • computerized operator support systems • critical function monitoring aids
personnel fail to consider the full complexity of the situation, leading to a simplistic solution	• training • procedures • integrated displays of higher level functions • computerized operator support systems
personnel placed in a novel and complex situation outside of existing procedures (e.g. a beyond design basis accident or multiple failures)	• training • function-based displays • crew composition • procedures • critical function monitoring aids
the indication that the task should be carried out is in conflict with the current diagnostic 'mindset'	• procedures emphasizing disconfirming as well as confirmatory signals • crew composition and teamwork supporting independent checking • training • signals • automation
multiple events causing a high level of complexity or a high workload	• task automation • staffing strategies • automatic information recording (trends, logs, print- outs) • crew composition, teamwork • decision/ diagnostic support facilities
personnel predisposed to misevaluate owing to under/over concern with particular consequences	• training emphasizing risk • procedures emphasizing criteria of concern in sequences

Table 3-13
Human Error Identification (Continued)

If an error were to occur involving the task, is it likely to be the result of personnel failing to act on a signal?	
Possible Causes	**Design Features to Consider**
the signal source fails	• diverse/redundant signal sources • higher-reliability signal system • training • procedures incorporate checks on ‘no signal’
the signal is normally irrelevant	• smart signals (mode dependant) • variable signal thresholds, set points
the signal is perceived as unreliable	• diverse signal sources • high signal reliability • training on signal reliability
the signal is inconspicuous	• prioritized signals • signals integrated in principal displays • alarms • training in signal priorities • procedures referencing the relevant signals • increased signal intensity
the signal is easily confused with other signals	• multiple-signal coding • layout of displays • distinctive signals
the signal occurs very rarely	• training for low-frequency events • alarms • diversity of signals, e.g., via alarm and display indication • signals prioritized into a multi-level hierarchy, e.g., higher-level alarms and lower level detailed alarms

Table 3-13
Human Error Identification (Continued)

If an error were to occur involving the task, is it likely to be the result of personnel lacking needed information?	
Possible Causes	**Design Features to Consider**
important information missing due to instrument failure or lack of instrument	• diverse signal sources, sensors, power supplies • annunciation of instrument failure • periodic manual checks • procedures specifying action in event of signal failure • automatic protection/action • higher-reliability components
erroneous information sources	• diverse signal sources • procedures specifying cross-checking • system-self-integrity monitoring • higher-reliability sources
personnel select a different but similar appearing information source	• unique coding of displays, coordinated with procedures • distinctive coding for units and trains • training
ambiguous data	• task-based displays • symptom-based diagnostic aids • diverse information sources • clarity of information display • alarm conditioning
large amount of redundant or irrelevant data	• prioritized information displays (especially alarms) • overview mimics (VDU or hard wired) • task-based displays • training and procedural emphasis on data-collection
needed data distributed across HSI, so that retrieving it is time consuming and unreliable	• task-based displays

Table 3-13
Human Error Identification (Continued)

If an error were to occur involving the task, is it likely to be the result of a failure to use the proper procedure?	
Possible Causes	**Design Features to Consider**
personnel unaware that procedure exists	• displays emphasize entry conditions • computerized operator aid • training
personnel fail to select the procedure in time	• entry conditions alarmed • computer-based procedures • automatic systems to protect components • training
personnel select the wrong procedure	• procedure design, checks • training • crew composition • task based displays emphasizing entry conditions
personnel too busy to select the procedure	• training • automation • interface and procedural prompts during events • crew composition • remote incident-monitoring

Table 3-13
Human Error Identification (Continued)

If an error were to occur involving the task, is it likely to be the result of a failure to correctly execute a procedure?	
Possible Causes	**Design Features to Consider**
personnel carry out the task too early	• training • perception (time) cues • time-related displays
personnel fail to carry out the action in time	• training • team training and crew-coordination trials • procedures • design of equipment • automation
personnel carry out the task inadequately	• training • design of equipment • detailed, explicit procedures • accurate and timely feedback • error-recovery potential • checking • automation
personnel lose their place in the procedure or forget one or more items	• procedures with built-in checks • error recovery potential • good system feedback • supervision and checking
personnel fail to follow the procedures entirely	• training in use of procedures • procedure design
personnel fail to observe cautions or warnings	• procedure design (e.g., sign-offs) • computerized procedures
personnel fail to complete the task	• memory aids in procedures • cues in task-based displays • checking and supervision • feedback • automatic procedure tracking • training

Table 3-13
Human Error Identification (Continued)

If an error were to occur involving the task, is it likely to be the result of a previous (latent) maintenance or calibration error, leading to difficulties or errors in responding to a situation?	
Possible Causes	**Design Features to Consider**
poor maintenance procedures	• procedure design (e.g., cautions, check-offs)
inadequate checking	• computerized or automated calibration
If an error were to occur involving the task, is it likely to be the result of a parameter check that failed, was omitted, done on the wrong system or at the wrong time, or simply the wrong kind of check?	
Possible Causes	**Design Features to Consider**
personnel omit key parameters in the evaluation process (i.e. fail to check them)	• task-based displays • evaluation aids in procedures • team training • automation • alarms
personnel check but ignore key parameters during the evaluation process	• task-based displays • training and supervision • procedures • remote incident-monitoring • automation • alarms
If an error were to occur involving the task, is it likely to be the result of an information communication error?	
Possible Causes	**Design Features to Consider**
the signals to carry out the task rely on oral communication	• physical back-up/ substitute signal • communications requirements specified in procedures • workplace design
information not transmitted effectively on shift turnover	• robust shift hand-over procedures • training • team training across shift boundaries • robust data-recording systems • specific shift-turnover displays
it is not clear who should respond	• training and task allocation among crew • team training

Table 3-13
Human Error Identification (Continued)

If an error were to occur involving the task, is it likely to be the result of an action being carried out incorrectly?	
Possible Causes	**Design Features to Consider**
personnel carry out the right action on the wrong equipment	• display/panel enhancements (paint/label/tape approaches) • design of controls and displays (e.g., modes) • procedure design • training
personnel carry out the wrong action on the right equipment	• training • supervision and checking • procedures with checking facilities • design of soft controls • error checking features • engineered limits on unwanted actions (e.g., interlocks) • error-recovery potential • prompt system feedback
If an error were to occur involving the task, is it likely to be the result of an incorrect action being carried out?	
Possible causes:	*Design features to consider:*
misdiagnosis, misevaluation (see above)	• (see design features related to misdiagnosis, etc. above)
execution error (i.e., slip)	• design of controls • engineered limits on unwanted actions (e.g., interlocks)

3.7 Human-System Interface and Procedure Design

3.7.1 Introduction

3.7.2 Design Process Steps

3.7.3 Methodology

3.7.3.1 Inputs

3.7.3.2 Requirements

3.7.3.3 Style Guide Development

3.7.3.4 Detailed Design

3.7.3.5 HSI Integration

3.7.3.6 Procedure Revisions

3.7.3.7 HSI/Procedure Tests and Evaluations

3.7.4 Documentation

3.7.5 Grading the HSI Design Effort

3.7.6 Use of the Results

3.7.7 Appendix – Vendor HSI Evaluation Questionnaire

3.7.1 Introduction

The human-system interface (HSI) provides the resources needed by personnel to interact with plant functions, systems, and components. The various aspects of the HSI are illustrated in Figure 3-19. The basic building blocks of computer-based HSIs are the information display and user-interface interaction and management features. With these building blocks, HSI resources can be developed to support other functions, such as monitoring and detection (alarms), situation assessment (computerized operator support systems), response planning (computer-based procedures), and response implementation (soft controls). There are unique display and interaction needs for each. Since nuclear power plant operation requires working in crews or teams, communications are needed for many tasks. HSI resources are integrated into workstations and workplaces. While detailed guidelines for HSI design are provided in Section 4, this section addresses the process by which the HSI is designed.

Computer-based HSIs provide an opportunity to significantly improve upon analog HSIs in which controls and indicators are discrete devices, alarms are presented using one or more standalone annunciators, and procedures are provided separately in paper form. Several aspects of computer-based HSIs and the potential improvements they offer are described below:

- *Integration* – The designer no longer has to think of alarms, displays, controls, and procedures as separate aspects of the HSI. Instead, these HSI resources can be fully integrated to meet the user's needs. Thus for example, HSIs can be developed in which procedure steps are presented on displays that contain all relevant alarms, data, and controls required for task performance. Controls can be developed that contain all data needed to take the control action, to provide feedback, and to reveal the control logic. All information related to the user's ongoing activity can be integrated into task-oriented display screens.
- *Processing* – Data can be presented to the user in the specific way in which it is needed. Lower-level data can be synthesized into higher-level information that is directly usable. Users can be given high-level displays to support monitoring and situation assessment with immediate access to lower-level displays to support trouble shooting.
- *Decision Support* – Support logic can be built into HSIs to help users make decisions, such as to find the most important alarm, to evaluate the status of a procedure step, or to diagnose the cause of a process disturbance. More advanced decision support, such as providing predictive displays for time to trip and time to PWR primary coolant boiling can be considered as well.
- *Flexibility* – The HSI can be tailored to better meet the demands of the user's ongoing tasks and to accommodate personal preferences.
- *Portability* – Computer-based HSIs exist in a virtual world, not a physical world. Thus the users can work at workstations at which all HSIs can be accessed, rather than users having to go to where specific HSIs are physically located. Further, HSIs can be made available essentially anywhere. A specific control, for example, may be accessible from any control room workstation and from local control stations.

- *Automation* – Computer-based HSIs can provide features that automate certain interface management tasks. For example, when an alarm occurs a computer-based display can automatically present a link to the associated alarm response procedure or provide other information that is needed to confirm and respond to the alarm.
- *Team Support* – Features can be provided in the design that enhance the ability of the crew to operate as a team. For example, large overview displays can be provided that are visible to the entire crew and provide a common view of the status of key plant systems, variables, trends and important alarms. A supervisor can access information that an operator is currently using for a task, helping to detect and correct any errors.

The guidance provided in this section and in Section 4 is designed to help realize these desirable features of computer-based HSIs.

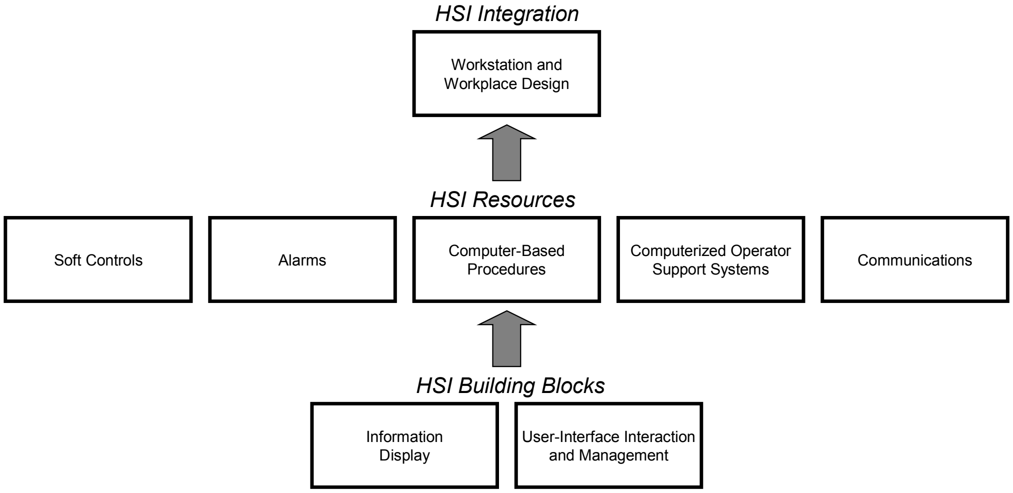

HSI Integration
Workstation and Workplace Design
HSI Resources
Soft Controls
Alarms
Computer-Based Procedures
Computerized Operator Support Systems
Communications
HSI Building Blocks
Information Display
User-Interface Interaction and Management

Figure 3-19
General Aspects of HSI Design

The HSI design process represents the translation of task and staffing requirements into HSI characteristics and functions. The HSI should be designed using a structured methodology that guides designers in identifying and selecting candidate HSI approaches, defining the detailed design, integrating new and old HSIs, and performing HSI tests and evaluations when needed. While the main emphasis of this section is on HSIs, it also addresses plant procedures since they are an integral part of the operators' task performance. Significant plant modifications can result in new procedures that need to be developed and modifications to existing procedures to reflect the changes in the plant and HSIs. For a variety of reasons, traditional conventional control rooms did not provide redundant HSI panel-mounted devices and resulted in compromise configurations and layouts that needed to be suitable for all possible situations and evolutions. Operating procedures often had to accommodate the limitations of the existing control panel layouts and the resulting staffing distribution of responsibilities dependent upon the control panel configurations. One of the great advantages of new distributed controls systems with computer-based HSIs is that the same displays and controls can be presented in different formats and on different screens. This permits development of task-specific control/display screens with configurations and layouts optimized for specific tasks, evolutions or events. This, in turn, can lead to development of more efficient operating procedures that take maximum advantage of the enhanced screen organization capabilities. With new soft control systems, the operating procedures and control screens should be developed together, each reflecting the other, regardless of whether the procedures use conventional paper-based or computer-based presentation media.

3.7.2 Design Process Steps

The objective of this section is to provide guidance on using HFE analyses to develop HSI and procedures that:

- reflect the plant's functional and physical design
- meet personnel task requirements
- exhibit the general characteristics of a well-designed HSI, listed in Table 3-14
- are easy to use and learn

Uses of the results are discussed in Section 3.7.6.

Table 3-14
General Characteristics of a Well-Designed HSI

Accurately represents the plant
Meets user expectations
Supports situation awareness and crew task performance
Minimizes secondary tasks and distractions
Balances workload
Is compatible with users' cognitive and physical characteristics
Provides tolerance to error
Provides simplicity
Provides standardization and consistency
Provides timeliness
Provides openness and feedback
Provides guidance and support
Provides appropriate HSI flexibility

Note: See Section 4.0 for a discussion of these characteristics

3.7.3 Methodology

An overview of the methodology is illustrated in Figure 3-20. For a discussion of grading this activity, see Section 3.7.5.

The process proceeds in the order indicated; however, there will be iteration involved and some of the activities are closely related and proceed largely in parallel. The major elements are as follows:

- The HSI design process begins with information developed in formulation of the endpoint definition and the HFE analyses that specify changes to human functions (automation), new and modified tasks and the requirements for their performance, and the expected allocation of work to various crewmembers. Other inputs are also important (as discussed in Section 3.7.3.1)
- Using the input information, one or more concept designs are developed that reflect these inputs (as discussed in Section 3.7.3.2)
- Once a concept design is selected, a style guide is developed, if one does not already exist from a previous modification. The style guide defines the detailed design criteria for the HSI elements. If one does exist, it should be evaluated for any needed revisions based on the current modification (as discussed in Section 3.7.3.3)
- The detailed design of the HSIs should be developed conforming to the principles in the style guide (as discussed in Section 3.7.3.4) (Actually, in practice, the style guide development and detailed HSI design are developed in parallel as an iterative process. The style guide should be based on limitations and features in the HSI being used, and details of the HSI implementation should consistently reflect decisions codified in the style guide.)
- As with any modification, the new HSIs must be integrated into their locations (e.g., main control room or local control stations) and must be compatible with existing equipment (as discussed in Section 3.7.3.5)
- Finally, procedures have to be developed and/or modified to reflect plant changes (as discussed in Section 3.7.3.6)

At any point along the way various types of tests and evaluations will need to be performed to collect needed information, obtain user feedback, resolve design options, or evaluate performance of the new HSIs (as discussed in Section 3.7.3.7). When tests and evaluations are involved, the methods and tools provided in Section 3.10 can be used. Each of these activities is discussed below.

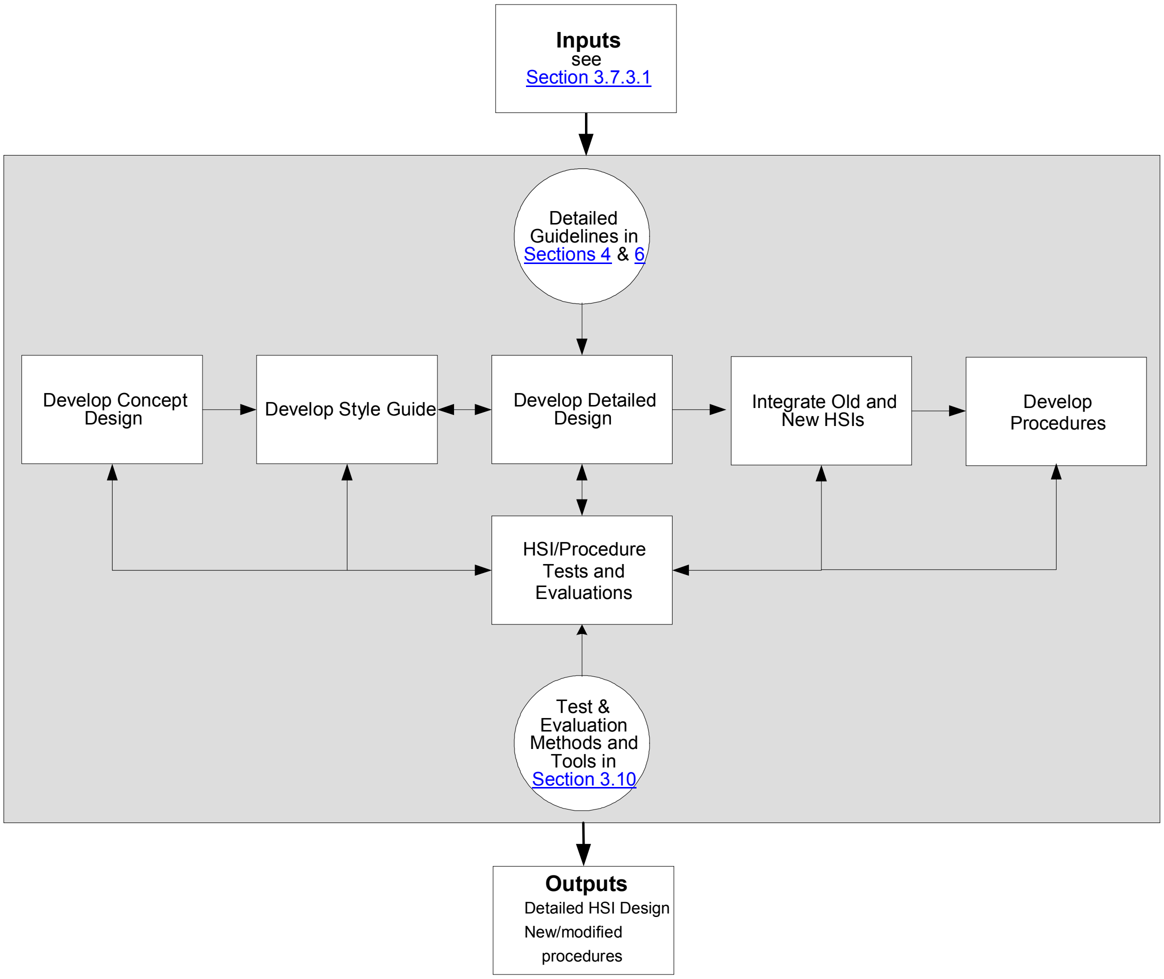


Figure 3-20
HSI Design Methodology

3.7.3.1 Inputs

The following inputs from HFE analyses conducted earlier should be used:

- *Endpoint Definition* and the scope and goals defined for the present modification
- *Operational experience review* – the operational problems and issues, targets of opportunity for improvements, and positive aspects of the current design that personnel do not want to lose
- *Functional analysis and allocation* – changes to automation and the related roles and responsibilities of personnel
- *Task analysis* – the specification of new, modified, and eliminated tasks, as well as their associated task requirements (which should reflect the demands associated with any new systems or equipment)

- *Staffing, Qualifications, and Integrated Work Design* – the changes in staffing and the responsibilities of individual crewmembers
- *Error analysis* – the evaluation of the types of errors that may occur in personnel tasks

Additional inputs to HSI design include:

- Capabilities and limitations/constraints of the chosen platform
- I&C design, e.g., signals that will be available, constraints on computer capabilities, how the controls will actually work
- Physical and environmental constraints, e.g., the size of the control room or the location of panels that will remain in place

3.7.3.2 Requirements

This section addresses the development of a general design concept by specifying functional requirements, identifying different ways these requirements can be met, and evaluating those alternatives so an alternative can be selected for detailed design activities. While functional requirements are needed for any modification, the extent to which the second two activities are performed depends on the maturity of the utility's modernization program. For utilities just beginning their program, it is suggested that alternative designs be considered so that the tradeoffs between different approaches can be explored. However, once this has been done, subsequent modifications may likely use the same approach, thus the second two activities will not be needed.[9]

Section 2.2 discusses the development of an endpoint definition that includes considerations of concept of operations, HSI design concepts, and failure management concepts. When just beginning the HSI design for the first time, the endpoint definition activity should be the starting place. If the reader has not already used the worksheets provided in Section 2.2 to specify the endpoint definition, that activity should be done before performing activities described later in this section. Once the HFE analyses described in Section 3.2 through 3.6 have been accomplished, the endpoint definition can be further developed and refined into a concept design(s) and candidate technological approaches to accomplishing it (them) can be defined.

The steps toward defining the concept design include:

- Develop Functional Requirements
- Develop Alternative Approaches to Meeting Functional Requirements
- Evaluate Alternative Approaches and Select a Concept Design

Each of these steps is discussed below.

[9] It should be noted that even for relatively small modifications, such as replacing recorders, there may still be alternative approaches that are worth considering, e.g., to replace analog recorders with digital recorders or to eliminate them altogether and record all such parameters in the computer system and present the trends on computer-based workstation displays.

3.7.3.2.1 Develop Functional Requirements

Using the inputs defined in Section 3.7.3.1, a set of functional requirements for the HSIs should be specified to address:

- Workplace considerations, including panel changes, workstation design, and general control room layout, if applicable to the current modification
- The general characteristics and functions of HSI resources, e.g., alarms, displays, and controls and their general functional requirements should be established for various types of HSIs

3.7.3.2.2 Develop Alternative Approaches to Meeting Functional Requirements

Alternative ways of meeting the functional requirements should be identified or developed. The reason that alternatives are recommended in this guidance is that they provide an opportunity to explore tradeoffs between different approaches. For example:

- Providing a plant overview in a single, large control room display or making such a display available at individual workstations
- Providing multiple but small workstations for individual crewmembers or one large workstation at which multiple crewmembers work
- Upgrading with panel-by-panel modifications or migration of control and displays to integrated workstations

In practice, this may be accomplished by utility engineers or may be done through vendor offerings in response to an RFP referencing the functional specification. Even for very simple modifications, such as replacing analog recorders with digital recorders, it is valuable to compare functions and features of several alternative designs or products available.

3.7.3.2.3 Evaluate Alternative Approaches and Select a Concept Design

Evaluating alternative designs and getting personnel feedback on them can help the identification of the best solution for an individual utility's overall objectives. Evaluation methods can include:

- trade-off evaluations
- personnel opinions and usability evaluations
- performance-based tests and evaluations

See Section 3.7.3.7, HSI/Procedure Tests and Evaluations for a discussion of specific methods and tools that can be used.

Based on the results of the evaluation, one concept should be selected for more detailed design. This may require some iteration of the features including some additional tests or evaluations.

3.7.3.3 Style Guide Development

Once a concept design is selected, a style guide is developed. A plant-specific style guide defines the detailed characteristics and functions of the HSI elements. If a style guide exists from a previous modification, it should be evaluated for any needed revisions based on the current modification. In this section, the uses and benefits of style guides are discussed followed a presentation of the methodology to develop and update a plant-specific style guide.

3.7.3.3.1 Style Guide Uses and Benefits

HSI design guidance exists at different levels of specificity. Industry guidelines and standards generally provide high-level guidance; Section 4 of this document is an example of this type of information. However, high-level guidance cannot be used, as is, for design. The guidance must be made more specific or precise and that is the role of a style guide. A style guide provides detailed specifications or rules that describe the characteristics and functions of a specific plant's HSI, such as the overall control room layout, display screen organization, the way system features and functions are presented to users, the navigational features and functions, and specific design features such as display fonts and use of color. Use of a style guide will provide for consistent HSI design across all new and upgraded HSIs, even though the designs may be created by different designers. Examples of the differences between high-level and plant-specific HSI guidelines as found in a plant's style guide are provided in Table 3-15.

Some plants already have style guides or their equivalents. Existing plant documents should be considered, and consistency be achieved to the extent possible.

Table 3-15
Examples of General and Plant-Specific HSI Guidelines

Guideline Level	Screen Organization	Font Size
High-Level Guideline (from Section 4 of this document)	Guideline 4.1.4.2-1 General HSI features (e.g., a data display zone, control zone, or message zone) should be displayed in consistent locations from one display to another.	Guideline 4.1.6.1-4 The height of characters in displayed text or labels should be at least 16 minutes of arc and the maximum character height should be 24 minutes of arc.
Plant-Specific Guideline	Each screen will be divided into four zones: an upper zone providing label and identifying information; a left zone providing navigation controls; a lower zone providing alarm, status, and message information; and a large center zone displaying user selected information.	The size of text in displays appearing at workstations (eye to monitor distance of 25 inches or 635 mm) will be as follows: Display Titles 5 mm Equipment Labels 4 mm Parameter values 3 mm General Messages 3 mm Warnings 4 mm

Additional examples appear later in this document in Figure 3-24.

While the primary use of a style guide is to define the detailed design criteria for the HSIs, there are a number of additional and important uses for the style guide.

- *Procurement Specification* – the guidelines in a style guide can be used as the basis for a design specification for HSIs to be procured from vendors. The style guide provides for a comparison of different vendor offerings.
- *HSI Evaluation* – The guidelines in the style guide should be use to evaluate HSI designs offered by suppliers or developed by plant engineering staff. In this application, a verification checklist is prepared using the style guide and the checklist is used to review the design. This usage is discussed further in Section 3.8 on V&V. The style guide may be used in formal Design Reviews to determine that the design has satisfied requirements.

While these are the three main uses of the style guide, it is suggested that the following additional items be considered for inclusion in the style guide *if they are not adequately documented elsewhere*:

- *Overview of the concept of operation* – It is desirable to include set of introductory sections to the style guide to capture key items that should be documented but often are not. This includes the following types of information:
  - the scope of operations in the control room, e.g., what gets automated and what is left to local operations
  - a description of the major control room organization and layout and its functional use
  - a specification of the number of operators, supervisors, and other personnel that must be accommodated in the control room and their division of responsibility (especially if there is a committed division by system or panel, etc.) and whether supervisors are allowed to operate controls
  - specification of sight distances in terms of who is expected to be able to read what qualitatively or quantitatively and from what distances
  - identification of any physical characteristics such as what anthropometrics are used and range to be accommodated (whether perceptually or mobility impaired users are to be accommodated)
  - how security and peer checking is handled
- *Documentation of Design Decisions* – The style guide can be used to track design decisions and their bases. Decisions resulting from development efforts, testing, and user feedback can be incorporated into the guide. That is, when decisions are made regarding preferred approaches to design, e.g., decisions to organize a screen in one way or another, the rationale can be recorded in the style guide for future reference. The availability of this type of documentation supports the design team's evaluation of proposals to modify aspects of the HSI. It also supports design reviews and other external evaluation activities, such as regulatory HFE reviews. The documentation also provides a means to transfer knowledge gained from the design project to other design teams within the organization and to successive generations of designers. As some plant modernization programs can last a decade or more, the latter is not a trivial consideration.

- *Track Feedback from Users* – The style guide can be used to record and track feedback on HSI characteristics and functions from users.
- *Generalization of Feedback* – The availability of a style guide helps to ensure that feedback concerning specific aspects of an interface can be linked to general principles that, in turn, can be generalized to all other HSIs that apply that principle. In that way, problems identified for individual screens can result in improvements to the entire HSI. This feedback should be used to suggest modifications to HSIs that should be reflected in the style guide.

There are benefits to developing and using a style guide. One benefit is that it helps to ensure standardization and consistency of HSI characteristics and functionality. When all members of a design team use the style guide, a standard and consistent look and feel is achieved. The style guide helps to ensure that information is always referred to in the same way, that it is always located in the same place from screen to screen, and that the same functions are performed the same way. When a high degree of consistency is established, the interface becomes almost transparent to users. Transparency enables users to know exactly how to interact with the HSI so they can devote their complete attention to the primary tasks. Excellent interfaces have this characteristic. To the extent that users must stop and think about how to interact with the HSI such as to decide what display has needed information, attention is directed away from the primary tasks. The user's task has shifted from starting the pump to figuring out how to use the HSI. At best, this can lead to frustration. At worst, it can lead to error, which in turn can cause problems such as delaying a startup or damaging equipment. Unless, of course, the non-standard presentation is a seldom-used specific feature to preclude inadvertent actuation-type errors.

A second benefit is that when a style guide is based on sound HFE, then the design is likely to be fully compatible with human physiological and cognitive characteristics. Users bring their physiological and cognitive characteristics to their interaction with HSIs. The HSI must accommodate human visual and auditory perception, information processing characteristics, physical size, and strength. Fortunately, the design engineers do not have to determine these characteristics for each project. Most physiological and cognitive characteristics that are important to HSI design are already reflected in the HFE guidelines (such as those provided in Section 4 of this document).[10]

Ensuring that the design is compatible with human characteristics and provides a high degree of standardization and consistency leads to a number of additional benefits, including:

- *Better and more efficient HSI use* – the principles help ensure compatibility with human characteristics
- *Lower user workload and fewer errors* – consistency makes HSIs more transparent and predictable.

[10] Consider the example of font height from Table 3-15. Font height values are based on visual angle. Visual angle is a measure, in degrees, of the size of the retinal image subtended by a viewed object. It represents the apparent size of an object based on the relationship between an object's distance from the viewer and its actual size (perpendicular to the viewer's line of sight). An object of constant size will subtend a smaller visual angle as it is moved farther from the viewer. Visual angle is typically defined in terms of minutes of visual arc. Minutes of arc can be converted into height for an assumed viewing distance using the formula provided in Guideline 4.1.6.1-4. But the HSI designer does not have to be concerned about the physiological basis for the guideline to design a good HSI. The guideline already has that knowledge built in.

- *Lower training burden* – a well-designed HSI is easy to learn and the knowledge and skills learned with respect to one aspect of the HSI will be easily transferable to other aspects of the interface. Never assume, however, that the designs and conventions implementing the style guide decisions will be self-evident or effective unless they are the subject of specific training for the users. If the users have not been taught the underlying codes, conventions or principles, even when they are perfectly implemented, they may not be effective.

For these reasons, it is highly recommended that utilities develop a style guide for their computer-based interfaces. Once developed the style guide can be used for all future HSI modifications.

3.7.3.3.2 Style Guide Development Methodology

The overall process for developing a style guide is outlined in Figure 3-21. The detailed HSI guidelines that are contained in Sections 4 and 6 of this document provide a significant input to style guide development.

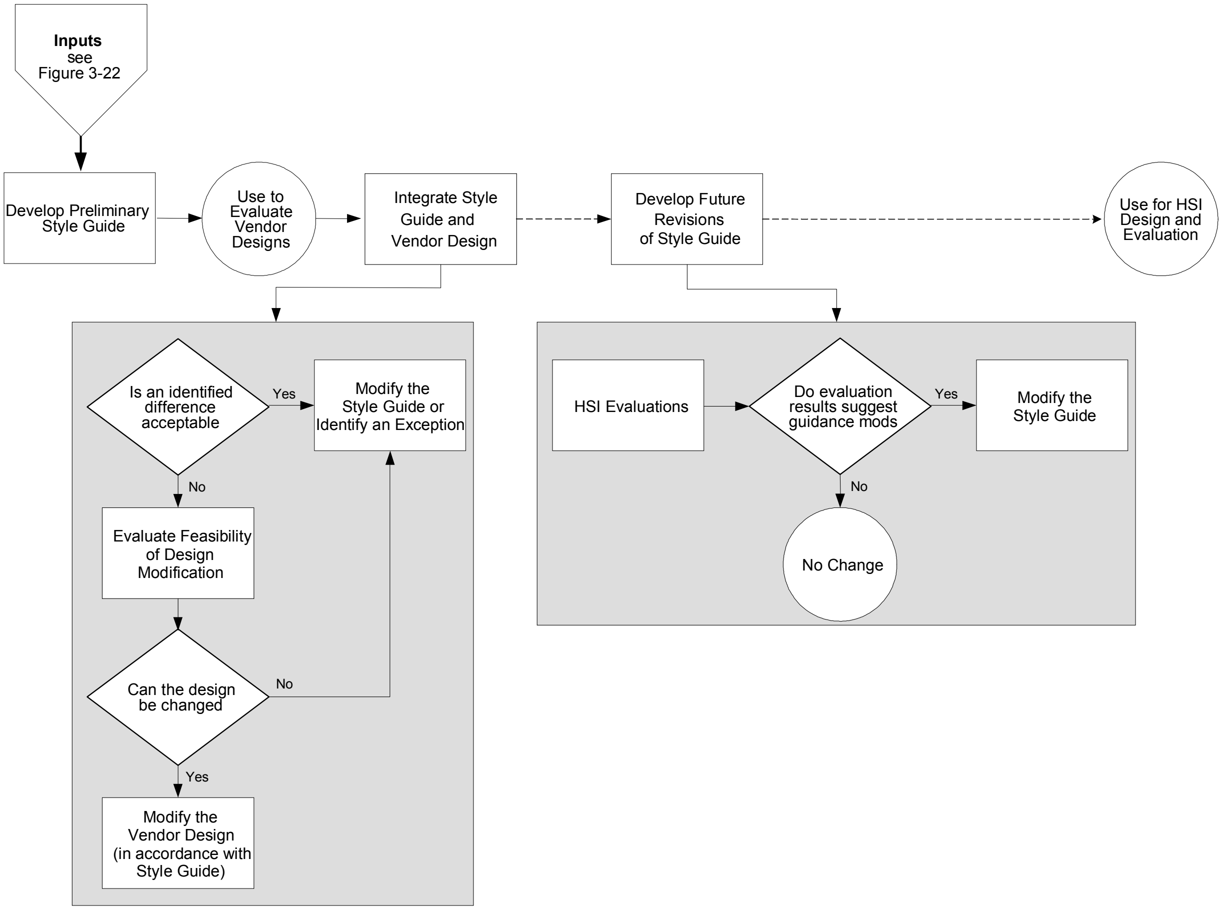

Inputs
see
Figure 3-22
Develop Preliminary Style Guide
Use to Evaluate Vendor Designs
Integrate Style Guide and Vendor Design
Develop Future Revisions of Style Guide
Use for HSI Design and Evaluation
Is an identified difference acceptable
Yes
Modify the Style Guide or Identify an Exception
No
Evaluate Feasibility of Design Modification
Can the design be changed
No
Yes
Modify the Vendor Design (in accordance with Style Guide)
HSI Evaluations
Do evaluation results suggest guidance mods
Yes
Modify the Style Guide
No
No Change

Figure 3-21
Style Guide Development

The recommended approach to preparing and using a style guide described in this section involves the following guidance.

- The style guide development should be evolutionary in that a high-level version of the guide should be developed prior to I&C vendor selection. The style guide should be made more detailed as part of the design process.
- A variety of inputs should used to provide the information from which a plant-specific style guide is developed. This includes input from the vendor design. This reflects the fact that in most cases, utilities will work with an I&C vendor to design their HSIs and that the vendor's approach to HSIs will constrain the design.
- The HSIs should undergo some form of test and evaluation and the findings from these activities should feed back into the HSI design and be reflected in the style guide.

It should be recognized that there are alternative approaches that can be followed. For example, a utility could develop a detailed style guide before vendor selection. The tradeoff is that that approach may require considerable modifications to a vendor's design to bring it into compliance with the HFE guidelines, or, more likely, the style guide will have to be revised to reflect the aspects of the vendor design that were too difficult or expensive to change.

Develop Preliminary Style Guide

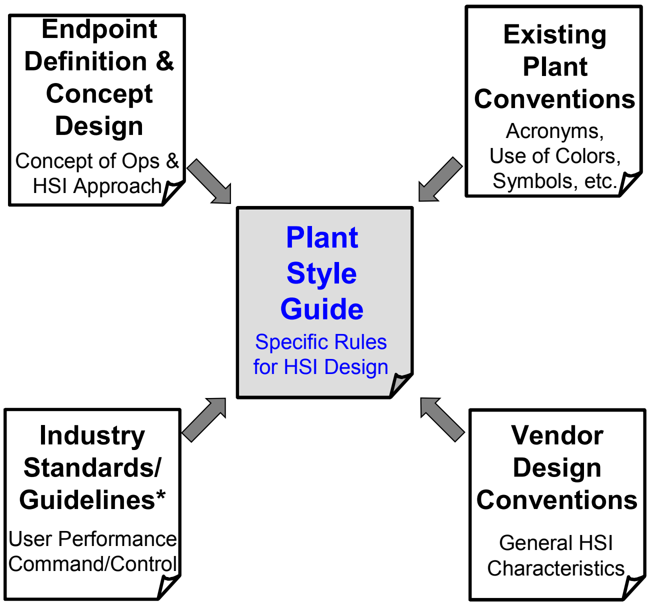
While the exact contents of a style guide will vary, a typical table of contents is shown in Table 3-16. Most of the individual sections shown in the table are self-explanatory or are related to organizational or administrative practices of the individual plant that is involved. The focus of the following discussion will be on Section 6, Guidelines; however, it is also important for the style guide to contain procedures for their use. The procedures should identify where and how HFE guidance is to be used in the overall design process. It should also address HSI modifications. This guidance should specifically address consistency in design across the HSIs. The style guide should be also maintained in a form that is readily accessible and usable by designers and that facilitates modification when the contents require updating as the design matures. Each guideline included in the guidance documentation should include a reference to the source upon which it is based.

The guidelines that are contained in a style guide reflect several sources of relevant inputs (see Figure 3-22). Each of the sources of material contributing to the preliminary style guide is briefly described below in terms of its contribution to the style guide except for vendor design conventions. They will be considered in the next section.

Table 3-16
Examples of General and Plant-Specific HSI Guidelines

1 Purpose and Scope
2 Statement Of Applicability
3 Definitions
4 Responsibilities
5 Procedures for Use
6 Guidelines
    6.1 General Characteristics of a Good HSI
    6.2 Information Display
    6.3 User-Interface Interaction and Management
    6.4 Soft Controls
    6.5 Alarm System
    6.6 Computer-Based Procedure System
    6.7 Computerized Operator Support Systems
    6.8 Communications
    6.9 Workstations and Workplaces
    6.10 Maintainability of Digital Systems
    6.11 Configuration Management and Security
7 Reference Documents (as needed)
Appendices (as needed, such as an HSI Evaluation Questionnaire)

Note: If the style guide is used to document the types of information discussed in Section 3.7.3.3.1, Style Guide Uses and Benefits, then additional sections will be needed.


Endpoint Definition & Concept Design
Concept of Ops & HSI Approach
Existing Plant Conventions
Acronyms, Use of Colors, Symbols, etc.
Plant Style Guide
Specific Rules for HSI Design
Industry Standards/ Guidelines*
User Performance Command/Control
Vendor Design Conventions
General HSI Characteristics

*Sections 4 and 6 of this document provide most of the guidance needed. Industry standards and guidelines can be used to supplement this document if necessary.

Figure 3-22
Style Guide Source Materials

Endpoint Definition and Concept Design for the Current Modification

The endpoint definition and the concept design for the current modification provide important input to the style guide. The concept design is used to identify which topics from the industry guidelines and standards will be needed for the design-specific style guide. For example, if the concept design specifies soft control of equipment and systems, then general HFE guidance for soft controls should be incorporated into the style guide.

Existing Conventions

Existing conventions should be incorporated into the style guide to the greatest extent possible. These conventions come from several sources:

- general cultural and population stereotypes and conventions
- professional and nuclear industry-specific conventions
- plant-specific conventions

General Cultural/Population Stereotypes and Conventions – Plant personnel bring many expectations from their cultural backgrounds to their interactions with HSI applications. These expectations may impact their interpretations of HSI features such as language use, colors, symbols, control actions, and measurement systems (for example, metric system). As the nuclear industry is international and vendor designs may incorporate features not consistent with more general conventions in the U.S., the style guide should also consider these more general standards and conventions. As a simple example, consider date formats. In North America, the convention is month/day/year. In Europe, the convention is day/month/year. While this may seem like a trivial distinction, there are many dates that cannot easily be distinguished simply by looking at the numbers, such as “05/04/02.” If a user is examining a dated maintenance log or an alarm list, misinterpreting the date can have significant consequences. Similarly, if a user has to input dates for system actions, using the wrong format could lead to operational problems. The HSI designers should identify those conventions and ensure the design is consistent with them. This can often be achieved by including such features as part of the initial system configuration.

Professional and Nuclear Industry-Specific Conventions – Plant personnel come from a particular training or professional background, and there are likely to be customary conventions and practices that are commonly used. These can include things such as the meaning of terms, acronyms, symbols, and colors. For example, if specific terms and acronyms are used to refer to system elements, the HSI should use the same terms and acronyms.

Professional conventions can differ from those of the general population. For example, suppose you wanted to show that a pump is “on” by color coding a pump icon. In the general population, you might use the color green to show that the pump is “on” or “going.” However, if the users are primarily from a process control background, green may mean the pump is “off” or “stopped,” while red means the pump is “on” or “going.” Professional and industry practices should take precedence over the general stereotypes when designing HSIs.

Plant-Specific Conventions – It is important to consider HSI conventions that are currently used in the plant for features such as acronyms, color conventions, symbols and icons. Where possible and appropriate, use existing plant conventions. These conventions should be available in documentation. However, it can also be obtained from plant personnel.

Since the HSIs in most plants will reflect a hybrid design, containing a mix of older HSIs and new computer-based HSIs, it is desirable to make the two as consistent as possible, without unduly constraining the computer-based HSIs.

It is also important to consider the relationship of HSI designs to other aspects of design, such as procedures, P&IDs and other plant technical documentation, and training. To the extent possible, the same conventions should be used across all of these information sources. The most important consistency required is between the interface devices and the plant procedures.

Modifications to these conventions should only be made where specific improvements are desired. For example, if at present color use in the plant is not consistent, the plant modernization program can be used as an opportunity to improve and standardize color usage. Similarly, modern computer-based displays can often present symbols and icons in ways that were not possible in older interfaces. The existing conventions may need to modified and expanded based on the new and modernized systems.

In cases where existing conventions may be changed, the changes have to be considered with respect to potential for increased training burden, and the potential for confusion and error that may result from changing the well-learned aspects of an interface. Tests and evaluations may be needed to select the final design of such changes.

Given these considerations, user interface conventions that are to be retained in the new interface will be identified and referenced in this style guide. Where changes are desired due to deficiencies in the current conventions or the desire to improve standardization and consistency, the changes should be identified and incorporated into the style guide or other applicable document to be referenced by the style guide.

Industry Standards and Guidelines

There are many industry standards and guidance documents for the HFE aspects of computer-based HSI design. This EPRI document is an industry guideline and should serve as the primary such input to the style guide development. Some other industry standards and guidance documents should be used to supplement this document as necessary. These industry standards and guidelines include:

- NUREG-0700, Rev. 2 (NRC, 2002)
- IEC 964 (IEC, 1989)
- ISO 11064 (ISO, 1997)

These documents are valuable in that they address:

- the characteristics and functions of key HSI resources, such as alarms, information presentation, and controls
- the design of basic elements of HSI interaction, such as menu bars, dialog boxes, windows, and various types of menus

The information provided in these documents is typically based on years of scientific research on human performance and on lessons learned from the design of different types of systems using this guidance. Thus, they address HSI design features that are needed to assure that the design properly accommodates human characteristics. When a style guide uses this guidance, the designer can have confidence that human characteristics are adequately addressed.

They also address design features that impact human command and control performance in a complex nuclear plant environment. That is the guidance considers the use of HSIs in the demanding task environment where a complex process is monitored and controlled by a highly trained team.

However, since industry guidelines and standards do not reflect one design, they are at a more abstract level than is needed for detailed HSI specification. There is a strong temptation to merely evoke one of these references, such as NUREG-0700, rather than preparing a plant specific style guide. This is seldom effective since many of the guidelines are too general and, as noted above, require further amplification. Further, many of the guidelines are simply not applicable to a given plant or modification, and, because of the way individual guidelines are written and the general tendency of all the subject matter of the individual guidelines to represent optimal levels of some feature or concept that can have negative effects on human performance with either too little or too much, there can usually be found conflicting guidelines. Thus, it is not appropriate to discuss *intended* compliance with all of the reference guidelines. If a plant-specific guideline/approach is obviously in conflict with a regulatory or other guideline, it might be worthwhile to include a specific discussion or justification in the style guide.

All three sources of information (Endpoint Definition and Concept Design for the Current Modification, Existing Conventions, and Industry Standards and Guidelines[11]) will be used to develop the preliminary version of the style guide using the following steps.

First, using the concept design, select the appropriate guideline sections from Section 4 of this document. As mentioned previously, Section 4 contains high-level HSI design guidelines for many types of computer-based HSIs (see Table 3-17 for the contents of Section 4). So the first step is to select those that are applicable to the concept design. The selection can first be made on a section-by-section basis. Thus for example, if the concept design includes computer-based information displays and alarms, but not soft controls, computer-based procedures, or workstations, then Sections 4.1 and 4.4 would be used. However, if the concept design was for an extensive modernization to a fully computerized control room, then probably all of the sections would be included.

[11] Note that the fourth input to style guides shown in Figure 3-22 is the vendor design conventions. That input is discussed in the next section.

Table 3-17
Detailed HFE Guidelines in Section 4

4.1	Information Display
4.2	User-Interface Interaction and Management
4.3	Controls
4.4	Alarms
4.5	Computer-Based Procedures
4.6	Computerized Operator Support Systems
4.7	Communication System
4.8	Workstation and Workplace Design

Once the major sections are identified, the same process can be used within each section to identify the relevant subsections. Also included at this stage are the existing conventions that should be incorporated into the HSI design.

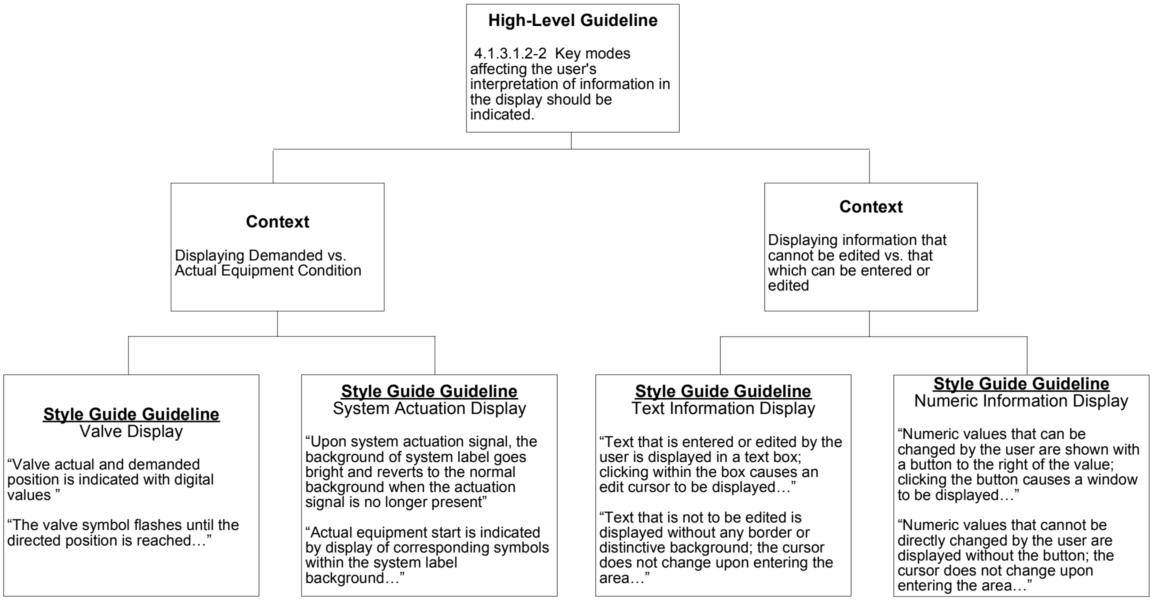
In the second step, the high-level guidelines have to be made specific so designers can use them reliably and unambiguously. This is illustrated in Figure 3-23. At the top of the figure is an HSI guideline from Section 4. It is stated in general terms. However, when it is considered in the contexts of displaying information about some aspect of an operators task, such as inputting a control or displaying what text can be changed or not, it can be made much more specific as the examples in Figure 3-23 illustrate. The items at the bottom of the figure are similar to those that might be found in a style guide.

As the HSI design is in the process of becoming more specific, the guidelines at this stage may not be all fully detailed, as not all design decisions have been finalized. Thus, the preliminary style guide will have a mixture of high-level and detailed guidelines.

The guidance can be used to develop an HSI evaluation questionnaire that addresses key aspects of computer-based HSI resources that can be used to help evaluate vendor offerings in response to the plant's RFP for the first phase of the I&C modernization program. A sample Vendor Evaluation Questionnaire, based on the Section 4 Guidance, is attached as an Appendix. Comparing the vendor product description to the style guide will enable the plant's proposal evaluators to determine if the HSIs proposed are consistent with (or can be easily modified to be consistent with): concept design for control room modifications, existing HSI conventions, and general HFE principles, as reflected in the preliminary style guide.

Integrate Style Guide and Vendor Design

The next evolution of the style guide is made following the selection of an I&C vendor. In fact there may be multiple vendors over the course of several modifications, so vendor conventions have to be evaluated as needed.



High-Level Guideline

4.1.3.1.2-2 Key modes affecting the user's interpretation of information in the display should be indicated.

Context

Displaying Demanded vs. Actual Equipment Condition

Context

Displaying information that cannot be edited vs. that which can be entered or edited

Style Guide Guideline
Valve Display

"Valve actual and demanded position is indicated with digital values "

"The valve symbol flashes until the directed position is reached…"

Style Guide Guideline
System Actuation Display

"Upon system actuation signal, the background of system label goes bright and reverts to the normal background when the actuation signal is no longer present"

"Actual equipment start is indicated by display of corresponding symbols within the system label background…"

Style Guide Guideline
Text Information Display

"Text that is entered or edited by the user is displayed in a text box; clicking within the box causes an edit cursor to be displayed…"

"Text that is not to be edited is displayed without any border or distinctive background; the cursor does not change upon entering the area…"

Style Guide Guideline
Numeric Information Display

"Numeric values that can be changed by the user are shown with a button to the right of the value; clicking the button causes a window to be displayed…"

"Numeric values that cannot be directly changed by the user are displayed without the button; the cursor does not change upon entering the area…"

Figure 3-23
Examples of Level of Specificity from High-Level HFE Guideline to Style Guide Level

Vendor HSIs reflect a specific development environment that is either a general environment, e.g., Microsoft Windows, or their own unique approach. In either case, vendor specific designs reflect specific approaches to HSI design. In some cases, a vendor specific style guide or guidance document may be available. These documents are at a much more detailed level than the industry documents discussed above. The vendor's HSI approach will constrain the characteristics and functions of the basic building blocks of the HSI, such as menu bars, dialog boxes, windows, and various types of menus.

The possible limitations of vendor designs are they do not necessarily reflect good HFE design. Thus, design features may be included that create usability issues or problems. For example, the organization of information in displays may not be consistent with the way plant personnel perform their tasks, thus requiring them to perform excessive display navigation.

Vendor designs also may not be consistent with plant conventions. For example, the icons used may be different from those used in the plant and may not be understandable to plant personnel. As another example, color conventions may be contrary to the way they are used in the plant.

However, the selected vendor's HSI approach provides an input to style guide development and it can be developed further or modified to reflect the approach. In that process, the possible limitations can be addressed.

The process of integrating a vendor design involves incorporating more detailed features into the style guide and evaluating any discrepancies between the design and the guide. This is shown in the left-hand shaded box in Figure 3-22. To evaluate discrepancies, one must first determine whether they are acceptable or not. Input of HSI users, e.g., operators or maintenance technicians, should participate in the evaluation. Three evaluation questions can be used:

- is the vendor design feature consistent with high-level HFE principles (even though it may be inconsistent with the style guide)?
- is the vendor design feature consistent with the endpoint definition?
- will the feature make the design worse in any foreseeable way?

If a positive evaluation to either of the first two questions is obtained, then the style guide might be modified to accommodate the vendor design.

If a negative evaluation is obtained, then an assessment should be made as to whether the design can be changed or not. If so, then a change to the vendor design should be sought. If not, then the style guide may be modified even though the feature may not be desirable, but the feature should be noted as such.

Another option is to “take exception” to the specific guideline in the style guide. For some pieces of equipment (e.g., a single PLC not part of the standard platform) it may be too expensive and not too disruptive to make the conscious decision to accept it even when it is inconsistent with the style guide. In this case, the style guide would not be changed.

If a positive evaluation is obtained from the third question, then the feasibility of a design modification should be explored.

Once resolved, the detailed HSI characteristics and functions can be specified. They will reflect the general HSI guidance (used to develop the preliminary style guide) and the more detailed guidance of the vendor’s HSI design. To illustrate the whole process, consider that the design team wants to specify how alarms will be displayed (e.g., on a message list or in a spatially-dedicated format). The first step may be to consult Section 4 of this document to determine what criteria are used to determine how alarms should be presented. Generally, these are based on operational considerations. This step should already be included in the preliminary style guide. Next the vendor’s approach to these two types of alarm presentations is considered, for example, how message lists are presented. Assuming it is acceptable, the vendor’s approach can be specified as the detailed design for message list design. Otherwise, modifications have to be negotiated. Thus using these sources, the plant design team will define the detailed design approach that is most acceptable to plant personnel and then document it in the style guide. This detailed guidance in the style guide can then be used to identify which alarm will be messages and which will be spatially dedicated, and design each using the detailed guidance.

With respect to specifying details of the HSI, two things should be considered: integration of HSI resources and tradeoffs. The HSI provides resources such as alarms, displays, and controls. It is important to consider the HSI as an integrated whole, rather than addressing each resource as a separate entity. For example, trend displays may be available to monitor system parameters. However, users may be looking at alarms and want parameter trend information. In some designs, the alarm system itself provides that functionality, but does it in a manner that is different from how the same information is provided through the monitoring system. This is not a good design practice. Ideally, all trend information should look and work the same no matter what part of the HSI the user is in.

Tradeoffs between approaches to HSI design are also important. For example, consider the decision of how many information items to put on a screen. The amount of information that can be placed on a screen depends on several factors, including how frequently users will use the screen (how familiar they will be with the design) and the requirement for users to navigate to other screens to perform their tasks. Designers may want to reduce the need for navigation, and therefore, the amount of information that is placed on one screen is increased. Dense screens can be very difficult for infrequent users. However, frequent users can more easily use high-density displays because, with experience, they gain a good sense of where everything is located. These types of tradeoffs should be considered with respect to the users of the HSI (as is discussed in Section 4 of this document).

Ultimately, the individual guidelines should be expressed in concrete, easily observable terms to provide unambiguous guidance to designers and evaluators. They should be detailed enough to permit their use by design personnel to achieve a consistent and verifiable design that meets the guideline. The Style Guide should be written so designers can readily understand it. The Style Guide should support the interpretation and comprehension of design guidance by supplementing text with graphical examples, figures, and tables.

In addition to guidelines, the style guide should also contain instructions for their use. The instructions should identify where and how HFE guidance is to be used in the overall design process. They should also address HSI modifications. This guidance should specifically address consistency in design across the HSIs. The style guide should be also maintained in a form that is readily accessible and usable by designers and that facilitates modification when the contents require updating as the design matures. The plant design and especially the modification administrative procedure should include provisions for requiring human factors screening, and, where applicable, evoking use of the style guide.

Develop Future Revisions to the Style Guide

A style guide should be a living document and, like all such documents, is subject to future modifications. It should be assured that the style guide accurately and completely represents the current plant practices.

Sources of modifications include:

- HSI evaluations that are conducted as tests, verifications, and validations are performed (see Figure 3-22)
- Plant modifications that require new HSI characteristics and functions or deletion of all examples of a feature described in the guidelines.
- Endpoint definition changes that result from of plant experience with digital technology
- Problems and issues that are identified in the course of plant operation

Instructions for making and controlling style guide modifications should be addressed in the plant's overall HFE procedure(s).

3.7.3.4 Detailed Design

The style guide will provide detailed guidance on the design of all HSI resources (see Figure 3-19). However, there are several specific additional considerations for HSI design that need to be addressed:

- Allocation of HSIs to Workplaces
- Design of Local Control Stations
- Design for Error Tolerance
- Design for Differing Levels of Automation
- Design for Teamwork
- Design for Variations In Staffing Levels
- Design for Long-Term HSI Use
- Design for Environmental Conditions
- Design for HSI Test, Inspect, and Maintenance
- Design for Coping with HSI and I&C Degradation and Failure

3.7.3.4.1 Allocation of HSIs to Workplaces

Two of the consequences of a digital I&C modernization program are that (1) there is usually a great deal of additional information available to plant personnel, and (2) information is available on a data highway, thus increasing the flexibility to make it available at different locations. For example, information that used to be obtained by sending an Auxiliary Operator (AO) out into the field can now be obtained at control room workstations. While it may be tempting to bring all information and/or control capability into the control room, that is not always a good idea. For example, by bringing the information into the control room we may create increased workload for the operators who now must take actions at their HSIs to retrieve it and control it. In addition, the actions to retrieve the information are potentially distracting and may cause operators to make errors in the performance of their other tasks. There is also the potential loss of the intimate contact with the process when personnel are not in the near vicinity of the equipment to see, feel, hear and smell the equipment in operation, which sometimes is the best and fastest way to recognize faulted performance or impending problems.

Detailed DCS alarms are another example. Many such alarms are mainly used by maintenance personnel. When these alarms go to operator workstations, they can be overwhelming and increase alarm management workload considerably. One consequence of this situation is that an important alarm may be missed in the “noise.”

Part of the HSI design process is to consider who should receive any information and where it should be used. HSIs that are used by maintenance personnel should not go to the operator workstations and vice versa (although the information can still be available at the operator workstations). In such cases, it may be that some higher-level form of the information should go to operators. In the case of a DCS failure, perhaps many detailed alarms for maintenance personnel can be replaced with a single DCS failure alarm so operators are aware of a problem but not the details.

The next consideration is location. While it may be possible to bring all information into the control room, it may not make sense to do so. The primary purpose of the control room is to monitor and control the plant from productivity and safety standpoints. Increasing the amount of activity in the control room, by locating maintenance and engineering workstations in it, or unnecessary process and/or administrative and security indication or controls can have a negative impact on those functions. In general there is a tradeoff between the benefits gained by creating awareness of the activities of other organizational functions in the plant and facilitating their communication and the negative effects of distractions. Unless the benefits are essential, e.g., less time and communication demand with minimal increase in workload, it may be better to locate these work places outside of the control room and provide less intrusive communications between them.

3.7.3.4.2 Design of Local Control Stations

Improvements to local control stations (LCSs) can be made as part of the plant modernization process. In general, LCSs did not undergo the improvements in HFE design that control rooms did in the 1980s and 1990s. Perhaps the greatest opportunity for improvement in LCS tasks can come from:

- relocation of HSIs now in environmentally challenging locations
- better integration of displays and controls into one HSI
- application of general HFE principles in the design of LCSs.

Some LCSs are located in areas requiring the use of protective clothing or the use of additional task support items, such as ladders or flashlights. It may be possible to relocate these HSIs so that the task can be performed under more favorable conditions.

Some existing plants LCS activities require the coordinated actions of two or more AOs, e.g., one AO operates a control while another reads a display in another location to provide feedback to the controlling AO. To make matters worse, the communication may be over walkie-talkies adding increased workload and opportunity for error due to miscommunication. This type of situation is an ideal opportunity to provide an HSI where the control and its associated display are integrated into the same work area.

Computer-based LCS HSIs can be designed in accordance with the style guide to help ensure that basic HFE principles are applied and to improve standardization and consistency across LCSs and between LCSs and the main control room. The exception is HSIs that must be used in environmentally challenging areas. They will require special design considerations (see topic of environmental conditions below). It is also possible that different groups of users have differing population stereotypes and expectations that need to be captured in the style guide. It is possible, for instance, that all operator interface in the control room and that used by operations personnel might use one color code or standard, but the cabinets used only by maintenance technicians use another code, convention or standard.

3.7.3.4.3 Design for Error Prevention and Tolerance

Error tolerance means designing HSIs such that they:

- minimize the occurrence of user errors
- provide a means for users to detect errors when they are made
- provide means to gracefully correct errors

While it is a good practice to make the HSIs tolerant to all errors, the added design effort may make this impractical. Thus, it is recommended that the following approach to error to lerant design be followed for at least the important human actions; i.e., those with potentially significant impact on safety, productivity, and equipment and personnel protection. At least a measure of error tolerance is achieved by the application of good HFE practices as part of the design. The measures discussed here provide special attention to important actions. An overview is provided in Figure 3-24. Each step is discussed below.

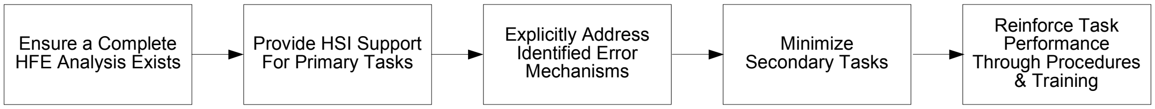

Ensure a Complete HFE Analysis Exists
Provide HSI Support For Primary Tasks
Explicitly Address Identified Error Mechanisms
Minimize Secondary Tasks
Reinforce Task Performance Through Procedures & Training

Figure 3-24
Steps in the Design of Error Tolerant HSIs

Ensure a Complete HFE Analysis Exists

Designing for error tolerance begins with the earlier HFE analyses, specifically:

- identification of operating experience related to the important human action
- consideration of the level of automation of the important human action
- task analysis of the important human action
- analysis of human errors associated with the important human action
- analysis of the staffing and qualifications associated with the human action

These analyses should have already been performed. However, if they have not, then they should be performed at this point so that the task requirements of the action are known.

Provide HSI Support for Primary Tasks

A general approach to making an HSI more error tolerant is to ensure that the primary task is supported and that secondary tasks are minimized. To make sure the primary task is supported, the key task elements have to be identified and explicitly addressed in the design. Table 3-6 in Section 3.4, Task Analysis, identifies these key elements. These elements are reproduced in Table 3-18 below along with HSI design features to address them.

Explicitly Address Identified Error Mechanisms

The analysis of human error (see Section 3.6) may have identified specific mechanisms for human error along with suggested design features to consider adding to the design to help manage or mitigate the errors. For example, if two or more situations are very similar yet require different responses, mistaking one situation for the other is an error. Designing HSI features to support personnel in discriminating between the situations can minimize this type of error. This can involve something as simple as providing information on a display that identifies the key parameters that distinguish situation A from B and the current status of each. This will aid the operator to evaluate the current conditions and identify which situation exists. A more sophisticated solution is to develop a decision aid that automatically analyzes the conditions and identifies the correct situation.

Minimize Secondary Tasks

Section 1 discusses the difference between primary and secondary tasks. One of the characteristics of a well-designed HSI is to minimize secondary tasks and distractions. Minimizing these tasks helps prevent error because it leaves more attention and cognitive resources available for the primary tasks.

The existence of secondary tasks, such as display navigation, should be examined and minimized to the extent possible. The use of several of the HSI design techniques identified above, such as a task-based display or a computer-based procedure, can help to minimize secondary tasks. Modern navigation techniques can also help. For example, a mouse click on a sensor symbol for a controlled process variable can result in the display of the related process control system and related HSI in addition to obtaining a trend plot of the controlled variable.

Reinforce Task Performance through Procedures and Training

Performance of important tasks can also be supported with procedures and specific training to provide the familiarization necessary to perform the tasks properly. Training can identify specific task performance criteria, the mastery of which can be assessed as a normal part of the training program. Training can also explicitly address potentially critical errors identified by the human error analysis or by the design team.

3.7.3.4.4 Design for Differing Levels of Automation

As discussed in Section 3.3, the allocation of functions leads to four possible outcomes: Full function/task (F/T) automation, partial F/T automation, manual F/T performance, and manual F/T performance with task support. The design implications of each are briefly discussed below.

Design for Manual Control

HSIs for manual control are designed based on guidance presented in Section 3. No special considerations apply.

Table 3-18
Suggested Error Tolerant Design Approaches for Key Task Elements

Task Element Related to Error *	Suggested Design Approaches
Purpose	• Ensure that the display used for the task provide information relative to goal attainment (see Guideline 4.1.3.1.2-3)
Task Initiation	• Explicit identification of plant conditions, events, or situations that indicate when the task must be performed • Alarms aligned to the above conditions
Preconditions	• Explicit identification of required preconditions for task performance • Display indication of the presence of interlocks or other conditions that would prevent the task from being performed
Instructions	• Provide explicit procedures for task performance. • Provide computerized procedures or task steps integrated with task-related information • Provide computerized operator support systems (see Section 4.6)
Cautions/Warnings	• Provide cautions and warnings related to task performance in the HSI (these will be automatically triggered when predefined conditions exist)
Information	• Provide task information in a Task-based display format (see Section 4.1.3.2)
Alarms	• Provide task-related alarms integrated into the task-based display • Provide access to alarm response procedures (in immediately accessible electronic form)
Controls	• Engineered features such as the use of lockouts and interlocks • HSI design features that incorporate error reduction features such as input checking, confirmation steps, and demand vs. actual displays, (see the appendix of Section 4.3, Soft Controls for a full list of such features)
Time	• Explicit display of time requirements
Failures	• Display of (or availability of) procedures for alternative actions when failures occur
Task Termination	• Display of the plant conditions, events, or situations that indicate that it is time to stop the task

Design for Automatic F/T Performance

While the design of automated F/Ts falls outside of the scope of HFE activities, there is still a human component to address. Personnel must be able to monitor the automation. In fact, much of the difficulty personnel experience with highly automatic systems reflects the poor design of the HSIs available to monitor it. Thus HSIs should be developed that enable personnel to know:

- when a F/T is needed
- that it has initiated
- that it is accomplishing its goal
- that it has terminated when it should.

In addition to HSIs designed for monitoring automation, it is important to design for personnel actions in the event of degradation or failure of the automatic system. This can involve providing an alternative means for accomplishing the task, shifting to manual operations, or change to an alternative plant configuration where the F/T is not needed. At the HSI, information and controls need to be available to support personnel actions in the event they are needed.

Design for Partial Automation

Designing for partial automation involves considerations for both manual and automatic task performance. The main difference is the need to make clear which aspects of the F/T are manual, which are automatic, and how they interact. The HSI and procedures should be designed to support the coordinated activity. For example, it is important that the manual and automatic actions are not in conflict – such as could occur if a manual action is taken and almost immediately an automatic action undoes the manual action. Task based displays are ideally suited to this purpose (see Section 4.1.3.2, Display Design for Task Performance).

For partial automation designs, personnel should be in overall control of the F/T and control the pace at which it is performed.

Design for Manual Control with Task Support

In some cases a F/T should be automated; however, the automation is not practical and manual control must be used. This is often a difficult design situation and generally requires additional task support to be provided to minimize the potentially negative effects on human performance of the F/T requirements and characteristics that make automation preferred.

These F/Ts should be selected for task analysis (see Section 3.4) and subject to verification and validation (see Section 3.9). F/T support can be in the form of:

- Computerized operator support systems (see Section 4.6) that automate activities such as monitoring and situation assessment
- Task based displays (see Section 4.1.3.2) that address the specific needs of the operators to perform the manual tasks
- The application of error tolerant design principles (see Section 4.3, Soft Controls – Appendix on Error Tolerant Design) that minimize the impact of operator errors in the course of the manual operations.

Performance of difficult F/Ts can also be supported with specific detailed procedures and specific training to provide the familiarization necessary.

3.7.3.4.5 Design for Teamwork

The effect of technology on teamwork is discussed in Section 3.5.3.4, Evaluate Teamwork. For modifications that are more extensive, HSI design features that support teamwork (crew coordination, peer checking, and supervision) should be considered. Specific approaches to addressing HSI support for teamwork are discussed in Section 4.1.3, Display Functions, and include:

- large displays that can be seen from anywhere in the control room
- the ability to share displays across workstations (e.g., from operator to operator, and operator to supervisor)
- the capability to work cooperatively on a single computer display

3.7.3.4.6 Design for Variations in Staffing Levels

HSI design, especially workplace and workstation design, should consider the entire staffing range. Most control rooms can expect considerable variation in the number of personnel that may be present. The design has to be acceptable for minimal, nominal, and high-level staffing. For example, under normal operating conditions, a control room may only have to accommodate a three-person shift crew, and often times when only a single reactor operator has the “at-the-controls” responsibility and controls the entire plant. However, during periods of maintenance, it may be necessary to accommodate HSI access by maintenance personnel. During emergencies and scheduled complex evolutions such as a plant startup, it may be necessary to accommodate additional supervisory and support personnel. The staffing and task needs under different situations should be considered in the overall design of the control room and support facilities.

3.7.3.4.7 Design for Long-Term HSI Use

When HSIs are being designed or evaluated, the context of their use should be considered. Sometimes the design of an HSI is acceptable for short-term or occasional use, but the same design can have a negative effect on performance if used for an extended period. The use of the HSIs over the duration of a shift where decrements in performance due to fatigue may be a concern should be considered in the design of the HSIs.

For example, consider a touch screen located on the vertical portion of a traditional control panel. To provide inputs, operators have to lean forward and extend an arm to reach the screen. This position may be acceptable for a few simple inputs by operators, but the same design would not be acceptable when operators have to make many inputs over several hours. The reaching motion would become fatiguing, thus increasing the chance of an input error.

Another example is reading text. Relatively short text can be read on a computer screen without problems. However, if the text is long and reading must take place over an extended period, the computer screen will lead to fatigue and eyestrain. Advances in display screen technology, however, may minimize these problems.

3.7.3.4.8 Design for Environmental Conditions

HSI characteristics should support human performance under the full range of environmental conditions, e.g., normal as well as credible extreme conditions. Requirements for the main control room should address conditions such as loss of lighting or high noise that may impact use of the HSIs.

For HSIs out in the plant, such as the remote shutdown facility and local control stations, the design should consider constraints imposed by the ambient environment (e.g., noise, temperature, contamination) and by protective clothing (if necessary).

If HSIs must be used with protective clothing, then the impact of the clothing on performance should be evaluated. Note that the HFE design guidelines in Section 4 are predominantly for a typical control room environment and may not be suitable for application to interfaces used while wearing protective clothing. For example, use of a standard keyboard while wearing gloves is almost impossible. If users must interact with the HSI while wearing gloves, then an alternative means of interaction should be considered. This can include use of voice input, an onscreen keyboard that can be poked with a stylus, or an onscreen keyboard with larger than typical keys that can be poked with the pointing finger of a gloved hand. The specific solution will depend on the type of clothing worn.

3.7.3.4.9 Design for HSI Test, Inspect, and Maintenance

The HSIs should be designed so that inspection, maintenance, testing, and repair of the HSIs do not interfere with other plant control activities. An example of such a problem would be if a technician has to replace a component of a workstation, and the only way to get at it is to block the operators' access to the operating screens. A better design would be to provide rear access. Having a redundant full capability workstation, for instance, using the supervisor's station temporarily for the duration of the repair, may also be a viable option. See Section 6.1, Maintainability of Digital Systems, for additional information on designing HSIs for test, inspect, and maintenance.

3.7.3.4.10 Design for Coping with HSI and I&C Degradation and Failure

As part of any design effort, considerations have to be given to conditions under which HSI performance degrades or fails. This will include degradation and failure of the I&C as well. On a small scale this can be addressed through the use of HFE design guidelines for signal validation and data quality indication (see Section 4.1, Information Display). However, this is not adequate for larger failures.

Section 6.4 of this guideline addresses the issues of degraded conditions and failures of a significant nature related to safety monitoring and control and concept of operations under degraded conditions.

However, between these two extremes, the designer has to consider issues such as the loss of a panel, workstation, monitor, or overview display and how these failures can be handled without a loss of operational safety or productivity.

3.7.3.5 HSI Integration

In this section the integration of new and old HSIs is addressed. This includes:

- Consistency Between New and Replaced HSI Components

- Consistency Between New HSI Components and the Rest of the HSI
- Functional Integration of the HSI
- Interactions With Old And New HSIs In Close Proximity
- Old HSIs Left In Place

3.7.3.5.1 Consistency Between New and Replaced HSI Components

When the HSI is upgraded, such as when a component is replaced, some of the design characteristics that support user performance may change, sometimes in ways that have safety significance. For example, an indicator light on a controller could represent normal status in the original design, but represent a serious condition in the replacement. If an operator applied knowledge of the old controller when viewing the new one, an important problem might not be diagnosed. Also, an action that produces a small adjustment in feedwater flow in the old controller may produce a large one in the new controller; applying the old skill to the new controller may upset feedwater flow. In such cases, the old and new HSI components may be considered to have poor consistency. Such inconsistencies should be identified and minimized.

The reason for considering the degree of consistency between old and new designs has to do with transfer of training. Positive and negative transfer, respectively, refer to the facilitative and inhibitory effects of prior learning upon performance in new (transfer) circumstances. A positive transfer of training is said to have occurred if the experience of learning to use the old component facilitates learning the new component. For example, if a new feedwater controller is installed in the CR and the operators who were skilled in using the old controller learn to use the new controller faster than operators who did not use the old one, then a positive transfer of training has occurred. In some cases, prior learning with an old component may inhibit the ability to learn the new one. This negative transfer of training can increase training times, decrease response time when using the upgraded HSI, and lead to errors. Such negative transfer-of-training type errors are apt to only appear under stress, when people tend to revert to the first-learned/best learned response.

Some general considerations on the conditions of training transfer includes:

- The greatest amount of positive transfer is generally produced when the old and new component are conceptual similar. That is, even though a new HSI may look different and have additional functionality, positive transfer will be fostered when the basic means of interacting with the HSI are similar.
- Negative transfer occurs when personnel actions that are appropriate in the old design lead to errors in the use of the new design. For example, if operators are used to retrieving a favorite display with a specific key stroke combination, it would be unwise if that same key stroke combination had a negative effect on the new HSI, such as suspending processing. A possible exception is when the original controls and displays conflict with population stereotypes, or are not designed consistently with each other. Then, personnel performance may already be affected by these inconsistencies, and modifying the responses may improve performance.
- Neither positive nor negative transfer will be likely when both the information presentation and responses are different between the old and new conditions.

Personnel who use the HSI should be consulted to evaluate the potential positive and negative effects of consistency between old and new HSI designs.

3.7.3.5.2 Consistency between New HSI Components and the Rest of the HSI

HSI upgrades often are installed in NPPs on a component-by-component basis. For example, in a transition to digital technologies, the old analog component is removed from the control panel and a digital HSI component is installed. However, many replacement and upgrade products are generically designed, such as flat panel displays and input devices, and each manufacturer may have different standards for them. Therefore, after several upgrades have been installed, the HSI may contain many similar-looking user interfaces with different conventions for presenting information and different mechanisms for accessing and controlling it. This can affect the overall consistency of the HSI. For example, information coding conventions may have different meanings on different devices, and the correct method of operating one device may be incorrect for a similar one.

This type of inconsistency is very disruptive to performance, and it may cause errors and slow execution times. Performance suffers when the user cannot remember which methods correspond to which interface. Further, when users lack the knowledge to properly operate some aspect of an interface, they may try to do so correctly through analogy with other, similar aspects of the device. Errors occur when the user derives an action sequence that is inappropriate because the user interface has a command structure that differs from (is inconsistent with) that on which the analogy was based, even though the commands appear to be related and share a common description of purpose, action, and are part of the command format.

3.7.3.5.3 Functional Integration of the HSI

Functional integration is the degree to which the information in different aspects of the HSI is truly integrated (in contrast to being functionally isolated systems). As an example, consider the situation where following an upgrade, a plant has a new digital alarm system for several systems. While the old alarm system is still used, some of its alarms are now shown in the digital alarm display as well. This situation can create confusion as to the amount of integration that exists. When operators are using the digital system, they may infer that specific alarms are not “in” because they do not appear in the alarm display, when in fact they are but are only displayed in the old alarm system. The fact that some of the alarms from the old system appear in the digital system creates the appearance of more functional integration than actually exists. Another example is the use of trend graphs. Suppose operators can access trend information within their computer-based procedure system or from the process displays used to monitor the plant. There may be an assumption that both trend graphs are the same, yet they may actually be generated from different data. When operators compare the two they may find discrepancies, and again confusion can result. Another example is given in Example 3-5.

The extent to which different HSI resources are integrated or isolated should be identified during the design and clearly indicated in the HSI and addressed in training.

Example 3-5 Example of a Problem of Apparent Functional Integration of a Safety Shutdown Trip Monitoring System

A computer based display system was installed as a CR upgrade to help operators monitor the trip parameters for one of the reactor's two safety shutdown systems. Operators could access displays that indicated the current values of the parameters and their difference from the trip limits. The safety shutdown system was controlled by a separate computer and, periodically, the trip limits had to be manually changed to reflect changing characteristics of the reactor core. However, the new display system did not communicate with the safety shutdown system's computer. Consequently, the trip limits had to be manually entered into both computers when the shutdown system's trip set points were changed. It was not apparent from the interface that these computers were not in communication. If the data were entered incorrectly into the computer based display system, it could create opportunities for mistakes; operators monitoring the reactor trip parameters might be unaware that the margin between the actual value and the trip limit did not represent the true state of the plant.

3.7.3.5.4 Interactions with Old and New HSIs in Close Proximity

When old and new HSIs are located in close proximity, they may interact with each other in ways that compromise their use. This can be addressed by considering the use of both old and new HSIs in their actual environment. When unwanted interactions are identified, take appropriate actions to mitigate or resolve the problem. Three examples are provided below to illustrate this issue.

Suppose that a flat panel display is used to replace displays and controls in one section of a control panel, while the rest of the panel is unchanged. It is possible that the color display on the flat panel may be more attention grabbing than an indicator light located next to it indicating a problem. Essentially, the new display makes the old display less conspicuous. There are several possible ways to resolve this problem. For example, the indicator light could be moved further from the display. Another approach is to change the color scheme on the flat panel display to reduce the interaction.

Two HSIs may have different environmental requirements. For example, the location and amount of light used to illuminate analog meters and control switches on a control panel may be too bright for the computer display and create glare, thus making it less visible than it should be. One solution may be to alter the lighting in the vicinity of the panel to provide task-oriented spot lighting on the old HSIs while computer monitors in the area have proportionally less light. However, changing control room lighting can be quite expensive. A more practical alternative solution may be to provide shields or shades for the computer monitors.

Another example is when a touch panel is used to replace a portion of the indicator/display section of a control panel. The touch panel may require operators to lean forward to touch the panel, increasing the chance of inadvertently operating controls left on the control section of the panel. One solution may be to use physical guards or covers on the controls so they cannot be inadvertently actuated. Another solution may be to not use a touch screen. Instead, install a track ball on the control portion of the panel that can be used to provide input to the computer display.

The best alternative for any of these examples depends on the unique circumstances of the situation.

3.7.3.5.5 Operational Conventional HSIs Left In Place

When new HSIs replace old HSIs, the old HSIs should be removed. However, if circumstances prevent that from being done, measures should be taken to ensure that the conventional HSIs do not interfere with personnel task performance. Where personnel can obtain information from both conventional and new computer-based screen display HSIs, it is quite possible that the information presented will be different. In such cases, personnel should be trained on how to use or how to interpret the differences.

3.7.3.5.6 Non-Operational HSIs Abandoned-In-Place

When existing devices are either replaced by new HSIs or their function deleted, the old non-operational HSIs should be removed. However, if circumstances prevent that from being done, measures should be taken to ensure that the abandoned non-operational HSIs do not interfere with personnel task performance. As a minimum the non-operational status should be made obvious. If possible, covers should be put over the devices, and any operational labeling should be removed.

3.7.3.6 Procedure Revisions

Utilities have well-established procedure management programs. It is not the intent of this section to impact or change those programs; rather the intent is to discuss how to identify and address the need for new procedures or to modify existing procedures so that the existing procedure management program can be followed. The focus in this section is on paper procedures. The design of computer-based procedures is addressed as part of HSI design (see Section 4.5).

Procedures can be impacted as the result of a modernization program for many reasons, including:

- New tasks are created because of new plant systems and components
- Changes in automation have eliminated either whole tasks or modified tasks significantly using new control approaches, such as partial automation
- Tasks are altered because of changing task demands
- Tasks are altered because of changes to HSIs, e.g., since all information now is available through a single workstation the task in now performed by one operator rather than two
- The HSIs used to perform a task have changed significantly

All of these situations give rise to the need to either develop a new procedure or to modify an existing procedure.

In such cases, the procedures should be created or modified in accordance with the procedure management programs that already exist. This will help ensure continuity and consistency with the full set of plant procedures.

New and modified procedures can be tested and evaluated to ensure their technical accuracy and usability.

A methodology for evaluating whether new procedures are needed or existing procedures need to be modified is shown schematically in Figure 3-25.

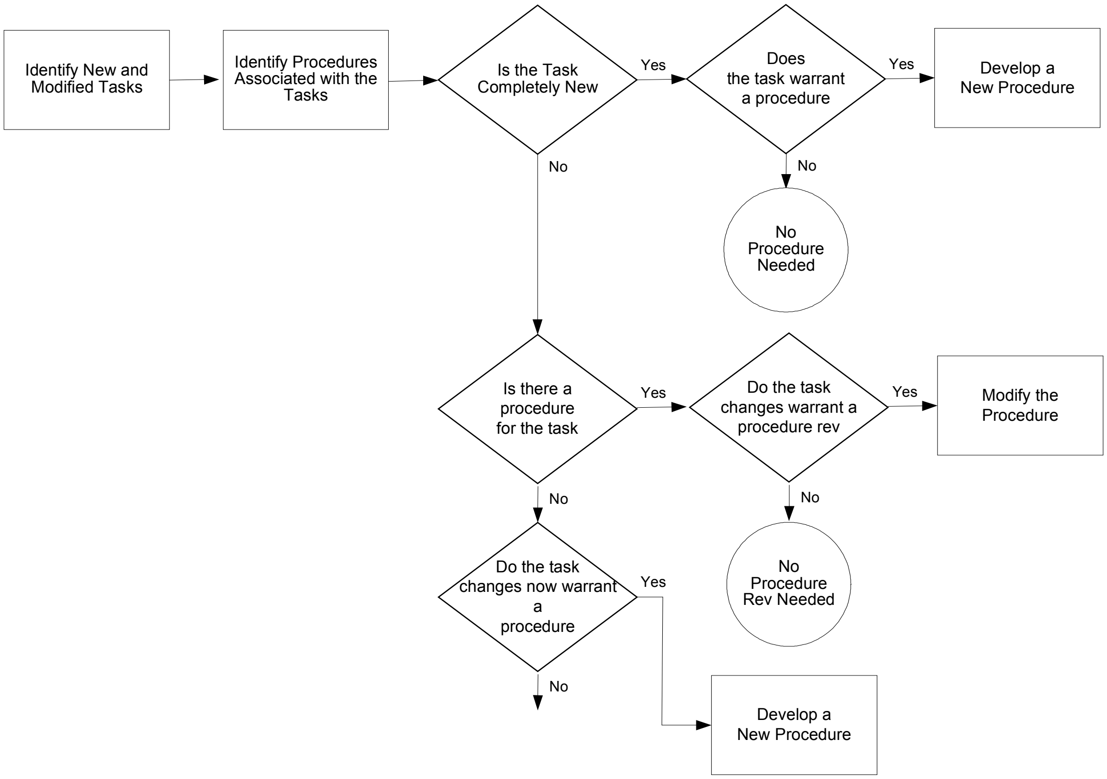

Identify New and Modified Tasks
Identify Procedures Associated with the Tasks
Is the Task Completely New
Yes
Does the task warrant a procedure
Yes
Develop a New Procedure
No
No
No Procedure Needed
Is there a procedure for the task
Yes
Do the task changes warrant a procedure rev
Yes
Modify the Procedure
No
No
No Procedure Rev Needed
Do the task changes now warrant a procedure
Yes
No
Develop a New Procedure

Figure 3-25
Basic HFE Activities Performed in the Design Modification Process

3.7.3.7 HSI/Procedure Tests and Evaluations

Tests and evaluations can be performed to:

- evaluate design options where more than one candidate approach meets the concept design
- obtain design information, e.g., to select a set of icons
- obtain user feedback on proposed HSI design approaches
- evaluate discrepancies between a design characteristic and a HSI guideline
- identify usability problems, i.e., design characteristics and features that will negatively impact user performance and/or create a negative experience while the user is interacting with the system, and determine whether the impact is acceptable
- evaluate the acceptability or performance with new or novel HSIs that are not be defined by HSI guidelines

- identify the need for procedure changes and determine their acceptability

HSI test and evaluation methods to meet these objectives include:

- trade-off evaluations
- personnel opinions and usability evaluations
- performance-based tests and evaluations

While each is discussed separately, in practice the methods can be combined and integrated in an overall evaluation. For example, a tradeoff study could use data collected in a performance-based test. Also, the information from a performance-based test can be enriched by also collecting personnel opinions.

In this section, the uses of tests and evaluations as part of the design process are discussed. Section 3.10 provides information on methods and tools that can be used to support testing and evaluation, especially where data from personnel will be collected. Tests and evaluations that are conducted as part of verification and validation activities are discussed in Section 3.8.

3.7.3.7.1 Trade-Off Evaluations

Tradeoff evaluations involve comparisons between candidate approaches, such as using a touch screen, a trackball, or a mouse as a computer input device or comparing alternative panel layouts. In the context used here, these are engineering evaluations and may or may not involve data collected from personnel. Candidate design approaches should be evaluated against a variety of considerations (specific factors will depend on the particular alternatives being evaluated):

- cost
- time to implement
- technological readiness
- physical characteristics, such as size, weight, power consumption, reflectance, color capability, etc.
- human performance requirements/considerations, such as speed, accuracy, workload, personnel acceptance, task requirements, satisfaction
- potential negative consequences (see discussion below)
- degree of regulatory involvement
- impact on risk, e.g., change in core damage frequency from the current design

Whenever changes are made in a control room, there is the possibility of negative consequences. Thus, the evaluation should identify and determine the extent to which each alternative has such consequences. Potentially negative factors are:

- increased training burden
- negative transfer of training

- teamwork and crew coordination difficulties
- time operating in interim configurations

3.7.3.7.2 Personnel Opinions and Usability Evaluations

Personnel opinions and evaluations involve, for example, having personnel evaluate HSIs or procedures during a table top evaluation using questionnaires or having them walk through a task using prototypes or mockups of an HSI. See Section 3.10 for details on conducting these types of evaluations.

Often usability evaluations (ANSI, 2001; ISO, 1997) address whether personnel can use HSIs and procedures:

- *Correctly* – personnel can use the HSIs and procedures to accomplish their tasks
- *Efficiently* – personnel can use the HSIs and procedures to accomplish their tasks in a timely manner and without unproductive, unwanted interactions with the system
- *Confidently* – personnel are sure of the actions they have to make and are confident that the system correctly responded to their input

Measurements of these aspects of HSI and procedure use can be obtained using personnel opinions and evaluations.

3.7.3.7.3 Performance-Based Tests and Evaluations

The distinguishing characteristic of performance-based tests and evaluations is that actual performance measures, such as time and workload, are collected under conditions of varying realism. For example, rather than simply doing a tradeoff study to choose between touchscreen or mouse input, both could be compared in the performance of an actual task. Time and errors could be used as performance measures. Section 3.10 provides methods for performing such evaluations.

3.7.4 Documentation

The detailed design may be documented in several sources. The general HSI characteristics and functions are documented in the style guide. The basis for the HSI design may reflect findings from operating experience and literature analyses, tradeoff studies, engineering evaluations and tests, and outcomes of tests and evaluations performed in support of HSI and procedure design. A record of findings from these activities that had significant impact on the final design should be available in HSI design files.

3.7.5 Grading the HSI Design Effort

Section 2.4.2, A Graded Approach to HFE, introduces the concept that the level of HFE effort for a modification should be based on the nature of the risk significance and complexity of the change. A methodology is provided to establish a grade for a modification in one of three levels: Level 1 – high risk, Level 2 – moderate risk, or Level 3 – low risk.

While many HFE activities presented in earlier sections were graded with respect to importance, this HSI and procedure design activity is not. The level of effort devoted to this activity is mainly related to the overall maturity of the modernization program. For utilities just embarking on a large modernization program, all of the activities described in this section should be performed.

For mature programs with a well-defined concept design and a style guide available for the design of new HSIs, HSI design will amount to using the analyses that are inputs to the design, applying the style guide, and addressing those detailed design considerations from Section 3.7.3.4 that are applicable. In addition, integration considerations will have to be dealt with. All of these design activities have to be addressed as a basic part of the design process, regardless of the importance of the modification.

Thus, no additional grading is recommended.

3.7.6 Use of the Results

The result of this activity is the detailed design of the HSIs and procedures. The results are then used as input to verification and validation activities. They are also used in training program development to train personnel for the accomplishment of their tasks.

3.7.7 Appendix – Vendor HSI Evaluation Questionnaire

Instructions

This questionnaire can be used to evaluate vendor HSI designs as part of the proposal reviews. The questions address general HSI characteristics, alarms, displays, controls, and user-system interaction features. The evaluation consists of a set of questions to ask about the HSI. Each feature is rated on a five-point scale conformance scale, shown below:

2 = the requested design feature is available or completely complied with

1 = the requested design feature is partially available or somewhat complied with

0 = the requested design feature is not available or not complied with

-1 = there is an undesirable approach used that not consistent with the requested design feature

-2 = there is an undesirable approach used that directly conflicts with the requested design feature

Since for a particular modification, some features may be more important than others, importance weights can be assigned. A higher number should be used for more important features. For example, weights could be used as follows:

3 = the feature is mandatory

2 = the feature is desirable

1 = the feature is not important in the design of this modification

A score on each feature can then be obtained by multiplying the rating by the weight.

conformance rating X importance weight = score

A comment field is provided to note explanatory information. The evaluator should note features that are especially positive or negative.

Before use, the questions should be reviewed to assign weights or to add questions that address some HSI characteristic or feature that is not captured by this set of questions.

In addition to rating design features, several supplemental questions about the vendor design are also presented to provide qualitative information.

Answers to the questions below can be obtained from three sources. First, the vendors should be able to provide answers to many of these questions, e.g., see question 1.1 below. Second, utility evaluators should request screen samples showing alarms, information displays, soft controls, interface management features, etc., and use these in answering the questionnaire. Third, some of the questions require an interactive demonstration of the interface to examine its dynamic characteristics. A desk-top small scale demonstration may be suitable for this purpose. While vendor input can be sought where needed, it is preferable for utility evaluators to do most of the evaluation.

When the evaluation is completed a total score can be computed by adding the individual scores. Vendor designs with higher scores are generally more compatible with the utilities HSI vision.

Evaluation Questions

1. General

1.1 Can HSIs be easily modified to accommodate utility preferences, standards, and conventions by the vendor before system installation?

________	X	________	=	________
Rating		**Importance Weight**		**Score**

Comments:

1.2 Can HSIs be easily modified to accommodate utility preferences, standards, and conventions by the utility after system installation?

________	X	________	=	________
Rating		**Importance Weight**		**Score**

Comments:

1.3 Can new HSIs be easily developed by the utility before system installation?

Rating X **Importance Weight** = **Score**

Comments:

1.4 Can new HSIs be easily developed by the utility after system installation?

Rating X **Importance Weight** = **Score**

Comments:

1.5 Is the overall organization of the screen consistent from one screen to another?

Rating X **Importance Weight** = **Score**

Comments:

1.6 Are the functions and dynamic aspects of the interface consistent from one screen to another?

Rating X **Importance Weight** = **Score**

Comments:

2 Alarms

2.1 Is the definition of what is included as an alarm flexible, i.e., can the utility specify what is alarmed and what is not?

Rating X **Importance Weight** = **Score**

Comments:

2.2 Does the system provide for alarm reduction processing or filtering (and if so, what types of processing are available)?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

2.3 Is the application of processing flexible?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

2.4 Are alarms prioritized and are the priorities clearly displayed?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

2.5 Is the indication of alarm status (e.g., acknowledged) very obvious?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

2.6 Can alarms be displayed in message lists?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

2.7 Can alarms be displayed in spatially-dedicated graphic windows?

Rating	X	**Importance Weight**	=	**Score**

Comments:

2.8 Can alarms be displayed in an integrated fashion into other displays, e.g., process **mimics**?

Rating	X	**Importance Weight**	=	**Score**

Comments:

2.9 Can alarm information be manipulated by the user, e.g., can operators sort alarm lists by time, system/component, and priority?

Rating	X	**Importance Weight**	=	**Score**

Comments:

2.10 Is technical data related to each alarm available in the system and easily retrievable?

Rating	X	**Importance Weight**	=	**Score**

Comments:

2.11 Can alarm response procedures be easily incorporated into the system?

Rating	X	**Importance Weight**	=	**Score**

Comments:

3 Displays

3.1 Is each screen clearly labeled and is its organization and content clear and easy to understand?

Rating X **Importance Weight** = **Score**

Comments:

3.2 Does the screen design appear simple, uncluttered, and predominantly free of extraneous decorative detail and nonfunctional screen elements?

Rating X **Importance Weight** = **Score**

Comments:

3.3 Will the information content provide for quick assessment of high-level system status and is more detailed information easily accessible in more detailed displays?

Rating X **Importance Weight** = **Score**

Comments:

3.4 Can all the types of display formats we want be used, e.g., trend plots, bar charts, flowcharts, and mimic diagrams?

Rating X **Importance Weight** = **Score**

Comments:

3.5 Are **display elements** used consistently throughout the HSI, e.g.:

- Abbreviations and Acronyms
- Numeric Data
- Icons and Symbols
- Labels
- Scales, Axes, and Grids
- Borders, Lines, and Arrows
- Visual and Auditory Coding

__________ X __________ = __________
Rating **Importance Weight** **Score**

Comments:

3.6 Is the display update rate acceptable for the tasks that have to be performed?

__________ X __________ = __________
Rating **Importance Weight** **Score**

Comments:

3.7 Is data quality indicated if it is poor?

__________ X __________ = __________
Rating **Importance Weight** **Score**

Comments:

3.8 Do system failures (due to sensors, instruments, and components) result in distinct display changes?

__________ X __________ = __________
Rating **Importance Weight** **Score**

Comments:

4 Soft Controls

4.1 If some controls require immediate access, are they spatially dedicated and continuously displayed?

__________ X __________ = __________
Rating **Importance Weight** **Score**

Comments:

4.2 For controls that are selectable, e.g., from a menu or icon, is the selection process simple?

_______________ X _______________ = _______________
Rating **Importance Weight** **Score**

Comments:

4.3 When soft controls are selected, e.g., from a menu or icon, is it obvious that the control is directly related to the object selected?

_______________ X _______________ = _______________
Rating **Importance Weight** **Score**

Comments:

4.4 Do the soft control displays provide a list of the commands that are possible?

_______________ X _______________ = _______________
Rating **Importance Weight** **Score**

Comments:

4.5 Do the soft control displays indicate receipt of the user input and what the input was?

_______________ X _______________ = _______________
Rating **Importance Weight** **Score**

Comments:

4.6 Do the soft control displays provide feedback on the results of the control action so operators can monitor its progress and clearly see when the action is completed?

_______________ X _______________ = _______________
Rating **Importance Weight** **Score**

Comments:

4.7 Do the soft control displays indicate the control modes, logic, and constraints?

Rating X **Importance Weight** = **Score**

Comments:

4.8 Are user inputs verified for reasonableness, i.e., does the system check and alert users if a control input is unreasonable?

Rating X **Importance Weight** = **Score**

Comments:

5 User-Interface Interaction and Management

5.1 Are the actions required by the user for retrieving information, navigation, and HSI configuration simple and efficient, e.g., most information can be retrieved with one or two user inputs?

Rating X **Importance Weight** = **Score**

Comments:

5.2 Is user-interaction flexible such that the same action can be accomplished in more than one way, e.g., display selection through a keyboard command, a menu, or on-screen link?

Rating X **Importance Weight** = **Score**

Comments:

5.3 Is a list of the permissible actions and options easily available to the user?

Rating X **Importance Weight** = **Score**

Comments:

5.4 Does the system provide prompts when user input is needed?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

5.5 Does the system provide prompt feedback for user actions?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

5.6 Are system advisory and error messages simple and easy to understand?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

5.7 If the system response is delayed, is the delay status indicated on the displays?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

5.8 Is help available?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

5.9 Are mistakes easy to correct?

________ X ________ = ________

Rating **Importance Weight** **Score**

Comments:

5.10 Are user input devices easy to use?

________	X	________	=	________
Rating		**Importance Weight**		**Score**

Comments:

5.11 Is access to information properly controlled to prevent accidental changes, e.g., access to set point changes?

________	X	________	=	________
Rating		**Importance Weight**		**Score**

Comments:

6 Supplemental Questions

6.1 Does the vendor have a standard, guidance document, or style guide that describes the principles governing HSI design?

6.2 Can the vendor show that the design is consistent with the HSI guidance in this EPRI document?

6.3 Can the vendor show that the design is consistent with the HSI design review guidance in NUREG-0700, Rev. 2?

Overall Summary

Total Score: ______________

Summary of Positive Features:

Summary of Negative Features:

3.8 HFE Verification and Validation Processes

- 3.8.1 Introduction
- 3.8.2 Objectives
- 3.8.3 Methodology
  - 3.8.3.1 Planning for HFE V&V
  - 3.8.3.2 Personnel Performing HFE V&V Activities and Criteria To be Used
  - 3.8.3.3 HSI Inventory and Characterization
  - 3.8.3.4 HSI Task Support Verification
  - 3.8.3.5 HFE Design Verification
  - 3.8.3.6 Operational Conditions Sampling
  - 3.8.3.7 Integrated System Validation
  - 3.8.3.8 Human Engineering Discrepancy Identification and Resolution
  - 3.8.3.9 Final Plant HFE Design Verification
- 3.8.4 Documentation
- 3.8.5 Grading the HFE Verification and Validation Effort

3.8.1 Introduction

This section describes HFE Verification and Validation (V&V), which consists of the techniques that should be used to establish that the design of the human-system interface meets the requirements that have been placed on it and to ensure that the interface is effective in supporting the performance of personnel tasks. This includes establishing that the design supports the performance of tasks, adheres to established human factors practices, meets all operational requirements, and that the final configuration and the design documents agree.

HFE V&V has many similarities to the approach to software V&V. According to IEEE 1012-1998, software V&V processes “determine whether development products for a given activity conform to the requirements of that activity, and whether the software satisfies its intended use and user needs.” Further, IEEE 1012-1998 clarifies that V&V should be considered “as part of the software life cycle processes” and that “V&V processes are most effective when conducted in parallel with software development processes.” Similarly, HFE V&V activities are not performed in a “single step”, but typically are carried out at various points throughout the design process.

HFE V&V consists of a variety of activities, which will vary depending on the nature of the design change and the grade assigned to the modification according to the grading methodology provided in Section 2.4.2. HFE V&V activities, in many cases (especially verification), should be performed as a part of the normal design process. This is discussed further in Section 3.8.3.

Implementation of HFE V&V as discussed in Section 3.8.3 involves the following factors as part of an organization’s HF program. The following factors would typically be documented in the HFE section of the project plan:

- Management – Establishing the responsibilities for managing the quality and scope of HFE V&V
- Scope – Establishing the requirements and objectives of HFE V&V activities and the bases for the requirements
- Participants – Identifying the personnel who will perform and participate in the HFE V&V activities, (i.e., designers, HFE personnel, HFE experts, Operators/other end users, witnesses, and auditors)
- Methods and Procedures – Establishing how HFE V&V activities will be performed
- Test Conditions, Data Collection, and Results Analysis – Establishing the detailed plans and procedures to be applied, in what form results will be captured, and how results will be applied
- Acceptance Criteria and Performance Measures – Defining the design and performance requirements that the various aspects of the design are to be verified and validated against
- Documentation, Reporting, and Integrating the Results – Establishing the level and status of documentation, the requirements for evaluating, communicating, and maintaining the results of HFE V&V activities, and the processes for integrating the results of HFE V&V into the overall modification
- Schedule – Establishing when HFE V&V activities will be performed and integrating HFE V&V into the overall modification schedule
- Tests and Evaluations – Determining the less formal tests and evaluations to be performed as part of design activities that support HFE V&V

HFE V&V should be applied to the following features of the design or changes to the design:

- Human-System Interface (i.e., controls, displays, and alarms)
- Procedures (hard copy, static computer-based, or automated computer-based)
- Crew coordination and communication
- Display navigation, information retrieval, and access to controls
- Automation and the features of automation, including monitoring and control
- Layout, configuration, and anthropometrics of workplaces and workstations and the features and equipment required for those spaces (e.g., laydown areas, access and egress, radios, phones, hard copies of procedures and drawings)
- Workplace environment (e.g., lighting, temperature, noise)
- Provisions for routine test and maintenance (e.g., cleaning displays, testing, routine consumable replacement)

3.8.2 Objectives

The objectives of HFE verification and validation (V&V) are to establish that the design of the human-system interface meets design requirements and to ensure that the interface is effective in supporting the performance of personnel tasks. To demonstrate this, it must be established that:

- *The interface meets all the requirements that have been placed on it*. For example, that all required control capabilities and displayed quantities are, in fact, provided and that all parts of the interface are configured as intended and required by human factors guidelines (Section 4 of this document and an organization's Style Guide as discussed in Section 3.7) and standardized practices. All conflicts between the various requirements and specifications should have been addressed and resolved. This requires that detailed configurations have been defined – one cannot reach a conclusion on configuration that has not been worked out in detail. This does not mean to imply that design elements cannot be verified until the entire design is complete. In fact, it is valuable to verify completed design elements as early as possible. Such activities are referred to as verification activities. These will also include test and evaluation activities as discussed in Section 3.10.
- *The interface will enable all the intended tasks to be carried out effectively.* That is, the interface has to be proven to function as intended. The premise is that even though every individual requirement is met, the integrated functioning needs to be confirmed. This leads to testing of the entire system and interface to establish that it can provide all the functions and achieve the performance that is needed. Such activities are referred to as validation activities.

The description of V&V provided above and discussed in this section is consistent with the description provided in NUREG-0711.

3.8.3 Methodology

Figure 3-26 provides an overview of HFE verification and validation activities and shows how they are integrated into the overall design process. The complete set of activities described in this section is for a Level 1 modification. For recommendations on grading the activities, see Section 3.8.5. In addition to the specific grading recommendations provided, the effort associated with conducting HFE V&V is also based on whether the modification uses the same or similar equipment or design that has been used in association with earlier modifications. The design team should start by determining whether aspects of HFE V&V performed for prior modifications can support the HFE V&V for the current modification. Prior to carrying out the V&V activities, the associated design activities should have been accomplished, a style guide or other criteria should be available, and the related function and task analysis steps should be completed. In addition, the scope of V&V activities should be defined and documented in the modification project plan (Section 3.8.3.1 and Section 3.8.4) and the participants in the HFE V&V activities should be identified (Section 3.8.3.2).

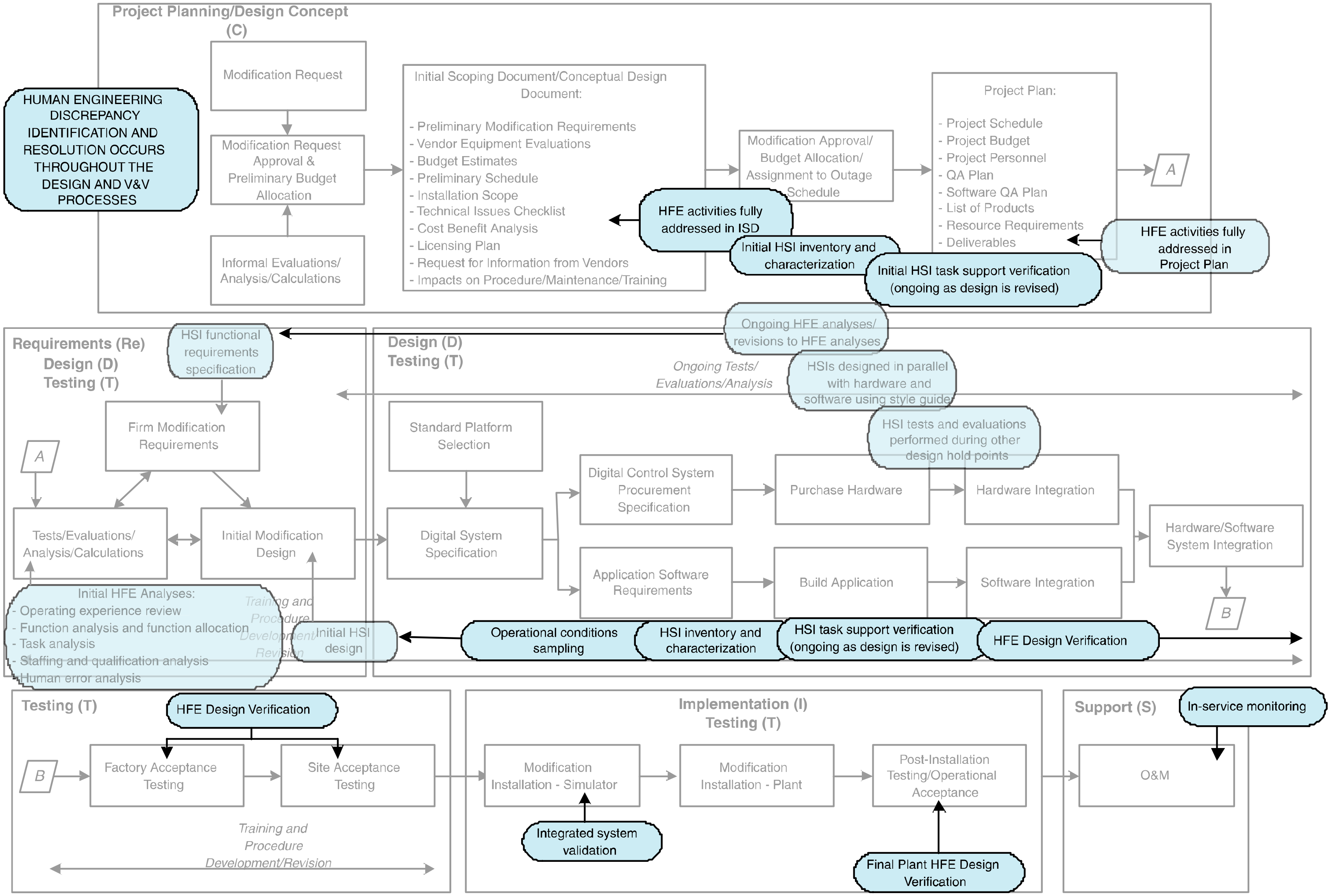

Project Planning/Design Concept (C)
Modification Request
Modification Request Approval & Preliminary Budget Allocation
Informal Evaluations/ Analysis/Calculations
Initial Scoping Document/Conceptual Design Document:
- Preliminary Modification Requirements
- Vendor Equipment Evaluations
- Budget Estimates
- Preliminary Schedule
- Installation Scope
- Technical Issues Checklist
- Cost Benefit Analysis
- Licensing Plan
- Request for Information from Vendors
- Impacts on Procedure/Maintenance/Training
Modification Approval/ Budget Allocation/ Assignment to Outage Schedule
Project Plan:
- Project Schedule
- Project Budget
- Project Personnel
- QA Plan
- Software QA Plan
- List of Products
- Resource Requirements
- Deliverables
A
HUMAN ENGINEERING DISCREPANCY IDENTIFICATION AND RESOLUTION OCCURS THROUGHOUT THE DESIGN AND V&V PROCESSES
HFE activities fully addressed in ISD
Initial HSI inventory and characterization
Initial HSI task support verification (ongoing as design is revised)
HFE activities fully addressed in Project Plan
Requirements (Re) Design (D) Testing (T)
HSI functional requirements specification
Firm Modification Requirements
A
Tests/Evaluations/ Analysis/Calculations
Initial Modification Design
Initial HFE Analyses:
- Operating experience review
- Function analysis and function allocation
- Task analysis
- Staffing and qualification analysis
- Human error analysis
Training and Procedure Development/ Revision
Initial HSI design
Design (D) Testing (T)
Ongoing HFE analyses/ revisions to HFE analyses
Ongoing Tests/ Evaluations/Analysis
HSIs designed in parallel with hardware and software using style guide
HSI tests and evaluations performed during other design hold points
Standard Platform Selection
Digital System Specification
Digital Control System Procurement Specification
Application Software Requirements
Purchase Hardware
Build Application
Hardware Integration
Software Integration
Hardware/Software System Integration
B
Operational conditions sampling
HSI inventory and characterization
HSI task support verification (ongoing as design is revised)
HFE Design Verification
Testing (T)
HFE Design Verification
B
Factory Acceptance Testing
Site Acceptance Testing
Training and Procedure Development/Revision
Implementation (I) Testing (T)
Modification Installation - Simulator
Modification Installation - Plant
Post-Installation Testing/Operational Acceptance
Integrated system validation
Final Plant HFE Design Verification
Support (S)
In-service monitoring
O&M

Figure 3-26
Overview of Verification and Validation Activities in the I&C Design Process

The first step in verification is to confirm the HSI configuration, i.e. identify the HSI components subject to verification. This is done by performing the HSI Inventory and Characterization activity (Section 3.8.3.3).

The next steps in verification activities include the HSI Task Support Verification (Section 3.8.3.4) and the HFE Design Verification (Section 3.8.3.5). The criteria for the HSI Task Support Verification are derived from the results of the HFE Analyses (Sections 3.3 and 3.4), which defined the tasks that the HSI needs to support and the HSIs that the user needs to perform those tasks. The criteria used for the HFE Design Verification are a defined set of HFE rules and practices derived from the plant "Style Guide," Section 3.7 of these guidelines, or other widely accepted HFE practices, such as, NUREG-0700.

Operational Conditions Sampling activity (Section 3.8.3.6), the purpose of which is to define a set of representative scenarios that will be used during the Integrated System Validation tests, will vary depending on the size, complexity, and criticality of the modification.

The Integrated System Validation activity (Section 3.8.3.7) should establish that the interface can support the performance of tasks and that the intended tasks can be carried out effectively. Discrepancies are identified in cases where the tests find that the design does not meet the established performance requirements. Since resolution of these discrepancies will most likely require that design changes be made, these design changes will not only have to be re-validated, but also re-verified.

Any discrepancies identified during verification should be resolved prior to proceeding with validation of the HSI design. Section 3.8.3.8 describes how identification, categorization, prioritization, and resolution of HEDs should be handled. While some discrepancies can be "accepted as is," many HEDs will, in fact, result in changes to the design. Following successful completion of the redesign activities, these changes will be re-verified to ensure adequate resolution of the problem.

The last HFE V&V activity to be performed is the Final Plant HFE Verification (Section 3.8.3.9). The purpose of this activity is to confirm that the design description and documentation match the installed configuration and to complete any V&V activities that could not be performed prior to installation. Any discrepancies identified at this stage should be resolved by updating the appropriate documentation, before the design is ready for operation.

In summary, HFE V&V consists of the following activities:

- HSI Inventory and Characterization (Section 3.8.3.3)
- HSI Task Support Verification (Section 3.8.3.4)
- HFE Design Verification (Section 3.8.3.5)
- Operational Conditions Sampling (Section 3.8.3.6)
- Integrated System Validation (Section 3.8.3.7)
- Human Engineering Discrepancy Identification and Resolution (Section 3.8.3.8)
- Final Plant HFE Design Verification (Section 3.8.3.9)

An important consideration for HFE V&V of digital systems is the impact changes may have on software V&V and vice versa. For example, a discrepancy with the design of a display screen discovered during HFE Design Verification such that it requires a design change may also affect software V&V. In the example, some parts of the software may have to be re-verified and re-validated after the change is implemented. Of course, the HSI design may also need to be re-verified and re-validated. Similarly, if the software design changes for reasons unrelated to HFE activities at any time after an HFE V&V activity is complete, the impact of the change on the HSI should be evaluated from an HFE perspective, and the HSI may need to be re-verified and re-validated. However, the scope of re-verification and/or re-validation activities needs to cover only the identified discrepancy and any other HSI components that may have been impacted by the change.

In some cases, when certain features of the modification have already been verified and/or validated during previous modifications, credit can be taken for some of the previously performed verification activities (for example, a recorder replacement using the same model of the device as was utilized in another, already completed modification). Thus, the scope of the V&V activities required can be reduced. However, sufficient documented justification should be provided to support this approach. The results of the previously performed successful V&V activities should be referenced in the V&V documentation for the modification under consideration.

3.8.3.1 Planning for HFE V&V

At the planning stage, the designers should consider the following elements and include them in the overall project plan. These will influence the schedule and required resources for HFE V&V. As the specific V&V activities are defined as they relate to the HFE V&V activities described in the remaining paragraphs of Section 3.8.3, the information developed should be factored back into the overall V&V plan and schedule.

- The timing of the V&V activities (e.g., coordination of HFE V&V activities with overall system V&V and the normal design and testing practices, including QA programs and plans, system V&V programs and plans, factory acceptance testing, system validation testing, site testing, simulator testing/training);
- The locations for performing the activities (e.g., vendor site, on-site, simulator facility);
- The assignment of responsible personnel (also considered should be the requirements for the qualifications and the independence of personnel);
- The need for support from the HFE experts. (The utilities should determine if sufficient resources exist within the organization to properly implement the HFE design program, including the necessary HFE V&V activities. Those utilities planning to carry out modifications for more complex or critical systems, or planning to install more than one large and complex modification at once, will almost certainly need HFE expertise);
- The scope of the HFE V&V activities;
- The availability of tools needed to carry out the V&V activities (e.g., full-scope simulator, partial task simulator, mockups, drawings, documentation);

- The additional requirements that may need to be incorporated into the system purchase specification and the resulting contract with the vendor supplying the HSI. Such requirements may include:
  - A prototype of the HSI that can be used for design test and evaluation purposes, as well as for the HFE V&V activities,
  - An allowance for the third party access to the vendor site and participation in vendor activities and the responsibilities and authority that third party personnel would possess with the vendor,
  - Assurance that changes in the design resulting from any V&V activities performed while the equipment is still in the vendor facilities will be implemented while the equipment or system is still at the vendor's site.

HSI tests and evaluations are related to HFE V&V activities in terms of scope (Section 3.10), but are usually less formal. These HFE V&V activities are performed as part of the design development process, the purpose of which may be confirming the validity of the conceptual design, evaluating various design options, etc. Such evaluations are also performed for some intermediate design products. HFE V&V activities should be done on completed design products. At the same time, though, in order to obtain early confirmation of the design, it is important to perform verification activities on completed portions of the design as early as they are available.

3.8.3.2 Personnel Performing HFE V&V Activities and Criteria to be Used

Verification and validation activities should be performed by a team of qualified personnel and include personnel involved in design activities. In general, the HFE verification activities should be performed by the designers, and HFE validation should involve independent reviewers and HFE experts. Personnel who participated in the design are the most knowledgeable about the technical aspects of the design and their input in the V&V activities is invaluable. However, for modifications to safety related systems, QA requirements will specify the level of independence required. An independent team for both verification and validation is recommended for Level 1 HFE modifications. An independent validation team is recommended for Level 2 modifications.

The criteria for HFE verification will largely be defined as part of the normal modification process. For example, a "Style Guide" (Section 3.7) or other HSI design criteria (such as the design guidance found in NUREG 0700) may be specified as a design requirement by the plant's engineering procedures or internal design standards. Therefore, some of the verification criteria for completed HSI are readily available. Other design requirements and the associated verification criteria are derived from the task analysis activities. Criteria for validation are derived from a variety of sources including, but not limited to, engineering analysis and subject matter expertise (e.g., process system descriptions, operations personnel, procedures and operator logs, system engineers).

3.8.3.3 HSI Inventory and Characterization

The purpose of the HSI Inventory and Characterization activity is to describe all HSI components and related equipment that are within the scope of the modification. The inventory should be created using the most up-to-date information sources, such as design specifications, equipment lists, drawings, etc. Further, the accuracy of the inventory should be confirmed by directly observing the HSI components and comparing them to the documented descriptions.

HSI inventory and characterization can be performed after the conceptual design is complete. It will undergo revision as the design evolves, but it needs to be completed before the HSI design itself is finalized to ensure that all HSI components with the appropriate characteristics associated with personnel tasks are included in the final design.

The inventory should provide an accurate and complete description of the HSI components. At a minimum, the inventory should contain the following information:

- A unique identification code or name
- The associated plant system and subsystem
- The associated personnel function or sub-function
- The type of component

In addition, the information for the components in the inventory should include characteristics of the components such as the following:

- Display characteristics and functionality
- Control characteristics and functionality
- User-system interactions and dialog types
- Location in the data management system (e.g., location of display screens in the screen hierarchy)
- Physical location

Note that all HSI components affected by the modification should be included in the inventory, regardless of the scope or the complexity of the modification and independent of the grade level assigned to the modification (i.e., Level 1, Level 2, or Level 3).

The basic purpose of creating the HSI inventory is to identify all the aspects of the interface needed to verify that the interface meets its requirements. Thus, the designers should focus on characterizing the HSI and not technical features of the devices that comprise the HSI.

The HSI inventory and characteristics information should be compared to the personnel task requirements during the HSI Task Support Verification (see Section 3.8.3.4). Such requirements should have been identified and documented during the HFE analyses (Section 3.3, Function Analysis and Allocation and Section 3.4, Task Analysis). In addition, the same HSI inventory information should also be used during the HFE Design Verification to make sure that the characteristics of the HSI conform to the plant Style Guide (see Section 3.7) and HFE guidelines, such as those in Section 4 of this document.

3.8.3.4 HSI Task Support Verification

HSI Task Support Verification (TSV) is intended to confirm that the modified HSI design supports the performance of the specified user tasks. It also should ensure that the HSI does not include unnecessary information, controls, displays, etc., i.e., that all components of the HSI support operator tasks. Identification of unnecessary HSIs requires keeping a tabulation of the HSIs that support the analyzed tasks. These should be evaluated to determine if they support tasks that were not included in the task analysis (and why they were not) or if they truly unnecessary. Additional HSIs needed to support the tasks should be identified.

Initial or Static TSV is performed as early as practical. Static TSV uses the results of the HSI Inventory and Characterization (Section 3.8.3.3), Task Analysis (Section 3.4), the PRA/HRA, and the operating procedures in a document-based, static evaluation process. Where functions are automated, Static TSV includes evaluation and verification of the availability of HSI components for tasks for monitoring automation functions and for backup manual actions. The purpose of Static TSV is to confirm that the inventory of HSI components support personnel tasks as defined by the design goals and the analysis. Static TSV should be performed for all grade levels of modifications. Static TSV may be sufficient for Level 3 modifications if the modification does not affect the timing of task execution and information access.

Dynamic TSV should be performed using the mature modification design and with the use of prototypes of the new design or the plant simulator. Dynamic TSV evaluates and confirms that HSI components meet specified operability requirements (e.g., response time, accuracy, precision) for selected tasks. Dynamic TSV should be applied for Level 1 modifications. Dynamic TSV may also be appropriate for Level 2 or Level 3 modifications if the timing aspects of these modifications could affect the success of the task execution or information access.

During HSI Task Support Verification, the HSIs (controls, alarms, displays, communication devices, etc.) and their characteristics as documented in the HSI Inventory and Characterization are compared to the personnel task requirements that were obtained in the Task Analysis. In the early design stages, this information should be supplemented by the preliminary versions of documentation such as System Design Descriptions, P&IDs, logic diagrams, and hardware and software specifications. As the design continues to develop, other tools may be used, such as full-size static mockups, panel drawings, paper displays, and room layout/arrangement drawings.

For Level 1 plant modifications, the scope of the HSI Task Support Verification should address all aspects of HSI relevant to the modification. It is important not only to verify the final HSI configuration, but also to evaluate all temporary configurations that may be created during the installation of the modification. For example, for a modification that replaces the annunciator system, the temporary system installed to monitor off-normal conditions during the outage would need to be included in the TSV.

The scope of the HSI Task Support Verification should also address HSI configurations in which old HSIs are deactivated and abandoned in place. While validation tests will confirm later that these deactivated HSIs do not distract or confuse the operator nor do they have potential negative effects on personnel performance, HSI Task Support Verification should at least ensure that they do not obstruct the view of other, operational HSIs or directly interfere with other operator tasks.

3.8.3.5 HFE Design Verification

HFE Design Verification, as with any other design verification, is an evaluation in which the final design is compared to the design requirements and the design specifications. In the case of HFE Design Verification, the design requirements should be largely derived from the Style Guide (See Section 3.7). The design verifiers should define the criteria for the verification and should capture it in a checklist of the relevant Style Guide requirements depending on the characteristics of the HSI components included in the design. The designers should justify and document any places where the design deviates from the specifications or established practices. HFE Design Verification should be performed as soon as design elements are complete, and it should be performed prior to the Integrated System Validation.

While designers should normally base the HSI design on a defined set of HFE rules and practices derived from the “Style Guide” or other widely accepted HFE practices, this is not always practical, especially with vendor designed HSIs. The system purchase specification may not have been detailed enough and compromises may have been made during design. While these compromises should have been documented, justified, and made available to the verifiers, it is imperative that the verifiers use well-defined HFE rules to do the verification in any case where a design was not implemented based on a defined set of guidelines.

The scope of the HFE Design Verification should include all HSIs affected by the modification and their interaction with the rest of the HSIs. As with the HSI Task Support Verification, this activity should also address all temporary configurations that may be created during the implementation of the modification. These temporary configurations should be reviewed against the same criteria as those that will be used for all other HSIs.

The scope of HFE Design Verification will depend on the scope of the modification of the HSI. Regardless of the grade assigned (i.e., Level 1, Level 2, or Level 3) to the modification, all of the design needs to be verified. The degree of independence of the verifiers and the nature of the documentation should be in accordance with the organization’s QA program requirements. The scope of HFE Design Verification may be reduced if there are any HSI components that are repeatedly used in the modification. For example, if a specific modification involves replacement of a dozen recorders with digital recorders, all of which are of the same type and model, then it would suffice to verify many of the characteristics of just one recorder and use the same conclusions for the others.

As previously recommended, checklists developed from the Style Guide should be used for HFE Design Verification. Additional tools may include panel drawings, computer display screen shots, and full-size static mockups – the same that were used during the HSI Task Support Verification, given that they provide sufficient amount of detail to perform the verification.

The methodology of performing this verification consists of comparing the characteristics of the HSI components to the design requirements. Note that it may not be possible to evaluate some characteristics of the HSI, such as general lighting, noise, control room layout, etc, prior to installation of the modified HSI in the control room. In this case, verification of these characteristics will be deferred until after the installation is complete and will be performed as part of the Final HFE Plant Verification activity (Section 3.8.3.9).

A Human Engineering Discrepancy (HED) should be identified for each instance when it is found that an HSI component does not conform to the design specifications or the “Style Guide.” These discrepancies should be fully documented and evaluated to ensure that no other potential issues exist, i.e. to evaluate the extent of condition. For example, if the elements of a particular display screen were found to be not in compliance with the chosen color coding scheme, other similar display screens should also be evaluated to ensure that this issue does not have generic implications.

However, the designers should keep in mind that some HEDs can be justified and may not warrant design changes. For example, a design requirement will likely be that components on a screen should be numbered left to right. In some cases, such as for feedwater heaters, the designers may develop a graphical design that results in a display-numbering scheme that violates the left to right convention. Upon evaluation, the evaluators may conclude that because the display depicts the feedwater heaters in a manner that reflects the actual layout in the plant, the benefit of meeting that positive expectation for the operator outweighs the negative aspects of the non-standard numbering scheme on the display.

That is not to say that the designers should attempt to resolve discrepancies by justifying them instead of correcting the source problem; rather, situations may exist when the designers may choose to take an exception to the rules and practices provided in the “Style Guide,” given that sufficient reasons exist for making such decisions. In this case, the basis for these design decisions should be documented, the alternative HSI design feature should be added to the Style Guide, and the resolution of the HED should reference these documents. For a more detailed discussion on HEDs, see Section 3.8.3.8.

3.8.3.6 Operational Conditions Sampling

Most I&C modernization projects and some individual modifications or series of modifications will involve a large number of HSI components, and thus, hundreds of personnel tasks can be affected. This, in turn, translates into a much larger number of possible events that could be encountered during operation of the plant. It is neither practical nor appropriate to evaluate all scenarios to confirm the adequacy and effectiveness of the modified HSI and ensure that the performance requirements can be met under all operating conditions. Sampling of the operational conditions should be used to choose a representative set of scenarios for validation. There are three sampling dimensions that should be addressed in the identification of scenarios for the Integrated System Validation. These are personnel tasks, plant conditions, and situational factors known to challenge personnel performance.

3.8.3.6.1 Personnel Tasks

The designers (or other personnel responsible for performing this activity) should address those personnel tasks that are related to the use of the modified HSI. As a minimum, the tasks identified in Section 3.4 should be considered. In addition, the sample set of tasks should be augmented to include all tasks that were found to be particularly difficult to implement, could be potentially troublesome or error-prone for the users, or for which some significant compromises had to be made during the design process. Further, the sample set should also cover those design features that were known problem areas for the old HSI design (e.g. as documented in the

Operating Experience Review) in order to confirm during validation that these problem areas were adequately addressed by the modification. Finally, the designers should consider including in the sample set some of the tasks associated with those HSIs that were not modified but whose use might be linked to the tasks associated with the modified HSIs.

3.8.3.6.2 Plant Conditions

It is important to ensure that the sample set includes representative plant conditions as appropriate for the HSI affected by the modification. These should include normal operating events such as, plant startup, plant shutdowns or refueling, and significant changes in operating power, failure events (instrument failures, HSI failures, and other system component failures, such as, pumps, valves, and motors), and transients and accidents. As appropriate depending on the systems being modified, the sample set should also consider the role of the equipment in achieving plant safety or plant production functions.

3.8.3.6.3 Situational Factors

Situational factors (such as lighting and noise) known to challenge human performance may be included in the sample set, depending on the nature of the modification. The effect of some situational factors may not need to be formally validated if it can be shown that these situational factors did not change and the effect that they may have on human performance will likely be the same as it was prior to the modification. For example, environmental factors, such as noise and extreme temperatures, will have very little effect on the operator’s ability to read the value displayed by the recorder, regardless of the type of recorder (e.g., a paper and ink recorder or a digital recorder installed as a part of the modification). However, some other environmental factors, such as poor lighting, may have a different effect on the operator’s performance of tasks associated with the digital recorder as compared to the old device, and therefore, such effects may need to be evaluated during validation testing.

Note that a set of scenarios similar to that chosen for the Integrated System Validation will also have to be developed by the plant training program at the simulator to test the proficiency of plant personnel.

A Level 1 HFE modification will require the most complete set of scenarios, which will need to cover as a minimum those tasks that meet the Level 1 criteria (high safety risk, high commercial risk or high personnel risk). A Level 2 HFE modification will need to cover those tasks that meet the Level 2 criteria. For Level 3, the scenarios chosen should be whatever is required for normal plant post-modification training as well as any “demanding or difficult” tasks as specifically identified (see Section 3.4.3.2).

The results of sampling are combined to identify a set of scenarios that will be used during the Integrated System Validation tests. Each scenario may combine several characteristics identified during the Operational Conditions Sampling. Note that the scenarios used during the tests should be realistic, but not limited to only those situations that are most likely to occur and would be typically encountered during day-to-day operations. The set of scenarios should also include a wide set of feasible failure events. Some scenarios, particularly those that include failure events, may have to be tested more than once to ensure repeatability of adequate operator’s response to a failure.

3.8.3.7 Integrated System Validation

The Integrated System Validation (ISV) is a performance-based evaluation of the integrated design and human task performance to ensure that the HSI is operable within all performance requirements and supports safe operation of the plant. The goal is to test the integration of personnel and plant systems and to validate the integration of the design with personnel actions, plant response, HSIs, procedures, etc. ISV is performed using dynamic HSI prototypes and high fidelity simulators.

A variety of tools and methods can be used to validate the design. These include interviews, questionnaires, checklists, dynamic prototypes, walk-throughs/talk-throughs, static mockups, part-task simulators, and the full-scope simulator. For Level 1 modifications and for complex Level 2 modifications, ISV tests should be performed using the modified, full-scope simulator. Especially for complex modifications, the use of a high fidelity simulator that has sufficient flexibility to realistically change the test conditions is important to successful validation. For a more detailed discussion on HFE tools and evaluations, see Section 3.10.

Unlike for new plant designs, the scope of the Integrated System Validation for modifications will not usually include the entire control area. For example, for a modification that replaces the existing controls and displays for a single system, the scope of the ISV should be limited to only those representative scenarios that involve the use of the new HSIs. For Level 2 and Level 3 HFE modifications, ISV may not require tests using the full-scope simulator, but may be limited to evaluations of the displays and performing walk-throughs/talk-throughs with operators.

For Level 1 and Level 2 HFE modifications, the Integrated System Validation should consider the integration of old and new HSI equipment with operators utilizing normal, abnormal, and emergency operating procedures, as applicable.

The simulator testing environment cannot fully replicate the actual Main Control Room environment, in terms of the influence that factors such as noise and stress would have on operator performance in real situations. Further, simulator testing environments can also bias operator behavior. For example, during a simulator test scenario, the operator is likely to anticipate the occurrence of an abnormal condition. This may artificially increase the level of the operator’s attention and alertness to an abnormal event. This potential for bias needs to be considered when evaluating test results. For further guidance, see NUREG/CR-6393.

For Level 1 HFE modifications, formal Integrated System Validation tests should be performed using the plant simulator with a representative set of realistic scenarios selected using input from Operational Conditions Sampling (see Section 3.8.3.6) to confirm that these HSIs, the modified procedures, the allocation of functions, and the task design will also support the operator in performing his tasks.

Prior to ISV tests, the simulator should be modified, the procedures should be revised and approved for use, and the operators should be trained to the revised procedures using the modified HSI. Since it is the purpose of the Integrated System Validation to demonstrate that the modified design is an effective interface, it is important to ensure that problems such as inadequate training or incomplete, unproven procedures are not encountered during the tests because it would make it more difficult to correctly interpret the results of the validation. A goal of ISV is to validate the revised procedures as well as the modified design. ISV is also useful in validating the effectiveness of training. Figure 3-27 provides a simple graphical representation of the importance of using operators who are properly trained on the new systems in a high fidelity environment.

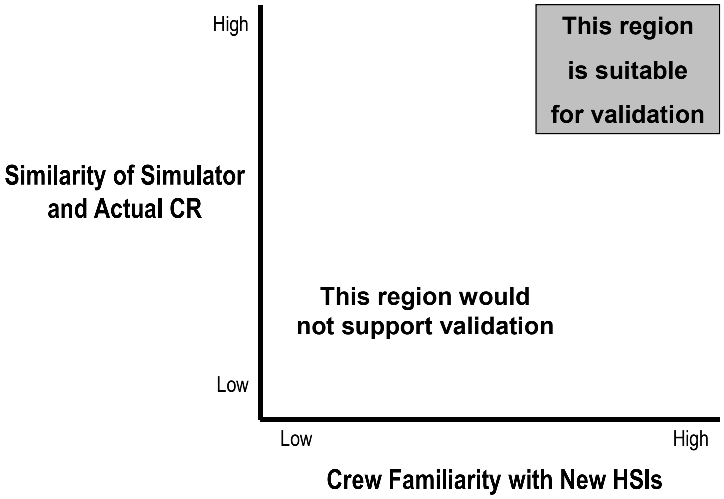

High
Low
Similarity of Simulator and Actual CR
This region is suitable for validation
This region would not support validation
Low
High
Crew Familiarity with New HSIs

Figure 3-27
Conditions for Integrated System Validation

For Level 2 and Level 3 HFE modifications, some aspects of initial tests and evaluations of the design can be conducted without operating procedures. For example, evaluation of display navigation can be performed using walk-through/talk-through techniques using the actual display set up in a laboratory or office-like conditions; evaluation of HSI component layouts on consoles can be performed using mockups. For Level 2 or Level 3 modifications, it may be acceptable to validate the new design using the results of observations and questionnaires that apply performance measures during the process of training the operators on the modified HSI and revised procedures.

Even for Level 1 modifications, where complete ISV testing will be performed later, some potential problem areas may reveal themselves during the training sessions if it is discovered that operators have difficulties learning to use certain features of the HSI or experience other challenges. To achieve the optimal benefits from training activities, HSI designers and HFE personnel should be actively involved with training personnel to identify useful areas of focus for HFE V&V activities. The designers should evaluate such issues if they come up and make decisions regarding proceeding with the Integrated System Validation or considering design changes based on these preliminary results. In either case, the designers should consider the effects of such decisions on the overall schedule and successful completion of other activities.

Even full-scope simulator tests by themselves cannot include all performance shaping factors such as ambient temperature and noise. Therefore, Final Design Verification is performed after ISV once the modification has been installed in the plant control areas. This is addressed in Section 3.8.3.9.

3.8.3.8 Human Engineering Discrepancy Identification and Resolution

The activities described in this section are applicable to all modifications – Level 1, Level 2, or Level 3.

Human engineering discrepancies (HEDs) refer to deficiencies in HSI design with respect to HFE issues. These should be captured as part of an organization's existing problem reporting or deficiency tracking system.

All discrepancies should be documented, i.e., identified, categorized, and prioritized throughout the HFE design process, including the HFE analyses, informal design reviews and iterations, and in each of the V&V steps. HED identification includes the relevant HSI, task criterion, an explanation of the basis for the deficiency, and, depending on the priority, a recommendation should be provided to the designers for correcting the problem, if applicable. Some HEDs will be evaluated as acceptable. In those cases, justification for the acceptability of the discrepancy should be provided, and the HED should be closed with concurrence of the HFE verifiers. After the designers have established a resolution for the discrepancy, the task or HSI component should be re-evaluated to ensure that it was adequately resolved. The HED records should be updated to show the changes. HEDs also serve as a means for tracking HFE issues; all such issues should be satisfactorily resolved by the completion of the final design.

HEDs created during the V&V process may be resolved iteratively with V&V. The discrepancies should be addressed and resolved prior to conducting other V&V activities. After a solution to a design problem documented in an HED is developed and installed, the corrected design should be re-evaluated by repeating the appropriate verification and validation activities. It may not be necessary to repeat the entire verification or validation activity in its full original scope. However, the scope of the re-verification or re-validation should be sufficient to ensure that the problem was adequately addressed by the design change, no new deficiencies were created, and that the new design conforms to the HSI design requirements.

HEDs should be tracked using the normal mechanisms that an organization has in place to identify problems and resolve design deficiencies, if the existing program is able to incorporate HFE-related discrepancies and meet the guidelines specified in this section and the objectives of an effective HFE program. A unique identifier for HEDs should be established, and the appropriate management authority should exist to resolve disputes consistent with the organization's objectives for the HFE program. In fact, resolution of some HEDs should be considered simultaneously with other discrepancies that may exist and are related to the I&C aspects of the system but may not have an immediate implication with regard to the HSI. Such an approach would ensure that when the designers make changes to some parts of the design, all outstanding problems are addressed and no incompatibilities between individual solutions are created.

Resolution of discrepancies should not be performed solely by the design organization; it should include concurrence and acceptance by personnel responsible for HFE verification. Where agreement cannot be reached between the designers and personnel performing HFE verification, discrepancy resolution should be obtained with participation from the plant modification review committee. This is one of the reasons why there needs to be independence between design and V&V for modifications of safety related systems and HSI, as typically required by the plant's QA program.

All existing HEDs require an action. This will be in the form of a justification for accepting the discrepancy as is or as a resolution by means of a change. The individuals responsible for HED closure should ensure that each HED is adequately documented and analyzed and that a solution is developed, implemented, and documented. HFE V&V activities should be repeated as necessary to ensure that the design change met its objectives. After successful discrepancy resolution is confirmed, the responsible individual should close the HED. The design may not be considered complete or final if there are any outstanding HEDs that have not been addressed.

For Task Support Verification, as an example, HEDs are identified when:

- An HSI needed for a task, such as an alarm or a control, is not available, i.e., unsupported tasks;
- An HSI characteristic(s) does not match the description provided in the HSI Inventory and Characterization (e.g., the display shows all required plant variables/parameters but the accuracy of these variables or parameters is incorrect; navigation within or between the display(s) does not function as described in the documentation; location of display elements is not consistent with the provided description, etc.), i.e., partially supported tasks; or
- There is an HSI not required for any task. In this case, the designers should first confirm that this discrepancy does not stem from an incomplete Task Analysis that could have overlooked the HSI component. It should also be confirmed that the HSI component was not erroneously included in the scope of this verification and thus, appears not to be addressed by the Task Analysis.

3.8.3.9 Final Plant HFE Design Verification

The Final Plant HFE Design Verification is the final step in the V&V process and is applicable to a Level 1, Level 2, or Level 3 modification. By completing this activity, the design team, in effect, declares that the modified HSI conforms to the design and is correct and ready for operation. During the Final Plant HFE Design Verification, the team verifies that the design description and documentation match the installed configuration and that the design is fully documented. They also complete any V&V activities that could not be performed before installation (e.g., verification of the final control room layout, evaluation of installed lighting, noise, in-plant communications, and plant specific features). Also included in this activity is the comparison of the final procedures and training with the design description to verify their conformance to the final HSI design and confirmation of adequate resolution of all previously created HEDs. Any new discrepancies should be corrected by updating the affected documentation.

Designers should have high confidence that the design will pass the final verification prior to the start of the formal verification activity. In addition, all of the equipment needs to be installed at the plant before the final verification is initiated.

Additional HEDs may be identified during plant operation after the upgrade due to In-Service Monitoring activities as described in Section 3.9.

3.8.4 Documentation

HFE V&V activities, as other HFE activities, should be performed in accordance with a documented plan that describes the implementation of the HFE V&V activities, the V&V requirements, and shows how these activities are integrated into the overall HSI design process. Therefore, HFE V&V activities should be included in the overall modification project plan. The results of the HFE V&V should also be documented. For modifications that are graded as Level 1, the results should be documented in an HFE V&V report that becomes part of the modification closeout package. For Level 3 modifications, approved design products and signed off work orders (i.e., the normal design modification process) are probably sufficient to document the HFE V&V activities. The degree of formal HFE V&V documentation for Level 2 modifications will depend on scope and complexity, and approved design products are probably sufficient for HFE verification. However, some additional documentation (e.g., implementation procedures, scenario descriptions, test plans, questionnaires, and evaluation checklists) should be developed for validation activities. Expectations for documentation requirements should be described in the project plan to the extent practical.

Upon completion of V&V activities, for Level 1 modifications, results summary reports should be created. These documents should explain what was done to ensure compliance with the implementation plan and meet its objectives, describe the V&V activities that were performed, summarize the results, and provide conclusions. The results summary reports should address the following:

- Scope and Objectives
- Identification of participants, including their qualifications
- Descriptions of HSIs involved
- Methods and procedures used
- Test conditions
- Personnel performance issues (e.g., level of training of participants)
- Deviations from test methods, procedures, and acceptance criteria, if any
- Identification of HEDs (Section 3.8.5)
- Records of resolution or justification of deviations
- Evaluation of test results and findings
- Conclusions

3.8.5 Grading the HFE Verification and Validation Effort

Section 2.4.2, A Graded Approach to HFE, introduced the concept that the level of HFE effort for a modification should be based on the nature of the risk significance and complexity of the change. A methodology was provided to establish a grade for a modification into one of three levels: Level 1 – high risk, Level 2 – moderate risk, or Level 3 – low risk.

In Sections 3.8.3.2 through 3.8.3.9, HFE V&V activities for a Level 1 modification are described. Guidance is provided for how HFE V&V activities can be tailored for Level 2 and Level 3 modifications. The plant's Quality Assurance program requirements should also be considered in defining the scope of HFE V&V.

Additional guidance on grading HFE V&V can be found in Sections 3.2 through 3.6 where the output of the HFE activities will have implications for HFE V&V depending on the scope of the activity.

3.9 In-Service Monitoring of Modifications

3.9.1 Introduction
3.9.2 Objective
3.9.3 Methodology
3.9.3.1 Planning and Administration
3.9.3.2 Requirements
3.9.3.3 Tracking and Documentation
3.9.3.4 Implementation
3.9.4 Use of the Results
3.9.5 Grading the In-Service Monitoring Effort

The purpose of this section is to describe the need for and implementation of an in-service monitoring program. The program is to promptly identify any problems encountered by plant personnel interacting with the new systems and HSIs following their installation and routine use. It is also intended to identify needs for performance improvements. That is, to provide an opportunity to make modifications or adjustments that, while not focused on fixing problems, provide performance improvement. Once identified, corrective actions should be planned and implemented.

3.9.1 Introduction

A common lesson learned from plants that have completed major digital I&C and HSI modernization programs is that once the new systems are used on a "day-to-day" basis, additional operational issues will arise. Such usage begins with the crew training on the new systems and extends for some time after the HSIs are used for actual plant operations.

Some of these issues will involve detailed aspects of the HSI design, such as:

- a label on a process display is incorrect
- an alarm message is not worded properly
- an HSI function behaves differently on the simulator than it does in the control room
- an item is missing from a display selection menu
- a change in the way a task is performed creates unanticipated difficulties
- unexpected negative interactions between old and new systems

Other issues reflect the integration of the new HSIs and new systems into the full context of the crew's overall work activities, such as:

- A change in the way a task is performed creates unanticipated difficulties
- The way a new task has to be performed impedes other crew tasks that are performed at the same time
- Unexpected interactions between old and new systems

This latter category of issues is often hard to detect during design and testing and becomes evident once the complete work environment and demands are experienced.

These types of issues should be identified and resolved. These types of "minor" issues are likely to be below the detection threshold of ongoing corrective action programs (as will be discussed further in Section 3.9.5). Treating them in a formal program can help to systematically identify and address issues, rather than depending upon anecdotal information and ad hoc fixes.

An additional benefit of such a program is that monitoring of the initial use of a modification provides valuable confirmation of what design approaches work well so that they can be used with confidence in subsequent modifications. In general, approaches that are used in early modifications will be followed in later modifications. There is much to be learned from early operation and from the early interactions between plant personnel and the modified HSI. These lessons will not be learned for future modifications, and the necessary adjustments made to assure the modification has maximum utility and usability, unless pro-active measures are taken.

The following section addresses the objectives and implementation of an in-service modification monitoring program. The program can be effectively accomplished using some straightforward and simple activities. The modification monitoring program can be phased out over time in favor of more routine monitoring and corrective action programs.

3.9.2 Objective

The primary objective of an in-service monitoring program is to confirm proper functioning of the modification and promptly identify any problems encountered with the new systems and HSIs following their installation and routine use. Once identified, corrective actions should be planned and implemented.

The monitoring program should ensure that:

- Performance improvements expected with the new design are realized.
- Changes made to the HSIs, procedures, and training do not have an adverse effect on personnel performance. An important aspect of the monitoring program is to identify any unintended consequences introduced into the overall work environment.
- Any changes in project scope are evaluated and tracked against completed project design expectations, human factors expectations, and end user expectations.
- The new design does not require users to develop ad hoc ways of interacting with the HSIs or system (e.g., 'work-arounds') due to design shortcomings.

Uses of the results of in-service monitoring are discussed in Section 3.9.5.

3.9.3 Methodology

The complete methodology is for a Level 1 analysis. For recommendations on grading the methodology, see Section 3.9.5.

3.9.3.1 Planning and Administration

Specific planning for the in-service monitoring activity is essential. Resources and personnel are needed to support the monitoring activities. These need to be explicitly included in the overall effort for the modification. It is easy for managers and planners to presume that installation of a modification ends any evaluation. Even though only modest effort will be required for most in-service monitoring, if no effort or funds are explicitly allocated to support it, it will not be done.

In order to carry out effective in-service monitoring, it will be necessary to establish an In-Service Monitoring Team to be responsible for each portion of the activity. Over the monitoring period, the team will be responsible for:

- collecting information from various sources suggested below
- accessing other individuals as necessary based on specialized expertise
- analyzing and resolving identified issues
- documenting the results of the in-service monitoring program and preparing brief summaries of the monitoring effort and the conclusions reached

The team will make recommendations to the sponsoring manager about what actions are needed to address ongoing and perceived issues and then initiate them through the proper plant channels, e.g., work requests, or put them into modifications that are in-process or planned.

Having access to other individuals for specific issues is an important consideration, e.g., it has been found to be extremely useful in most cases for members of the design team to meet directly with users of the modified system to get their reactions first hand and be able to ask follow-up questions. However, in most cases many of the personnel involved in a modification may be re-assigned to other work before the modification is even installed or operated. Management should review resource allocation in order to provide for continuity in the design responsibility and must make it clear to others on the plant staff that they will be expected to cooperate during execution of the monitoring function. The operations, training, maintenance, and other affected departments need to know that the monitoring effort will take place and that their personnel need to support this effort.

3.9.3.2 Requirements

In-service monitoring is used to identify and resolve problems or issues related to topics such as:

- Task performance during normal, abnormal, and emergency conditions

- Effectiveness and actual usage of special features and functions of new systems, HSIs, and procedures
- Interfaces and interactions between new HSIs/procedures and old HSIs/procedures
- Changes to personnel roles and responsibilities
- Teamwork, crew coordination, and communication
- Training program modifications
- Procedure modifications

Issue identification is based largely on feedback from users, including those in the control room, local control stations, maintenance personnel, and technicians. The in-service monitoring must be a pro-active effort since users will seldom spontaneously inform the monitoring team of their problems and impressions without specific prompting. Although major problems may surface through regular problem reporting practices and systems, minor issues are unlikely to be brought to the design team's attention without a program in place to capture such feedback. Certainly, favorable comments and impressions are unlikely to be recorded unless they are actively solicited.

For input to modification still in progress or potential future modifications, it is also important to confirm when approaches work well and capture any serendipitous benefits of a particular technology or approach. Favorable comments and impressions are unlikely to be recorded unless they are actively solicited, a "problem" oriented reporting system will not capture them. These 'lessons learned' should be tracked for applicability to both ongoing and future modifications.

Thus, methods must be in place to enable personnel to not only identify problems that are observed and also capture useful positive feedback. Three methods of information collection are recommended.

3.9.3.2.1 Observation of Work Practices

One source of information is observations made in the control room or other work areas. Someone knowledgeable in operations, teamwork, and the use of the new systems should make these observations. The observations can be used to see if difficulties in the use of the new systems or their interactions with other control room activities occur. Any potential issues noted can be discussed with the personnel involved to help identify the source of the problem. Actual observations can probably be limited to very early use of the new systems by its users. Data collection after that can mainly rely on interviews and reporting sheets.

3.9.3.2.2 User Interviews

Another source of information is interviews with personnel who interact with the modified systems and HSIs, such as operations, training, and maintenance personnel. Early project interaction with these individuals is necessary. The in-service monitoring team needs to be identify other unexpected or indirect interactions with the modified system such as engineering, procedure writers, security, etc., who might also be interviewed. Interviews should address both positive and negative aspects of use of the new systems.

3.9.3.2.3 Problem Reporting Sheets

It is desirable to prepare problem-reporting sheets and have them readily available to users, where they are working. This will make it easier for users to document issues they identify before they are forgotten. Use of this type of problem reporting sheet has been a common feedback tool in plants that have performed major upgrades. The sheets are used during training as well as actual operations.

Where an issue does not have an obvious cause, e.g., an incorrect label, it is necessary to work toward a root cause determination so that effective corrective actions can be identified. When conducting such an analysis, the team should also consider whether the issue is isolated or has generic or common cause implications.

Perhaps a more effective way to report problems than using reporting sheets is to incorporate a problem reporting application into the HSI. For example, personnel could easily click on an icon that opens a problem report sheet. If users have logged onto the DCS, this sheet could be prefilled with the user's name, etc. The electronic form could also have pull down selection lists that allow the problem report to be categorized (e.g. DCS functional area, severity of problem, etc.).

3.9.3.3 Tracking and Documentation

A simple tracking method should be established to ensure that all observations and issues (both good and bad) are documented, reviewed by the team, and necessary actions initiated. Each observation should be "closed out" in some fashion and documented. It is also important to ensure that this information is readily available and its existence known for other modifications.

Determine whether to use an existing tracking system or implement a special one for this purpose. The complexity of this tracking system should match the complexity of the modification. For a relatively simple modification for which only a few dozen observations may have to be tracked, a simple manual system kept by the person responsible for the design team would be adequate. However, for an extensive modification that could involve hundreds of observations, a more sophisticated system may be needed.

3.9.3.3.1 Use of an Existing Plant Monitoring System

Most nuclear plants have systems in place to identify major problems and assure that those problems are corrected such as the licensed operator-training program and the corrective action program. There may be technical or organizational problems using such existing systems for the short term, focused in-service monitoring function, including:

- *Focus on HFE* – Existing systems of problem reporting may not be concerned with human factors-related problems. If human factors-related problems are not accommodated in the plant problem reporting and resolution system, those existing tracking systems will not be of much help in monitoring the use of the HSIs. On the other hand, in plants where there is a consistent and effective HFE involvement in the resolution of any identified problem, this should be less of an issue.

- *Activation Threshold* – Existing reporting systems may have a high threshold of activation, i.e., their customary use may be limited to problems of serious consequence. Such a reporting system would provide considerable assurance that very serious problems will not be missed. However, if used without modification, it would not capture lower-level problems and those without serious consequences, and would be completely insensitive to 'near-miss' information. It may be possible to simply lower the threshold for reporting occurrences having to do with the plant modifications. However, some plants may use data from their reporting systems as a basis for measures of organizational performance, and the needed changes might not be simple at all, possibly requiring a change in management approach and plant culture.
- *Sensitivity to Tracking System Results* – if data from plant reporting systems is a basis for poorly conceived or interpreted measures of organizational performance, there will be an obvious reluctance to add a potential source of input when the results could reflect adversely on management performance.
- *Scope* – Existing reporting systems are oriented toward problems occurring during actual operations. However many features of an HSI are essentially never exercised. In normal plant operation, accidents and serious events are extremely rare events. Many systems, particularly safety systems, will never experience actual operation under conditions that will reveal human factors problems. If there are human factors problems with such plant systems, it is unlikely that any scheme to report operational problems will disclose them unless the problem occurs during some periodic testing or training. If these rare events are regularly exercised in the plant simulator and if the particular HSI is adequately represented by the simulator, then observations and performance can be a source of information on the use of the HSI. Most simulators normally have some sort of system that records and tracks problems with the simulator itself. For example, simulator behavior that the operators find does not match the actual plant performance would normally be noted so that the simulator programming could be modified or, if that is not practical, the training of the operators could be changed to include discussion of the lack of prototypic behavior. If such a reporting and tracking system exists at the simulator, it could be used to monitor the performance of systems that are not exercised in normal day-to-day operation of the plant.

If these limitations exist in the existing systems available, it is advisable to handle these in-service monitoring as described here as a separate effort.

3.9.3.3.2 Use of a Special Modifications Issues Tracking System Established for the Modification

As part of HFE program planning, it was recommended that an Issues Tracking System be implemented during upgrade process (see Section 2.4 for a discussion of the Issues Tracking System). Using an existing issues tracking system has the advantage of being specifically oriented towards the plant modifications and of being separate from existing performance improvement systems, which, as noted above, may not be suitable for use in this context.

See Section 2.4.1.4 for discussion of a separate HFE tracking system, when appropriate. Such a system is useful with there is a large volume of relatively minor findings that would be inappropriate for tracking in other tracking systems. At some point such an HFE tracking system should be closed out and its few remaining open items transferred to the more general tracking systems. Depending upon the nature and scope of the modification, it may be useful to keep the tracking system open and use it for the initial post installation in service monitoring.

Thus, the decision to create a new program or use an existing one is based on whether any existing problem detection and tracking system is available that can be used to accomplish the objectives of in-service monitoring. If there is, then the in-service monitoring discussed here can be made a part of it. If not, then establishing such a program is desirable. In the latter case, coordination with ongoing programs is necessary.

3.9.3.4 Implementation

The intent of this program is to identify problems encountered in personnel interactions with the new systems and HSIs during early use and to correct them. The frequency with which such problems arise can be expected to decrease over time. Thus, the in-service monitoring system can be phased out when it is determined that most issues have been identified. Subsequent problems would then be captured by existing, long-term performance improvement programs. However, for upgrade programs extending over multiple outages, it may make sense to keep the program running so that it is already in place for the next of the series of modifications.

The criteria for ending the special, focused monitoring effort will obviously vary depending on the complexity and character of the modification that is being tracked. However, specific (and relatively objective) criteria for declaring the special monitoring effort complete need to be established in the planning phase. The effort should come to a defined end point.

One might be tempted to claim that the in-service monitoring should continue throughout the entire life cycle of the modification. Although that might be good in theory, in practice projects need to have a defined end point. Continuing in-service monitoring programs for the entire HSI are not within the scope of these guidelines. Note that effort and personnel would have to be allocated explicitly for that purpose – it might be difficult to justify. In developing a plan for in-service monitoring, it is important to provide justification by identifying potential benefits.

Some criteria for ending focused in-service monitoring of a modification as a specific task are:

- *Frequency of Use* – If a modification is used extensively, e.g., is involved in normal plant operations, and most of its features have been regularly exercised by a substantial number of users, it is reasonable to expect that the majority of the important problems and observations will surface quickly. Further special monitoring should, therefore, not be necessary. However, if a modification is infrequently used, e.g., manipulated only during cold shutdown or refueling, then effective monitoring can really only take place during the time the modified HSI is in use. In that case there would be little monitoring needed (or possible) until the modification is used. The in-service monitoring effort might well be “put on hold” until the particular modified HSI is actually used sufficiently. Some modifications (e.g., protection systems, many safety systems) can only be monitored on the plant simulator.
- *Training* – An important part of the monitoring task involves obtaining feedback from training of personnel on the use of the modified HSI. The monitoring effort should not be terminated until a large number of the potential users have been through the training on the

new systems and HSIs. The training department should be consulted and should be an active participant in the monitoring effort, as they often have valuable insights into potential problems and advantages during the course of training. The training department will be able to establish when a large number of the operators have been through the relevant training.

- *Simulation or drills* – If the modification is related to emergency use and would only be exercised in simulator or plant drills, the special monitoring effort should not be ended until the related planned evolutions are conducted and the results evaluated. Assistance from the training, licensing, and operations personnel will be needed to identify any such drills and special simulations. It will probably be necessary to observe the drill multiple times with different participants to have confidence in the generality of the results.
- *Time* – If none of the above considerations can be used, maintaining a special monitoring program for a complex modification for a year should be adequate; for simple modifications, a few months may be sufficient. The appropriate time will depend, however, on how much actual use of the modified systems and HSIs there is.
- *Maintenance* – No period of tracking should be ended without a comprehensive search of maintenance work orders (or similar records of maintenance) to establish what maintenance work has been done on the modified interface. If the modified HSI design involves some routine maintenance, such as calibration and adjustments, the monitoring should normally not be ended until at least two[12] routine maintenance operations has been conducted and evaluated. Records of maintenance should show who performed the maintenance. Those persons who have actually worked on the system should be included in any program of interviews.

3.9.4 Use of the Results

The results of these analyses are used to correct any aspect of the modification that may detract from personnel performance.

3.9.5 Grading the In-Service Monitoring Effort

Section 2.4.2, A Graded Approach to HFE, introduces the concept that the level of HFE effort for a modification should be based on the nature of the risk significance and complexity of the change. A methodology is provided to establish a grade for a modification in one of three levels: Level 1 – high risk, Level 2 – moderate risk, or Level 3 – low risk. The methodology presented in this section is appropriate for a Level 1 effort. For a Level 2 effort, the formal in-service monitoring activities detailed in this section should be limited to those tasks, which are identified as problematic during the V&V activities described in Section 3.8. In addition, for a Level 2 effort, the monitoring program may be phased out more quickly than for a Level 1 effort (Section 3.9.3.4 describes the criteria to be used for phasing out the formal monitoring).

Modification programs engaged in Level 3 activities, may consider further streamlining the methodology in the following manner. For all levels, aspects of the complete Level 1

[12] If there is something wrong in the maintenance procedure or some hidden flaw it might not show until after the first maintenance, which might not reveal that it was not effective.

methodology that may be useful to a particular utility's specific modification could also be included where clear benefits would be obtained. It is recommended that for Level 3 analyses, any issues identified when the modification is in-service be identified and tracked through normal plant improvement processes.

3.10 Methods and Tools for Collecting Information from Users

3.10.1 Introduction

3.10.2 General Approaches to Information Collection

3.10.2.1 Interviews

3.10.2.2 Surveys, Questionnaires, and Rating Scales

3.10.2.3 Focus Groups

3.10.2.4 Observational Studies

3.10.2.5 Walk-Throughs

3.10.2.6 Performance-Based Tests

3.10.2.7 Computer Modeling

3.10.3 Methodological Considerations for Collecting Information

3.10.3.1 Identifying Who Should Conduct the Activity

3.10.3.2 Developing Information Collection Plans and Procedures

3.10.3.3 Selecting Users to Participate

3.10.3.4 Selecting Testbeds

3.10.3.5 Selecting and Developing Scenarios

3.10.3.6 Choosing Aspects of Performance to Measure

3.10.3.7 Analyzing the Results

3.10.4 Appendix – Rating Scale for General HSI Evaluation

3.10.5 Appendix – Questions for Detailed Usability Evaluation

3.10.1 Introduction

In Sections 3.2 to 3.9, many of the HFE activities discussed methods for collecting information from plant personnel, including interviews, surveys, walkthrough, and tests and evaluations using simulators. Since the same methods are used for many different HFE activities, the decision was made to discuss the details of those methods in one place, rather than repeating them in each section in which they were used. This is the section that provides that more detailed discussion. Section 3.8.3.7 addresses integrates system validation. The methods and techniques presented in this section can be used to support the development and conduct of the validation activities described in that section.

This section addresses methods and tools for collecting information from plant operators, maintainers, and other personnel who are the users of the plant systems and HSIs being modified. For simplicity, all these personnel will be referred to as "*users*." Also for simplicity, the person or group collecting the information will be referred to as the "*HFE analyst*." The term "*information*" as used in this section is quite broad. It includes everything from user opinions about how the control room should be modified to data, such as task time, the users generate while the HSI design is being evaluated in simulator exercises. Collectively, all the information that users provide in the design and evaluation of plant modifications is included.

The information provided by users contributes in many significant ways to the design and evaluation of plant modifications. For example, the design team may wish to resolve a tradeoff (for example, whether to use touch screen or mouse input), obtain design information (for example, determine the meaning of a set of icons), or to try out a new approach (for example, web based monitoring and control of remote equipment). The design team may also perform an evaluation of the HSI design, e.g., to evaluate whether a computer-based procedure design meets performance requirements when use by operators during realistic scenarios (as might be done as part of integrated system validation, see Section 3.8.3.7). Some additional examples are given in Table 3-19.

Table 3-19
HF Planning Activities

HFE Activity	Example of the Use of Test and Evaluation Methods
Endpoint Vision	Conducting a focus group with operators about their vision of how the control room may be improved
Operating Experience Review	Interviews with operators concerning potential areas of task difficulties or HSI shortcomings
Function Allocation	Questionnaires regarding the need for new functions and tasks
Task Analysis	Walkthroughs of tasks to help identify task requirements
Staffing levels	Evaluating task allocations to individual crew members using task network modeling (see Section 3.10.2.7 for an explanation of task network modeling)
HSI Design	Using questionnaire-based rating scales to obtain operator evaluations of HSI prototypes
	Measuring operator use of two alternative approaches to display navigation
Integrated System Validation	Collecting plant and task performance data during key scenarios using the plant simulator

The quality of the information obtained is a function of good data collection methods and good data collection "instruments," such as good questionnaires, rating scales, or task performance measures. Thus, this section addresses both of these considerations. In addition, several data collection tools are provided, such as a rating scale for General HSI evaluation. These tools can be used and adapted to the requirements of an individual modernization program.

While collecting information from plant personnel is an important and integral part of HFE, it does not have to be a large, expensive undertaking. Obtaining survey information from maintenance personnel, or walking down tasks with a few operators, can be done quite efficiently. Of course, some of the methods are more resource intensive, such as conducting tests using the plant simulator, but these approaches are only recommended in sections 3.2 through 3.9 when necessary.

In the next section, several approaches to collecting information are discussed. Then the remainder of the section discussed some of the basic methodological considerations that go into planning and conducting information collection activities. These include things such as who should collect information, how to sample participants, how to conduct tests, how to select performance measures, and how to establish performance criteria.

Much of the information in this section was adapted from NUREG-/CR-6393 (O'Hara, et al., 1997). The NUREG/CR discusses a methodology for conducting integrated system validation from a safety perspective. While the purpose of this document is much broader, the information presented in the NUREG/CR is applicable to information collection in general. The reader is referred to that document for additional information of the topics discussed in this section.

3.10.2 General Approaches to Information Collection

There are many different ways to collect information. Some are relatively easy to use; others are more difficult and costly. A number of approaches are discussed below:

- Interviews
- Surveys, Questionnaires, and Rating Scales
- Focus Groups
- Observational Studies
- Walkthroughs
- Performance-Based Testing
- Computer Modeling

These methods are often used together. For example, while the use of questionnaires can be a complete method in its own right, questionnaires may also be used in conjunction with performance-based testing in order to collect user opinions. Each is discussed below along with their unique methodological considerations. General methodological considerations are presented in Section 3.10.3.

3.10.2.1 Interviews

Interviews may be used alone or in combination with other methods and techniques to obtain information from users. Interviews can be conducted in support of design activities, such as interviewing operators to determine desired improvements in the control room, or evaluation activities, such as conducting debriefings following the use of new HSIs. Interviews are one of the best methods to solicit user comments and opinions and to determine the root causes of difficulties and problems they encounter and how they can be improved. There are two types of interviews: unstructured or structured (although they can be used in combination).

3.10.2.1.1 Unstructured Interviews

Unstructured interviews usually involve dialogues between the HFE analyst and the users that are not highly scripted. To conduct successful unstructured interviews, the analyst must have adequate technical knowledge of the subject; otherwise important questions may not be asked. The analyst asks open-ended questions in the user's area of knowledge and experience. Initial unstructured interviews permit the analyst to gain some understanding of the jobs and tasks about which the interviewee has knowledge. As the interview progresses, the analyst can add more structure to the questions that are posed. The analyst can also use the responses to develop a set of specific probe questions to administer during a subsequent structured interview.

Analysts typically take notes to record the user's comments. Although note taking during the interview may be sufficient in some situations, it is a good practice to make an audio recording. The analyst can then review the information and make notes or have the record transcribed for further review and analysis.

A potential limitation with unstructured interviews is that the users may get sidetracked, talking at length about topics that are not pertinent to the goals of the interview. In that case the analyst has to steer the user back to the topic of the interview.

3.10.2.1.2 Structured Interviews

Structured interviews are designed and planned in advance. Rather than exploring a topic generally, and then delving into specific areas when the opportunity presents itself (as in an unstructured interview), a structured interview involves asking specific probe questions. The probes may relate directly to the job, task, or interface that is associated with a modification. Users may be asked questions about why they take (or do not take) certain actions, how they know that an action should be taken, how they know that an action has succeeded (or failed), and how they recognize and correct errors.

A potential limitation of structured interviews is that the very structure can inhibit users from providing important clarifications or supplemental information. In addition, there may be a very important aspect of the topic that is not addressed by the questions. Thus, an opportunity has to be built into the process to obtain for this type of information.

3.10.2.2 Surveys, Questionnaires, and Rating Scales

Questionnaires and surveys are structured lists of questions in written form. A rating scale is a structured means of obtaining a user's response to a question. The value of these methods is that a lot of information can be collected inexpensively. The design and administration of questionnaires or surveys is described below.

3.10.2.2.1 Survey/Questionnaire Design

Questionnaires/surveys can address any aspect of the design, e.g., the questions presented can address how users use the current HSIs or an extensive evaluation of the HSI. Whether a short or long set of questions is used depends on the goals of the information collection activity and the stage of design maturity. A short list of questions is best when:

- The goals are fairly high-level, such as getting an overall HSI evaluation from many users
- The goals are narrowly focused on a particular aspect of the design, such as the meaning of icons
- The design is in early stages of development

While short questionnaires/surveys are good for the situations noted above, they are not diagnostic. For example, they will indicate if the design is generally good or where general problems may be found, but will not expose details. For this purpose, questionnaires that are more detailed are better. The negative side of longer questionnaires is that they are more burdensome for the user to complete, so that detailed questions will require knowledgeable and motivated participants.

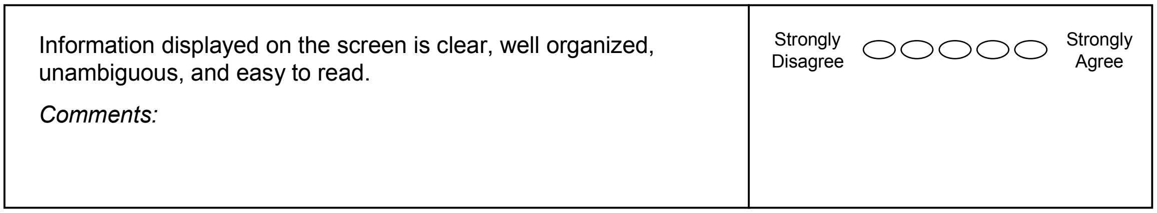
An example of a short questionnaire for general HSI usability is presented in Section 3.10.4. Questionnaire items for a more detailed and diagnostic evaluation are given in Section 3.10.5. Questions from either of these examples can be adapted to create a questionnaire to evaluate any design.

The wording of the questions can be user oriented or system oriented. User-oriented questions are framed in terms of the user's experience and opinions. When using a system-oriented wording, questions are framed in terms of system characteristics. The questions in Section 3.10.5 are user oriented and those in Section 3.10.4 are system oriented. When the participants are actual users, user-oriented questions are best. When participants are not users, then the system-oriented questions are best.

Questionnaires should also give users space to include comments so they can explain their rating or provide suggestions and recommendations.

3.10.2.2.2 Rating Scales

Rating scales are composed of a question or statement that the user answers using a scale provided that usually offer a finite set of options that vary along some underlying continuum. Section 3.10.4 is an example of a set of rating scales for user to evaluate HSIs. One of the scales is presented in Figure 3-28.



Information displayed on the screen is clear, well organized, unambiguous, and easy to read. *Comments:*	Strongly Disagree ○○○○○ Strongly Agree

Figure 3-28
Example of a Rating Scale

A user reads the statement, and then decides which of five options best meets his/her opinion. In this case, the underlying continuum is the degree to which users feel a statement reflects an interface they are familiar with. The scales can force participants to think critically about particular aspects of the design. Users often find it much easier to provide ratings than to answer open-ended questions about the same topics; therefore the time and effort involved in the evaluation is reduced. In addition, the structure imposed by the rating scale method of data collection can make the participants' responses easier to summarize and use.

The design of the rating scales should be uncomplicated. Most participants will be familiar with the use of ratings for expressing opinions, and the appearance of the scales should conform to their experience. Even so, clear instructions should be given; e.g., "circle the tick mark corresponding to your response" or "place a mark in the circle below the word that best describes your judgment of each item."

The scales can be either labeled hierarchically (e.g., very good, good, average, poor, very poor), or only at the endpoints (very good, very poor). A common technique is to compose a statement concerning the aspect of the interface about which the users' opinion is sought, and ask the users to rate the extent to which they agree or disagree with it. Taking item 1.1 in Section 3.10.5 as an example, the question, "Is each screen clearly identified with an informative title or description?" could be recast as "Screens are clearly identified with an informative title or description," and participants asked to agree or disagree. The form in Section 3.10.4 is structured in this way. Alternatively, the same question could be rephrased, "To what extent are screens clearly identified with an informative title or description?" and followed by a scale anchored at the endpoints by 'never' and 'always.' Other things being equal (i.e., assuming that the same information can be obtained), the former approach may be preferred. It is easier for the evaluators because it is not necessary to create many different sets of opposite or hierarchical adjective labels, and may be easier for the users because the predictable structure of the items can allow responses to be made with less effort.

Rating scales usually have a 5-, to 9-point scale. The number of points really should reflect the degree of precision of the discriminations users can make in their ratings. If a neutral judgment is a legitimate response, scales with an odd number of points should be used, since they have a 'middle' point. (In the context of design evaluations, it is probably not important to force a positive or negative judgment by using a scale with an even number of categories, and it may even bias the results). Also, unless the rating scales are customized so that all items apply to any evaluation, a 'not applicable' (N/A) option should be provided.

The scales should be designed so that each item is consistently worded relative to the scale. For example, positive evaluations are always higher numbers to the right or lower numbers to the left. This is because users get familiar with the scales and then do not read them carefully so they may miss the fact that a high number meant good on the last question and bad on the current question.

3.10.2.2.3 Administration Considerations

Try to contact users in advance to explain the purpose of the survey/questionnaire/rating scale and to ensure their cooperation. When initiating contact with users, be sure to follow the guidance for interacting with users provided in Table 3-20. When using questionnaires, offer participants an opportunity to give more information, either as part of the questionnaire itself (e.g., an ‘additional comments’ area), or by providing a means to contact the HFE analysts at a later time; users with a stake in the outcome of the effort will often continue to think about the questions after completing the questionnaire.

The limitation of these methods is that actual performance is not measured, so there is a chance that users’ responses may not reflect how their performance is actually affected by different aspects of the design. It is therefore, good to carefully screen the questions to those for which users can provide valid information. As noted above, another limitation is that users may find responding to long questionnaires burdensome. So emphasizing the importance of their input is important.

Another aspect of administering surveys, questionnaires, and rating scales is to establish a means to distribute them and collect them following their completion. Providing a specific deadline for completion that is not too far away will help ensure maximum response.

These instruments may be presented to user in hard copy or via computer presentation. An advantage of computer-based presentations is that analysis of the results is facilitated by having user responses in computer files.

3.10.2.3 Focus Groups

Focus groups typically consist of a group of users (usually 5 or 6), a moderator (HFE analyst), and possibly a limited number of observers. The value of a focus group is that many users can be surveyed in a short time. Bringing users together (rather than interviewing them individually) is cost effective and has the potential to yield more information due to the added value of the users interaction with each other (e.g., they can challenge each others’ assumptions or cite counterexamples). When the issues are well defined (as would be the case if a particular modification were being evaluated), the moderator of the group should direct the discussion to insure that each topic is addressed. In some cases a hybrid approach may be desirable, such that the group is self-managed, but the moderator has a list of previously identified topics to introduce or issues to follow up on in the later part of a session. The focus group participants may also be asked to fill out brief questionnaires.

A potential limitation is group dynamics. Sometimes one or two individuals emerge as “leaders” and dominate the discussion. This places a burden on the moderator to make sure that all participants have an opportunity to contribute.

3.10.2.4 Observational Studies

Observational studies involve users carrying out tasks in their actual work environment, such as the control room, or representations thereof, such as a mock-up or training simulator. This type of unobtrusive observation is often used in an exploratory way at the beginning of a design effort (to develop a better understanding of the tasks), and to assess the design’s integrated performance when it is completed.

The HFE analyst observes user activity as unobtrusively as possible and generally does not interact with the users while they are doing their work (there is usually opportunity after the observation session is completed to interview users to obtain clarifications and additional information).

If users are not accustomed to having "outsiders" in the workplace, it may be necessary to allow a day of so of time in the workplace before actual data collection. This will help users get used to the presence of others and resume normal behavior.

The HFE analyst records information by taking notes or using checklists of expected user actions. If it is possible, videotaping is helpful and can make data collection more reliable, since it provides an opportunity to replay the tape to observe behavior that was either missed the first time or to conduct a more detailed analysis of any specific problems. However, it should be recognized that transcribing from recordings can be time consuming and should not be regarded as a substitute for defining in advance the user behaviors of interest and noting them in real-time.

A limitation of this approach is the analyst lacks control. That is, in observational studies, users are typically free to attend to whatever aspects of the situation they chose and perform functions by whatever means they deem appropriate. Thus it's possible that limited time is spent in the types of interactions the analyst is trying to collect information on. Thus, more interactive techniques are typically used when performance is being examined for a specific purpose (e.g., to evaluate alternative design options).

3.10.2.5 Walk-Throughs

In a walk-through, users perform selected activities and provide information to the HFE analyst either in response to questions from the analyst or as a narrative of their thoughts as they carry out their actions. When users verbalize what they are thinking as they performing the task or interact with the HSIs, they may reveal the strategies they use, the resources they require from the interface, and their expectations about how the resources will be made available. It will also draw attention to points in the interaction where the design of the interface does not complement the user's goals.

To supplement and better focus on the HFE analyst's information needs, analyst's may asks questions such as:

- Why do you do this?
- How do you do it?
- What are the preconditions for doing this?
- What information do you consult in doing this?
- What are the results of doing this?
- Do errors occur when doing this?
- How do you discover and correct these errors?

The walk-through can be used in an exploratory way (e.g., task analysis), or later in the process to refine the design of interfaces; it is applicable at any point at which a representation of the interface is available, and can also be used as part of the evaluation of operational systems (IEEE, 1999).

Walk-throughs can be oriented toward the tasks users have to perform or to the HSIs they use. Each is briefly discussed below.

3.10.2.5.1 Task-Oriented Walkthroughs

In applying the task-oriented approach, the HFE analyst should focus on the tasks that will be impacted by the modification. Information is gained by walking through tasks with users, such as walking through a procedure with an operator. Personnel are asked to verbalize their thought process so that their actions can be understood. As the tasks are being described, the HFE analyst should ask the personnel to identify any especially positive or negative features of the tasks or the HSI (including procedures). If users are experienced with the tasks and interfaces, such as when tasks are being walked down in an existing control room prior to a modification, they should be asked to think of past experiences and any difficulties they have encountered. Users should also be asked about any aids that could potentially improve performance, efficiency, and safety.

Personnel should be asked for the root cause of the problems identified and any suggestions they have for improving the design. Note that such information should only be treated as a suggestion since:

- the issue may be unique to one individual
- the individual may not accurately identify the root cause
- the suggested improvement may not reflect the capabilities of the new systems being designed – other solutions may be more appropriate
- the impact of the problem must be assessed and evaluated against cost-benefit criteria and the impact of the specific problem must be compared with the overall expected benefit of the proposed modification.

3.10.2.5.2 HSI-Oriented Walkthroughs

In the HSI-oriented approach, users are specifically asked to address how they work with various aspects of the HSIs themselves. Instead of centering on specific tasks, the focus is on HSI resources, e.g.,

- alarms
- displays (including detailed aspects such as labeling, abbreviations, acronyms, coding)
- controls
- procedures (including technical correctness, format, and usability)
- job performance aids

- control room layout
- local control stations

The HFE analyst asks users about their experiences with each of the HSI resources. Again, positive and troublesome aspects of the HSIs should be identified along with the users' evaluation of root causes and suggestions for improvements.

If possible, the analyst should audio or video record the session showing the actions taken with respect to the interface along with the participant's narrative.

3.10.2.6 Performance-Based Tests

Performance based tests involve asking users to perform scenarios, such as a plant startup, and measures of performance are obtained. The measures of performance can then be used, for example, to compare old and the new HSIs. A wide range of measures can be obtained, including plant, task, workload, and user opinions. This type of test requires a fairly controlled environment where the same scenarios can be repeated and performance measures obtained. Thus they are typically performed using some type of simulation or engineering test facility.

There are many methodological considerations for conducting this type of test. These include selecting the users to participate, developing the scenarios that are needed, identifying an appropriate testbed, selecting measures of performance, and establishing criteria against which performance can be compared. All of these considerations are discussed in detail in Section 3.10.3.

3.10.2.7 Computer Modeling

As used in this context, modeling refers to modeling human performance. The other methods discussed thus far, the information was obtained from users themselves. When modeling techniques are used, information is provided by the human behavior models, rather that the users.

Modeling is increasingly being used in the design of complex systems. By representing the behavior of the system and of the users that interact with it, it is possible, for example, to consider in iterative fashion the effects of design options on task performance. In the nuclear industry, this type of modeling has been used, for example, to compare staffing profiles under different plant designs. A value to modeling is that it does not require access to users or difficult to access facilities, such as training simulators. Also, once developed, the models can be run over and over as modifications are made to the design.

Since modeling human performance is relatively new, a potential limitation is that it typically requires time and specialized expertise to develop process and user models that are of high enough fidelity to produce data that can replace actual human performance observed in context. Accordingly, it would probably be used only as part of large-scale modifications, where the investment would be easier to justify.

Another limitation is that modeling cannot be used for all HFE information needs. Models are good for examining global considerations, such as function allocation and staffing, but are at this point fairly limited for evaluating concerns like the impact of display design on situation awareness and diagnosis.

3.10.3 Methodological Considerations for Collecting Information

In preparing a methodology for collecting information, the following considerations should be addressed:

- Identifying Who Should Conduct the Activity
- Developing Information Collection Plans and Procedures
- Selecting Users to Participate
- Selecting and Developing Scenarios
- Choosing Aspects of Performance to Measure
- Analyzing the Results

Each of these considerations is discussed below.

3.10.3.1 Identifying Who Should Conduct the Activity

Someone (or group) has to plan and perform the information collection activity. When the purpose of the information gathering is to support design development activities, the HFE analyst can be a member of the design team.[13] However, when the goal is HSI evaluation, the HFE analyst should be independent from the design team. This is important for two reasons. First, it is hard for designers to look at the design independently and critically. Designers are familiar with the constraints and considerations that shaped the design. This knowledge can impact how they interpret the informant provided by users. Second, it is easier for users to be candid when providing information to someone they feel is not personally invested in the design.

In an evaluation activity, the HFE analyst should have a challenging attitude; that is, challenge the design and try to reveal its weaknesses. It is far better to do this during evaluation, than to discover weaknesses during and after installation, and especially after users are already using the design.

3.10.3.2 Developing Information Collection Plans and Procedures

The goal of any information collection effort is to obtain accurate and reliable information. This is accomplished, in part, through the use of detailed, clear, and objective procedures. The procedures should include:

- Detailed and standardized instructions for interacting with and briefing users. The type of instructions given to users can affect their responses and task performance. Inconsistent instructions can make the information obtained less useful.
- Guidance on when and how to interact with users when difficulties occur.

[13] The person serving as the HFE analyst should probably be the member of the design team that is HFE qualified, if there is such a person. Some basic HFE knowledge is generally needed to conduct these activities. If such a person is not available, it may be a good idea to solicit some outside help.

- Instructions regarding when and how to collect and store data.
- Procedures for documentation. The instructions should detail the types of information that should be recorded (for example, when tests were performed, deviations from test procedures, and any unusual events that may be of importance to understanding how a test was run or interpreting test results) and when it should be recorded.

Introductions and instructions given to users should follow the general guidance in Table 3-20. The instructions should be neutral in tone and not bias the users in any way.

Table 3-20
Guidelines for Interacting with Personnel

When interacting with personnel participating in HFE activities, HFE analysts should adhere to the following guidelines and personnel should be so informed:

1. Personnel should be told that their participation is being requested because of their knowledge and expertise and that the information they provide will be used to guide the design.
2. The information being collected is being used to design or evaluate the HFE aspects of the plant, e.g., HSIs and procedures, and *NOT* to evaluate personnel.
3. The anonymity of personnel should be maintained and users should be told that their comments will be treated as anonymous.
4. No punitive actions will be taken from any information learned about previously unknown personnel mistakes that might be brought up, e.g., in the course of conducting an operating experience review.

For critical or complicated information collection activities, a pilot test should be conducted. This is a run-through of the procedure before actual users are involved. Pilot tests also enable the HFE analysts to become familiar with the procedures and to debug any problems that arise.

If users are expected to address aspects of a new design, they should have an opportunity to become familiar with the design prior to participating in the information collection activity.

3.10.3.3 Selecting Users to Participate

User participants are often operators or maintainers, although they may also include knowledgeable coworkers, or independent subject matter experts, depending on the aims and requirements of the information gathering or evaluation.

Many of the methods discussed below require a sample of users. If one or very few users participate, the results may not reflect the range of user opinions and capabilities in the user population. Thus, the sample should be large enough to reflect the characteristics and demographic factors of the user population that can be expected to influence the information collected. Several factors should be considered in determining sample representativeness:

- Skill/Experience – A range of skill/experience levels should be included to represent the range of knowledge and capabilities found in the user population.
- Position – Users should reflect the range of positions, such as ROs and SROs.

- Age/Background – The sample should reflect the makeup of the user population.
- General characteristics – Where applicable, characteristics such as physical size that may be relevant to the specific application should be representative of the range of these characteristics in the population of potential users.

The size of the sample depends to a large extent on what type of information is being collected. Realistically it is also impacted by the availability of users to participate. Design oriented information collection generally requires fewer participants than evaluations. But in general, it is good obtain information from at least five people (assuming that the right mix of factors can be achieved).

3.10.3.4 Selecting Testbeds

Most information collection activities and evaluations are conducted with the aid of some "testbed" that represents the design. Several general classes of testbeds are:

- Physical Mockups
- Prototypes
- Partial Simulators
- Full-Scope Simulators
- Virtual Reality Simulators
- Actual Plant

These testbeds vary in the degree to which the actual operational conditions are approximated. The dimensions along which testbeds vary are:

- *HSI completeness* is the degree to which the HSI is completely represented in the prototype. A prototype may represent one aspect of the HSI, such as the screens for one user task, or the entire application.
- *HSI physical fidelity* is the degree to which the physical characteristics of the actual HSI are represented. High physical fidelity means that the HSI is essentially a replica of the final HSI design in form, appearance, and layout.
- *HSI functional fidelity* is the degree to which the functional characteristics of the HSI are accurately represented. High functional fidelity means that the HSI is essentially a fully functional replica of the final HSI design.
- *System model fidelity* is the degree to which the HSI realistically displays what users would see if the HSI were hooked up to an actual system (real equipment)
- *Timing and dynamics fidelity* is the degree to which the flow of data and response to user input accurately represents the actual system.

In general, the relationship between information collection needs and the class of testbed that can be used is shown in Table 3-21. However, it should be realized that these relationships are only general because there is a lot of variation in overall fidelity within each of the classes of testbeds identified.

A description of each class of testbed is provided below.

Table 3-21
Guidelines for Interacting with Personnel

Class of Testbed	Uses for HFE Information Collection
Physical Mockups	• Compare alternative control room layouts • Obtain personnel feedback on a design • Optimize panel design • Evaluate lines of sight and reach issues • Examine physical movement and access issues, e.g., in a maintenance context
Prototypes	• Obtain user feedback on early detailed HSI design concepts where limited functionality is required
Partial-Scope Simulators	• Optimize new task performance and procedure development • Obtain user feedback on detailed HSI design concepts where functionality is required but where a full operational context is not needed.
Full-Scope Simulators	• Conduce detailed validation of detailed HSI design where full functionality and a full operational context is needed.
Virtual Reality Simulators	• Compare alternative control room layouts • Obtain personnel feedback on a design • Optimize panel design • Evaluate lines of sight and reach issues • Examine physical movement and access issues, e.g., in a maintenance context
Actual Plant	• Walkdown of existing tasks • Evaluation of HSIs a part of in-service monitoring

3.10.3.4.1 Physical Mockups

A physical mockup is a large-scale, proportioned model of the equipment that is part the modification. Mockups are extremely valuable for depicting three-dimensional relationships that would otherwise be difficult to represent before the modification is actually implemented. Mockup evaluations can contribute significantly to the development of the HSI, and should be conducted before the equipment is built, especially when the modification entails extensive changes to panels or rearrangement of workstations. (Evaluation of modifications that are confined to relatively minor changes within panels or to the design of specific screens will probably not involve physical mockups). Full-scale mockups are preferred since they give actual sizes of and distances between panels and components. However, if space or cost factors are limitations, reduced-scale mockups provide adequate representations to help design and evaluate control board enhancement features.

3.10.3.4.2 Prototypes

A prototype is a model of the actual interface. Prototypes can vary in sophistication and fidelity. A low-fidelity prototype may model the HSI using paper and pencil. This can provide a good first approximation of how the HSI will look, but not how it works (e.g., paper prototypes). The HSI analyst can use such prototypes to conduct walkthrough evaluations of the HSI to get early feedback from users on the acceptability of the design. High-fidelity prototypes model the HSI so that it looks and functions very much like the final product. They can be used to support late design activities, such as evaluating specific design features and walking down tasks to develop procedures.

Paper Prototypes

A paper prototype is a paper-based depiction of an interface that can be used to refine user requirements or to evaluate design alternatives. Paper prototypes offer a number of advantages beyond the obvious fact that they can be produced quickly and at little cost. They help designers avoid the temptation to put too much effort into representing something that is bound to change. More importantly, from an evaluation point of view, it has been suggested that if a prototype looks too complete or refined users may regard the design as finished and confine their comments to superficial details; rather than thinking about how well the interface will support the associated user tasks. Because the prototype is easily altered, alternative designs can be compared (e.g., control and display elements of the prototype ‘screens’ can be represented on self-adhesive note paper, so that they can be repositioned within and between ‘screens’ on the fly, based on participants’ responses or suggestions.)

Software Prototypes

Software prototypes have the considerable advantage of being very easily changed according to user feedback. It is also possible to create prototypes that ‘look and feel’ very similar to actual interfaces. It is possible to create highly developed, functioning representations of an interface at any point in the design process. Widely available rapid prototyping software facilitates HSI creation and modification.

3.10.3.4.3 Partial-Scope Simulators

Testbeds using plant simulation models allow walkthroughs and evaluations to be conducted with realistic dynamic system responses. Partial-scope simulators include facilities such as engineering simulators or simulation models linked to a workstation that presents plant information through the new HSIs (see the case study entitled, “Training and Simulation for a Turbine Controls Upgrade” at the end of Section 6.3 for an example of a partial-scope simulator). This type of simulation also can be very effective for training, serving a dual purpose of initial engineering evaluation and later familiarization and training of the operators on the final design. See Section 6.3 for further discussion of simulation in support of training.

3.10.3.4.4 Full-Scope Simulators

Plants have full-scope training simulators that may be available for use in conducting some information collection activities. However, these simulators are not designed to be readily reconfigurable, and it may therefore be difficult to evaluate an alternative modification design in this context. Also, because full-scope training simulators are in use nearly full-time for operator training and license exams, it can be difficult to gain access to the simulator. As a practical matter, evaluation in the plant's full-scope training simulator may only be possible at the later stages of the design process, when the modification has been implemented in the simulator in advance of training. Integrated system validation typically uses a full-scope simulator (see Section 3.8) Of course they may be used for observational studies early in the design to establish current working practices or after modifications have been installed so that the use of the new HSIs can be observed (In-service Monitoring).

3.10.3.4.5 Virtual Reality Simulators

Virtual reality technology has matured to a point where it can be used in the design of control rooms. It offers many of the advantages of full-scope simulation without the costs involved in creating physical environments and mockups with which users can interact.[14]

3.10.3.4.5.6 Actual Plant

HFE evaluations can be performed in the actual control room or at actual HSIs where users work. This is especially useful early in the design process when current work practices are being understood. This method can also be used after modifications are installed as part of In-Service Monitoring. Using the actual plant has many of the same disadvantages as with the full-scope simulator. However, an additional disadvantage is that there is no control over the environment, thus only observational studies can be performed, and therefore, there is little opportunity to observe disturbance conditions.

3.10.3.5 Selecting and Developing Scenarios

Many evaluations will require scenarios to be defined within which the interfaces will be tested. For the evaluation to be successful, the scenarios will need to be chosen carefully. Since it is not possible to test every condition in which the design may be used, it is important to sample scenarios, in much the same way the user population is sampled.

Several dimensions can be used to guide the sampling of the operational conditions that will be combined to form scenarios. One individual test scenario may reflect characteristics of many of the sampling dimensions. The sampling dimensions are grouped into three broad categories:

- Plant conditions
- Personnel tasks
- Situational factors that are known to challenge human performance

[14] Halden has developed and used VR software for these applications in several industries, and has the software available for licensing. EdF is using Halden's software. EPRI in a continuation of the visualization project will possibly obtain and apply such software to a control room upgrade project.

These sampling dimensions are not exhaustive nor are they entirely independent of each other. Considerations for each dimension are provided below. However, it is important to note that not all of these considerations would be appropriate for all modifications. The HFE analyst should select those from the list below that are related to the modification.

3.10.3.5.1 Plant Conditions

Scenarios should include the following, as appropriate to the systems involved in the modification:

- Normal operational events including plant startup, plant shutdown or refueling, and significant changes in operating power
- Failure events, including both system failures (e.g., break in a multiplexer line) and HSI failures (e.g., loss of processing and/or display capabilities for alarms)
- Transients (e.g., turbine trip) and accidents (e.g., main steam line break)
- Reasonable, risk-significant, beyond-design-basis events that are suggested based on the PRA

3.10.3.5.2 Personnel Tasks

The scenario should reflect a range of interactions between personnel and with HSI components:

- Risk-important human actions as defined by the task analyses and PRA and HRA, including those performed outside the control room.
- Important procedure guided tasks, especially those procedures that are new or modified as part of the plant modification
- Range of human decision-making activities, such as monitoring and detection, situation assessment, response planning and response implementation (e.g., interpretation of alarms and displays for diagnosis of faults in plant processes and automated controls).
- Range of HSI components used – The scenarios should include the need to use new HSI features and functions
- Range of human interactions – The scenarios should reflect the range of interactions between plant personnel, including tasks that are performed independently by individual crew members and tasks that are performed by crew members acting as a team.
- Tasks that are performed with high frequency

3.10.3.5.3 Situational Factors that are known to Challenge Personnel Performance

The scenario should reflect a range of situational factors that are known to challenge personnel performance, such as:

- Tasks considered by personnel or the design team to be difficult

- Tasks for which errors have significant consequences (including situations designed to elicit human errors enable assessment of the error tolerance of the system).
- Task having high workload or which require multitasking
- Task for which there is significant workload transition, e.g., a sudden increase in the number of signals that must be detected and processed following a period in which signals were infrequent
- Tasks that may be impacted by fatigue, such as inducing fatigue with long scenarios and conducting some tests on backshift hours
- Task that may be influenced by environmental conditions such as hot areas, poor lighting, extreme temperatures, and high noise

Once the appropriate factors have been selected, they have to be developed into detailed scenarios. Detailed scenarios represent combinations of the dimensions that were described above. The scenario fidelity requirements depend on what is needed for the information collection activity. For simulator evaluations, for example, the scenarios should have sufficient task fidelity so that realistic task performance will be observed. On the other hand, as part of a HSI walkdown, it may not be necessary to be as detailed.

For very detailed scenarios, the following information should be defined:

- Description of the scenario mission and any pertinent “prior history” necessary for operators to understand the state of the plant upon scenario start-up
- Specific start conditions (precise definition provided for plant functions, processes, systems, component conditions and performance parameters, e.g., similar to plant shift turnover)
- Events (e.g., failures) to occur and their initiating conditions, e.g., time, parameter values, or events
- Precise definition of workplace factors, such as environmental conditions
- Task support requirements (e.g., procedures and technical specifications)
- Staffing requirements
- Communication requirements with remote personnel (e.g., load dispatcher via telephone)
- Data to be collected and the precise specification of what, when and how data is to be obtained and stored (including videotaping requirements, questionnaire and rating scale administrations)
- Specific criteria for terminating the scenario

3.10.3.6 Choosing Aspects of Performance to Measure

Evaluation implies a relative comparison of design options with each other, or to some standard, typically using measures of performance. An overview of the types of measures that can be used is given below. ANSI (1993) has additional information about measuring human-system performance.

3.10.3.6.1 Plant Performance Measures

Plant parameters represent the performance of the functions, systems and components the user is monitoring and controlling. For example, if the HSI is being used to monitor or control reactor temperature, some measure of temperature or temperature variability can be obtained as an indicator of performance. While these measures possess the advantage of being easy to interpret and having a clear relationship to the ultimate aims of the design, they are only available in the context of a full simulation of the relevant plant processes (or after the modification has been placed in service).

3.10.3.6.2 Task Performance Measures

Measures of user task performance provide data that complement the plant performance measures. Even when plant measures are maintained within acceptable ranges, shortcomings in the design may place unnecessary demands on users. These demands can be manifested in the users' behavior, for example, the accuracy and timeliness of event detection and decision-making.

Development of user task measures for a given scenario begins with identifying the associated user actions. These actions can be of two types:

- actions performed by users in carrying out their functions with respect to the plant (e.g., monitoring parameters and operating controls), and
- actions performed by users in the course of interacting with the human system interface (e.g. arranging display windows and selecting menu options); see Table 3-22.

It is important to consider both types.

For most tasks, enumerating the individual user actions (of either type) that should occur during a scenario is readily accomplished by referring to procedures or training materials (or, in the case of new actions associated with a modification, the task analyses). The set of required actions is the starting point for the most basic performance measures (e.g., number of required steps completed, or number of steps omitted). It is also desirable to identify actions that could be performed in the course of a scenario. While these should include the required tasks, they will include others as well because of the interactions between user actions (or inactions) and plant dynamics. This larger set of actions will enable a post hoc analysis of the effects of interactions. It will also provide for another basic performance measure (e.g., number of unnecessary or erroneous actions committed).

Table 3-22
Examples of Types of Actions Taken by Users

Examples of actions taken by users with respect to the plant processes – Starting or stopping equipment – Monitoring parameter values or trends – Responding to alarms – Carrying out procedures
Examples of actions taken by users with respect to the human-system interface – Configuring the workstation, e.g., adjusting monitors and keyboards – Selecting mode configurations for computer support functions or equipment – Navigating between or within displays – Formatting and manipulating displays (e.g., changing display type and setting scale) – Paging or searching through procedures

Measurement of user performance will typically go beyond noting the occurrence or non-occurrence of specified actions. Examples of ways in which actions performed by users can be quantified are shown in Table 3-23. Particular performance measures should be chosen to reflect the important aspects of user performance with respect to the tasks involved in the scenario. For example, the time taken to respond to a given indication will not provide meaningful information if it is applied to a situation in which neither the state of the plant nor the procedures being followed mandates an immediate overt response. When task analyses indicate that coordination or communication among operators is required to complete a task, measures of task performance that are defined in terms of the crew (rather than an individual) should be provided. In addition, global measures should be considered, e.g., HSI "overhead" (time spent engaged in tasks directed at the interface per se, rather than plant processes, as a fraction of total time available). Also, choose performance measures that address specific aspects of the design that are of interest or of particular concern; for example, when early feedback from operators identifies potential shortcomings in specific areas of the design, or there are areas where exceptions to normal HFE design standards had to be taken. Plant training personnel and SMEs may be helpful in identifying aspects of performance that are important for accomplishing particular tasks.

Table 3-23
Examples of Measures of Task Performance

Time	Reaction time, e.g., time to perceive event, initiate action, initiate correction, detect trend of multiple-related events Time to complete activity Overall task time (duration) Time-sharing among actions
Accuracy	Correctness of observation, i.e., identifying stimuli internal and external to system detection of changes or trends, recognition of signal in noise, recognition of out-of-tolerance condition Response correctness, i.e., accuracy in control positioning, margin to safety or performance limits, decision making, communicating Error characteristics, e.g., frequency
Frequency	Number of responses per unit, activity, or interval, e.g., control and manipulation responses, communications, user interactions, diagnostic checks Number of performance consequences per activity, unit, or interval, e.g., number of errors, number of out-of-tolerance conditions Number of observing or data-gathering responses: observations, verbal or written reports, requests for information, rate of engagement
Amount achieved or accomplished	Degree of success Percentage of activities accomplished Measures of achieved performance (e.g., terminal or steady-state value)
Subjective reports of participants	Rating scales (see Section 3.10.2)
Behavior categorization by observers	Judgment of performance: rating of operator and crew performance adequacy to evaluate the design (not users), rating of task or mission segment performance adequacy, estimation of amount (degree) of behavior displayed, measures of achieved maintainability, equipment failure rate (mean time between failures), cumulative response output, proficiency test scores (written) Magnitude achieved: terminal or steady-state value (e.g., temperature high point), changing value or rate (e.g., degree of changes per hour)

3.10.3.6.3 Situational Awareness

There are aspects of users' interaction that are not readily measured objectively but are nevertheless related in important ways to the effectiveness of user performance. One such aspect is situational awareness, which involves a user establishing a full understanding of what is going on in a given situation, seeing each element within the context of the overall goal, and having all the pieces fit together into a coherent picture. It can obviously be affected by the design of the interfaces and by how tasks are structured. Assessing users' situational awareness can help designers gain insight into how operators understand situations, and how well the interfaces and aids support users' comprehension. This information can help identify instances in which the system fails to adequately support users' information requirements, and provide a basis for needed design improvements.

It is possible to assess situation awareness by simply asking users about their perception, understanding, or expectation regarding situations that are presented to them. This can be done in a variety of contexts. For example, users might be shown prototype displays and asked for their interpretation of the data that are shown. They might be presented with a dynamic prototype representing a plant condition and asked to predict the status at some time in the future. In a simulation of task performance in an operational context, they might be asked a series of detailed questions about past, present and future aspects of the scenario. When such questions are asked after a scenario is completed the response depends heavily on memory and may be influenced by the outcome of an exercise. Questioning the operator about aspects of the situation while an exercise is in progress can avoid some of the above difficulties, but it is necessarily intrusive. In this case, responding to questions is in effect an added task for the operator, which can disrupt performance.

The Situation Awareness Global Assessment Technique (SAGAT; Endsley, 1995) is intended to avoid the above limitations. The technique takes advantage of the fact that a simulator exercise can be stopped at any point and then continued. At an apparently random point the simulation is stopped and all displays go blank. Operators can then be asked a series of questions related to their current awareness of the situation. A sample of items for assessing situational awareness are given in Table 3-24. Of course the specific questions depend on the scenario. When the simulation is completed, the operator's responses can be compared with what was actually happening at the time the simulation was halted. Dynamic changes in situation awareness can be detected by including several data collection stops during a single scenario. The content of the questions and the times at which they are to be asked must not be predictable by the operator to avoid altering the task (e.g., changing the operator's sampling of instrument readings). One might expect the method to be intrusive, especially when applied during fast-paced tasks; however, it has been used successfully in experiments with nuclear plant operators (Hogg, Folleso, Torralba, and Volden, 1994).

A potential problem is that the questions posed may cue operators to details of the scenario. This is avoided by imbedding key situation awareness questions within other, less relevant questions. Preparing sets of relevant questions for various points of each scenario will require considerable involvement of subject matter experts (e.g., experienced operators and training personnel). To minimize disruption of the ongoing tasks, questions should be brief and simple; equivocal or vague questions will not evoke useful responses.

Table 3-24
Examples of Situation Awareness Questions

Past

In comparison with the recent past, the number of active primary circulation pumps

greatly increased -- increased -- same -- decreased -- greatly decreased

In comparison with the recent past, the temperatures after the low-pressure pre-heaters

greatly increased -- Increased -- same -- decreased -- greatly decreased

Present

In comparison with the normal status, how would you describe the current temperatures in the hot legs of the primary circuit

much greater -- greater -- same as normal -- less -- much less

In comparison with the normal status, how would you describe the current neutron flux of the reactor

much greater -- greater -- same as normal -- less -- much less

Future

In comparison with now, do you expect the level in the pressurizer to

greatly increase -- increase -- stay the same -- decrease -- greatly decrease

In comparison with now, do you expect the temperatures in the cold legs of the primary circuit to

greatly increase -- increase -- stay the same -- decrease -- greatly decrease

3.10.3.6.4 Workload

Workload refers to the amount of effort users must expend in carrying out tasks. It has cognitive as well as physiological components. All other things being equal, a design that imposes greater workload on users is less desirable than one that imposes less.[15]

There are many ways to quantify user workload that involve potentially intrusive methods and specialized equipment, such as measuring performance on additional tasks or recording physiological data. However, good results are obtained by simply asking users to rate their experience of workload. One such rating method is the NASA Task Load Index (TLX). Users rate their experience on six dimensions:

- *Mental Demand* (Low/High) – How much mental and perceptual activity was required (thinking, deciding, calculating, remembering?)
- *Physical Demand* (Low/High) – How much physical activity was required (for example, pushing, pulling, turning, controlling, activating, etc.)? Was the task slow or brisk, slack or strenuous, restful or laborious?
- *Temporal Demand* (Low/High) – How much time pressure did you feel due to the rate or pace at which the task elements occurred? Was the pace slow and leisurely or rapid and frantic?

[15] Very low workload is undesirable as well, because it impairs attention and vigilance.

- *Performance* (Failure / Perfect) – How successful do you think you were in accomplishing the goals of the task set? How satisfied were you with your performance in accomplishing these goals?
- *Effort* (Low / High) – How hard did you have to work (mentally and physically) to accomplish your level of performance?
- *Frustration* (Low / High) – How insecure, discouraged, irritated, stressed and annoyed versus secure, gratified, content, relaxed and complacent did you feel during the task?

One advantage of having different scales is that it can point the HFE analysts toward the particular aspects of the interaction that require the greatest effort. The TLX rating scales are shown in Figure 3-29.

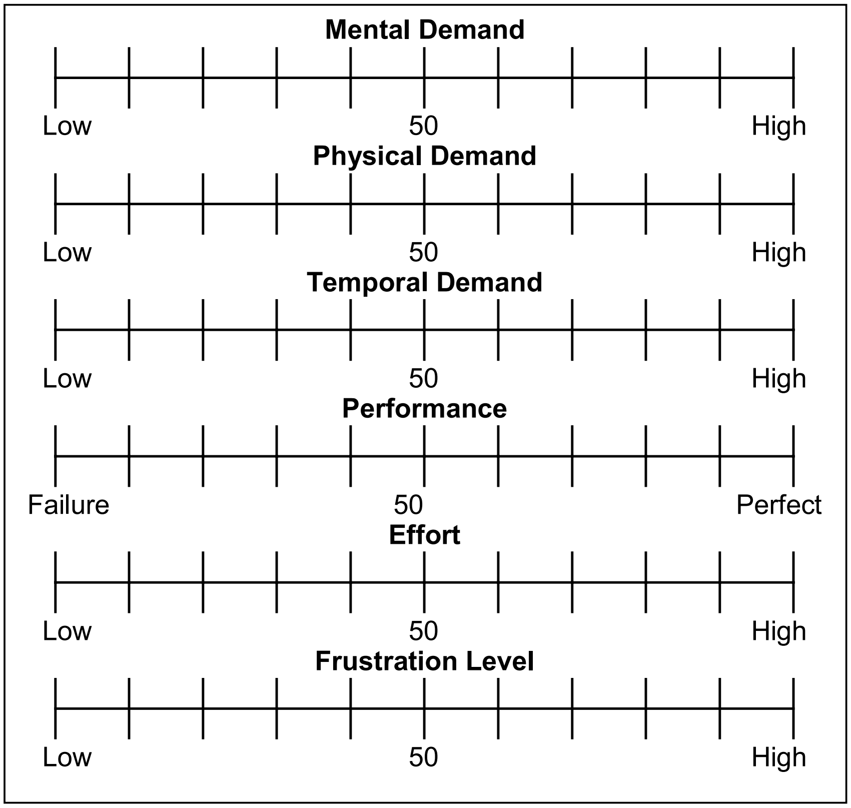


Figure 3-29
NASA Task Load Index Rating Scales

The TLX has been used in many different industries including the commercial nuclear industry. This technique requires participants to become familiar with the meaning of the dimensions in order to be used efficiently.

3.10.3.6.5 User Opinions

A rich source of HFE information comes from the opinions of users. Collecting information from operators, maintainers, and other personnel at many times during the design and evaluation effort is an important activity. The opinions can relate to essentially any aspect of the design including:

- the allocation of responsibilities between automatic systems and personnel
- staffing and the allocation of responsibilities to crewmembers
- teamwork
- the way tasks are performed
- strengths and weaknesses of system operation
- features and functions of the HSIs
- procedure design
- training

The principle means of obtaining user opinions are through interviews, surveys, questionnaires, and rating scales (see Section 3.10.2.2).

3.10.3.7 Analyzing the Results

When the information is to be used as design input, it should be reviewed by the HFE analyst and organized in a manner needed for the design activity it supports. Thus, if the information was a walkdown of a task in support of task analysis, the results should be organized to provide a high-level task description providing the information shown in Table 3-7 and more detailed information that can be organized into task decomposition figures such as those in Figure 3-16. After the information is organized as needed for the analysis, the users should be asked to review the analysis to ensure it is correct. At that time, any missing information that was not captured the first time can be obtained and incorporated into the results. Also, if information obtained from different users was inconsistent, it can be clarified and resolved at this point.

When the information obtained was data in support of an evaluation of various aspects of the design, the analysis is more involved. The information obtained in a testing situation describes performance, e.g., the task was completed in 16 minutes on average. However, to evaluate the system, we need criteria with which to judge the acceptability of the average task time obtained.

Thus, criteria are needed to draw conclusions about a design. There are four basic approaches to establishing criteria that vary with respect to the source of the criteria. They are shown in Table 3-25.

Table 3-25
Establishing Performance Criteria

Criterion Source	Definition	Example
A Requirement	Measured test performance is compared to a quantified performance requirement; i.e., requirements for system, subsystem, and operator performance defined through engineering analysis.	Thermodynamic analyses indicate that the task must be performed in 20 minutes.
A Benchmark	Measured test performance is compared to a benchmark system, e.g., a current system, which is predefined as acceptable.	The task is acceptably performed on the old system in 20 minutes.
A Normative	Measured test performance is compared to a criterion established through use in many system evaluations (rather than a single benchmark system). The advantage of this approach is that the same measure can be used in the evaluation of different designs.	In PWRs of this type, the task is generally performed in 20 minutes.
Expert-Judgment	Measured test performance is compared to a criterion established using the judgment of experts.	Operations experts determined that this task has to be performed in 20 minutes.

Evaluations are likely to require a combination of these approaches, since the types of performance are qualitatively different.

Test data should be analyzed to compare design options and to identify design deficiencies and potential areas of improvement. Any performance issue that doesn’t seem to have been an isolated occurrence (e.g., one encountered consistently, or by more than one participant) should be addressed. Issues identified by only one user should be evaluated to determine whether they are design deficiencies or testing artifacts.

In addition to the HFE analyst or team, the analysis of information may require input from additional personnel, such as operations, maintenance, and training personnel. It may also require input from vendors and suppliers.

3.10.4 Appendix – Rating Scale for General HSI Evaluation

Information displayed on the screen is clear, well organized, unambiguous, and easy to read. *Comments:*	Strongly Disagree	○○○○○	Strongly Agree
The way the system looks and works is consistent at all times. *Comments:*	Strongly Disagree	○○○○○	Strongly Agree
The way the system looks and works is compatible with your conventions and expectations. *Comments:*	Strongly Disagree	○○○○○	Strongly Agree
The system provides clear, informative feedback on where you are in the system. Comments:	Strongly Disagree	○○○○○	Strongly Agree
The system provides clear, informative feedback on what actions you have taken. Comments:	Strongly Disagree	○○○○○	Strongly Agree
The system provides clear, informative feedback on whether these actions have been successful. Comments:	Strongly Disagree	○○○○○	Strongly Agree
The system provides clear, informative feedback on what actions should be taken next. Comments:	Strongly Disagree	○○○○○	Strongly Agree
The way the system works and is structured is clear. *Comments:*	Strongly Disagree	○○○○○	Strongly Agree
The system meets your needs and requirements when carrying out tasks. *Comments:*	Strongly Disagree	○○○○○	Strongly Agree
You feel in control of the system. Comments:	Strongly Disagree	○○○○○	Strongly Agree
The system design minimizes error, and has features that detect and handle those that do occur. You are able to check your inputs and to correct errors before the input is processed. *Comments:*	Strongly Disagree	○○○○○	Strongly Agree
Informative, easy-to-use, and relevant guidance and support is provided to help you understand and use the system. *Comments:*	Strongly Disagree	○○○○○	Strongly Agree
The system is easy to learn. *Comments:*	Strongly Disagree	○○○○○	Strongly Agree

3.10.5 Appendix – Questions for Detailed Usability Evaluation

Section 1: Visual Clarity

Design Objective: Information displayed on the screen should be clear, well organized, unambiguous, and easy to read.

1.1 Is each screen clearly identified with an informative title or description?

1.2 When the user enters information on the screen, is it clear where the information should be entered?

1.3 When the user enters information on the screen, is it clear in what format the information should be entered?

1.4 Does information appear to be organized logically on the screen (for example, menus organized by probable sequence of selection, or alphabetically)?

1.5 Are different types of information clearly separated from each other on the screen (for example, instructions, control options, data displays)?

1.6 Is the information on the screen easy to see and read?

1.7 Do screens appear uncluttered?

1.8 Is it easy to find the required information on a screen?

1.9 Overall, how would you rate the system in terms of visual clarity?

Section 2: Consistency

Design Objective: The way the system looks and works should be consistent at all times.

2.1 Are abbreviations, acronyms, codes and other alphanumeric information used consistently throughout the system?

2.2 Is the same type of information (for example, instructions, menus, messages, titles) displayed in the same location on the screen?

2.3 Is the same item of information displayed in the same format, wherever it appears?

2.4 Is the method of selecting options (for example, from a menu) consistent throughout the system?

2.5 Where a keyboard is used, are the same keys used for the same functions throughout the system?

2.6 Are there standard procedures for carrying out similar, related operations (for example, starting a motor and changing a set point)?

2.7 Overall, how would you rate the system in terms of consistency?

Section 3: Compatibility

Design Objective: The way the system looks and works should be compatible with user conventions and expectations.

3.1 Are abbreviations, acronyms, codes, and other alphanumeric information displayed easy to recognize and understand?

3.2 Is jargon and terminology used within the system familiar to the user?

3.3 Is information presented and analyzed in the units with which the user normally works?

3.4 Where the user makes an input movement in a particular direction (for example, using a direction key, mouse, or joystick), is the corresponding movement on the screen in the same direction?

3.5 Is information presented in a way that fits the user's view of the task?

3.6 Does the organization and structure of the system fit the user's perception of the task?

3.7 Does the sequence of activities required to complete a task follow what the user would expect?

3.8 Does the system work in the way the user thinks it should work?

3.9 Overall, how would you rate the system in terms of compatibility?

Section 4: Informative Feedback

Design Objective: Users should be given clear, informative feedback on where they are in the system, what actions they have taken, whether these actions have been successful and what actions should be taken next.

4.1 Is it clear what actions the user can take at any stage?

4.2 Is it clear what the user needs to do in order to take a particular action (for example, which options to select, which key to press)?

4.3 When the user enters information on the screen, is it made clear what this information should be?

4.4 Is there always an appropriate system response to a user input or action?

4.5 Are status messages (for example, indicating what the system is doing, or has just done) informative?

4.6 Are status messages (for example, indicating what the system is doing, or has just done) accurate?

4.7 Does the system clearly inform the user when it completes a requested action (successfully or unsuccessfully)?

4.8 Is it clear to the user what should be done to correct an error?

4.9 Overall, how would you rate the system in terms of informative feedback?

Section 5: Explicitness

Design Objective: The way the system works and is structured should be clear to the user.

5.1 Is it clear what the user needs to do in order to complete a task?

5.2 Is it clear what part of the system the user is in?

5.3 Is it clear what the different parts of the system do?

5.4 Is the structure of the system obvious to the user?

5.5 Is the system well organized from the user's point of view?

5.6 Overall, how would you rate the system in terms of explicitness?

Section 6: Appropriate Functionality

Design Objective: The system should meet the user's task requirements.

6.1 Are the input devices available to the user (for example, pointing device, keyboard, joystick) appropriate for the tasks to be carried out?

6.2 Is the way in which information is presented appropriate for the tasks?

6.3 Does each screen contain all the information that the user feels is relevant to the task?

6.4 Are users provided with all the options that they feel are necessary at any particular stage in a task?

6.5 Can users access all the information that they feel they need for their current task?

6.6 Does the system allow users to do what they feel is necessary in order to carry out a task?

6.7 Is system feedback appropriate for the task?

6.8 Overall, how would you rate the system in terms of appropriate functionality?

Section 7: Flexibility and Control

Design Objective: The interface should be sufficiently flexible in structure, in the way information and data are presented and in terms of what the user can do, to suit the needs and requirements of all users, and to allow them to feel in control of the system.

7.1 Is there an easy way for the user to ‘undo’ an action, and step back to a previous stage or screen where practical in a process control application (for example, if the user makes a wrong choice, or does something unintended)?

7.2 Can the user look through a sequence of screens in either direction?

7.3 Can the user access a particular screen in a sequence of screens directly?

7.4 Is it easy to return to the main menu from any part of the system?

7.5 Can the user move to different parts of the system as required?

7.6 Can the user choose the rate at which information and data are presented?

7.7 Can the user choose how to name and organize information and data that may need to be recalled at a later stage?

7.8 Where it is acceptable to do so, can users tailor aspects of the interface for their own preferences or needs?

7.9 Overall, how would you rate the system in terms of flexibility and control?

7.10 Is a method provided to easily return to a previously defined default system configuration (not the process systems, only the I&C system)

Section 8: Error Prevention and Correction

Design Objective: The system should be designed to minimize the possibility of user error, with features for detecting and handling those that do occur; users should be able to check their inputs and to correct errors, or potential error situations before the input is processed.

8.1 Are users able to check what they have entered before it is processed?

8.2 Is the system protected against common errors?

8.3 Does the system ensure that the user double-checks any requested actions that may be problematic if requested unintentionally?

8.4 In general, is the system free from errors and malfunctions?

8.5 When system errors occur, can the user access all necessary diagnostic information to resolve the problem (for example, where and what the fault is, what is required to resolve it)?

8.6 Overall, how would you rate the system in terms of error prevention and control?

Section 9: User Guidance and Support

Design Objective: Informative, easy-to-use and relevant guidance and support should be provided, both on the computer (via an on-line help facility) and in hard-copy document form, to help the user understand and use the system.

9.1 If there is some form of help facility (or guidance) on the computer, can the user request this easily from any point in the system?

9.2 If there is some form of help facility (or guidance) on the computer, is it clear how to get in and out of the help facility?

9.3 Is the help information presented clearly, without interfering with the user's current activity?

9.4 When the user requests help, does the system clearly explain the possible actions that can be taken.

9.5 Is the HELP in the context of what the user is currently doing?

9.6 When using the help facility, can the user find relevant information directly, without having to look through unnecessary information?

9.7 Overall, how would you rate the system in terms of user guidance and support?

Section 10: General Usability

Design Objective: The system should be easy to learn and easy to use for tasks it is intended to support.

10.1 Did you find the system easy to learn with few problems learning how to use it?

10.2 Was the system documentation good and support your intended use of it?

10.3 Did you understand how to carry out the tasks?

10.4 Did you always know what to do next?

10.5 Did you understand how the information on the screen relates to what you are doing?

10.6 Did you find the information you want?

10.7 Were you able to read the information clearly?

10.8 Did you find the system flexible enough to meet your needs?

10.9 Did you find the HELP (guidance) easy to use?

10.10 Did you always know where you are were in the system?

10.11 Was the amount of information you needed to remember while carrying out a task acceptable?

10.12 Were the system response times acceptable?

10.13 Did you understand all the actions of the system?

10.14 Was the input device, e.g., mouse or touchscreen, easy to use?

10.15 Did you always know where and how to input information?

10.16 Was the time you spend inputting information acceptable?

10.17 Were errors easy to correct?

4
HFE GUIDELINES

This section contains detailed HFE guidelines for design and evaluation of HSIs. These guidelines have many applications, including: supporting the development of an endpoint vision (see Section 2.2), providing the basis for development of style guides (see Section 3.7), and providing criteria for HFE verification (see Section 3.8). In this introduction, the following topics will be discussed:

- Characteristics of a Well-Design HSI
- Brief Description of HFE Guideline Sections
- Format of the Guidelines

Characteristics of a Well-Designed HSI

HFE guidelines, when used in conjunction with the HFE activities described in Section 3, will result in HSIs that are well-designed from the user's perspective and that will help ensure that the changes made will improve human performance and exploit the advantages on the new technologies. In general, a well-designed HSI exhibits the following characteristics:

- Accurately Represents the Plant
- Meets User Expectations
- Supports Situation Awareness and Crew Task Performance
- Minimizes Secondary Tasks and Distractions
- Balances Workload
- Is Compatible with Users' Cognitive and Physical Characteristics
- Provides Tolerance to Error
- Provides Simplicity
- Provides Standardization and Consistency
- Provides Timeliness
- Provides Openness and Feedback
- Provides Guidance and Support
- Provides Appropriate HSI Flexibility

Each of these general HSI characteristics is briefly defined below.

Accurately Represents the Plant

The HSI should accurately represent the plant, i.e., its functions, processes, systems, components, and parameters. A well-designed HSI can serve as an external "mental model" of the plant. That is, it is consistent with and supports a user's understanding and awareness of the system, its status, and the relationship between individual system elements.

Meets User Expectations

The HSI design should meet the users' expectations. User expectations are based on factors such as:

- General cultural/population stereotypes and conventions
- Professional/industry conventions
- Prior experience with similar systems
- Experience with HSIs installed in the plant prior to HSI modernization

Since there is more than one user group (such as operations, maintenance, and engineering) who will be affected by a plant modernization program, the HSI developers may have to consider the different expectations of the various user groups. Violating expectations is one of the best ways to guarantee users will make mistakes and be dissatisfied with the HSI.

Supports Situation Awareness and Crew Task Performance

The HSI should fully support users to accomplish their primary tasks of monitoring, situation assessment, response planning and response execution by providing alerts, information, procedural guidance, and controls when and where they are needed. For example, the HSI should provide timely alerts to abnormal conditions, high-level information for system monitoring, detailed information for situation assessment and troubleshooting, controls to adjust the system or manipulate equipment, and feedback on actions taken.

The HSI design should address the tasks of different user groups. In addition, the design should reflect the demands of the total work environment, for example, whether the HSI will be used while gloves are worn or in low-light environments.

Minimizes Secondary Tasks and Distractions

In general, the HSI should not distract users from their tasks. Users should not need to shift attention from their primary tasks to the interface. Therefore, the need for users to perform secondary tasks such as window manipulation, display selection, and navigation should be minimized as much as possible. Distracting users from their primary tasks increases both task time and workload and this can have a negative impact on performance and can increase the chance that users will make errors.

Similarly, the HSI should minimize the need for users to:

- Perform mental calculations in order to transform data to the information they need; such calculations are better done in software
- Recall lengthy lists of codes, complex command strings, information from one display to another, or lengthy action sequences that can be represented in the HSI
- Perform many actions to accomplish a simple task
- Enter information already in the HSI or information the HSI can generate from available data

Balances Workload

Human performance suffers under conditions of high and low workload. High workload requires personnel to manage workload by performing some tasks and not others or by performing tasks in a sub-optimal manner. Low workload creates problems of loss of vigilance. In such situations, personnel lose situation awareness and the ability to quickly respond when actions are needed. The design of the plant automation, personnel tasks, and HSIs should provide a balanced workload level.

Is Compatible with Cognitive and Physical Characteristics

The HSI design should accommodate the following human physiological and cognitive characteristics and limitations:

- Visual/auditory perception, for example, users should be able to see all screen elements from their normal working positions
- Information processing and memory, for example, since recognition is easier than recall, display all appropriate options so that users can recognize what is available
- Anthropometrics and biomechanics, for example, the layout and design of workstations and panels should be consistent with the characteristics of human size, reaching ability, strength, and control precision

Provides Tolerance to Error

Error tolerance means minimizing the occurrence of user errors and providing a way for users to detect and correct errors when they do occur. HSI developers should anticipate common or predictable errors that users may make and protect against their consequences. This is especially important when an error can damage equipment, impact data, or cause injuries. The HSI should provide simple and comprehensible notification of the error and simple, effective methods for recovery.

Provides Simplicity

The HSI should be the simplest design that meets the task requirements. Potentially distracting features such as excessive decorative detail or nonfunctional icons should be avoided.

Provides Standardization and Consistency

There should be a high degree of standardization of the interface. That is, the way the HSI functions and appears is always consistent, reflects a high degree of standardization, and is fully consistent with procedures, manuals, and training. The HSI should also be consistent with established conventions. The HSI should use common terms rather than abstract, unusual, or arbitrary terms. The HSI should also be consistent with the user's understanding and expectations about HSI behavior (as developed through training, use of procedures, and experience). Standardization and consistency make the HSI predictable and predictability lowers the workload associated with using the interface, leaving more attention for doing the primary tasks. Predictability also lowers the possibility of user error and makes the system easier to learn, which is important to users and their management.

Provides Timeliness

The HSI design should ensure that tasks can be performed within the time required. This requires consideration of the user's capabilities and system-related time constraints. If information flow rates and control responses are too fast or too slow, user performance can diminish. Users become frustrated by systems they perceive as slow.

Provides Openness and Feedback

The HSI should never seem mysterious to the user. For example, it should never provide information or take action that the user doesn't understand or cannot learn more about. When the HSI integrates data or provides decision support, users should be able to determine the basis for the information provided. For example, if the system provides the user with a fault diagnosis; the system could provide the data used as a basis for the diagnosis, the way the data was analyzed to form a conclusion, etc. In this sense, the user should view the HSI as a "team player." Similarly, the HSI should provide useful feedback to the user regarding its status, permissible operations, and validity of data. Users can tolerate delays in processing requests much better if the system gives them feedback that it is working to process their request.

Provides Guidance and Support

The HSI should provide an effective "help" function. Informative, easy-to-use, and relevant guidance should be provided on line and off line to help users understand and interact with the HSI.

Provides Appropriate HSI Flexibility

Where possible, the HSI should be flexible enough to provide users with multiple means to carry out actions and permit HSIs to be formatted in ways that are most convenient for the current task and to accommodate personal preferences. However, flexibility should be limited to situations where it offers advantages in task performance (such as to accommodate different levels of experience). Flexibility should never be used as a substitute for a well thought-out design.

It is important to keep in mind that computer-based HSIs provide an opportunity to significantly improve upon analog HSIs in which controls and indicators are discrete devices, alarms are presented one or more standalone annunciators, and procedures are provided separately in paper form. Several aspects of computer-based HSIs and the potential improvements they offer are emphasized in the guidelines as described below:

- *Integration* – The designer no longer has to think of alarms, displays, controls, and procedures as separate aspects of the HSI. Instead, these HSI resources can be fully integrated to meet the user's needs. Thus for example, HSIs can be developed in which procedure steps are presented on displays that contain all relevant alarms, data, and controls required for task performance. Controls can be developed that contain all data needed to take the control action, to provide feedback, and to reveal the control logic. All information related to the user's ongoing activity can be seamlessly integrated.
- *Processing* – Data can be presented to the user in the specific way in which it is needed. Lower-level data can be synthesized into higher-level information that is directly usable. Users can be given high-level displays to support monitoring and situation assessment with immediate access to lower-level displays to support trouble shooting.
- *Decision Support* – Support logic can be built into HSIs to help users make decisions, such as to find the most important alarm, to evaluate the status of a procedure step, or to diagnose the cause of a process disturbance.
- *Flexibility* – The HSI can be tailored to better meet the demands of the user's ongoing tasks and to accommodate personal preferences.
- *Portability* – Computer-based HSIs exist in a virtual world, not a physical world. Thus the users can work at workstations at which all HSIs can be accessed, rather than users having to go to where specific HSIs are physically located. Further, HSIs can be made available essentially anywhere. A specific control, for example, may be accessible from any control room workstation, from local control stations, or even from handheld devices that the user brings into the plant.
- *Automation* – Computer-based HSIs can provide features that automate certain interface management tasks. For example, when an alarm occurs a computer-based display can automatically present a link to the associated alarm response procedure or provide other information that is needed to confirm and respond to the alarm.

Where appropriate in the HFE guidance contained in this section, we have suggested some approaches to achieve these benefits of modern HSIs.

Brief Description of HFE Guideline Sections

The guidelines are divided into sections following traditional distinctions among HSI resources, such as alarms, controls, and displays. This was done because the variation in scope and extent of modernization programs ranges considerably from limited replacements of specific systems to essentially new control rooms. Thus, while one utility may narrowly focus on an upgrade to their plant alarms, another may broadly look to replace their existing control room with a fully computerized, workstation-based control room. To support both types of modernization programs, Section 4 follows an organization using traditional HSI distinctions, e.g., it provides sections on alarms, displays, etc.

The guidelines are organized into the following subsections:

- Information Display
- User-Interface Interaction and Management
- Soft Controls
- Alarms
- Computer-Based Procedures
- Computerized Operator Support Systems
- Communications
- Workstation and Workplace Design

The first two sections address the basic building blocks of computer-based HSIs: information display and user-interface interaction and management. With these building blocks, HSI resources can be developed to support other specific cognitive functions, such as monitoring and detection (alarms), situation assessment (COSSs), response planning (computer-based procedures), and response implementation (soft controls). There are unique display and interaction needs for each. Since NPP crews are teams, communications are needed for most personnel tasks. HSI resources are integrated into workstations and workplaces, so guidance for these considerations is provided. A brief description of each section follows.

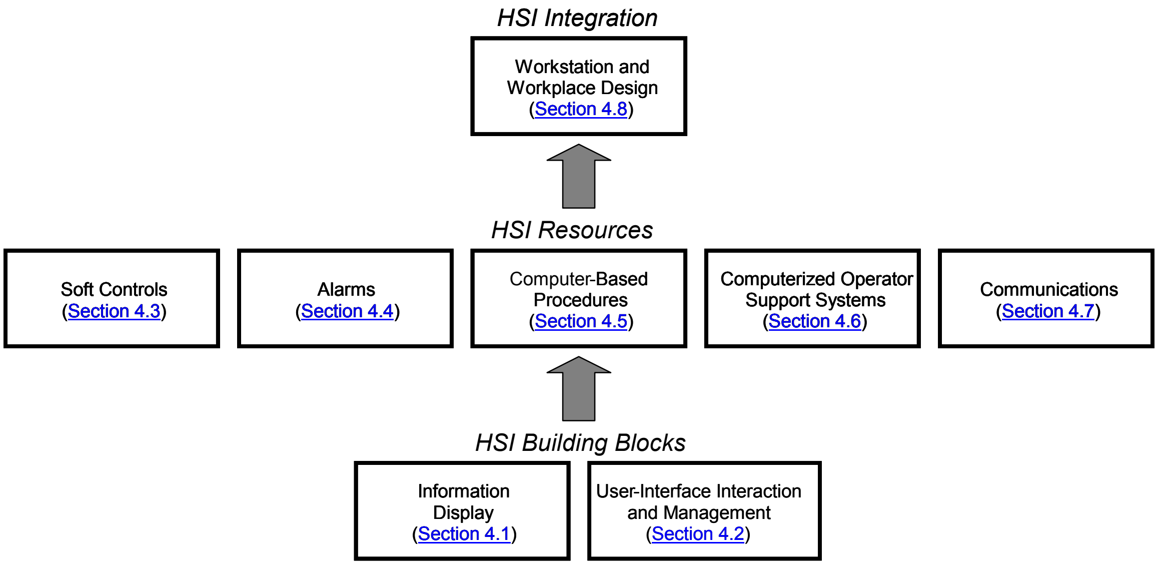

HSI Integration
Workstation and Workplace Design (Section 4.8)
HSI Resources
Soft Controls (Section 4.3)
Alarms (Section 4.4)
Computer-Based Procedures (Section 4.5)
Computerized Operator Support Systems (Section 4.6)
Communications (Section 4.7)
HSI Building Blocks
Information Display (Section 4.1)
User-Interface Interaction and Management (Section 4.2)

Figure 4-1
HFE Guidance for HSI Design

Information Display – Section 4.1

This section provides HFE guidelines for the design of visual displays. First, the general functions that the information displays can support are discussed, including: monitoring and situation assessment, task performance, and teamwork. Included in this discussion is the monitoring of critical plant performance and safety functions. Guidance for developing displays for each of these functions is provided.

Guidance is also provided for developing display pages. These are the retrievable units that a user accesses for information. Pages are made up of a variety of display formats, e.g., mimics, trend graphs, tables, barcharts, digital parameter displays, and configural displays (unique graphic displays). Display formats themselves are built from a variety of display elements (such as labels, icons, symbols, color, text, and coding). In addition, “physical” aspects of displays such as data quality and update rate are vital to the use of information that is provided. Guidance addressing all of these aspects of information display is included in this section.

User-Interface Interaction and Management – Section 4.2

User-interface interaction and management refers to the means by which personnel provide inputs to an HSI, receive information from it, and manage the tasks associated with access and control of information. The guidance in this section first addresses the general design aims associated with user interaction and management. This includes topics such as: simplifying input, establishing consistency of interface and interaction, minimizing demands on the user, guiding and assisting users, and providing flexibility. The section also addresses detailed design considerations for interaction and management functions, such as display navigation, controlling and manipulating displays, computer-system feedback, and information management. In addition, general design considerations for windows and cursors are provided.

Soft Controls – Section 4.3

Soft controls are user input devices presented as displays through which personnel interact with plant functions, processes, systems, components, and variables. Guidance is first provided to support the decision as to whether controls should be implemented as hard controls, dedicated soft controls, or retrievable soft controls. When controls are retrievable, then a selection display (from which to retrieve the controls) is needed. Guidance on the design of selection displays is provided. The centerpiece of a soft control is the control display. The guidance on control displays addresses (1) the identification and management of control displays; (2) the display of control modes, logic, and constraints; and (3) control input and commands. The design of feedback and monitoring aspects of soft controls is also provided. This section contains an appendix on error tolerant design as well.

Alarm System – Section 4.4

The operators’ task of monitoring the operating condition of the plant and detecting problems is supported by the availability of alarms. This section first addresses general design considerations for alarm system modifications. It then provides guidance for defining alarms and developing approaches to their prioritization and processing. The latter are ways to reduce the number of alarms to manageable levels. In modern alarm systems, designers have choices as to how to display alarms, e.g., in dedicated displays (such as alarm tiles), on alarm message lists, or integrated into other displays (such as mimic displays). Guidance for making these decisions and for the design of each, including their auditory characteristics, is provided. Guidance is also provided for alarm control and management, e.g., the sorting of alarms according to time and priority. Finally, alarm response procedures are addressed.

Computer-Based Procedures – Section 4.5

Computer-based procedures (CBP) assist personnel by presenting procedural information, such as decision and action steps, in a manner that help users effectively, efficiently, and reliably achieve procedure goals. The guidance in this section first addresses the scope and functionality aspects of CBP. CBP functionality ranges from translations of traditional procedures for use via a VDU, to systems that integrate process and equipment information and alarms with procedure steps, and provide control and automation features to aid the execution of tasks. Next, guidelines for the display of procedure information are presented, including format and screen layout, procedure steps, cautions, and supplementary information. One of the key features of CBPs is their interactive capabilities. Guidance is provided to address such interactive features as user control of procedure execution, indication of the status of procedure execution, navigation, and explanation and help. The guidance also addresses specific functional aspects of CBPs related to the sensing of plant conditions, providing relevant parameter values and equipment status, resolving step logic, and monitoring user actions. Finally, the guidance addresses user interaction with CBPs under degraded conditions and failure situations. The section includes an appendix to provide information to utilities on the transition from paper procedures to CBPs and their maintenance.

Computerized Operator Support Systems – Section 4.6

Computerized Operator Support Systems (COSSs) are aids provided to personnel to support their monitoring, situation analysis, and decision-making activities. This section first addresses general considerations such as deciding if a COSS should be included in a plant modification, the integration into operations and maintenance activities, modes of COSS operation, and user control of COSS interaction. Then guidance for three specific COSS applications are provided: Condition Monitoring, Fault Detection and Diagnosis, Core Surveillance, and Accident Management Support. As these applications are fairly new to most plants, the section includes a detailed appendix providing technical descriptions of some of the technology underlying COSS design.

Communications – Section 4.7

This section provides HFE guidelines for the design of speech and computer-mediated communication between plant personnel, e.g., preparing, addressing, transmitting, and receiving messages.

Workstations and Workplaces – Section 4.8

This section provides HFE guidelines for the design of workstations and workplaces. Workstations, including consoles and panels, are locations where HSIs are integrated together so personnel can perform their tasks. Workstation design considerations include control-display integration and layout, labeling, and ergonomics, e.g., vision and reach. Workstations are located inside workplaces, such as the main control room and remote shutdown facilities. Workplace design considerations include the overall layout of the workstations and other equipment such as group-view displays within the workplace, provision of support equipment, and environmental characteristics such as lighting and noise.

Format of the Guidelines

Each of the HFE guideline sections is divided into four main parts: overview, checklist, detailed guidelines, and reference list.

- *Overview* – An overview is presented including a relatively short characterization of the specific HSI resource addressed, e.g., soft controls. The characterization is a description of the characteristics and functions of the HSI resource. The characterization is generic in that it is not based on any one system. It describes the HSI topic in general terms so that the users of the guidance can apply it to their systems or to the systems they are evaluating.
- *Checklist* – A guidelines checklist is provided. The checklist provides only the guidelines and not the additional information, figures, and tables (see next bullet). Guideline users who are very familiar with the technical content of the guidance may wish to use the checklist only. However, if a checklist level of information is not sufficient for one or more of the guidelines, additional information can be accessed in the detailed guidance section.
- *Detailed Guidelines* – Detailed guidance is provided here. Each individual guideline has a unique number and is preceded by an arrow, ⇒**,** for emphasis. The number corresponds to its section/subsection location. Individual guidelines are often followed by additional information intended to explain the guideline and give examples of its application. The additional information includes figures and tables as well. To readily distinguish this information from the guideline, additional information is indented.
- *Sources of Additional Information* – A short reference list of key documents is provided for those wishing to obtain more information.

4.1 Information Display

4.1.1 Overview

4.1.2 Display Guidelines Checklist

4.1.3 Display Functions

4.1.3.1 Display Design for Plant Monitoring, Detection, and Situation Assessment

4.1.3.2 Display Design for Task Performance

4.1.3.3 Display Design for Teamwork, Crew Coordination, and Collaborative Work

4.1.4 Display Pages

4.1.4.1 Identification of Information

4.1.4.2 Organization of Information

4.1.4.3 Clarity of Presentation

4.1.4.4 Coding and Highlighting of Information

4.1.5 Display Formats

4.1.5.1 Continuous Text Displays

4.1.5.2 Tables and Lists

4.1.5.3 Data Forms and Fields

4.1.5.4 Numeric Readouts

4.1.5.5 Bar Charts and Histograms

4.1.5.6 Graphs

4.1.5.7 Pie Charts

4.1.5.8 Flowcharts

4.1.5.9 Mimics and Diagrams

4.1.5.10 Maps

4.1.5.11 Integral and Configural Displays

4.1.5.12 Graphic Instrument Panels

4.1.5.13 Speech Displays

4.1.6 Display Elements

4.1.6.1 Alphanumeric Characters

4.1.6.2 Abbreviations and Acronyms

4.1.6.3 Numeric Data

4.1.6.4 Icons and Symbols

4.1.6.5 Labels

4.1.6.6 Scales, Axes, and Grids

4.1.6.7 Borders, Lines, and Arrows

4.1.6.8 Visual Characteristics

4.1.6.9 Auditory Coding

4.1.7 Data Quality and Update Rate

4.1.8 Sources of Additional Information

4.1.1 Overview

Understanding information is at the center of human performance in complex systems. Introduction of advanced technology may significantly affect how personnel get information about plant systems, processes, and conditions. This section addresses the design of information display systems. Its organization reflects a design process that proceeds from general issues surrounding computer-based display of information to specific aspects of display design; see Figure 4-2.

Display Functions
(Section 4.1.3)

Display Pages
(Section 4.1.4)

- Identification of Information
- Clarity of Presentation
- Organization of Information
- Coding and Highlighting of Information

Display Formats
(Section 4.1.5)

- Continuous Text Displays
- Data Forms and Fields
- Bar Charts and Histograms
- Pie Charts
- Mimics and Diagrams
- Integral and Configural Formats
- Speech Displays
- Tables and Lists
- Numeric readouts
- Graphs
- Flowcharts
- Maps
- Graphic Instrument Panels

Display Elements
(Section 4.1.6)

- Alphanumeric Characters
- Numeric Data
- Labels
- Borders, Lines, and Arrows
- Auditory Coding
- Abbreviations and Acronyms
- Icons and Symbols
- Scales, Axes, and Grids
- Visual Characteristics

Data Quality and Update Rate
(Section 4.1.7)

Figure 4-2
Display Design Considerations Addressed in this Section

Section 4.1.3, Display Functions, describes the implications that computer-mediated access to information has in designing information systems. It addresses at a high-level the functions that the information system serves based on both traditional and newer approaches to display design, such as “Ecological Interface Design,” that are made possible by digital technology. By considering both approaches, the section describes approaches for structuring information effectively and for identifying information needed to support the tasks that comprise user functions.

While requirements identify what information is needed by the user, the way in which that information is presented is called information representation, and is composed of the following aspects: display pages, formats, and elements (see Figure 4-10). The information needed to support a particular task is typically arranged and presented on one or more display pages (Section 4.1.4). The figure illustrates two display pages selected from the network (see below) of available displays; the pages are displayed on separate screens, which may correspond to discrete display devices or windows. (Each screen comprises the particular display page and some other relatively constant content areas, e.g. navigation buttons, message areas, and display selection tools). The type of information to be presented and the use that will be made of it determine the display formats (Section 4.1.5 that are used on a page. Display formats are made up of display elements (Section 4.1.6), such as alphanumeric characters, icons, arrows, and axes. Important considerations when using information are its quality (how valid the information is, i.e., whether the operators trust the information) and update rate (how current the information is); these are addressed in Section 4.1.7.

Figure 4-10 also illustrates the organization of display pages in a display network. Guidance for supporting users’ navigation through and use of these (typically hierarchical) collections of pages is given in Section 4.2.5.3, Supporting Navigation in Systems of Displays. Pages may be displayed in different windows and/or display devices; guidance for designing the appearance and functionality of windows is given in Section 4.2.6.1, Windows.

4.1.2 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
4.1.3	Display Functions						
	4.1.3.1	Display Design for Plant Monitoring, Detection, and Situation Assessment					
		4.1.3.1.1	Defining a Hierarchy to Serve as a Basis For Displays				
		=>	4.1.3.1.1-1 Displays for monitoring and situation assessment should be organized according to an abstraction hierarchy. The hierarchy should: • Completely describe the plant in terms of its main purposes or missions, i.e., supply power to the grid and maintain safety • Reveal goal status at each level • Reveal both physical and functional relationships • Reveal interactions and dependencies of the hierarchy elements • Be applicable to all operational situations and reflect differences associated with different operating modes • Be meaningful to the users				

Guidelines						Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
			=>	4.1.3.1.1-2	Displays should reflect the hierarchy and provide information at various levels that are appropriate to the various operator functions and tasks. Higher level displays should support monitoring of plant status and situation assessment functions and increasingly detailed displays should support troubleshooting or more detailed status monitoring.				
			=>	4.1.3.1.1-3	Each display in the hierarchy should use the same general design principles.				
		4.1.3.1.2	Content of Individual Displays						
			=>	4.1.3.1.2-1	Displays should include a representation of the main functions, processes, systems, and component of the plant's AH and their relationships.				
			=>	4.1.3.1.2-2	Displays should indicate the key modes of operation that affect the user's interpretation of information.				

Guidelines						Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
			=>	4.1.3.1.2-3	The important AH elements should be presented so the status can be determined at a glance, i.e., that status is very easily recognized. The types of information that should be considered include: • Goal attainment Status – the current function or system goal is being achieved or not. • Availability Status – available or not available (e.g., bypassed/inoperable; tagged-out; key locked) and whether an action is required for use (e.g., line-up). • Capability Status – the current capability to contribute to the satisfaction of the functional goal in question. This relates to the sufficiency of system or component to achieve a goal. For example, current operating conditions may be such that a system cannot achieve its function because it is not designed to operate under those conditions. Consider, for example, low-pressure safety injection as one of the alternatives that is available to satisfy the Control RCS Water Mass Inventory function. It is only effective in satisfying the goal if the RCS pressure is low enough.) • Service Status – in service or not in service (the element is ready to achieve its purpose). Being ready to achieve a purpose may require going through several stages of successful functional states. • Equipment Functional Status – (e.g., flow/no-flow, energized/de-energized, on/off, and open/closed).				

Guidelines						Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
			=>	4.1.3.1.2-4	Important performance indicators for key AH elements should be provided. These may be measured parameters or derived values. Any analyses or information integration by which lower-level data are analyzed to produce higher-level performance indicators should be available to users so they can easily determine the meaning of higher-level indicators.				
			=>	4.1.3.1.2-5	The display should have information readily available on plant dynamics, i.e., indicate when the performance indicators are changing at significant rates.				
			=>	4.1.3.1.2-6	Overview displays should address safety parameter display system (SPDS) requirements.				
			=>	4.1.3.1.2-7	The display should indicate conditions requiring operator actions related to the main AH elements.				
			=>	4.1.3.1.2-8	Upon control actuation, a display should be immediately available to allow the operator to evaluate the performance of the system, e.g., information on the control input and output actuation signals and the resulting states of plant process components. Comparison of these states with expected states should also be made and deviations displayed in the abnormality indication portion of the HSI.				
			=>	4.1.3.1.2-9	To the extent possible, the functionality of the displays should be preserved at all power levels and plant operating modes.				
			=>	4.1.3.1.2-10	Higher-level overview display(s) should be available at the user workstations. If the control room layout will permit, the overview display(s) should also be located so that it can be seen from anywhere in the control room.				

		Guidelines	Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.3.1.2-11	Providing overviews not only supports monitoring but access to more detailed information as well (by means of navigation features to drill down to more detailed displays).				
=>	4.1.3.1.2-12	Displays at each level should alert users to important changes to the plant that may be indicated in higher- and lower-level displays. The method of alert should communicate to the user whether the change is at higher levels or lower levels and facilitate navigation to the appropriate display showing the applicable plant changes.				
=>	4.1.3.1.2-13	Displays in each level of the hierarchy should present information that effectively communicates the plant relationships at that level and which minimizes the need to access multiple displays.				
4.1.3.1.3		Navigation Within the Display Hierarchy				
=>	4.1.3.1.3-1	Each display should be clearly labeled as to its contents and its relationship in the hierarchy.				
=>	4.1.3.1.3-2	The system should provide on-screen navigational links to and from high-level and lower-levels of information with references and supporting information.				
=>	4.1.3.1.3-3	Navigation tools should provide for flexible approaches to searching for information.				
=>	4.1.3.1.3-4	The system should include a history function allowing users to keep track of the sequence of displays they have accessed to facilitate retracing their steps.				
=>	4.1.3.1.3-5	A list of all displays, e.g., on a menu, should be available to provide access to displays that do not have on-screen links.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.3.1.3-6	Visual search within each display should be supported by coding and other display features that enable users to easily see associated information in the display.				
=>	4.1.3.1.3-7	When conditions signal changes in display pages the user is not currently viewing that the user should attend to, special navigation aids should be presented to enable those displays to be easily retrieved. However, the displays should not be immediately displayed unless the user requests them.				
=>	4.1.3.1.3-8	To be effective, sufficient display area should be provided for users to display needed information in parallel and to minimize the need for navigation.				
4.1.3.2	Display Design for Task Performance					
4.1.3.2.1	Task Selection					
=>	4.1.3.2.1-1	Tasks requiring highly-reliable human performance should be considered for task-based display support. These tasks are mostly: • Important to nuclear or personnel safety • Important to maintaining power generation • Important to equipment protection for significant items • Time critical • Complex				
=>	4.1.3.2.1-2	Tasks that have high interface management and navigation demands (if performed without a specialized display) should be considered for task-based display support.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.3.2.1-3	Tasks for which improved efficiency is desired should be considered for task-based display support.				
	4.1.3.2.2	Task-Based Display Design				
=>	4.1.3.2.2-1	The task display requirements should be identified.				
=>	4.1.3.2.2-2	The system should provide notice of when the task is required.				
=>	4.1.3.2.2-3	The display should indicate the conditions that must be met before a task or step can be undertaken. Information about preconditions should be displayed so that users will be informed before starting the task or step.				
=>	4.1.3.2.2-4	Where the task is proceduralized, instructions and sequences should be provided for performing the task or step.				
=>	4.1.3.2.2-5	Specific plant information needed to perform the task should be displayed in the order and organization in which it is needed, to minimize interface management demands.				
=>	4.1.3.2.2-6	Cautions and warnings related to task performance should be displayed when the information is displayed to the user. Cautions or warnings should be distinctively presented, so that they are easily differentiated from each other and from other display elements.				
=>	4.1.3.2.2-7	Any alarms related to the task or step that may impact the user's ability to perform, or may alter the actions the user should take, should be presented in the task-based display.				

Guidelines						Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
			=>	4.1.3.2.2-8	If soft control capability is provided, controls needed to perform the task or step should be directly available in the display.				
			=>	4.1.3.2.2-9	When the task or steps requires operating systems/equipment/controls, then expected and actual feedback should be provided in the display.				
			=>	4.1.3.2.2-10	The task display should provide indication when a task or step can or should be terminated.				
			=>	4.1.3.2.2-11	The information presented in the task display should be conducive to efficient task execution.				
			=>	4.1.3.2.2-12	The task display should provide support for tracking task progress.				
			=>	4.1.3.2.2-13	The overall structure of the task elements (alarms, information, instructions, controls, etc.) reflecting the task requirements should be: • Sequentially structured when the task steps need to be completed in a specific order • Structured into groups of parallel information when no specific sequence is needed				
			=>	4.1.3.2.2-14	When a task requires more than one display, onscreen navigation aids should be provided to easily access the displays.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
4.1.3.3	Display Design for Teamwork, Crew Coordination, and Collaborative Work						
	=>	4.1.3.3-1	Displays should include functionality to support teamwork when the following conditions exist: • There is a high need for users to work together on the same task/problem (e.g., complex diagnoses of plant failures) • Face-to-face interaction/collaboration is difficult due to the arrangement of the workplace and the demands of concurrent tasks (e.g. multi-location coordinated activities)				
	=>	4.1.3.3-2	A common frame of reference for plant status should be provided.				
	=>	4.1.3.3-3	A user-addressable frame-of-reference should be provided if users have to collaborate to perform an activity.				
	=>	4.1.3.3-4	A CSCW display should support each crewmember's understanding of the others' activities. This can be accomplished by providing information for common team activities, such as in shift turnovers and for maintenance activities.				
	=>	4.1.3.3-5	Supervisor workstations should provide the capability to access the same displays as those at operator workstations.				
	=>	4.1.3.3-6	A coding scheme or designation system should be used to identify users when they manipulate information on a group-view display.				
	=>	4.1.3.3-7	When multiple users have to work together on the same task, displays should provide a collaborative workspace.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.3.3-8	The display should provide tools that enable users to interact with the HSI or the plant. Other users should be able to infer information about the nature of the task and the specific actions taken by observing the HSI.				
		=>	4.1.3.3-9	Display controls should prevent individuals from making changes to CSCW displays in ways that would reduce their usefulness to others.				
		=>	4.1.3.3-10	When multiple users have access to on-screen pointing devices (such as cursors) for interacting with the group-view display, features should be provided to manage access to the cursor and indicate current user.				
		=>	4.1.3.3-11	When transferring information between individual displays and the CSCW displays, the information should be presented promptly and with minimal delay.				
4.1.4	Display Pages							
	4.1.4.1	Identification of Information						
		=>	4.1.4.1-1	A title or header should be placed at the top of every display page, briefly describing the contents or purpose of the display.				
		=>	4.1.4.1-2	Every display page should have a unique identification to provide a reference for use in requesting the display of that page.				
		=>	4.1.4.1-3	Where displays have several levels of titles (and/or labels), the system should provide visual cues to aid users in distinguishing among the levels in the hierarchy.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.4.1-4	General labels and row/column labels should remain along the edges of the display.				
=>	4.1.4.1-5	When displays are partitioned into multiple pages, function/task-related data items should be displayed together on one page.				
=>	4.1.4.1-6	Users working with multipage displays should be provided with a page location reference within the display sequence.				
=>	4.1.4.1-7	Users viewing a portion of a larger display should be provided with an indication of the location of the visible position of a display (frame) in the overall display.				
4.1.4.2	Organization of Information					
=>	4.1.4.2-1	General HSI features (e.g., a data display zone, control zone, or message zone) should be displayed in consistent locations from one display to another.				
=>	4.1.4.2-2	The HSI functional zones and display features should be visually distinctive from one another, especially for on-screen command and control elements (which should be visibly distinct from all other screen structures).				
=>	4.1.4.2-3	Information on a display should be grouped according to principles obvious to the user, e.g., by task, system, function, or sequence, based upon the user’s requirements in performance of the ongoing task (see Table 4-1).				
=>	4.1.4.2-4	Information needed by the operator to accomplish a given task should be presented so that it is immediately seen to be related.				

		Guidelines	Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.4.2-5	A uniform nondistracting background color should be used with a hue/contrast that allows the data (foreground) to be easily visible and which does not distort or interfere with the coding aspects of the display.				
=>	4.1.4.2-6	When information is grouped on a display, the groups should be made visually distinct by such means as color blocking or padding or separation using blanks or demarcation lines.				
4.1.4.3		Clarity of Presentation				
=>	4.1.4.3-1	Displays should present, in an immediately usable form, only the data needed for the task they are designed to support; data irrelevant to the task should not be displayed, and extraneous and graphics should not be present.				
=>	4.1.4.3-2	Redundancy in the presentation of information items should be limited to cases where needed for backup or to avoid excessive movement.				
=>	4.1.4.3-3	Displays should be as uncluttered as possible.				
=>	4.1.4.3-4	Displayed information which temporarily overlays and obscures other display data should not erase the overlaid data.				
4.1.4.4		Coding and Highlighting of Information				
=>	4.1.4.4-1	Highlighting should be used sparingly.				
=>	4.1.4.4-2	The prominence of graphic features should reflect the importance of the information.				
=>	4.1.4.4-3	Coding and highlighting should not interfere with the readability of displayed information nor delay its presentation.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.4.4-4	Highlighting should be removed if it no longer has meaning.				
		=>	4.1.4.4-5	When highlighting is not sufficient to indicate the specific nature of some outstanding or discrepant feature that merits attention by a user, supplementary text should be displayed to make it clear.				
		=>	4.1.4.4-6	Coding of important information should incorporate redundancy.				
		=>	4.1.4.4-7	Coding should be provided when a user must distinguish rapidly among different categories of displayed data.				
		=>	4.1.4.4-8	Meaningful or familiar codes should be used, rather than arbitrary codes.				
		=>	4.1.4.4-9	Consistent meanings should be assigned to codes across user interfaces in the plant (including existing interfaces).				
		=>	4.1.4.4-10	A characteristic used for coding should have only one meaning.				
		=>	4.1.4.4-11	Highlighting should be clear and easily recognizable and should attract the users' attention.				
		=>	4.1.4.4-12	Inverse video should be used only to show the selection of on-screen items or to highlight small segments in a larger block of text.				
4.1.5	Display Formats							
	4.1.5.1	Continuous Text Displays						
		=>	4.1.5.1-1	A standard text display format should be used from one display to another.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.5.1-2	VDU displays of textual data, messages, or instructions should generally follow design conventions for printed text.				
		=>	4.1.5.1-3	Text to be displayed should be worded so that it is quickly and easily understood.				
		=>	4.1.5.1-4	When a user must read continuous text on line, at least four lines of text should be displayed at one time.				
		=>	4.1.5.1-5	Continuous text should be displayed in wide columns, containing at least 50 characters per line.				
		=>	4.1.5.1-6	In display of textual material, words should be kept intact, with minimal breaking by hyphenation between lines.				
		=>	4.1.5.1-7	Conventional punctuation should be used in textual display.				
		=>	4.1.5.1-8	Consistent spacing between the words of displayed text should be maintained, with left justification of lines and ragged right margins. A minimum of one character width (capital N for proportional spacing) should be used between words.				
		=>	4.1.5.1-9	A minimum of two stroke widths or 15 percent of character height, whichever is greater, should be used for spacing between lines of text.				
		=>	4.1.5.1-10	Displayed paragraphs of text should be separated by at least one blank line.				
		=>	4.1.5.1-11	When tables and/or graphics are combined with text, each figure should be placed near its first citation in the text, preferably in the same display frame.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.5.1-12	When a line is placed under an item to mark or emphasize it, the line should not impair the legibility of the item, e.g., by obscuring the descenders.				
=>	4.1.5.1-13	Within a text file or table, the use of a different font style should be preferred over the use of a different size for highlighting information.				
=>	4.1.5.1-14	When a special symbol, such as an asterisk, is used to draw attention to a selected item in alphanumeric displays, the symbol should be separated from the beginning of the word by a space.				
=>	4.1.5.1-15	When a user must read lengthy textual material, that text should be available in printed form.				
4.1.5.2	Tables and Lists					
=>	4.1.5.2-1	Information should be organized in some recognizable logical order to facilitate scanning and assimilation.				
=>	4.1.5.2-2	A table should be constructed so that row and column labels represent the information a user has prior to consulting the table.				
=>	4.1.5.2-3	Each row and column should be uniquely and informatively labeled and should be visually distinct from data entries.				
=>	4.1.5.2-4	Labels should include the unit of measure for the data in the table; units of measurement should be part of row or column labels.				
=>	4.1.5.2-5	Consistent column and row spacing should be maintained within a table, and from one table to another. Similarly, spacing between rows should be consistent within a table and between related tables.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.5.2-6	The spacing between columns should be greater than any internal spaces that might be displayed within a tabulated data item.				
		=>	4.1.5.2-7	In dense tables with many rows, a blank line, dots, or some other distinctive feature (to aid horizontal scanning) should be inserted after a group of rows at regular intervals.				
		=>	4.1.5.2-8	The font and size of alphanumeric characters should be consistent within a table and between related tables.				
		=>	4.1.5.2-9	Columns of alphabetic data should be displayed with left justification to permit rapid scanning.				
		=>	4.1.5.2-10	Columns of numeric data should be justified with respect to a fixed decimal point; if there is no decimal point, then numbers should be right justified.				
		=>	4.1.5.2-11	Arabic rather than Roman numerals should be used when listed items are numbered.				
		=>	4.1.5.2-12	Item numbers should begin with one rather than zero.				
		=>	4.1.5.2-13	When a list of numbered items exceeds one display page, the items should be numbered continuously in relation to the first item on the first page.				
		=>	4.1.5.2-14	Complete numbers should be displayed for hierarchic lists with compound numbers, i.e., repeated elements should not be omitted.				
		=>	4.1.5.2-15	Lists should be formatted so that each item starts on a new line.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.5.2-16	When a single item in a list continues for more than one line, items should be marked in some way so that the continuation of an item is obvious.				
=>	4.1.5.2-17	Where lists of items extend over more than one display page, the last line of one page should be the first line on the succeeding page.				
=>	4.1.5.2-18	For a long list, extending more than one displayed page, a hierarchic structure should be used to permit its logical partitioning into related shorter lists.				
=>	4.1.5.2-19	If a list is displayed in multiple columns, the items should be ordered vertically within each column rather than horizontally within rows and across columns.				
=>	4.1.5.2-20	When lists or tables are of variable length and may extend beyond the limits of one display page, the user should be informed when data are continued on another page and when data are concluded on the present page.				
4.1.5.3		Data Forms and Fields				
=>	4.1.5.3-1	Data fields to be compared on a character-by-character basis should be positioned one above the other.				
=>	4.1.5.3-2	The ordering and layout of corresponding data fields across displays should be consistent from one display to another.				
=>	4.1.5.3-3	The format of a VDU data form should be similar to that of commonly used hardcopy source documents.				
=>	4.1.5.3-4	When forms are used for data entry as well as for data display, the formats of these forms should be compatible.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.5.3-5	Clear visual definition of data fields should be provided so that the data are distinct from labels and other display features.				
		=>	4.1.5.3-6	The label and the data display area should be separated by at least one character space.				
		=>	4.1.5.3-7	At least three spaces should appear between the longest data field in one column and the rightmost label in an adjacent column.				
		=>	4.1.5.3-8	When label sizes are relatively equal, both labels and data fields should be left justified. One space should be left between the longest label and the data field column.				
		=>	4.1.5.3-9	When label sizes vary greatly, labels should be right justified and the data fields should be left justified. One space should be left between each label and the data field.				
		=>	4.1.5.3-10	If appropriate, labels should be used to help the user interpret the data displayed in a field.				
		=>	4.1.5.3-11	A field group heading should be centered above the labels to which it applies.				
		=>	4.1.5.3-12	At least five spaces should appear between groups of data fields.				
		=>	4.1.5.3-13	When headings are located on the line above related screen fields, the labels should be indented a minimum of five spaces from the start of the heading.				
		=>	4.1.5.3-14	When headings are placed adjacent to the related fields, they should be located to the left of the topmost row of related fields. The column of labels should be separated from the longest heading by a minimum of three blank spaces.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.5.3-15	A data form should have a logical organization.				
=>	4.1.5.3-16	The number of pages in a data form required to complete an activity should be minimized to reduce the amount of navigation.				
4.1.5.4	Numeric Readouts					
4.1.5.5	Bar Charts and Histograms					
=>	4.1.5.5-1	Each bar on the display should have a unique identification label.				
=>	4.1.5.5-2	When bars are displayed in groups, they should be labeled as a unit, with individual distinguishing labels for each bar.				
=>	4.1.5.5-3	When data must be compared, bars should be adjacent to one another and spaced such that a direct visual comparison can be made without eye movement.				
=>	4.1.5.5-4	In a related series of bar charts, a consistent orientation of the bars (vertical or horizontal) should be adopted.				
=>	4.1.5.5-5	If one bar represents data of particular significance, then that bar should be highlighted.				
=>	4.1.5.5-6	The zero reference should be the center of the deviation bar chart.				
=>	4.1.5.5-7	On a deviation bar chart, the range of normal conditions for positive or negative deviations should represent no more than 10 percent of the total range.				
=>	4.1.5.5-8	The magnitude of each variable should be displayed when a deviation bar display is used as a main display format for safety function parameters.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.5.5-9	Segmented bars, in which differently coded segments are shown cumulatively within a bar, should be used when both the total measures and the portions represented by the segments are of interest.				
=>	4.1.5.5-10	The data categories should be ordered within each segmented bar in the same sequence, with the least variable categories displayed at the bottom and the most variable at the top.				
4.1.5.6	Graphs					
=>	4.1.5.6-1	Graphs should convey enough information to allow the user to interpret the data without referring to additional sources.				
=>	4.1.5.6-2	When multiple curves are included in a single graph, each curve should be identified directly by an adjacent label, rather than by a separate legend.				
=>	4.1.5.6-3	If a legend must be displayed, the codes in the legend should be ordered to match the expected or typical spatial order of their corresponding curves in the graph itself.				
=>	4.1.5.6-4	Coding should be used when multiple variables are displayed in a single graph.				
=>	4.1.5.6-5	Line coding should be used consistently across graphs.				
=>	4.1.5.6-6	In displays of multiple curves, if one curve represents data of particular significance, then that curve should be highlighted (see Section 4.1.4.4).				
=>	4.1.5.6-7	Trend displays should be capable of showing data collected during time intervals of different lengths.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.5.6-8	When the user must compare trend data represented by separate curves, the curves should be displayed in one combined graph.				
		=>	4.1.5.6-9	If operators must read exact parameter values from displayed curves, features should be provided to support this.				
		=>	4.1.5.6-10	Curves representing planned, projected, or extrapolated trend data should be distinctive from curves representing actual data.				
		=>	4.1.5.6-11	Combining several individual curves into a single average curve should only be done when users do not need to know the pattern of individual curves or when curves differ on the basis of minor irregularities.				
		=>	4.1.5.6-12	Where curves represent cyclic data, the scale should be selected so that at least one complete cycle is shown.				
		=>	4.1.5.6-13	The target area, preferred combination of X- and Y-axis values, should be graphically defined.				
		=>	4.1.5.6-14	Old data points should be removed after some fixed period of time to prevent clutter.				
		=>	4.1.5.6-15	A linear profile chart should form recognizable geometric patterns for specific abnormal conditions.				
		=>	4.1.5.6-16	The area below the profile line should be shaded to provide a more distinguishable profile.				
		=>	4.1.5.6-17	Labels should be provided along the bottom of a linear profile chart to identify each parameter.				
		=>	4.1.5.6-18	All segments in a segmented curve graph should be related to the total value.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
	=>	4.1.5.6-19	The data categories in a segmented curve graph should be ordered so that the least variable curves are displayed at the bottom and the most variable at the top.				
	=>	4.1.5.6-20	The different bands of segmented curve graphs should be made visually distinctive by coding, such as by the texturing or shading of bands (see Patterns).				
	=>	4.1.5.6-21	Where space permits, the different bands of segmented curve graphs should be labeled directly within the textured or shaded bands.				
	=>	4.1.5.6-22	If some plotted points represent data of particular significance, they should be highlighted to make them visually distinctive from others.				
	=>	4.1.5.6-23	When relations among several variables must be examined in scatterplots, an ordered group (matrix) of plots should be displayed, each showing the relation between just two variables.				
	=>	4.1.5.6-24	When scatterplots are grouped in a single display to show relations among several variables, an interactive aid should be provided for analysis so that if a user selects a set of data in one plot then the corresponding data points in other plots will be highlighted.				
4.1.5.7	Pie Charts						
	=>	4.1.5.7-1	There should be no more than five partitions in a pie chart.				
	=>	4.1.5.7-2	Pie chart segments should be labeled directly rather than by a separate legend. If a segment is too small to contain the label, the label should be placed outside the segment with a line from it to the segment.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
	=>	4.1.5.7-3	If the task requires precise values, numbers should be added to pie chart segment labels to indicate the percentage and/or absolute values.				
	=>	4.1.5.7-4	If a particular segment of a pie chart requires emphasis, it should be highlighted by special hatching or displaced slightly from the remainder of the pie.				
4.1.5.8	Flowcharts						
	=>	4.1.5.8-1	The available decision options should be displayed in logical order.				
	=>	4.1.5.8-2	Only a single decision should be required at each step.				
	=>	4.1.5.8-3	When a flowchart is designed so that a user must make decisions at various steps, the available options should be displayed in some consistent order from step to step.				
	=>	4.1.5.8-4	While flowcharts should display only the data immediately required by the user, more detailed data should be available by means of a simple action.				
	=>	4.1.5.8-5	Flowcharts should be designed so that the path of the logical sequence is consistent with familiar orientation conventions.				
	=>	4.1.5.8-6	There should be a standard set of flowchart symbols.				
4.1.5.9	Mimics and Diagrams						
	=>	4.1.5.9-1	Mimics and diagrams should contain the minimum amount of detail needed for the task they were designed to support.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.5.9-2	Plant components represented on mimic lines should be identified.				
=>	4.1.5.9-3	Indications of the actual status of plant systems and equipment, as opposed to demand status, should be provided when required by the task.				
=>	4.1.5.9-4	All flow path line origin points should be labeled or begin at labeled components.				
=>	4.1.5.9-5	All flow path line destination or terminal points should be labeled or end at labeled components.				
=>	4.1.5.9-6	Flow directions should be clearly indicated by distinctive arrowheads.				
=>	4.1.5.9-7	Flow paths should be coded (e.g., by color and/or width) to indicate important information (see Color).				
=>	4.1.5.9-8	Overlapping of flow path lines should be avoided.				
=>	4.1.5.9-9	Where symbols are used to represent equipment components and process flow or signal paths, numerical data should be presented reflecting inputs and outputs associated with equipment.				
=>	4.1.5.9-10	When a graphic display contains some outstanding or discrepant feature that merits attention by a user, supplementary text should be displayed to emphasize that feature.				
=>	4.1.5.9-11	When users must evaluate information in detail, computer aids for calculation and visual analysis should be provided.				
4.1.5.10	Maps					

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.5.10-1	Significant features of a map should be labeled directly on the display unless cluttering or obscuring of other information would result.				
		=>	4.1.5.10-2	When several different maps will be displayed, a consistent orientation should be used so that the top of each map will always represent the same direction.				
		=>	4.1.5.10-3	The user should be able to select different map orientations and reference points.				
		=>	4.1.5.10-4	If the map orientation can be changed, the map labels and symbols should remain oriented to the user's position.				
		=>	4.1.5.10-5	When a map exceeds the capacity of a single display frame, users should be able to change the display in order to show different areas of current interest.				
		=>	4.1.5.10-6	Codes, such as texture patterns, color, or tonal variations, should be used when different areas of a map must be defined, or when geographic distribution of a particular variable must be indicated.				
		=>	4.1.5.10-7	Tonal codes (different shades of one color) rather than spectral codes (different colors) should be used when users must make relative judgments for different colored areas of a display.				
		=>	4.1.5.10-8	Where different areas of a map are coded by texture patterns or tonal variation, the darkest or lightest shades correspond to the extreme values of the coded variable.				
		=>	4.1.5.10-9	In applications where the geographic distribution of nongeographic data must be displayed, other graphic elements should be added to a map for that purpose.				

				Guidelines	Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.5.10-10	When changes in mapped data are significant for a user's task, auxiliary graphic elements should be included to highlight those changes.				
		=>	4.1.5.10-11	When the use of mapped data may be complex, computer aids should be provided for data analysis.				
		=>	4.1.5.10-12	The user should be able to rapidly remove non-critical information from a map or map overlay display.				
	4.1.5.11			Integral and Configural Displays				
		=>	4.1.5.11-1	Integral displays should be used to communicate high-level, status-at-a-glance information where users may not need information on individual parameters to interpret the display.				
		=>	4.1.5.11-2	Configural displays should be used when users must rapidly transition between high-level functional information and specific parameter values.				
		=>	4.1.5.11-3	The methods by which lower-level data are analyzed to produce higher-level information and graphical elements should be understandable to users.				
		=>	4.1.5.11-4	Users should have access to the rules or computations that link process parameters and graphical features, and to an explanation of how the information system produces higher-level information.				
		=>	4.1.5.11-5	A perceptually distinct reference aid should be provided in an object display to support users in recognizing abnormalities in the object's characteristics.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.5.11-6	The display elements should be organized so that the emergent features that arise from their interaction correspond to meaningful information about the process or system, e.g., when the aspect of the system represented by the emergent is disturbed, the disturbance is visible in the emergent feature.				
=>	4.1.5.11-7	The emergent features or patterns within the display should be nested (from global to local) in a way that reflects the hierarchical structure of the process.				
=>	4.1.5.11-8	Each emergent feature should be clearly distinguishable from other emergent features and from information on individual parameters.				
=>	4.1.5.11-9	Each relevant process parameter should be represented by a perceptually distinct element within the display.				
=>	4.1.5.11-10	The display should support the user in performing tasks requiring lower-level information.				
=>	4.1.5.11-11	The emergent features and their interactions should not be so complex as to be susceptible to misinterpretation.				
4.1.5.12	Graphic Instrument Panels					
=>	4.1.5.12-1	Zones indicating operating ranges should be color coded by edge lines or wedges for circular scales.				
=>	4.1.5.12-2	When check-reading positive and negative values on rotary meters (circular displays), the zero or null position should be at 12 o’clock or 9 o’clock.				
=>	4.1.5.12-3	The pointer on fixed scales should extend from the right of vertical scales and from the bottom of horizontal scales.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
	=>	4.1.5.12-4	The pointer on fixed scales should extend to but not obscure the shortest graduation marks.				
	=>	4.1.5.12-5	Tick marks should be separated by at least 0.07 inches (1.75 millimeters) for a viewing distance of 28 inches (71 centimeters) under low illumination.				
	=>	4.1.5.12-6	Scales should not be cluttered with more marks than necessary for the precision needed the tasks for which the scale is used.				
4.1.5.13	Speech Displays						
	=>	4.1.5.13-1	Speech should be limited to provide only a few messages.				
	=>	4.1.5.13-2	The user should be able to have speech messages repeated.				
	=>	4.1.5.13-3	Messages should be short and simple.				
	=>	4.1.5.13-4	A distinctive and mature voice should be used.				
	=>	4.1.5.13-5	Spoken messages should be presented in a formal, impersonal manner.				
	=>	4.1.5.13-6	Words in a speech message should be concise, intelligible, and appropriate for the information presented.				
	=>	4.1.5.13-7	A speech message priority system should be established such that more critical messages override the presentation of messages having lower priority.				
	=>	4.1.5.13-8	If speech is used to provide warnings as well as other forms of user guidance, spoken warnings should be easily distinguishable from routine messages.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.5.13-9	Speech signal intensity should be clearly audible for the expected ambient noise environment.				
4.1.6	Display Elements							
	4.1.6.1	Alphanumeric Characters						
		=>	4.1.6.1-1	Text to be read (except labels) should be presented using upper and lower case characters.				
		=>	4.1.6.1-2	A clearly legible font should be utilized. Fonts should have true ascenders and descenders, uniform stroke width, and uniform aspect ratio.				
		=>	4.1.6.1-3	For a given font, it should be possible to clearly distinguish between the following characters: X and K, T and Y, I and L, I and 1, O and Q, O and 0, S and 5, and U and V.				
		=>	4.1.6.1-4	The height of characters in displayed text or labels should be at least 16 minutes of arc (4.7 mrad) and the maximum character height should be 24 minutes of arc (7 mrad).				
		=>	4.1.6.1-5	For fixed (as opposed to proportionally spaced) presentations, the height-to-width ratio should be between 1:0.7 to 1:0.9.				
		=>	4.1.6.1-6	A 4x5 (width-to-height) character matrix should be the minimum matrix used for superscripts and for numerators and denominators of fractions that are to be displayed in a single character position.				
		=>	4.1.6.1-7	Horizontal separation between characters or symbols should be between 10 and 65 percent of character or symbol height.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
4.1.6.2	Abbreviations and Acronyms					
=>	4.1.6.2-1	Abbreviations should be avoided (except when terms are commonly referred to by their initialisms, e.g., SPDS).				
=>	4.1.6.2-2	When defining abbreviations that are not common to the user population, a simple rule should be used that users understand and recognize.				
=>	4.1.6.2-3	Abbreviations should be distinctive so that abbreviations for different words are distinguishable.				
=>	4.1.6.2-4	Abbreviations and acronyms should not include punctuation.				
=>	4.1.6.2-5	When arbitrary codes must be remembered by the user, characters should be grouped in blocks of three to five characters, separated by a minimum of one blank space or other separating character such as a hyphen or slash.				
=>	4.1.6.2-6	The use of the letters O and I in a non-meaningful code should be avoided since they are easily confused with the numbers 0 (zero) and 1 (one), respectively.				
=>	4.1.6.2-7	When codes combine letters and numbers, letters should be grouped together and numbers grouped together rather than interspersing letters with numbers.				
4.1.6.3	Numeric Data					
=>	4.1.6.3-1	Numeric values should ordinarily be displayed in the decimal number system.				
=>	4.1.6.3-2	Leading zeros in numeric entries for whole numbers should be suppressed.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
	=>	4.1.6.3-3	A number should be displayed at the number of significant digits required by users to perform their tasks; displays should not imply precision beyond the capabilities of the underlying sensors.				
	=>	4.1.6.3-4	Numeric displays should accommodate the variable's full range.				
	=>	4.1.6.3-5	Numeric displays should change slowly enough to be readable.				
	=>	4.1.6.3-6	If users must rapidly discern directional change, numeric displays should be provided with arrows to indicate the direction of change.				
	=>	4.1.6.3-7	If users must evaluate the difference between two sets of data, the difference should be presented on the display.				
	=>	4.1.6.3-8	All numbers should be oriented upright.				
	=>	4.1.6.3-9	If more than four digits are required, they should be grouped and the groupings separated as appropriate by commas, by a decimal point, or by additional space.				
4.1.6.4	Icons and Symbols						
	=>	4.1.6.4-1	Symbols and icons should be simple and immediately recognizable.				
	=>	4.1.6.4-2	The meanings of icons and symbols should be obvious.				
	=>	4.1.6.4-3	Icons and symbols used in interfaces should conform to existing conventions and users' expectations.				
	=>	4.1.6.4-4	The use and meanings of symbols should be consistent throughout the plant as well as within a given interface.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.6.4-5	Icons or symbols that can be interacted with (e.g., that cause an action when clicked) should be readily distinguishable from those the have no such function.				
		=>	4.1.6.4-6	Changes in the ‘look’ of icons or symbols that are intended to convey the state of equipment or status of control systems should be conspicuous.				
		=>	4.1.6.4-7	The layout and arrangement of groups of symbols should follow a consistent and defined logic.				
		=>	4.1.6.4-8	The primary use of icons in graphic displays should be to represent actual objects or actions.				
		=>	4.1.6.4-9	Icons should be designed to look like the objects, processes, or operations they represent, by use of literal, functional, or operational representations.				
		=>	4.1.6.4-10	Each icon and symbol should represent a single object or action, and should be easily discriminable from all other icons and symbols.				
		=>	4.1.6.4-11	Special symbols to signal critical conditions should be used exclusively for that purpose.				
		=>	4.1.6.4-12	Words and symbols should not be used alternately.				
		=>	4.1.6.4-13	Icons and symbols should be large enough for the user to perceive the representation and discriminate it from other icons and symbols.				
		=>	4.1.6.4-14	An icon or symbol should be highlighted when the user has selected it.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.6.4-15	Icons that may not be immediately and unambiguously recognized should be accompanied by a text label.				
=>	4.1.6.4-16	If icons are used to represent control action options, a label indicating the action should be associated with the icon.				
4.1.6.5	Labels					
4.1.6.5.1	Labeling Principles					
=>	4.1.6.5.1-1	Controls, indicators, and other individual display elements that must be located, identified, or manipulated, should contain appropriate, distinct, unique, and descriptive labels.				
=>	4.1.6.5.1-2	A hierarchical labeling scheme should be used to reduce confusion and search time.				
=>	4.1.6.5.1-3	Major labels should be used to identify major systems, subordinate labels should be used to identify subsystems or functional groups, and component labels should be used to identify each display element.				
=>	4.1.6.5.1-4	Labels should be consistent within and across panels in their use of words, acronyms, abbreviations, and part/system numbers.				
=>	4.1.6.5.1-5	All discrete functional control positions (for example, “ON” and “OFF” positions of a particular controller) should be labeled.				
4.1.6.5.2	Label Location					

Guidelines						Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
			=>	4.1.6.5.2-1	Control and indicator labels should be located consistently, either below or above the display element, especially on the same display.				
			=>	4.1.6.5.2-2	Avoid placing adjacent labels together. Labels should be separated one from another by at least two standard character spaces.				
			=>	4.1.6.5.2-3	The labels used to identify a group of controls and or indicators corresponding to major systems or functional groups (subsystems) should be located above that group.				
			=>	4.1.6.5.2-4	Curved patterns should not be used for labeling.				
			=>	4.1.6.5.2-5	Labels should not detract from or obscure any other information displayed on the screen that must be read by the user.				
			=>	4.1.6.5.2-6	Labels should not be obscured by other information displayed on the screen.				
			=>	4.1.6.5.2-7	The label for a specific graphical object (i.e., an icon) should be placed in close proximity to the object.				
			=>	4.1.6.5.2-8	Labels may be placed directly on certain types of components (e.g., pushbuttons) for the purpose of increasing the utility and efficiency of control identification.				
			=>	4.1.6.5.2-9	Control position information should be visible to the user before, during, and after operation of the control.				
			=>	4.1.6.5.2-10	The user should not be allowed to move or hide labels for any visual display components, excepting graph legends.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
4.1.6.5.3	Label Content						
	=>	4.1.6.5.3-1	Use common terms that originate form typical language usage and/or from standard terminology for nuclear power plants.				
	=>	4.1.6.5.3-2	Trade names and other irrelevant information should not appear on labels.				
	=>	4.1.6.5.3-3	Use whole words rather than abbreviations whenever space permits.				
	=>	4.1.6.5.3-4	Use standard abbreviations as created and used at the plant.				
	=>	4.1.6.5.3-5	Use standard acronyms if they have been well established.				
	=>	4.1.6.5.3-6	Avoid the use of words that may be interpreted as both a noun or adjective and as a verb (e.g., “OPEN” in the case of “OPEN VALVE”).				
	=>	4.1.6.5.3-7	Words and abbreviations of similar appearance should be avoided where an error in interpretation could occur.				
	=>	4.1.6.5.3-8	When special precautionary words are required, select ones that provide an appropriate sense of urgency, hazard, or danger.				
	=>	4.1.6.5.3-9	All danger, warning, and safety instruction labels should be designed in accordance with appropriate safety standards.				
	=>	4.1.6.5.3-10	The label should briefly and simply express the intended action of controls or the meaning of the given indication.				

		Guidelines		Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
	=>	4.1.6.5.3-11	Nomenclature printed on labels should be consistent with that used in procedures.				
	=>	4.1.6.5.3-12	When presenting a list of options, labels should reflect the question or decision being posed to the user.				
4.1.6.5.4		Label Lettering					
	=>	4.1.6.5.4-1	Labels should be uniquely and consistently highlighted, boxed, or otherwise emphasized to differentiate them from other screen structures and data.				
	=>	4.1.6.5.4-2	Always use capital letters for labels and not a mix of capital and lowercase letters.				
	=>	4.1.6.5.4-3	The lettering for all labels should be oriented so that they read from left to right, not around corners, on their side, or up and down.				
	=>	4.1.6.5.4-4	Labels should be graduated in size such that the labels used for the group on the higher hierarchy level are about 25 percent larger than the labels used for the group on the preceding level of hierarchy.				
	=>	4.1.6.5.4-5	Absolute label size should be determined starting with the smallest lettering size that will be compatible with the display resolution and the typical average viewing distance.				
	=>	4.1.6.5.4-6	Lettering and background colors should provide high contrast and legibility.				
	=>	4.1.6.5.4-7	Ensure that all numbers and characters are clearly distinguishable.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
4.1.6.6			Scales, Axes, and Grids				
	=>	4.1.6.6-1	Numbers on a scale should increase clockwise, left to right, or bottom to top.				
	=>	4.1.6.6-2	Nine should be the maximum number of tick marks between numbers.				
	=>	4.1.6.6-3	Scales should have tick marks at a standard interval of 1, 2, 5, or 10 (or multiples of 10) for labeled divisions; intervening tick marks to aid visual interpolation should be consistent with the labeled scale interval.				
	=>	4.1.6.6-4	For one-revolution circular scales, zero should be at 7 o'clock and the maximum value should be at 5 o'clock.				
	=>	4.1.6.6-5	Axes should be clearly labeled with a description of what parameter is represented by the axis.				
	=>	4.1.6.6-6	The units of measurement represented by the scale should be included in the axis label.				
	=>	4.1.6.6-7	Conventional scaling practice should be followed, in which the horizontal X-axis is used to plot time or the postulated cause of an event, and the vertical Y-axis is used to plot the effect.				
	=>	4.1.6.6-8	If users must compare graphic data across a series of displays, the same scale should be used for each.				
	=>	4.1.6.6-9	The scales should be consistent with the intended functional use of the data.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.6.6-10	A linear scale should be used for displayed data, in preference to logarithmic or other non-linear methods of scaling, unless it can be demonstrated that non-linear scaling will facilitate user interpretation of the information.				
		=>	4.1.6.6-11	When users must compare aggregate quantities within a display, or within a series of displays, scaling of numeric data should begin with zero.				
		=>	4.1.6.6-12	When graphed data represent positive numbers, the graph should be displayed with the origin at the lower left, such that values on an axis increase as they move away from the origin of the graph.				
		=>	4.1.6.6-13	Only a single scale should be shown on each axis, rather than including different scales for different curves in the graph.				
		=>	4.1.6.6-14	If different variables on a single graph require different scales, they should be scaled against a common baseline index, rather than showing multiple scales.				
		=>	4.1.6.6-15	When a graphic display has been expanded from its normal coverage, some scale indicator of the expansion factor should be provided.				
		=>	4.1.6.6-16	Users should be able to manually change the scale to maintain an undistorted display under different operating conditions.				
		=>	4.1.6.6-17	If the system is designed to automatically change scale, an alert should be given to the user that the change is being made.				
		=>	4.1.6.6-18	If interpolation must be made or where accuracy of reading graphic data is required, computer aids should be provided for exact interpolation.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
=>	4.1.6.6-19	When grid lines are displayed, they should be unobtrusive and not obscure data elements (e.g., curves and plotted points).				
=>	4.1.6.6-20	Graphs should be constructed so that the numbered grids are bolder than unnumbered grids.				
=>	4.1.6.6-21	When data comparisons of interest fall within a limited range, the scaled axis should emphasize that range, with a break in the displayed axis to indicate discontinuity with the scale origin.				
=>	4.1.6.6-22	When scaled data will contain extreme values, duplicate axes should be displayed, so that the X-axis appears at both the top and bottom, and the Y-axis at both the left and right sides of the graph.				
=>	4.1.6.6-23	Unless required, use of three-dimensional scales (i.e., where a Z-axis is added to the display) should be avoided.				
4.1.6.7	Borders, Lines, and Arrows					
=>	4.1.6.7-1	Meaningful differences between lines appearing in graphic displays, such as flow paths, should be depicted by using various line types, e.g., solid, dashed, dotted, and widths.				
=>	4.1.6.7-2	In flow charts and other graphics displays, arrowheads should be used in a conventional fashion to indicate directional relations in the sequential links between various elements.				
=>	4.1.6.7-3	Unnecessary borders should not be used in the display.				
=>	4.1.6.7-4	A border should be used to improve the readability of a single block of numbers or letters.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
	=>	4.1.6.7-5	If several labels or messages are clustered in the same area, distinctive borders should be placed around the critical ones only.				
4.1.6.8			Visual Characteristics				
	4.1.6.8.1		Color				
	=>	4.1.6.8.1-1	Color use and the meanings attached to colors should be consistent throughout the plant as well as within a specific upgrade project.				
	=>	4.1.6.8.1-2	Color should be utilized as part of the overall labeling and demarcation strategy.				
	=>	4.1.6.8.1-3	Color should be used as part of the overall strategy to emphasize particular items of information.				
	=>	4.1.6.8.1-4	Colors should be considered for use as part of the overall strategy to identify the status of components or systems.				
	=>	4.1.6.8.1-5	Color should be considered for use as part of the overall strategy to convey the magnitude of measured quantities.				
	=>	4.1.6.8.1-6	The number of colors should be limited to those that can be easily distinguished.				
	=>	4.1.6.8.1-7	Colors should have adequate contrast and luminance with respect to the surroundings.				
	=>	4.1.6.8.1-8	The uses of color as a coding should normally be backed up with another coding method.				
	=>	4.1.6.8.1-9	When a user must distinguish rapidly among several discrete categories of data, a unique color should be used to display the data in each category.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
	=>	4.1.6.8.1-10	When color coding is used, each color should represent only one category of displayed data.				
	=>	4.1.6.8.1-11	Color coding should not create unplanned or obvious new patterns on the screen.				
	=>	4.1.6.8.1-12	Colors and color combinations that may cause problems owing to the workings of color vision should be avoided.				
4.1.6.8.2	Size						
	=>	4.1.6.8.2-1	Use of size coding should be limited to avoid crowded displays.				
	=>	4.1.6.8.2-2	No more than three size levels should be used to represent for discrete information.				
	=>	4.1.6.8.2-3	Each discrete size should be between 50% and 100% larger than the smaller size.				
	=>	4.1.6.8.2-4	Image proportions should be maintained when varying an image’s size.				
	=>	4.1.6.8.2-5	If size is used to convey quantitative information, the area should vary in proportion to the measurement.				
4.1.6.8.3	Shape						
	=>	4.1.6.8.3-1	Shape coding should be used to represent discrete, nominal information, as opposed to relative values.				
	=>	4.1.6.8.3-2	No more than 15 distinct and clearly identifiable shapes should be used.				
4.1.6.8.4	Pattern						

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
	=>	4.1.6.8.4-1	Pattern codes should be simple.				
	=>	4.1.6.8.4-2	When using pattern density to convey quantity, the least dense pattern should represent the lower extreme, and the densest pattern should represent the higher extreme.				
4.1.6.8.5	Brightness						
	=>	4.1.6.8.5-1	No more than two levels of brightness coding should be used on VDUs.				
	=>	4.1.6.8.5-2	Higher brightness levels should signify more importance and higher priority.				
4.1.6.8.6	Flashing						
	=>	4.1.6.8.6-1	Flash coding should be used very sparingly.				
	=>	4.1.6.8.6-2	Flash coding should not be used on text or detailed data that must be read.				
	=>	4.1.6.8.6-3	Only small area of the screen should flash at any time.				
	=>	4.1.6.8.6-4	No more than two flash rates should be used to ensure that the rates are clearly distinguishable.				
	=>	4.1.6.8.6-5	Faster flashing rates should correspond to more critical information.				
	=>	4.1.6.8.6-6	Some method of flash suppression or acknowledgement should be provided.				
	=>	4.1.6.8.6-7	Flashing should not be used with long-persistence phosphor displays.				

Guidelines			Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
4.1.6.9		Auditory Coding				
=>	4.1.6.9-1	Auditory signals should be provided to alert the user to situations that require attention, such as an incorrect input action or a failure of the HSI to process an input from the user.				
=>	4.1.6.9-2	Systems used to transmit non-verbal auditory signals should be used only for that purpose.				
=>	4.1.6.9-3	Auditory signals should provide localization cues that direct users to those control room workstations where attention is required.				
=>	4.1.6.9-4	Auditory signals should be selected to avoid interference with other auditory sources, including verbal communication.				
=>	4.1.6.9-5	Advisory or caution signals should be readily distinguishable from warning signals and used to indicate conditions requiring awareness, but not necessarily immediate action.				
=>	4.1.6.9-6	Auditory alerts, as well as caution and warning sounds, should accompany visual displays.				
=>	4.1.6.9-7	Once a particular auditory signal code is established for a given operating situation, the same signal should not be designated for some other display.				
=>	4.1.6.9-8	If the audio signal varies on one dimension only (such as frequency), the number of signals to be identified should not exceed four.				
=>	4.1.6.9-9	One audio signal may be used in conjunction with several visual displays, provided that immediate discrimination is not critical to personnel safety or system performance.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.6.9-10	Audio warning signals that might be confused with routine signals or with other sounds in the operating environment should not be used.				
		=>	4.1.6.9-11	The intensity, duration, and source location of the signal should be compatible with the acoustical environment of the intended receiver as well as with the requirements of other personnel in the signal area.				
		=>	4.1.6.9-12	Noncritical auditory signals should be capable of being turned off at the discretion of the user.				
		=>	4.1.6.9-13	When the signal must indicate which user (of a group of users) is to respond, a simple repetition code should be used.				
		=>	4.1.6.9-14	Sound sources (speakers or buzzers) should direct sound toward the center of the main operating area.				
		=>	4.1.6.9-15	When an audio signal must bend around major obstacles or pass through partitions, its frequency should be less than 500 Hz.				
		=>	4.1.6.9-16	Auditory alert and warning signals should be audible in all parts of the control room.				
		=>	4.1.6.9-17	The intensity of auditory signals should be set to unmistakably alert and get a user’s attention.				
		=>	4.1.6.9-18	When an audio signal must travel over 1000 feet, its frequency should be less than 1000 Hz.				
		=>	4.1.6.9-19	When the noise environment is unknown or expected to be difficult to penetrate, audio signals should have a shifting frequency that passes through the entire noise spectrum and/or be combined with a visual signal.				

Guidelines					Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
		=>	4.1.6.9-20	Audio warning signals should not interfere with any other critical functions or warning signals, or mask any other critical audio signals.				
		=>	4.1.6.9-21	The audio display device and circuit should be designed to preclude warning signal failure in the event of system or equipment failure and vice versa.				
		=>	4.1.6.9-22	Auditory alarm systems should be designed so that false alarms are avoided.				
		=>	4.1.6.9-23	Coding methods should be distinct and unambiguous, and should not conflict with other auditory signals.				
		=>	4.1.6.9-24	Similar auditory signals must not be contradictory in meaning with one another.				
		=>	4.1.6.9-25	Auditory signals may be pulse coded by repetition rate. Repetition rates should be sufficiently separated to ensure discrimination.				
		=>	4.1.6.9-26	If modulation of the frequency (Hz) of a signal denotes information, center frequencies should be between 500 and 1000 Hz.				
		=>	4.1.6.9-27	If discrete-frequency codes are used for audible signal coding, frequencies should be broad band and widely spaced within the 200 to 5000 Hz range (preferably between 500 and 3000 Hz).				
		=>	4.1.6.9-28	Using the intensity of a sound to convey information is not recommended.				
		=>	4.1.6.9-29	It should be possible to test the auditory signal system.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
4.1.7	Data Quality and Data Uprate						
	=>	4.1.7-1	The maximum update rate should be determined by the time required for the user to identify and process the changed feature of the display.				
	=>	4.1.7-2	The user should be capable of controlling the rate of information update on the display, but the allowable rate should not exceed that capable of being met by the information source and the processing equipment.				
	=>	4.1.7-3	Changing alphanumeric values that the user must reliably read should not be updated more often than once per second.				
	=>	4.1.7-4	When the computer generates a display to update changed data, the old items should be erased before adding new data items to the display.				
	=>	4.1.7-5	Items on a graphic display should not move faster than 60 degrees of visual angle per second, with 20 degrees per second preferred.				
	=>	4.1.7-6	The timeliness of displayed data should be such that, for the purposes of their tasks, users can consider it to represent current conditions at the time it is viewed.				
	=>	4.1.7-7	Data values displayed in any part of the workspace should be able to be considered, for purposes of users' tasks, consistent in time with all other displayed data.				
	=>	4.1.7-8	Each variable should be displayed with an accuracy sufficient for the users to perform their tasks.				
	=>	4.1.7-9	Variables that are subject to validation (e.g., checks for accuracy) should be identified and an indication should be provided when these data are invalid.				

Guidelines				Complies	Does Not Comply, but with Justification	Does Not Comply, but without Justification	Not Applicable
	=>	4.1.7-10	When checks for accuracy could not be performed, the unvalidated status of the data should be clearly indicated.				
	=>	4.1.7-11	Data entered by personnel should be identified such that it is easily distinguished from validated data.				
	=>	4.1.7-12	Analytical redundancy should be considered to help ensure the appropriateness of displayed values.				
	=>	4.1.7-13	A display feature should be provided to indicate to the user that the system is operating properly (or that a system failure has occurred).				
	=>	4.1.7-14	Information system failures (due to sensors, instruments, and components) should result in distinct display changes that directly indicate that depicted plant conditions are invalid.				
	=>	4.1.7-15	When task performance requires or implies the need to assess currency of information within a display, the information should be annotated with time information.				
	=>	4.1.7-16	When task requirements dictate that current information changes be continuously viewed and the display is changing so rapidly that the information is difficult to read, the user should have the capability of simultaneously viewing the information in a supplemental ‘snapshot’ display (i.e., a display frozen to enhance readability) along with the continuous display.				
	=>	4.1.7-17	If a display has a freeze capability, the display should have an obvious reminder that it is in the freeze mode.				

4.1.3 Display Functions

In the introduction to Section 4, some of the characteristics of computer-based HSIs that can be used to improve upon conventional HSIs, such as HSI integration and data processing, were discussed. Perhaps nowhere is this potential clearer than when one considers display functions, i.e., the purposes that displays can serve.

Plant personnel work individually and as teams. They engage in several cognitive activities that are all part of decision making and that form a basis for performing all of their functions and tasks. While it is possible to discuss general cognitive functions in different ways, we use a simple breakdown into: (1) monitoring and detection of disturbances, (2) situation assessment, (3) response planning, and (4) response execution.

In older plants employing predominantly analog HSIs, the cognitive activities listed above are not very well supported by the variety of control room resources available. The HSIs simply provide data. The interpretation of data needed to make decisions and the decision-making process itself resides in the memory and reasoning capability of the end-user. This is supported by paper procedures. However, in a computerized control room, most of these activities may be better supported through the use of computer displays. In addition, some activities can be provided with greater support. This can be seen from an examination of the various sections in this document (see Table 4-1). In a computer-based control room these resources can be almost completely integrated together to provide a seamless interface, i.e.:

- An end-user can move across HSI boundaries without having to make changes in the methods used to interpret data
- The data is organized and presented in the same way
- The context of data is maintained
- The navigation methods and schemes are consistent

Table 4-1
HSI Resources Supporting Crew Cognitive Activities

Cognitive Activity	Conventional Control Room	Computer-Based Control Room
Monitoring and detection	alarm tiles, status lamps meters, gauges, charts, SPDS	alarm displays (Section 4.4) information displays (Section 4.1)
Situation assessment	meters, gauges, charts, SPDS' status lamps, control status feedback	information displays (Section 4.1) COSS (Section 4.6)
Response planning	paper procedures	computer-based procedures (Section 4.5)
Response execution	hard controls	soft control displays (see Section 4.3)

[1] The section numbers in parentheses refer to section of this document where the topic is addressed.

With respect to computer-based information displays, the primary form of information presentation in many plants is typically system-oriented mimic displays. While system-oriented mimics are well suited to some personnel tasks (such as certain aspects of monitoring and situation assessment), they may not be effective for other important activities personnel perform. An example is the task of plant start-up. Crews need access to information about many different systems. Thus for start-up, when only system-oriented displays are available, operators need to access many different displays to retrieve needed task information.

Display access is part of interface management, i.e., the activities required by personnel to access and organize the information they need. A poor fit between the personnel task and the presentation of the required information usually means that the time personnel must spend performing interface management tasks increases. In part, this additional time is due to the added mental workload imposed when the end-user needs to know the relationships between what information is needed, where it is in the HSI, and how to manipulate the HSI to get to it. In some situations, the added time means that the abnormal conditions will last longer, and as a result, may get worse. If the situation is exacerbated by a “mistake” caused by faulty operator memory or inadequate experience, the situation can further worsen.

When the viewing area is limited, such as when information is viewed through a small number of monitors, personnel may be required to perform many interface management tasks. In particularly bad situations, they may be forced to make repetitive transitions among displays. Some approaches to overcoming these problems are discussed and additional information can be found in Section 4.2, User-Interface Interaction and Management.

The main implications of this issue are that: (1) displays should be designed to best meet the information needs of plant personnel, and (2) HSIs should be designed to minimize the need for interface management tasks, especially under high workload situations.

Well-designed displays can serve to integrate information in ways that are unachievable with analog hard-wired technology. Computer based HSIs provide the opportunity to present information at just the right level needed for the task at hand. With good information design, there is little need to transform or mentally integrate the information to make it useful, little demand on memory, and little to distract users from their tasks. The information displays can be designed to require far less interface management effort. Navigation cues embedded in high-level displays can provide access to lower levels for greater detail, thus easing the burdens of interface management. For example, a sensor symbol associated with a process variable can serve as a cue for the display of a trend plot of the process variable.

In this section, guidance is presented for augmenting system-oriented information displays to address the following functions:

- Monitoring, Detection, and Situation Assessment (Section 4.1.3.1)
- Task Performance (Section 4.1.3.2)
- Teamwork, Crew Coordination, Collaborative Work (Section 4.1.3.3)

When used together with the guidance for other HSI resources, such as alarms and soft controls (see Table 4-1), the information presented here can support design of HSIs that address the full spectrum of activities.

In advance of discussing the guidance for displays supporting each of these functions, several related considerations are discussed, including:

- Scope of the Modernization Program
- Operational Philosophy
- Information Requirements Analysis
- User Training
- Effects of Failures
- Display Design for Special Situations
- Effects on Overall Design Complexity

Scope of the Modernization Program

Many of the concepts for display design presented here can be implemented by utilities without the need for extensive planning of modifications. Modernization programs of limited scope may consider implementing better overview displays (described in Section 4.1.3.1) and a limited number of task-based displays (described in Section 4.1.3.2). For utilities planning more extensive modernization programs, the types of displays presented here can be integrated into plant operations and maintenance.

For any modernization project, utilities should consider:

- The degree to which different HSI resources will be integrated, e.g., the integration of soft controls into process displays.
- The degree to which the HSIs should support higher-level cognitive functions, e.g., HSIs support decision tasks, using displays that integrate lower-level data into higher-level information needed for decision-making.

As noted above, the range of functionality of computer-based HSIs can be wide, so it is important to decide which cognitive activities will be supported by the new HSIs (i.e., monitoring and detection, situation assessment, response planning and response execution), if not all of them.

While a single individual can perform these activities, NPP personnel work as a crew, so it must be decided whether the new HSIs will support teamwork (crew coordination and communication) as well.

Operational Philosophy

The issues associated with display functions are tied to overall operational philosophy, or concept of operations. For example, the types of information included in overview displays for monitoring are linked to the concept of operations and how the team is supposed to work and coordinate their activities.[1] For example, if a utility establishes clear divisions of responsibility between the reactor and turbine operators, then the information needed on displays to support

[1] There are many other key issues involved in operational philosophy, such as degree of centralization (i.e., which tasks and functions are migrated into control room and what is kept outside of the control room). These broader consideration are addressed in Section 2 and Section 3.7.

these operators is different than it would be if clear divisions were not made. This issue also relates to overall control room layout; e.g., how workstations are organized and what information is presented at each. Many of these more detailed considerations are discussed in Section 4.8, Workstations and Workplaces.

In this framework, it is important to consider the desired "mental model" that should be reflected in the displays. Well-developed displays provide a useful "overall" mental model of the plant. That is, the displays reveal the important relationships in the plant: between components, systems, and functions. At the same time, it is important that the displays reflect understanding of the plant and the behavior of different user groups (e.g., operators or maintainers). That is why it is so important to get "end-users" involved in the design of the displays rather than having them developed solely by designers. Cognitive aspects of display design are discussed in detail in EPRI-1002830.

Information Requirements Analysis

While most of this section addresses how to display information, perhaps the greater challenge in display design is deciding what information to display. This is referred to as information requirements analysis. A systems-engineering approach is commonly used for specifying information requirements. Task analysis methods are used to identify the specific alarm, information and controls needed for personnel to perform their tasks. More recently, new approaches to this process have been developed, including ecological interface design (EID), participatory ergonomics (involving end-users in display design), and rapid prototyping.

Whatever methods are used, information requirements analysis must be performed to identify the needed displays and their information content. Section 3 of this report presents methods for performing information requirements analysis by task analysis with a consideration of some of the new display developments. Information requirements analysis is also addressed in EPRI-1002830.

User Training

Computer-based displays require training to address:

- Clarifying the relationship between the representation of the plant as seen in the displays and the operator's mental model of the plant. Operators should be trained on the relationship between the display form and the plant states it is intended to represent, including the effect of failure modes on graphical representation.
- Identifying the relationship between displays and other HSI resources, such as alarms, controls, and procedures.
- Performance of interface management tasks, including navigation within and between displays, manipulation of on-screen features such as windows, and user-definable characteristics and features.

Training implications for the use of new, more integrated HSI resources are discussed more fully in Section 3.3.1, New Training Issues.

Effects of Failures

Failures of sensors, communications, and computer systems can have significant effects on displays, especially when the information presented is a synthesis of lower-level information. The failure modes of the systems and the effects they produce on the displays must be carefully examined for the impact on plant operations. Failures of the displays themselves and the systems supporting them also need to be carefully considered.

The effects of instrumentation failures need to be understood to ensure that they do not lead to incorrect situation assessment; e.g., operators mistakenly interpreting a graphic change due to an instrument failure as a change in process state. Considerations include:

- Can users detect instrumentation failures that affect displays?
- Can failures of instruments result in displays that are interpreted by users as process failures; and, perhaps more importantly, can real process failures be misinterpreted as failures of instruments? (Note that signal validation techniques can be of significant benefit here.)
- When failures are detected, how should the use of a display be changed?
- When a display integrates many individual parameters to present higher-level information, what is the operational effect resulting from the loss of this display and how effectively can users switch to using lower-level displays in its place?
- Can trending and forecasting functions cope with instrument failures?

Display Design for Special Situations

Even in plants with the most well conceived display systems, situations may arise that were not anticipated by the display designers. To assist crews in managing these situations, the display system can provide tools for the easy creation of user-defined displays. Examples of such situations include:

- The need to monitor a combination of plant parameters that are not presented together on any single display (for example, to provide enhanced monitoring of a system or piece of equipment that has been causing trouble)
- The need to monitor from the control room (CR) an important maintenance activity in the plant using a display that includes an onscreen task sequence list and a window containing a closed-circuit television (CCTV) view of the activity

Such tools need to be used with caution to ensure that users do not negatively impact existing displays or the plant's configuration management, and that the quality and correctness of new displays is assured. Providing some administrative controls over user-defined displays can address these issues.

Effects on Overall Design Complexity

When implementing the guidance in this section, it is important to consider the potential effects of the complexity of the overall design. As the number of displays increases, additional design, integration, testing, and training is needed and this impacts the eventual cost of a display system.

The effects on I&C performance should be considered as well. For example, the CCTV used in the example above, takes up a lot of bandwidth on a network used for plant data exchange and may make it difficult to cost effectively meet response time or through put requirements, which may be of higher priority in the big picture than an integrated CCTV/maintenance procedure display. System design considerations, such as establishing a separate CCTV network and display system, can often circumvent specific obstacles.

The key point is that implementing the guidance presented needs to be considered and evaluated in the context of the overall modernization program.

4.1.3.1 Display Design for Plant Monitoring, Detection, and Situation Assessment

In this section, the design of displays for plant monitoring and situation assessment[2] is discussed. Since monitoring activities require personnel to be concerned sometimes with individual low-level process values and sometimes with the relationships among many different types of information, these displays need to present information at varying levels.

This section is divided into three subsections. The first describes the general characteristics of display hierarchies. The second provides guidance for the design of displays in the hierarchy. The last provides guidance on the design of rapid and efficient navigation strategies through the displays in the hierarchy.

An important activity for plant personnel is to monitor the status of the plant from high-level functions down to the lower-level of equipment status and to identify the nature of problems when detected. In this context, a function is a provision for using all or part of one or more plant systems for fulfilling a particular mission.

In this section, the design of displays for plant monitoring and situation assessment is discussed. Since monitoring activities require personnel to be concerned sometimes with individual values and sometimes with the relationships among many different types of information, these displays need to present information at varying levels.

The basic elements of the displays for supporting monitoring and situation assessment are:

- A hierarchy of displays with various “levels of abstraction” from high-level summary information to very detailed information.

[2] To avoid confusion, the term “situation assessment” is user here to refer to the cognitive activity involved in determining the current status of the plant (or some part of it). As discussed in Section 1.3.4 of this document, a distinction is made between situation assessment and “situation awareness,” which is the result of the assessment process, i.e., the user’s understanding of what the plant’s status is.

- Top-level overview displays that provide broad overviews suitable for plant monitoring.
- Displays providing progressively more detailed information suitable for situation assessment in the event something is not normal.
- Navigation aids to enable users to quickly and easily move from higher-level displays and lower-level displays in the hierarchy.

Organizing information in this way enables crews to quickly visualize plant status, the complexity of the process, and the propagation of failures between low levels to high functional levels.

Two additional considerations are noted. First, monitoring and situation assessment displays may contain controls as well. Plant controls are addressed in Section 4.3, Soft Controls. Second, the guidance in this section only addresses information presentation and access aspects of monitoring and situation displays. These tasks can be supported by computerized operator support systems. For example, techniques such as expert systems and neural networks can be well suited for monitoring, alerting, and diagnostics applications. The user interface aspects of these types of aids are discussed in Section 4.6, Computerized Operator Support Systems.

4.1.3.1.1 Defining a Hierarchy to Serve as a Basis for Displays

⇒ 4.1.3.1.1-1 Displays for monitoring and situation assessment should be organized according to an abstraction hierarchy. The hierarchy should:

- *Completely describe the plant in terms of its main purposes or missions, i.e., supply power to the grid and maintain safety*
- *Reveal goal status at each level*
- *Reveal both physical and functional relationships*
- *Reveal interactions and dependencies of the hierarchy elements*
- *Be applicable to all operational situations and reflect differences associated with different operating modes*
- *Be meaningful to the users*

The first step in designing displays to support monitoring, detection, and situation assessment is to define the type of hierarchy to be used in organizing the displays. Following from the work or Rasmussen (1986), the concept of an “Abstraction Hierarchy” (AH) provides a framework to define a hierarchy of information displays from high level information to increasingly more detailed information as one proceeds to lower-level displays.

Information about a plant’s missions for supplying power to the grid and maintaining safety can be structured into abstraction hierarchies using the plant’s natural composition of functions, processes, systems, and components. Figures 4-3 and 4-4 illustrate a hierarchy for supplying power to the grid and maintaining safety, respectively. Figure 4-4 is very similar to the SPDS hierarchy used in many plants today.

The specific approach used should be consistent with plant operating practices and training.

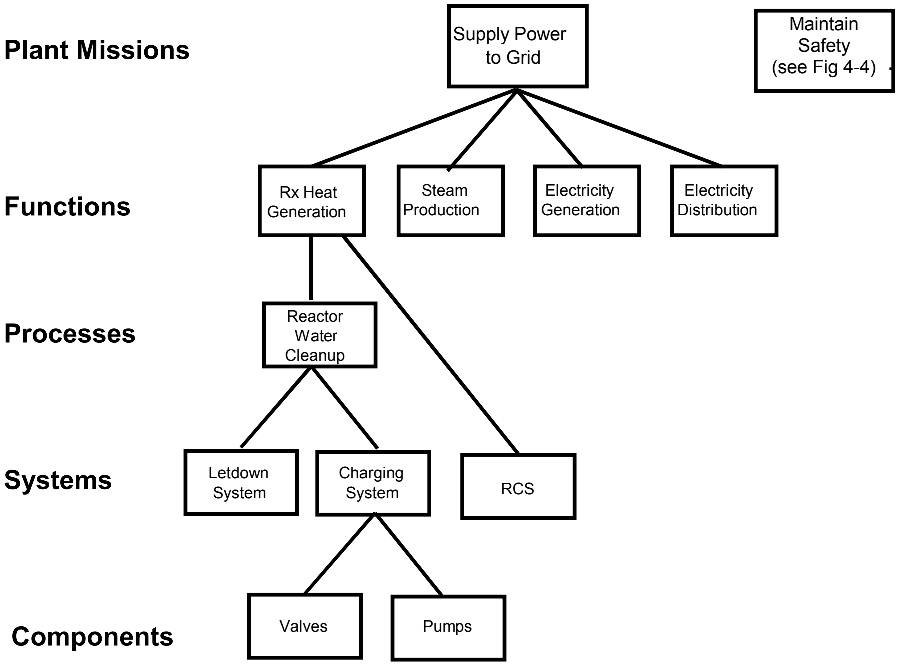


Figure 4-3
Plant Abstraction Hierarchy for Supplying Power to Grid
(Note: Only a portion of the hierarchy is shown.)

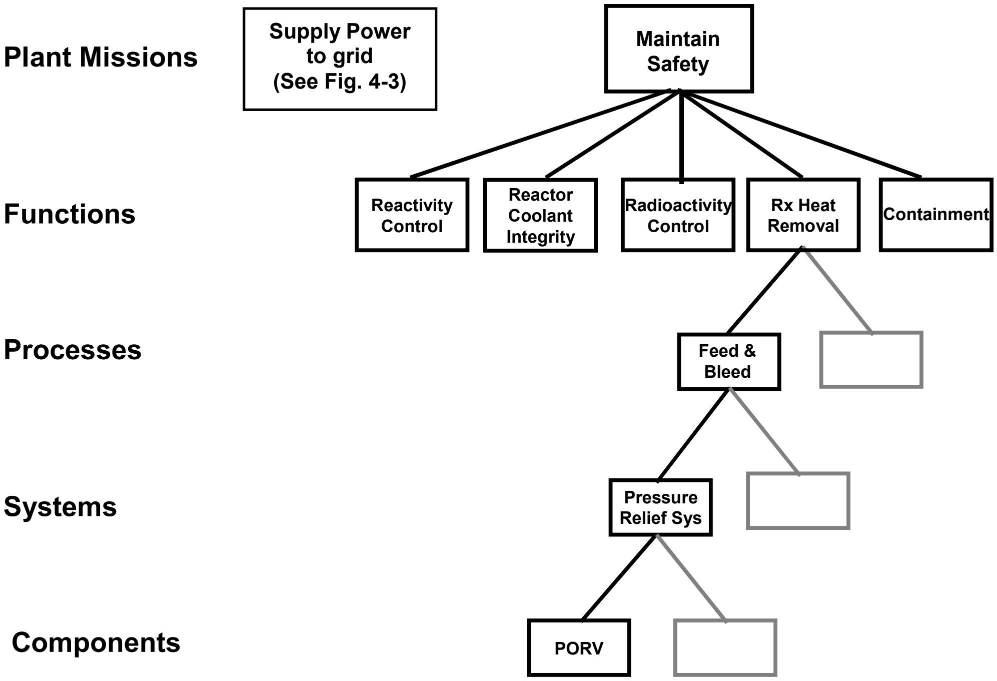


Figure 4-4
Plant Abstraction Hierarchy for Maintain Safety
(Note: Only a portion of the hierarchy is shown.)

⇒ 4.1.3.1.1-2 Displays should reflect the hierarchy and provide information at various levels that are appropriate to the various operator functions and tasks. Higher level displays should support monitoring of plant status and situation assessment functions and increasingly detailed displays should support troubleshooting or more detailed status monitoring.

Using such a hierarchy, displays can be designed to reflect information about each level. At the *higher-levels* of the hierarchy, overall plant performance and higher-level functions are depicted. This may involve providing:

- Overall summary measurements for mission achievement, such as megawatt production and integrity of critical safety functions.
- Information about the integrated status of functions. Model-based displays can be used for this purpose, e.g., mass and energy balance displays. These could show identified and unidentified RCS leakage rates (deviations between calculated and measured), as well as real-time measurements that depict the overall plant thermal efficiency for overall electricity production cycle (including nuclear, thermal, and electric measurements). When problems are identified, such as increasing leakage rates or a drop in efficiency, operators can consult the lower-level displays. Displays based on mass and energy balance are discussed in EPRI-1002830.
- Performance or status indicators of important plant functions.

At the *intermediate levels*, plant processes and systems are shown. While some functions directly link to systems, there are times when several systems contribute to the outcome of an intermediate process. Examples include “Reactor Water Cleanup” under the Supply Electricity to the Grid mission (see Figure 4-3) and “Feed and Bleed” under the Maintain Safety mission (see Figure 4-4). When processes involve many manual actions, as is the case in feed and bleed, a task-based display could be considered (see Section 4.1.3.2).

How system elements are shown in displays can vary. For example, one approach is to organize the display of systems by the division of responsibility for the aspect of the plant they address, e.g., primary and secondary. Such an organization would make sense for a utility that assigns operational responsibilities along these lines. A second approach is to organize them according to “frontline” and “support” systems. The required support system(s) and components of each frontline system are provided in lower-level displays. In this organizational hierarchy, common support system problems affecting frontline systems can be quickly identified. Figure 4-5 illustrates part of a hierarchy using this structure. Systems are often divided into trains, so the hierarchy may reflect this organization as well.

At the *lower levels* – individual components, instruments, etc., are represented. The displays may provide detailed component performance data, technical information, and physical description, such as component drawings.

Individual displays may combine levels of information as necessary. For example, an individual overview display may show the status of all levels (along with key/important information from lower levels).

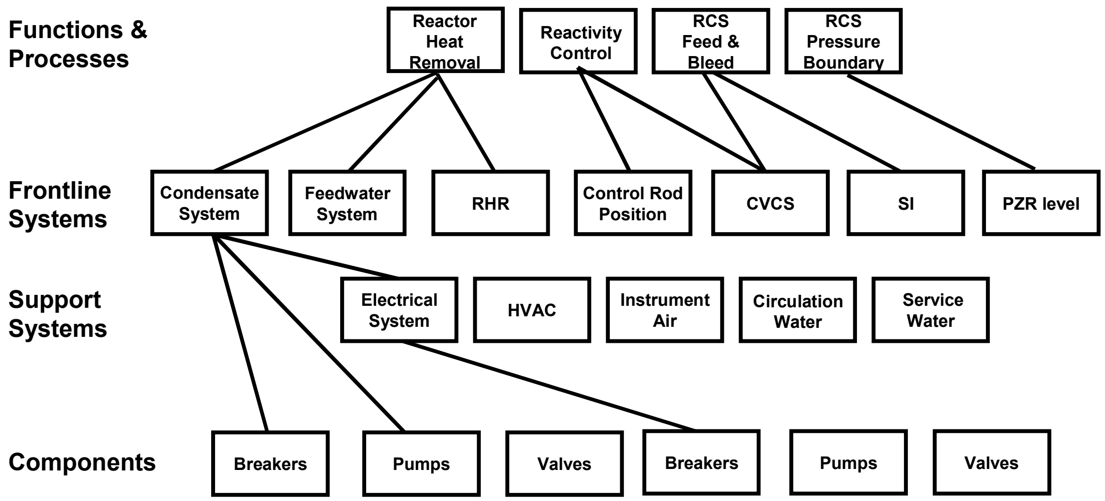


Figure 4-5
Partial Hierarchy Based on PWR Frontline and Support Systems
(Note: Only a portion of the hierarchy is shown.)

Regardless of which specific levels are shown, the hierarchy should enable operators to monitor status using very few high-level displays and to quickly transition to the displays at the system and component levels to obtain more detailed information should a problem be detected or if additional information is desired. Using such an approach, the relationship between equipment failures and higher-level functions can be readily determined.

⇒ 4.1.3.1.1-3 Each display in the hierarchy should use the same general design principles.

Consistency will enable rapid understanding of the meaning of each display and how to easily move to other needed displays.

4.1.3.1.2 Content of Individual Displays

With respect to monitoring and situation assessment, one of the main things that the users need to know is whether functions/systems/components, etc. are working properly or not. And, if not, what alternative is needed to reach the current control goal. Thus each function/system/component has to be depicted in terms of its status and its purpose or goal. Considering and following procedures as part of the process by which users choose between alternatives can be supported by the HSI. The HSI's real-time indication of the current status of degraded or failed function/system/components can also assist to provide possible alternative choices that are available.

Thus, each display should enable users to quickly determine the overall status of the function/system/component it represents. To achieve this goal, displays should include:

- A representation of the main elements of the plant's abstraction hierarchy (AH) appropriate to the level of abstraction of the display.
- Indication of important modes relevant to the information contained in the display.

- Overall status indicator for key AH elements (including safety functions).
- Performance indicators for key AH elements.
- Dynamic information (where information is changing, such as trends).
- Signaling of conditions requiring operator actions.
- Signaling for results of automatic control system actions that automatically result in changes to process equipment configuration or state.
- Signaling of changes to other displays above and below the display in the hierarchy.

Guidance on these aspects of displays is provided below.

Indicators in higher-level displays may be based on synthesis of many lower level conditions and parameters. For example, the status of a function is not generally determined by a single parameter. Instead it is a combination of the status and performance of the lower level systems that support it.

Of course, higher-level displays need to provide access to lower-level displays providing detailed information. This is addressed in Guideline 4.1.3.1.3-2. There are many different ways this can be achieved. For example, the display may include a direct link to lower-level displays. Another approach is to provide specific keyboard keys on a workstation to access displays below the higher-level display.

⇒ 4.1.3.1.2-1 Displays should include a representation of the main functions, processes, systems, and component of the plant's AH and their relationships.

A variety of formats can be used to construct a display, including mimics, trend graphs, and digital value displays or a combination thereof. An overall plant mimic, for example, may enhance personnel performance by (1) communicating relationships between components, or (2) providing a means of organizing information to facilitate plant monitoring and information retrieval. Mimics are a prominent feature of many overview displays in advanced control rooms. They provide a useful framework for organizing plant information to support the operators in locating specific information and monitoring particular portions of the plant.

⇒ 4.1.3.1.2-2 Displays should indicate the key modes of operation that affect the user's interpretation of information.

Plant, function, system, and component modes of operations can affect the meaning of information. For example, the status of many components differs significantly between start-up and full power operations. Indication of plant mode will help user's understand these differences. In some circumstances, displays can be dynamically adjusted to better reflect information dependent on the mode of operation.

⇒ 4.1.3.1.2-3 The important AH elements should be presented so the status can be determined at a glance, i.e., that status is very easily recognized. The types of information that should be considered include:

- *Goal attainment Status – the current function or system goal is being achieved or not.*
- *Availability Status – available or not available (e.g., bypassed/inoperable; tagged-out; key locked) and whether an action is required for use (e.g., line-up).*

- *Capability Status – the current capability to contribute to the satisfaction of the functional goal in question. This relates to the sufficiency of system or component to achieve a goal. For example, current operating conditions may be such that a system cannot achieve its function because it is not designed to operate under the those conditions. Consider, for example, low-pressure safety injection as one of the alternatives that is available to satisfy the Control RCS Water Mass Inventory function. It is only effective in satisfying the goal if the RCS pressure is low enough.)*
- *Service Status – in service or not in service (the element is ready to achieve its purpose). Being ready to achieve a purpose may require going through several stages of successful functional states.*
- *Equipment Functional Status – (e.g., flow/no-flow, energized/de-energized, on/off, and open/closed).*

A status-at-a-glance display should enable users to quickly determine overall status. A list of example equipment for which status information might be presented on an overview display is given below (of course, the specific selections should be identified during the design process based on the unique design of the plant and the level of equipment importance to the contribution to the plant overall goals):

- Reactor coolant pump status for PWRs
- Recirculation pump status for BWRs
- Feedwater and condensate system pumps and valves
- Key safety system pumps and valves
- Decay heat removal pumps and valves
- Power supply breakers
- Emergency and vital electrical power
- Main steam isolation valves (MSIVs)
- Safety relief valve status for BWRs
- PORV and block valve status for PWRs
- Protection systems status
- Radioactivity levels

There are specific status conditions that are important for the crew to know. It is important that crews quickly determine that a function, system, or component is available and in-service. It is also important to identify the bypassed and inoperable status of systems and components for functions important to safety (per Regulatory Guide 1.47). Similarly, tagged-out (e.g., for maintenance) status of major equipment should be indicated.

Another important status indicator is whether a component is “key locked.” Many plants have added protection against inadvertent actuation by requiring the added action of using a key to unlock the control. Components that are “key locked” in this manner should be identified as such in the display screen, so that operators know this and do not apply needless effort. Further, the computer may be capable of providing a convenient means to prevent unauthorized access to control items. The means to do so should be commensurate with the level of protection needed. Passwords, special caution messages, and required supervisory approval are all methods to accomplish this. The important point here is that the need for such additional actions can be indicated in the display of that component.

Functional status of important systems, structures and components could be visible as well, such as whether important valves are open or closed.

Figure 4-6 - Display A, provides an oversimplified illustration of depicting high-level status. (As noted in the previous guideline, overview displays will usually contain graphic representations of the functions, systems, equipment, etc.) In the figure, a single graphic element is used to represent each system. These boxes are color coded - green for available and red for unavailable (and shape coded for redundancy).[3] System 8 is shown as unavailable. The boxes themselves can be organized to give higher-level information, such as grouping by function.

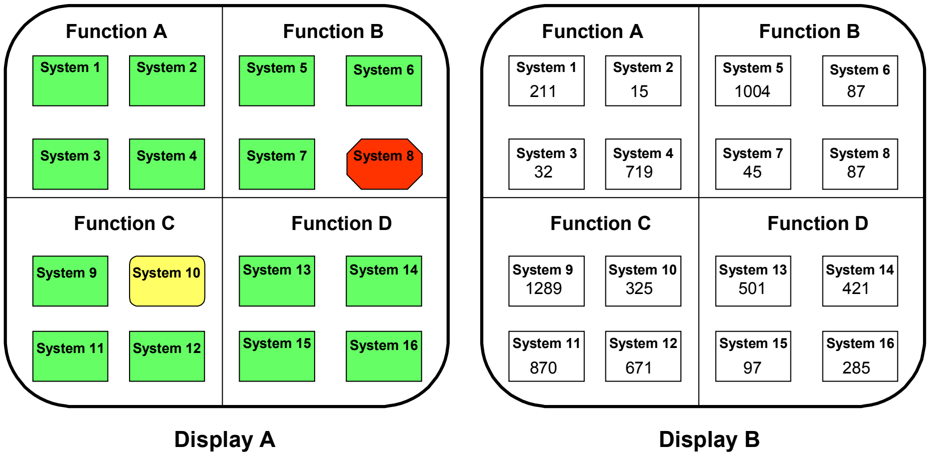
User situation awareness can suffer when users focus on other information and fail to attend to important data. This can happen if the display does not draw their attention when required. In some systems it may be more important to know whether the system is available or unavailable. There may be intermediate operating states that must be known. If a system has a primary and a backup power source, and the system is operating successfully, but on a backup power source, the status box might be coded “yellow” to indicate a less than optimal situation, but not necessarily needing the operator’s immediate attention. Where intermediate states are known, they can be coded into the primary display. The logic of status coding must be carefully defined, i.e., the definitions of red, yellow, and green must be precisely defined and consistently applied.

The solution to status-at-a-glance functionality is to provide the user with means to see the big picture quickly and easily, and at a high level without needing further navigation. The user needs to quickly know the consequences to the plant operating conditions with any change in system/equipment/component status. If the user has to search for high-level information, it is not a status-at-a-glance display. Compare the status determination of Figure 4-6, Display A with Display B. In Display B, performance indicators are provided. The user has to determine whether the performance indicator for each system is within an acceptable range. The information should be presented in an immediately usable form. If determining status requires reading the value and mentally comparing to some numerical reference value, then the display becomes much less effective, and the chance of the user missing something becomes much greater. This is not status-at-a-glance functionality.

It is important that the representations used to indicate problems be highly salient. High salience quickly captures the user’s attention. In the example, color and shape are used. However, other coding strategies could be used as well.

Users must be able to judge the correctness of status information. For example, users should be able to determine how the status of the systems in Display A is determined. This may require some navigation to determine the basis for their status. A help display could also assist in providing indication of the basis for the condition. This display could also provide direct links to the different elements that make up the displayed status.

[3] In these examples, color is used differently than it is used in most U.S. plants where *red* means on, energized, or flow and *green* means off, deenergized, no flow. They are meant as illustrations only and the selection of specific color codes to be used should be made in consultation with system users.



Display A

Display B

Figure 4-6
Representing High-Level Status of Multiple Systems

⇒ 4.1.3.1.2-4 Important performance indicators for key AH elements should be provided. These may be measured parameters or derived values. Any analyses or information integration by which lower-level data are analyzed to produce higher-level performance indicators should be available to users so they can easily determine the meaning of higher-level indicators.

A candidate list of performance indicators that should be considered for presentation in an overview display is presented below (of course, the specific selections should be identified during the design process based on the unique design of the plant):

- Power level
- Plant efficiency (energy balance)
- Leakage (mass balance)
- Reactor coolant system pressure
- Reactor coolant system temperature
- Steam flow and pressure
- Condenser vacuum
- Reactor coolant flow rates
- Pressurizer level of PWRs
- Steam generator levels for PWRs
- Margin to saturation for PWRs
- Reactor vessel level for BWRs
- Emergency power status

Performance indicators are more meaningful to users when they are put into context of what the indicator means. For many indicators, the status indication (normal or off-normal) may be sufficient. However, for others, it may be important for users to know the relationship between the current value and limits or setpoints associated with the parameter or variable.

From the example illustrated in Figure 4-6, in addition to status color and shape coding, the boxes could contain some key performance indicators (see Figure 4-7). With this type of simple display, the user can quickly glance at the screen and determine immediately whether any of the systems need attention. If a red box is observed, the key performance indicator may indicate how serious the situation is. And if the boxes are grouped and several boxes are red, then the user could quickly determine if there is a correlation between the systems needing attention, such as a degraded common support function, like chilled water for HVAC or instrument air for valve and solenoid control.

Users should be able to easily access the means by which derived values were calculated in order to verify the value and to better understand their meaning (i.e., by a single input/navigation action such as by one mouse or trackball click, touchscreen action, etc.). Depending on the method use to derive higher-level information, it may not be feasible or even advisable to provide detailed explanations of the full basis for a displayed values. For example, they may be based on complex computations, simulations, or expert systems, that would not be particularly useful to user. The important point is to provide an explanation that the user can use to better understand and verify the value. The explanation should be at that level.

In addition, as per Section 4.1.7, Data quality and update rate, users should be alerted if the data quality is poor.

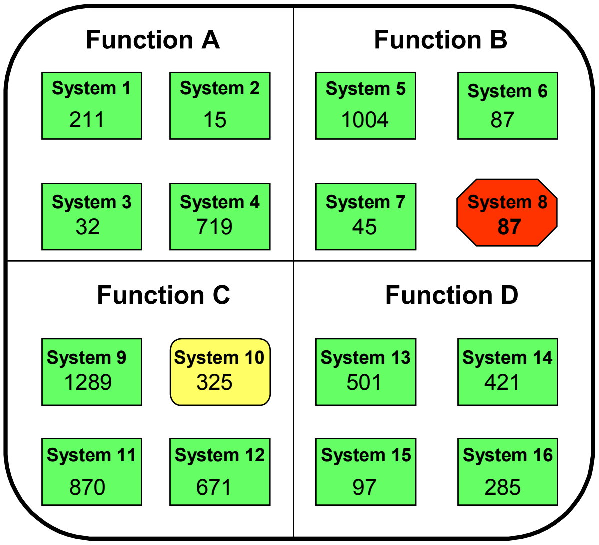


Figure 4-7
Displaying Status and Performance Indicators

⇒ *4.1.3.1.2-5 The display should have information readily available on plant dynamics, i.e., indicate when the performance indicators are changing at significant rates.*

A computer-based display of plant dynamics is dependent on sampled data, which is a subset of a continuous or changing instrument signals. The sample rate must be such that it is representative of the measured plant parameter. For example, a pressure value likely requires quicker sampling than a temperature one. Additionally, being able to understand the plant's current state is often dependent on knowing where it has been and projecting where it is going. This information should be readily available (e.g., one or two mouse clicks) for display from the overview. Changes in status or dynamics should be displayed using trend over time and projection to future states (where technically feasible and valid). Trends may be shown in a variety of ways, e.g., an arrow to indicate direction of change, or for significant parameters, a trend graph. Plant status projections can be based on mathematical prediction, past performance, or simulation models. In addition, intermediate displays may offer "rate of change" parameters associated with limits and set-points.

If the display itself does not have sufficient space to display plant dynamics of interest, users should be able to access them on nearby supplemental display(s) with some indication of the need to look at the supplemental display(s).

⇒ 4.1.3.1.2-6 Overview displays should address safety parameter display system (SPDS) requirements.

The SPDS requirements are specified in Supplement 1 of NUREG-0737 (NRC, 1980) and NUREG-1342 (NRC, 1988). The review criteria for the human factors aspects of SPDS are contained in NUREG-0700, Rev 2 and are summarized in Table 4-2 (below). NUREG-1342 recommends parameters reflect the following safety functions:

- Reactivity control
- Reactor core cooling/primary system heat removal
- Reactor coolant system integrity (e.g., steam generator pressure, containment sump level)
- Radioactivity control (e.g., stack, steam line, and containment radiation)
- Containment conditions (e.g., containment pressure and isolation status)

While the original SPDS concept was to retrofit control rooms whose HSIs were predominantly of the conventional technology, plant modernization programs offer an opportunity to use better information technology and provide integration of SPDS objectives into the primary displays. The goals of an overview display are consistent with the purpose of the SPDS by providing the capability of high-level monitoring.

NUREG-1342 notes that SPDS parameters should be continuously displayed, not just continuously available. However, acceptable SPDS systems either provide a dedicated, single display of plant variables or a hierarchy of display pages on a single display device, with perceptual cues to alert the user of changes in the safety status of the plant (such as when safety functions are challenged). Thus, parameters presented on the overview display intended to address SPDS requirements should be continuously displayed, or have an alerting mechanism, such as critical safety function status indicators. It should be noted that additional displays are likely to be needed to meet all SPDS requirements.

SPDS should be a prominent and distinctive group of status indicators on the display and be easily discernable from those that are not, even if other plant parameters are similar to SPDS ones. The presentation of the other parameters should not interfere with the ability of personnel to rapidly assess the plant safety status.

Table 4-2
NRC HFE Guidance for SPDS Review

Information Display

- Critical plant variables and parameters should be displayed to help users evaluate the plant's safety status.
- The display system should display information about severe accident symptoms associated with the plant safety parameters and functions.
- Plant parameters and variables important to safety should be displayed in a way that is convenient and readily accessible.
- Critical safety function displays should be readable from the workstations of users needing access to these displays.
- Critical plant variables should be displayed in a concise format.
- Each critical variable should be displayed with sufficient accuracy for the user to discriminate between normal conditions and those affecting plant safety status.
- The display should provide magnitudes and trends for critical plant variables or derived variables.
- The display's response to transient and accident sequences should keep the user informed of the current plant status.
- Critical safety function displays should allow users to comprehend a change in safety status in a matter of seconds.
- The sampling rate for each critical plant variable should be consistent with the users' needs for performing tasks.
- Displays for monitoring safety parameters and functions should continuously display this information.
- Where plant operating modes impose different demands, separate display pages should be provided for each mode.

User-System Interaction

- The system should assist the user in monitoring critical parameters, especially parameters that change very rapidly or very slowly, by alerting the user when values are out of range.
- Where feasible, the system should provide perceptual (audible or visual) cues to alert personnel to abnormal operation conditions that potentially warrant corrective action.
- User interactions with the display system should be within the skill capability of the control room crew and should not significantly increase personnel workload.

Reliability, Test, Maintenance, and Failure Indication Features

- The display should not give false indications of plant status.
- Critical plant variables should be reliable and should be validated in real time.
- The status of the data should be displayed to the operator with an appropriate data quality indicator (e.g., valid, invalid, or unvalidated; or a derived numerical estimate).

Integration with Other HSI Elements

- The location of displays for monitoring safety parameters and functions should not interfere with the normal movement of the control room crew.
- The display system should not interfere with visual access to other control room operating systems or with displays that are important to safe operation of the plant.
- Display devices for monitoring safety parameters and functions should be labeled and readily distinguished from other devices.

Note: Source is NUREG-0700, Rev 2, Section 5, Safety Function and Parameter Monitoring System.

NUREG-1342 states that the U.S. Nuclear Regulatory Commission (NRC) staff found acceptable some SPDS systems that consisted of a single VDU display augmented by conventional control room instruments. However, any SPDS was found unacceptable that caused the user to leave the SPDS to gather information necessary to assess the status of the critical safety functions, or otherwise turn attention away from the primary SPDS location. Since the overview display most likely does not present all SPDS parameters, there should be a smooth transition to the more detailed data where needed (which is addressed in Section, 4.1.3.1.3 below). This will support rapid assessment of the plant safety status.

⇒ 4.1.3.1.2-7 The display should indicate conditions requiring operator actions related to the main AH elements.

These signals may be alarms to show that main functions, systems, or equipment are in a degraded condition. Alarms may be spatially dedicated and integrated into the display to better depict the relationship between alarm conditions and the AH elements affected.

⇒ 4.1.3.1.2-8 Upon control actuation, a display should be immediately available to allow the operator to evaluate the performance of the system, e.g., information on the control input and output actuation signals and the resulting states of plant process components. Comparison of these states with expected states should also be made and deviations displayed in the abnormality indication portion of the HSI.

Failure in a process control system may not be evident until the control system is required to respond. Thus, the display should contain the controlled item, set point, error signal, and controlled variable so that the user's can evaluate the response of the control system. See Section 4.3, Soft Controls, for guidance on designing displays for such controls.

For example, upon ESF actuation, the display system can indicate that an ESF monitoring and control display is available. The display should be accessed with one user action (displays should not automatically appear on the user's screen).

⇒ 4.1.3.1.2-9 To the extent possible, the functionality of the displays should be preserved at all power levels and plant operating modes.

Monitoring plant status during non-full power operations can be difficult. To the extent possible, the characteristics of the display should provide the same status-at-a-glance features for situations when the plant is not at full power. This may be accomplished by having separate overviews for different plant states. Such displays could automatically change when the plant mode changes, but indications must be provided that the displays have changed in response to the plant change.

⇒ 4.1.3.1.2-10 Higher-level overview display(s) should be available at the user workstations. If the control room layout will permit, the overview display(s) should also be located so that it can be seen from anywhere in the control room.

When implemented as a "group-view" display, the overview will permit the operating crew to monitor the plant status from anywhere in the control room (i.e., while not at their workstations). This is especially important in control rooms that are largely workstation based.

⇒ 4.1.3.1.2-11 Providing overviews not only supports monitoring but access to more detailed information as well (by means of navigation features to drill down to more detailed displays).

⇒ 4.1.3.1.2-12 Displays at each level should alert users to important changes to the plant that may be indicated in higher- and lower-level displays. The method of alert should communicate to the user whether the change is at higher levels or lower levels and facilitate navigation to the appropriate display showing the applicable plant changes.

Figure 4-8 illustrates display of status in a hierarchy of displays. The example depicts a four level hierarchy (only a portion of which is shown). Each of the numbered boxes is one display in the hierarchy. Display 1 is a high-level overview display of, for example, the Containment Heat Removal (CHR) function in a BWR plant. Displays 2, 3, and 4 are at the system level and represent the Residual Heat Removal (RHR) System in the Suppression Pool Cooling (SPC) mode, RHR in the containment spray mode, and containment venting. Displays 5 and 6 are train level displays for the SPC mode of RHR and represent Train A and Train B. Displays 7, 8, and 9 are component level displays for RHR Train A, and display information about the RHR Heat Exchanger (HX), RHR Pump A and RHR Pump C.

Color is used in this example to illustrate status. Green means everything is OK, red means failed, and yellow means something is compromised (i.e., the function/system/component is operable but with some reduced status).

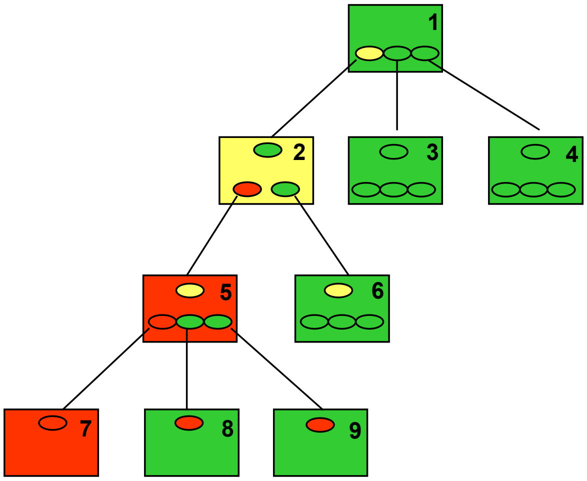
The boxes have ovals that show the status of functions/systems/components represented by displays both above and below a given display in the hierarchy. In this example, displays above are shown in the higher-centered oval and those below in the set of lower-level ovals. Since Display 1 is the top-level display, only the next lower-level status indicators are shown. And since Displays 7, 8, and 9 are at the lower level, they only show the next upper-level status indicators.

To be operable, RHR Train A (shown in Display 5) requires its HX and one of its two pumps to work. However, as can be seen by the red color in Display 7, the HX is not working. Thus, while the pumps represented by Displays 8 and 9 are working (green), the Train represented in Display 5 is not and is red. If an operator is looking at Display 5, he can see that one of his three components is not working, and that Train A has failed. However, he can also see that the system represented by Display 2 is still operating, but is compromised (as is indicated by the yellow oval at the top of the display). This is because the system in Display 2 only requires one out of two Trains to work. While the Train in Display 5 is not operable, the redundant Train in Display 6 is OK. Thus, the SPC mode (Display 2) is still functional, but with reduced redundancy (as is indicated by the yellow color).

An operator looking at Display 2 can see that SPC is operable, but compromised because one of its two Trains has failed. But the operator can also see that the overall higher-level function (CHR) is fine (as is illustrated by the green oval at the top of the display showing the status of the high-level function in Box 1).

If the operator is monitoring at that top level (Box 1), he can see that the high-level function of CHR is fine, but that one of its possible systems/modes is compromised.

The key point illustrated in this simple example is that no matter what display an operator is looking at, the operator can tell the working status above and below in the hierarchy.



Function Level
1 = BWR Containment Heat Removal function

System Level
2 = Residual Hear Removal (RHR) System
in the Suppression Pool Cooling (SPC) mode
3 = RHR in the containment spray mode
4 = containment venting

Train Level
5 = SPC mode of RHR Train A
6 = SPC mode of RHR Train B

Component Level
7 = RHR Heat Exchanger (HX)
8 = RHR Pump A
9 = RHR Pump C

Figure 4-8
Alerting User to Changes in Higher and Lower Level Displays
(Note: Example uses the Containment Heat Removal Function in a BWR Plant)

⇒ 4.1.3.1.2-13 Displays in each level of the hierarchy should present information that effectively communicates the plant relationships at that level and which minimizes the need to access multiple displays.

One consideration during the display design process is the amount of information put into each display. Displays that are relatively filled with information enable users to more easily use parallel information, reduce memory load (the demand of remembering what is in one display when looking at another), and reduce information management workload. Thus, a tradeoff is needed between distributing information over many less-dense displays that require a lot of navigation, and filling displays with data potentially resulting in a crowded appearance making information harder to find, but requiring less navigation. Displays that initially appear crowded to operators can become preferred and effective in supporting performance as operators gain experience with them.

4.1.3.1.3 Navigation within the Display Hierarchy

It is essential to situation assessment that users be able to easily navigate through the display hierarchy with minimal effort and minimal need to shift attention away from the process information. This will allow them to devote attention to situation assessment activities, but not loose situation awareness. The guidance in this section addresses such navigation support. This guidance is limited to the specific issue of navigation in the hierarchy of displays. See Section 4.2 for detailed guidance on interface management and interaction.

⇒ 4.1.3.1.3-1 Each display should be clearly labeled as to its contents and its relationship in the hierarchy.

Displays should contain information for users to determine where they are in the hierarchy. Providing such landmarks will help to minimize loosing orientation in the information system and errors associated with misinterpretation of information users are looking at one display, but think they are looking at another.

⇒ 4.1.3.1.3-2 The system should provide on-screen navigational links to and from high-level and lower-levels of information with references and supporting information.

Navigation to and from related information displays can be time consuming, distracting, and error prone. Computer support, such as accessing display pages through hyperlinks and on-screen buttons, can reduce the workload. For example, a user can point and click on a system icon to get the mimic for that system. Compare this approach to navigation where the user must move his attention away from the first display to a hierarchal menu, then move the cursor down the menu until the desired display is reached, and then click to retrieve it. The former offers the ability to look at the first display and immediately retrieve the more detailed display. This creates visual flow and minimizes the disrupting effects of navigation. Where feasible, this type of approach should be used. This type of navigation is faster and more direct than requiring the user to access other displays by means needing more navigation effort. The attention shift created by accessing menus for navigation can impair situation awareness and/or assessment.

Figure 4-9 gives a high-level illustration of how a user can move through the hierarchy using navigational links on each display screen to lower and upper level displays (similar links can be made available to displays not in the hierarchy, see Guideline 4.1.3.1.3-7 for an example). This figure is the same as Figure 4-8 that was used to illustrate presenting information about status changes in displays above and below the one the user is looking at. In this example, assume that the ovals, in addition to providing status information, provide links to the other displays. With such a design, if the operator is looking at Display 1 and sees the yellow “compromised” status indicator, he can click on it and immediately navigate to Display 2 depicting the compromised function. Here he can see that one of the supporting systems has failed. Clicking on the red oval, showing a failed system, he can navigate to Display 5, where he can see the failed system/equipment/component. If necessary, he can navigate further to Display 7 to investigate the details. Similarly, if he was looking at Display 6 and saw that while that system was fine, the function was compromised (as indicated by the yellow upper oval), he could click on it to move to Display 2 and then down the hierarchy as above to investigate the cause.

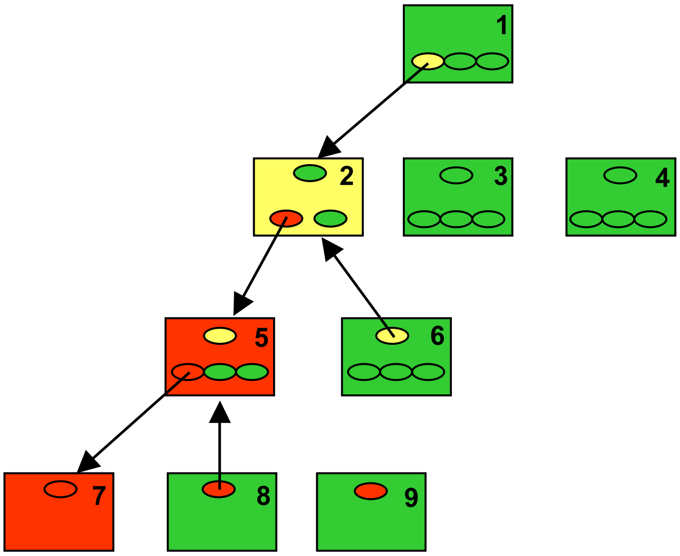


Figure 4-9
On-Screen Navigation to Lower and Upper Level Displays

Such a navigation scheme enables users to retrieve information without having to remember where information is in the information system.

⇒ 4.1.3.1.3-3 Navigation tools should provide for flexible approaches to searching for information.

In addition to on-screen navigation aids, displays should provide flexibility in the search for information users might employ to assess plant status. Displays should support the operator in making rapid overall assessments of plant condition using various types of searches, including:

- Event/Data driven – searching for information that describes conditions that were specifically alerted. For example, when an alarm comes in, the user could navigate directly to the appropriate function, system, or component display directly associated with the alarm message.
- Knowledge driven – searching for information that the users decided they may need. For example, when testing assumptions or conjecture about plant status, the user can directly move around the display hierarchy using embedded links such as was discussed in Guideline 4.1.3.1.3-2 above.

Other approaches to navigation should also be available, such as menus or special function keys and other techniques (see Section 4.2 for more general information about display interaction).

⇒ 4.1.3.1.3-4 The system should include a history function allowing users to keep track of the sequence of displays they have accessed to facilitate retracing their steps.

As part of situation assessment activities, users may move up, down, and across the hierarchy of displays several times. A function that enables them to retrace their steps will facilitate the location of previously viewed displays. “Back” and “Forward” functions also should be available.

⇒ 4.1.3.1.3-5 A list of all displays, e.g., on a menu, should be available to provide access to displays that do not have on-screen links.

The availability of such a list can greatly reduce navigation burden and will provide more rapid access to important information.

⇒ 4.1.3.1.3-6 Visual search within each display should be supported by coding and other display features that enable users to easily see associated information in the display.

For example, in a display of a two-train system, one train of a system might be coded with the use of one single color, while a second color is used to depict the second train. The background in an adjacent table of data pertinent to each train could the associated train’s color. The color helps the user to perceptually associate the two aspects of the display.

Related elements also should be spatially grouped, and information should be imbedded within graphical objects to reduce the need for shifts in attention caused by excessive eye movement. For example, organizing data by plant safety function; use of bar charts and digital values within symbols for major plant components reduces visual travel. A specific example is to show pump speed with the pump symbol (when the pump is running) and temperatures and pressures at appropriate points in symbolized piping sections.

⇒ 4.1.3.1.3-7 When conditions signal changes in display pages the user is not currently viewing that the user should attend to, special navigation aids should be presented to enable those displays to be easily retrieved. However, the displays should not be immediately displayed unless the user requests them.

Providing on-screen support for interface management may reduce interface management workload. For example, if there is an alarm for a specific component, the HSI might provide an icon on the VDU screen that, upon operator request, automatically retrieves the relevant equipment display, and/or reference to the specific alarm response procedure. Predetermined information groupings may also help to reduce interface management demands. For example, a specific alarm icon associated with every dynamic system/equipment/component could provide the path for the user to link directly to the source display page of the generating alarm.

⇒ 4.1.3.1.3-8 To be effective, sufficient display area should be provided for users to display needed information in parallel and to minimize the need for navigation.

There are advantages to limiting the number of VDUs in a control room from a design perspective. Fewer VDUs (or more properly less display area) mean smaller control rooms, more simplicity since there are fewer HSIs to integrate, less cost for equipment, and a lower maintenance burden. However, the advantages of fewer VDUs may not be justified when it is not consistent with how the HSIs are used. Fewer VDUs can increase the time operators spend navigating among displays (especially during emergencies), and considering the likelihood that during emergencies, operators may think that they do not have time to navigate among displays. Thus, the advantages of fewer VDUs may be offset by the increase in workload associated with navigating for information access.

By increasing the amount of available display area, in size, resolution, and quality of VDUs, operators can display more information at any one time. This reduces the demand to remember information from one display page to another and reduces the need for navigation tasks to retrieve and manage information. With additional display area, operators can also have the opportunity to use some VDUs as spatially dedicated displays. They can monitor overview displays or specific information, such as parameter trends, that may be important to the current ongoing task.

Determining the appropriate amount of display area should include:

- Control room organizational layout for appropriate viewing by appropriate personnel
- Critical tasks required and information retrieval under abnormal conditions
- Determining the number of operators, supervisors, and other personnel that will need access to VDUs
- Determining the information that will be needed in parallel by operators
- The arrangement of information within display pages
- The arrangement of pages within the display hierarchy
- The means used to access information
- Coordination of activities among crew members

Regarding group activities, some displays could be shared by multiple users at a workstation, which may reduce the total number needed depending on the scheduling of tasks. Alternatively, additional display devices may be needed to present group-view displays to support communication and coordination among personnel. Overlay windows could be useful in presenting data that is needed for a short period of time. Clicking on a navigation cue would activate the overlay window. Once the data in the overlay window is read and evaluated, the window is closed, which would provide the operator with a full view of the display format.

4.1.3.2 Display Design for Task Performance

While monitoring and handling disturbances are important activities, plant personnel spend most of their time engaged in more routine tasks, such as conducting surveillance activities and performing maintenance. Some of these tasks can be supported by displays that organize information differently than is found in system-oriented displays.

This section addresses the development of displays to support task performance. Task based displays are made up of information presented in a variety of forms, including system mimics, trend displays, informational lists, etc. Their defining characteristic is that the specific information presented in the display and its organization are centered on task requirements. It should be noted that computer-based procedures are a form of task-based display. When the task requiring display support is highly composed of procedures, then the guidance in the computer-based procedure section should be used (see Section 4.5).

The task display guidance section is organized into two parts. The first addresses the selection of tasks to be supported by task-based displays. The second addresses design of task-based display pages.

4.1.3.2.1 Task Selection

Plant personnel perform many types of tasks for which task-oriented displays could provide support. However, it is not practical to develop specific displays for every conceivable task. The guidance provided below can be used to help identify the tasks for which task-based displays may be developed, i.e., the tasks that may be supported by task-based displays to improve efficiency and decrease human error.

The design team should make the selection of displays with input from final users, e.g., operators, technicians and maintainers, because they are familiar with and regularly deal with the complexities of actual task performance.

⇒ 4.1.3.2.1-1 Tasks requiring highly-reliable human performance should be considered for task-based display support. These tasks are mostly:

- *Important to nuclear or personnel safety*
- *Important to maintaining power generation*
- *Important to equipment protection for significant items*
- *Time critical*
- *Complex*

Task-based displays can support reliable performance by reducing the demands on human memory to remember information from one display to the next and by reducing the distracting effects of performing navigation tasks. Some examples of the types of general tasks that might be considered as candidates for task based displays include:

- Starting up and shutting down the plant
- Changing system configurations
- Changing operational mode
- Keeping logs
- Following of plant procedures
- Following surveillance and test procedures
- Performing maintenance operations

Specific examples include:

- Letdown and makeup for a PWR
- RCP operations for a PWR
- Feed and bleed for a PWR
- Suppression pool cooling for a BWR
- Monthly emergency power testing

⇒ 4.1.3.2.1-2 Tasks that have high interface management and navigation demands (if performed without a specialized display) should be considered for task-based display support.

If the number of tasks falling into this category is high, then the next guideline (4.1.3.2.1-3) should be used to help select the tasks most in need of task-oriented dedicated display support.

⇒ 4.1.3.2.1-3 Tasks for which improved efficiency is desired should be considered for task-based display support.

Task-based displays can support efficient performance by reducing the time taken in retrieving supporting information to perform a task. Candidate tasks falling into this category are ones that are performed frequently and/or ones that take a long time to perform. Maintaining operating logs is an example of this type of task.

4.1.3.2.2 Task-Based Display Design

As noted above, task based displays can use information presented in a variety of forms, including system mimics, trend displays, informational lists, etc. Depending on the task demands and the type of format used, some of the guidelines below may not be applicable. Thus the designer should use those appropriate to each specific task-based display design.

⇒ 4.1.3.2.2-1 The task display requirements should be identified.

Once the contending tasks have been evaluated and selected, the requirements for those displays should be identified. Task-based displays are obviously closely coupled to the requirements of the task. This information can come from established procedures and formal or informal analyses. If the tasks to be supported do not have procedures, or have not been analyzed, then information for establishing display requirements can be obtained from manuals, training materials, and from interviews with appropriate personnel or subject matter experts.

In the following discussion, the word "task" is used to mean the whole task, as well as, the steps that are followed to complete the task.

The specific requirements for any one task are unique, but the task elements needed to design the displays include:

- Information indicating that the task is needed
- Necessary preconditions
- Task instructions and sequences
- Plant information needed to perform the task
- Cautions and warnings
- Task-related alarms
- Controls needed to perform the task
- Expected and actual feedback from system/equipment/component
- Task termination criteria

⇒ 4.1.3.2.2-2 The system should provide notice of when the task is required.

Some tasks are made necessary by plant conditions. When this is the case, the system should monitor those conditions and the HSI should notify when the user should perform the task, e.g., by providing an alarm or reminder to signal the need for the task to be started.

⇒ 4.1.3.2.2-3 The display should indicate the conditions that must be met before a task or step can be undertaken. Information about preconditions should be displayed so that users will be informed before starting the task or step.

Information given in other locations may be overlooked, or require additional actions to retrieve it, which may be distracting and time consuming. Further, if conditions are implied, users may easily miss or misinterpret them.

Where the actions taken may have significant consequences, interlocks for preconditions should be considered. These interlocks should be indicated on the task-based display.

⇒ 4.1.3.2.2-4 Where the task is proceduralized, instructions and sequences should be provided for performing the task or step.

Explicit instructions may not be necessary for all tasks. However, they can certainly aid user performance, especially when the users may not be fully familiar with the task. The instructions should include what conditions need to be met and what decisions must be made. Computer assistance for decision-making guidance should be considered. For example, if the task step requires that the user determine if the pump flow is below a certain flow rate, then computer support for making that determination should be provided.

If a task requires actions to be executed in a specific sequence, then the display should provide assistance by indicating the required step sequence. The display can also provide indication of which ones have been completed, the step in progress, and an indication of the next step as well as the quantity of remaining steps before sequence termination can occur.

⇒ 4.1.3.2.2-5 Specific plant information needed to perform the task should be displayed in the order and organization in which it is needed, to minimize interface management demands.

Where available to the computer-system, any information needed to perform a task or step should be displayed at the time the information is needed or requested. The information should be presented in a format and at the level of detail needed by the task, e.g., status, state, parameter value, trend, etc.

⇒ 4.1.3.2.2-6 Cautions and warnings related to task performance should be displayed when the information is displayed to the user. Cautions or warnings should be distinctively presented, so that they are easily differentiated from each other and from other display elements.

Displaying warnings and cautions at the same time as their associated instructions will help ensure that users read the information. Information provided elsewhere may be overlooked, or may require retrieval by distracting and time-consuming actions.

⇒ 4.1.3.2.2-7 Any alarms related to the task or step that may impact the user's ability to perform, or may alter the actions the user should take, should be presented in the task-based display.

Alarms reflect conditions in which functions, systems, or components may not be in a condition where they can support task performance. Providing this information with task related information support the user's task performance. Such alarms or warning may already be displayed in the preconditions for the task. However, even if they are not critical to successful completion of the task, they should be repeated at the concerned step.

⇒ 4.1.3.2.2-8 If soft control capability is provided, controls needed to perform the task or step should be directly available in the display.

When controls are simple, it may be possible to include them directly in the display. However, the design of the controls may require a considerable amount of information in itself, and therefore, may not be easily integrated into the task display. In such cases, the soft control should be immediately retrievable from the task display at the point it is needed. The retrieving of the soft controls should be indicated in the task-based display.

Whether directly integrated into the task display or immediately retrievable from it, the controls should be designed using the guidance in Section 4.3, Soft Controls, so that appropriate control design features are included, such as providing feedback on any actions the user takes.

⇒ 4.1.3.2.2-9 When the task or steps requires operating systems/equipment/controls, then expected and actual feedback should be provided in the display

When the task involves operating systems/equipment/controls using manual controls or soft controls, then feedback from the process, if available, should be provided. For example, the effect of opening a valve manually should be indicated on the display. This may be accomplished by selecting the appropriate process variable (such as flow) to be displayed. The expected feedback should be included in the task display instructions. This will assist the user in performing the task efficiently and safely.

If process feedback is not available, then the display should clearly indicate the next available instrument to be used for confirming the action. The instrument needs to be confirmed in working order by the user before the task should be allowed to begin.

⇒ 4.1.3.2.2-10 The task display should provide indication when a task or step can or should be terminated.

When the computer system can monitor task termination criteria, the user should be informed when the task is complete or when actions can be stopped.

⇒ 4.1.3.2.2-11 The information presented in the task display should be conducive to efficient task execution.

In many cases, the accomplishment of tasks will require multiple pages of display. It is likely that some user confirmation in the display will be required, enabling task display progress. It is important that the task, the steps and the sequences of operations and expected feedback events be presented as clear and as grouped as possible.

For example, if a task requires iterative adjustments, such as adjusting zero, offset and linear gain in a speed loop, then the adjusting parameters together with the feedback variables should be presented in a single page. The user should not have to navigate any pages to display the parameters and make the adjustments.

⇒ 4.1.3.2.2-12 The task display should provide support for tracking task progress.

When a task has defined steps and the computer system can monitor their completion, the user's progress should be tracked and feedback provided. This will facilitate the user's ability to verify that all task-required actions have been completed.

⇒ 4.1.3.2.2-13 The overall structure of the task elements (alarms, information, instructions, controls, etc.) reflecting the task requirements should be:

- *Sequentially structured when the task steps need to be completed in a specific order*
- *Structured into groups of parallel information when no specific sequence is needed*

Some tasks require steps to be taken one at a time, e.g., the user does A, then B, then C, and so on. In such cases, the display should provide all the information, preconditions, warnings, etc., needed for each step.

Some tasks are not highly structured. Instead of sequential order, information can be structured and recalled from the display according to ways in which users will approach the task. If no structure can be anticipated, the task information can be combined into one or more display pages and organized according to general grouping principles, e.g., organized by function, system, component, frequency of use, etc. (see Section 4.1.4.2, Organization of Information). In this way the user has all the information assembled and can take actions in the order that are appropriate at the time they perform the task.

⇒ 4.1.3.2.2-14 When a task requires more than one display, onscreen navigation aids should be provided to easily access the displays.

A task may require more than one display for many reasons, e.g., that task's length or complexity is such that all the needed steps or supplemental information cannot fit on one display, (such as additional details or instructions). Navigation between related task displays should be made easy, and should require minimal attention. Section 4.2 provides guidance on navigation.

4.1.3.3 Display Design for Teamwork, Crew Coordination, and Collaborative Work

A nuclear plant crew works as a team. They share information and perform their tasks in a coordinated fashion to achieve operational goals and safe plant operation. Several crewmembers may perform a task cooperatively from one location; while in other cases, a control room operator may have to coordinate tasks with a user in a remote location.

The guidance provided in this section addresses the use of computer-based displays to support teamwork. They are hereafter referred to as computer-supported cooperative work displays or "CSCW displays." The key elements of CSCW functionality include:

- Providing a common frame-of-reference
- Supporting awareness of the activities of others
- Availability of collaborative workspaces
- Availability of tools for team interaction with CSCW displays

When considering the implementation of CSCW displays, it should be recognized that it may require specific new displays as part of the overall information display system, or may be implemented as added functionality onto the other monitoring/situation assessment, or task-based displays already available.

Prior to presenting the guidance, two additional considerations should be addressed. First, displays supporting teamwork should have the capabilities to include any changes to crew organization or staffing. Second, the provision of CSCW displays should be capable of being coordinated with any changes to control room layout that may be planned and the resources that may be available, such as wall panel displays and workstations.

⇒ 4.1.3.3-1 Displays should include functionality to support teamwork when the following conditions exist:

- *There is a high need for users to work together on the same task/problem (e.g., complex diagnoses of plant failures)*
- *Face-to-face interaction/collaboration is difficult due to the arrangement of the workplace and the demands of concurrent tasks (e.g. multi-location coordinated activities)*

The following tasks are candidates for the application of CSCW displays. These tasks may be applicable to activities performed by operators within the CR (e.g., from separate workstations or consoles), or activities performed by CR personnel in collaboration with personnel at remote facilities:

- Shift turnover
- Assessing plant condition – it may be necessary for the crew to review the plant displays in a collaborative manner. This may involve pointing to or highlighting items of interest, annotating existing graphical displays, and searching/retrieving information in a collaborative manner.
- Collaborative control actions – The coordinated effort of multiple operators can benefit from the means provided by CSCW displays. Two or more users may access the same schematic view of a plant system from separate workstations to coordinate a control action, such as a valve line up, by providing inputs to the display in a coordinated and structured manner. This is analogous to multiple operators performing the control actions on different portions of a hardwired mimic display. Presenting this control activity on a CSCW display provides the crew with an opportunity to more closely observe control actions and detect mistakes, if they occur. Collaborative control may also be applicable to control actions performed by personnel in different locations in the plant, such as CR personnel working with personnel at a local control station.
- Data recording/form filling – Data entry and data recording tasks that require input from more than one crew member, may be accomplished via CSCW displays. For example, a maintenance control form requiring input from the shift supervisor and operators, who are either in the CR or out in the plant, may be completed via a display in which crewmembers complete those portions that are relevant to their responsibilities. Another application may be the annotation of schematic displays to record important operational or maintenance information.

Supporting communication and collaboration may also be beneficial to other personnel in the CR by allowing them to more easily monitor the communication and collaboration activities of the operators.

⇒ 4.1.3.3-2 A common frame of reference for plant status should be provided.

A high-level overview display, such as that discussed in Section 4.1.3.1.2, can serve as a common frame-of-reference for the crew. As was recommended in the guidance for this display, it is desirable, if possible, that it be presented as a group-view display (i.e., as a wall panel or large display visible from anywhere in the control room). In addition to supporting crew interaction, the overview display can provide a common frame of reference by indicating current status and activities, especially for activities such as shift turnover.

⇒ 4.1.3.3-3 A user-addressable frame-of-reference should be provided if users have to collaborate to perform an activity.

While overview displays provide a high-level frame-of-reference that should be permanently in view, it is equally important that the display system support user-addressable frames-of-reference. That is, CSCW displays should have a workspace area in which they can put display images or pages that they wish to bring to the attention of other crew members. Attempting to coordinate activities when looking at different displays can be very difficult. If users need to collaborate on some aspect of a task, they should be able to view the same information, whether locally or remotely. This will enable multiple personnel to work on the same task without leaving their workstation. Space allocation will need to be coordinated when more than two displays are used in collaborative work.

While it is ideal if such a space is provided in a group-view display, it can also be presented at individual workstations. This type of functionality can also support the coordination of situation assessments and actions (where appropriate) at different locations, e.g., between the main control room, local control stations, Technical Support Center (TSC), and the Emergency Operations Facility (EOF).

⇒ 4.1.3.3-4 A CSCW display should support each crewmember's understanding of the others' activities. This can be accomplished by providing information for common team activities, such as in shift turnovers and for maintenance activities.

CSCW displays are intended to assist crewmembers in maintaining awareness of the actions of the other crewmembers, so that activities can be coordinated and users can monitor each other's activities to provide insight, guidance, or correct potential errors, or promptly lend support when needed. This assistance may take many forms, including providing information about users' locations in the display system, locations in ongoing procedures, and actions being performed using soft controls.

The display can serve as a focal point for discussions of the current plant state similar to the way that operators walk through the panels of conventional control rooms during shift turnover. It may also serve to orient other personnel, while causing minimal disruption to personnel on duty. For example, during plant upsets the overview display may allow personnel, such as additional technical support, NRC inspectors, and plant managers to follow changes in plant conditions while causing minimal disruption to ongoing activities. Overview displays (without control capabilities) may also be placed in remote facilities such as the TSC and the EOF for this purpose.

On-line logs of high-level activities that identify who is working on what and can be monitored by all users are valuable in coordinating activities, especially for users not co-located. The logs can display the status of activities. This type of display can support shift turnover as well.

There are many benefits that an overview display brings to collaborative and team oriented work. For example, a group-view display may be used to allow operators verifying a plant system line up performed by another operator. This allows others to monitor the control actions and feedback indications for system anomalies or miss-operation. Errors can occur when operators believe that a control system is in one operating mode and thus behave according to a set of rules, when in reality it is in a different mode and a different set of rules should be applied. Crew coordination can be enhanced by providing displays that convey the activities and statuses of human and machine controlling agents, and by providing positive indication of current operating modes.

One approach to using displays to support user awareness of the activities of other crewmembers is described by Tani, Masato, Yamaashi, Tanikoshi, and Futakawa (1994). The system includes a large group-view display, which presents an overview of plant status using a mimic format. Each crewmember can operate a separate cursor on this group-view display via a mouse located at their individual workstation. By moving their mouse over an item of interest on the group-view display and then pushing a "select" button, users can cause more-detailed information to be retrieved and presented via a smaller VDU located at their individual workstations or in a designated location of the group-view. This group-view display supports crewmembers in maintaining awareness of each other's activities.

A group-view display can also present checklists to tell personnel where they are in a work process, what has been accomplished, what remains to be done and what should be done next. Coordination may be further enhanced via these displays if they identify responsible individuals, or provide timeline information.

⇒ 4.1.3.3-5 Supervisor workstations should provide the capability to access the same displays as those at operator workstations.

This capability can be accomplished by providing small windows on the supervisor's workstation that access the same displays as at other workstations. If such a display is provided, the supervisor could click on any one of the windows to enlarge the view for closer inspection. If windows are used they should be designed according to the guidance provided in Section 4.2, User-Interface Interaction and Management.

⇒ 4.1.3.3-6 A coding scheme or designation system should be used to identify users when they manipulate information on a group-view display.

Such a scheme can help make users aware of what other crewmembers are taking action.

⇒ 4.1.3.3-7 When multiple users have to work together on the same task, displays should provide a collaborative workspace.

A collaborative workspace is a display, or portion of a larger group display that is common to all users, on which an individual user can place information that can be viewed by all others.

⇒ 4.1.3.3-8 The display should provide tools that enable users to interact with the HSI or the plant. Other users should be able to infer information about the nature of the task and the specific actions taken by observing the HSI.

The display should allow personnel to observe a control action, such as the alignment of a fluid processing system. In this case, a mimic display, in which operators manipulate graphical objects, may provide more useful information to an observer than if the same task were performed via text commands on a keyboard. This is because the display conveys to the observer physical characteristics of the task, such as the type of valve being operated, and functional characteristics, such as the relationship of the valve to the overall piping system. This provides the observer with a better understanding of what action has been performed and its significance to the plant system.

To support collaboration, the HSI should provide a representation of the activity and the tools needed for coordinating actions. In conventional CRs, this is done by walking through the CR to examine various alarms and displays while discussing status and safety challenges. It is also done by reviewing mimic displays and other graphical representations of the plant for evaluating the involvement of specific system components. In computer-based control rooms, displays may be used as a focal point for these types of activities. If the displays are located where the team members can conveniently use them, then communication may be conducted as in conventional CRs.

⇒ 4.1.3.3-9 Display controls should prevent individuals from making changes to CSCW displays in ways that would reduce their usefulness to others.

Control of changes in a CSCW display, such as changing variables, their names, or their ranges, may lead to misinterpretation or confusion. Use of administrative procedures is one way to control changes that may be confusing or otherwise detract from personnel performance. Changes affecting configuration management of the HSI should be prohibited and prevented by appropriated system safeguards. Control actions preventing other users from interacting with the CSCW display should be regulated by an activity leader, such as a SRO.

⇒ 4.1.3.3-10 When multiple users have access to on-screen pointing devices (such as cursors) for interacting with the group-view display, features should be provided to manage access to the cursor and indicate current user.

A distinct coding method should be used to indicate that the cursor is in use and to identify the user.

⇒ 4.1.3.3-11 When transferring information between individual displays and the CSCW displays, the information should be presented promptly and with minimal delay.

When a sender transfers information to the CSCW display, a significant lag could be an obstacle to the communication of ideas. This is especially true if other modes of communication, such as verbal, are available and significantly lead or lag behind the CSCW display.

4.1.4 Display Pages

Display pages are defined sets of information presented as a single unit to support particular user tasks. Typical display pages may combine several different formats in a single video display or window, such as combining bar charts and numeric displays within a representation of a piping and instrumentation diagram. The content of a display page, i.e., the formats that make up the page, is usually intended to provide an organized view of some aspect of the process. For example, a page may provide a high-level status overview of the primary system. Each display page typically has a label and designation within the computer system so users can access it as a single "display."

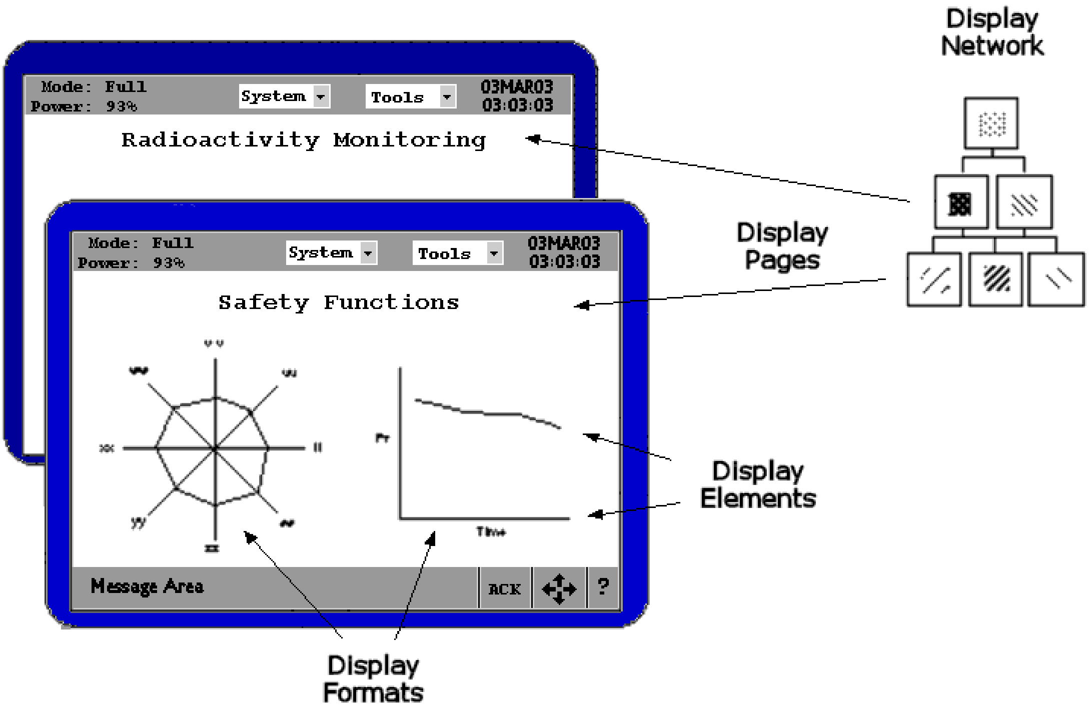


Figure 4-10
Characteristics of Information Display Systems

4.1.4.1 Identification of Information

⇒ 4.1.4.1-1 A title or header should be placed at the top of every display page, briefly describing the contents or purpose of the display.

If a system's displays all have common headers (containing, e.g., navigation buttons or general purpose tools), the identifying information for the page should be placed at the top of the area containing the unique information for that particular page. There should be a distinct separation between the title and the body of the page. If a display device is dedicated to a particular page, the title may be a label mounted on the display device itself.

⇒ 4.1.4.1-2 Every display page should have a unique identification to provide a reference for use in requesting the display of that page.

The page identification could be its title, and/or an alphanumeric code or abbreviation that is prominently displayed in a consistent location. It should be short enough (3-7 characters) and/or meaningful enough to be learned and remembered easily. Displaying both a title and a code can be useful. The title describes the purpose of the display, while the code might indicate its position in a hierarchy. Showing both allows users to learn the codes for frequently used pages, so that they can call the displays up directly via keyboard entry of the codes (if this interaction is supported).

⇒ 4.1.4.1-3 Where displays have several levels of titles (and/or labels), the system should provide visual cues to aid users in distinguishing among the levels in the hierarchy.

Character size variation and indentation are two common methods of expressing a hierarchy. Bolding, underlining and letter case are also frequently used, but conventions for their use have not been well established.

⇒ 4.1.4.1-4 General labels and row/column labels should remain along the edges of the display.

Display formats such as tables, lists, forms, and graphs may be scrollable. When this capability is available, all labeling information should be preserved.

⇒ 4.1.4.1-5 When displays are partitioned into multiple pages, function/task-related data items should be displayed together on one page.

Relations among data sets should appear in an integrated display rather than partitioned into separate display pages. When dividing a display, it is important to keep task-related data together to avoid (1) requiring the user to frequently switch back and forth between pages when performing the task or (2) requiring users to remember information from one page while looking at another.

⇒ 4.1.4.1-6 Users working with multipage displays should be provided with a page location reference within the display sequence.

Each page of a multipage display sequence should be numbered. Typically, the phrase “page x of y” is used for this purpose. A recommended format is to identify pages by a note immediately to the right of the display title. Leading zeros should not be used in the display of page numbers.

⇒ 4.1.4.1-7 Users viewing a portion of a larger display should be provided with an indication of the location of the visible position of a display (frame) in the overall display.

A graphic indication of the frame’s location in the overall display will provide a visual context to help a user maintain a conceptual orientation between the visible part and the whole display. For example, in a corner of the frame, the computer might show a rectangle representing the overall display, in which a smaller rectangle is placed to indicate the position and extent of the currently visible portion of that display. Sectional coordinates should be used when large schematics must be panned or magnified.

4.1.4.2 Organization of Information

⇒ 4.1.4.2-1 General HSI features (e.g., a data display zone, control zone, or message zone) should be displayed in consistent locations from one display to another.

Consistent display screen organization will help establish and preserve user orientation. Display formats should be consistent with accepted usage and existing user habits.

⇒ 4.1.4.2-2 The HSI functional zones and display features should be visually distinctive from one another, especially for on-screen command and control elements (which should be visibly distinct from all other screen structures).

Different display areas can be separated by blank spaces, lines, or some other form of visual demarcation.

⇒ 4.1.4.2-3 Information on a display should be grouped according to principles obvious to the user, e.g., by task, system, function, or sequence, based upon the user's requirements in performance of the ongoing task (see Table 4-3).

Table 4-3 provides grouping principles and examples of their appropriate uses. Grouping conventions should be used consistently within sets of displays of a particular type. For example, grouping by function may take precedence over other grouping methods for mimic-type plant displays. Grouping for data comparison may take precedence over other grouping methods for displays that present only text. Since users' tasks can vary, advanced HSIs should provide the user with the flexibility to group information by alternative grouping principles to reflect changes in task requirements (e.g., to resort a sequence according to the functions involved).

⇒ 4.1.4.2-4 Information needed by the operator to accomplish a given task should be presented so that it is immediately seen to be related.

To minimize the disadvantages of divided attention, the number of attention shifts should be minimized, both within a display page and between them. Information that must be compared or mentally integrated will be more readily associated if it is

- presented in the close spatial proximity – if possible, the information items should be contained in the same display page and grouped together
- color coded similarly – this is particularly important if the information items cannot be placed in close proximity
- represented by similar physical dimensions – for example, related quantities would all be represented by the height of a line, rather than having some be represented by the area of a shape
- presented using similar presentation formats – for example, either analog or digital

⇒ 4.1.4.2-5 When information is grouped on a display, the groups should be made visually distinct by such means as color blocking or padding or separation using blanks or demarcation lines.

⇒ 4.1.4.2-6 A uniform nondistracting background color should be used with a hue/contrast that allows the data (foreground) to be easily visible and which does not distort or interfere with the coding aspects of the display.

Patterned backgrounds should be avoided. Background color can influence the way a user perceives a color symbol (e.g., shapes and lines). When a color is surrounded by another color, the surrounding color can change the appearance of the enclosed color. For example, green on a yellow background will appear more blue than the same shade of green on a blue background.

Different colored backgrounds may be used as a coding method to meaningfully group information, provided that colors are chosen to maintain good contrast and legibility. One drawback to using different colored backgrounds is that color coding schemes (e.g., for valve position, equipment status, alarms, or piping), which are difficult to optimize for a single background color, may be impossible to optimize for multiple background colors.

4.1.4.3 Clarity of Presentation

⇒ 4.1.4.3-1 Displays should present, in an immediately usable form, only the data needed for the task they are designed to support; data irrelevant to the task should not be displayed, and extraneous text and graphics should not be present.

Displayed information should be tailored to user needs; no calculation or transformation of the displayed data should be required. See Section 4.1.3, Display Functions.

⇒ 4.1.4.3-2 Redundancy in the presentation of information items should be limited to cases where needed for backup or to avoid excessive movement.

⇒ 4.1.4.3-3 Displays should be as uncluttered as possible.

While display clutter can be a problem, designers should consider the tradeoff between distributing information over many less-dense displays that require a lot of navigation and packing displays with data potentially resulting in a crowded appearance but requiring less navigation.

Techniques that support mental integration of displayed items, such as grouping related items close together, using mimics to organize information, selected use of demarcation lines, may enhance performance while actually increasing display density. Also, it has been found that displays which initially appear crowded to operators can become well liked and effective in supporting performance as operators gain experience with them.

⇒ 4.1.4.3-4 Displayed information which temporarily overlays and obscures other display data should not erase the overlaid data.

Overlay displays that are generated by the display system can allow additional information to be shown when needed and then removed to reduce visual clutter. Overlays are acceptable when they improve the user’s interpretation of displayed information by giving additional information about an object (e.g., the past values of a parameter, or the control knob of a valve). They should not distract the user or interfere with the observation of displayed information.

4.1.4.4 Coding and Highlighting of Information

Coding and highlighting of information in displays is used to exploit people’s natural sensitivity to physical similarities or differences and to changes; these techniques take advantage of the fact that users tend to

- readily identify elements with characteristics that differ from those of other elements
- perceive as related elements with similar characteristics
- notice changes in the physical characteristics of elements

Because these processes are ‘automatic,’ coding and highlighting, when properly applied, can lessen the mental effort associated with

- directing attention to information that is noteworthy
- searching for information of a specific type
- comparing displayed information to limits or criteria
- getting feedback for actions

Highlighting is most effective when used sparingly, adding emphasis to a display that is relatively uniform in appearance except for just a few highlighted items. For some purposes, location coding (e.g., displaying important items consistently in a particular location) might be a sufficient means of highlighting, as when an error message appears in a space otherwise left blank. However, auxiliary codes may still be needed to highlight important items, even if they are positioned consistently. For example, line coding by color or bolding might be used to highlight displayed paths, and/or the boxes or other graphic elements representing displayed states. Guidelines on using visual characteristics of display elements for highlighting or coding information are given in Section 4.1.6.8.

⇒ 4.1.4.4-1 Highlighting should be used sparingly.

All methods of highlighting become less effective the more they are used. A good rule of thumb is to highlight less than 10% of the presented information at any time.

⇒ 4.1.4.4-2 The prominence of graphic features should reflect the importance of the information.

The most conspicuous features of a graphic display should be those aspects of the representation that are most important (i.e., the most eye-catching part of a display should be that which the operator is expected to need to see first when the display is called up).

⇒ 4.1.4.4-3 Coding and highlighting should not interfere with the readability of displayed information nor delay its presentation.

For example, capitalization should not be used to emphasize extended passages of text since it reduces readability. Similarly, if a different background color is used for emphasis, it m must be chosen to maintain adequate contrast with the color of the text, or legibility may be diminished.

⇒ 4.1.4.4-4 Highlighting should be removed if it no longer has meaning.

For example, highlighting that is used to indicate a special condition (e.g., a variable outside of its normal operating range) should be removed when the special condition no longer exists (e.g., when the variable returns to its normal operating range).

⇒ 4.1.4.4-5 When highlighting is not sufficient to indicate the specific nature of some outstanding or discrepant feature that merits attention by a user, supplementary text should be displayed to make it clear.

For example, a flow diagram for process control might include a current advisory message (e.g., 'Possible Pressure Valve Failure') as well as appropriate graphic indications of a problem.

⇒ 4.1.4.4-6 Coding of important information should incorporate redundancy.

All coding techniques have certain inadequacies, which may be intensified under adverse viewing conditions. It is often necessary to use redundant coding to reduce the probability of errors. For example, a red color code may already identify a certain alarm as high priority, but it is possible for a VDU to fail, such that this color is indistinguishable from some others; redundant coding may involve use of text or characters, flashing of the alarm light, an increased alarm indicator size, and/or an audible tone.

⇒ 4.1.4.4-7 Coding should be provided when a user must distinguish rapidly among different categories of displayed data.

Graphic coding methods (e.g., symbols, boxes, underlines, use of color as a background to grouped items) can greatly aid users' utilization of data.

⇒ 4.1.4.4-8 Meaningful or familiar codes should be used, rather than arbitrary codes.

While the meanings of some coding methods must be learned (e.g., shape and auditory signal coding), other codes have inherent meaning (e.g., a higher brightness or flash rate 'naturally' conveys greater importance). Coding schemes should not conflict with 'natural' associations.

⇒ 4.1.4.4-9 Consistent meanings should be assigned to codes across user interfaces in the plant (including existing interfaces).

When coding is not consistent, the user's task of display interpretation may be made more difficult than if no auxiliary coding were used at all. Typically, an analysis of the coding methods already in use at the plant should be performed. Where there are inconsistencies in the plant or in the new design, they should be resolved or justified, and the results should be documented. As a practical matter, the same color may be used to mean different things in different contexts. For example, red may mean 'high priority' in an alarm display and 'fire suppression' in a piping & instrumentation diagram. This will not necessarily cause confusion, as long as the context in which the color code is being used easily recognized by users.

⇒ 4.1.4.4-10 A characteristic used for coding should have only one meaning.

If one coding method is used to show too many things simultaneously, it is possible for users to be confused about the applied meaning. For example, if flash coding is used with alarms to indicate alarm status (i.e., unacknowledged, acknowledged, cleared), it should not also be used to indicate alarm priority or the need for user action.

⇒ 4.1.4.4-11 Highlighting should be clear and easily recognizable and should attract the users' attention.

Highlighting should not interfere with the readability of the underlying data. Highlighting should not be too bright to look at or so dense that it obscures the data. It should not interfere with color coding or any other type of coding (see Guideline 4.1.4.4-3).

⇒ 4.1.4.4-12 Inverse video should be used only to show the selection of on-screen items or to highlight small segments in a larger block of text.

The conventions used in typical commercial computer applications have accustomed users to this method of coding.

4.1.5 Display Formats

Display format refers to methods of information presentation consisting of an organized arrangement of smaller display elements. They are the most significant "unit of analysis" of the information system because the selection of format greatly influences the ability of users to easily and correctly understand the information presented. Display formats range in complexity from simple, such as data fields and tables, to more complicated forms, such as configural and mimic displays. The ability of computer graphics to portray an essentially limitless set of novel graphic forms has offered great possibilities to provide users with enhanced representations of the plant. Most of the major types of displays are addressed in these guidelines.

The choice of a display presentation format, e.g., table, graph, or flowchart, should be governed by:

- the nature of the information to be conveyed (e.g., verbal/numeric, qualitative/quantitative, discrete/continuous)
- the users' information requirements, as determined by their tasks (e.g., comparison with a standard or with other values, judgments about the relationships among variables, evaluation of a trend over time)

Information can be broadly classified as either verbal or numeric (i.e., words or data). Examples of display formats for verbal information are given in Table 4-4.

Table 4-5 illustrates some display formats for numeric information and gives brief notes on their appropriate use with respect to these considerations (i.e., data type and task).

A means for judging the suitability of various data display formats for particular data types and uses is described in Frey, Sides, Hunt, and Rouse (1984); it is an abbreviated version of a more formal treatment of display format selection in Danchak (1981). Table 4-6 is adapted from Frey et al. To use the table, one first characterizes the type of data to be displayed in terms of the number of dimensions, variables, and samples involved.

Number of dimensions – how many dimensions (or different units) are to be displayed? For example, a display showing one or more temperature values is unidimensional; a display including pressure values and temperature values is duodimensional.

Number of variables – how many variables are involved? Displays may depict a single variable (univariate), a small set (fewer than six) of variables (limited multivariate), or a larger number of variables (multivariate). For example, a display showing steam generator pressures in a four-loop plant would be unidimensional and (limited) multivariate.

Number of samples – how many samples of the variable(s) are needed? Tasks may require a single (discrete) variable value, a limited series of values (defined as from two to fifteen), or a series of more than fifteen values.

Next, one characterizes the general type of use that is to be made of the displayed data; i.e., are the tasks or judgments involving the data quantitative or qualitative? The use of quantitative data is further characterized as exact, approximate, or relative (i.e., involving a comparison). Qualitative uses are characterized as status indication, prediction, or pattern recognition.

The table gives a three-point rating of the suitability of each of the display formats for the data and task characteristics.

Guidance provided here addresses several classical display formats; novel formats can be acceptable if their support for the users' tasks can be demonstrated. Since tasks can vary, advanced HSIs should provide the user with the flexibility to display information in alternative formats that reflect changes in task requirements.

4.1.5.1 Continuous Text Displays

This format consists of alphanumeric character strings (e.g., words and numbers) arranged in sentences and paragraphs, e.g., a textual description of a plant system. Reading extended text passages on a display device can be difficult. Typographical techniques (indentation, white space between blocks of text) can help improve readability. Designers should also be alert for opportunities to use more efficient information presentations, such as list formats for presenting a series of items or tables for parameter values.

The guidance below applies generally to textual material. Guidance for the use of text in specific contexts that may have unique requirements (e.g., procedures or alarm messages) is given in the appropriate specialized sections of this document.

⇒ 4.1.5.1-1 A standard text display format should be used from one display to another.

⇒ 4.1.5.1-2 VDU displays of textual data, messages, or instructions should generally follow design conventions for printed text.

⇒ 4.1.5.1-3 Text to be displayed should be worded so that it is quickly and easily understood.

Reading text a on a VDU can be more difficult than reading printed material. Therefore it is especially important for displayed text to follow established good practices for clear written communication:

- The main topic of each sentence should be located near the beginning of the sentence.
- The text should be worded concisely to aid comprehension, but should not be cryptic. Omitting articles ('the,' 'a'), prepositions ('of,' 'by') and relative pronouns ('that,' 'which,' 'who') may save some space, but may also reduce understandability.

- Distinct words rather than contractions or combined forms should be used, especially in phrases involving negation. For example, ‘will not’ should be used rather than ‘won’t.’
- When words in text displays are abbreviated, each abbreviation (or acronym) should be defined in parentheses following its first appearance. An on-line dictionary of abbreviations for convenient reference should be available to users.
- Affirmative statements rather than negative statements should be used; i.e., the user should be told what to do rather than what to avoid. For example, “Start the pump before opening the valve” is preferred over “Do not open the valve before starting the pump.”
- Sentences should be composed in the active rather than the passive voice. Sentences in the active voice will generally be easier to understand. For example, “Press RESET to clear the screen” is preferred over “The screen is cleared by pressing RESET.”
- When a sentence describes a sequence of events, it should be phrased with a corresponding word order. Temporal order is clearer. Reverse order may confuse a user. For example, “Start the pump before opening the valve” is preferred over “Before opening the valve, start the pump.”

⇒ 4.1.5.1-4 When a user must read continuous text on line, at least four lines of text should be displayed at one time.

Four lines of text is the minimum that should be displayed when the reading material is simple in content. If the content is more complex, or if a reader will need to refer frequently to previous material, then more lines of text should be displayed.

⇒ 4.1.5.1-5 Continuous text should be displayed in wide columns, containing at least 50 characters per line.

When space for text display is limited, a few long lines of text rather than many short lines of text should be displayed. Line lengths of less than 50 characters result in slower reading times, but line lengths from 50 to 80 characters do not produce differences in reading time.

⇒ 4.1.5.1-6 In display of textual material, words should be kept intact, with minimal breaking by hyphenation between lines.

⇒ 4.1.5.1-7 Conventional punctuation should be used in textual display.

⇒ 4.1.5.1-8 Consistent spacing between the words of displayed text should be maintained, with left justification of lines and ragged right margins. A minimum of one character width (capital N for proportional spacing) should be used between words.

Reading is easier with constant spacing, which outweighs the advantage of an even right margin achieved at the cost of uneven (nonproportional) spacing. Uneven spacing is a greater problem with narrow column formats than with wide columns. Uneven spacing handicaps poor readers more than good readers. Full justification slows reading time and should only be employed if it can be achieved by variable spacing, maintaining constant proportional differences in spacing between and within words, and consistent spacing between words in a line.

⇒ 4.1.5.1-9 A minimum of two stroke widths or 15 percent of character height, whichever is greater, should be used for spacing between lines of text.

The specified spacing is in addition to the space used for uppercase accent marks or for lower case descenders of characters.

⇒ 4.1.5.1-10 Displayed paragraphs of text should be separated by at least one blank line.

⇒ 4.1.5.1-11 When tables and/or graphics are combined with text, each figure should be placed near its first citation in the text, preferably in the same display frame.

Users may not bother to find and look at a figure if it is displayed separately from its citation in the text. As an exception, if a figure is cited at several points in the text, then it might be desirable to allow optional display of the figure at user request, perhaps as a temporary window overlay at each point of citation. Also, if a figure is cited at several points in printed text, and particularly if that text may be accessed at different places by its readers, then it might be desirable to group figures consistently at a particular location, such as at the end of each section.

⇒ 4.1.5.1-12 When a line is placed under an item to mark or emphasize it, the line should not impair the legibility of the item, e.g., by obscuring the descenders.

⇒ 4.1.5.1-13 Within a text file or table, the use of a different font style should be preferred over the use of a different size for highlighting information.

It is often not possible to introduce into displayed text differences in type size large enough to be readily discernable.

⇒ 4.1.5.1-14 When a special symbol, such as an asterisk, is used to draw attention to a selected item in alphanumeric displays, the symbol should be separated from the beginning of the word by a space.

⇒ 4.1.5.1-15 When a user must read lengthy textual material, that text should be available in printed form.

Reading lengthy text on an electronic display may be 20-30 percent slower than reading it from a printed copy.

4.1.5.2 Tables and Lists

A table is a display containing alphanumeric characters arranged by rows and columns. Tables are useful for presenting sets of corresponding information. They may also be used for displaying small sets of numeric data (although for large amounts of data, graphical techniques are more appropriate).

A list is a display containing alphanumeric strings arranged in a single column by rows. Presenting a series of items in a list (rather than in the context of a sentence) makes it easier to use the information. For example, compared with continuous text, lists make the number of items and the manner of their ordering immediately apparent, and are easier to search for needed information.

⇒ 4.1.5.2-1 Information should be organized in some recognizable logical order to facilitate scanning and assimilation.

If the data in the rows has order, the order should be increasing from left to right. If the data in the columns has order, the order should be increasing from top to bottom of the display. Items in lists should be arranged in a recognizable order, such as chronological, alphabetical, sequential, functional, or importance. Where no other principle applies, lists should be ordered alphabetically. It is the user's logic that should prevail rather than the designer's logic, where those are different.

⇒ 4.1.5.2-2 A A table should be constructed so that row and column labels represent the information a user has prior to consulting the table.

The left-most column should contain the labels for the row variables, and the top row should contain the labels for the column variables. When tables are used for reference, the reference item should be displayed in the left column, and the material most relevant for user response should be displayed in the next adjacent column.

⇒ 4.1.5.2-3 Each row and column should be uniquely and informatively labeled and should be visually distinct from data entries.

On multi-page tables, the heading should appear on all pages.

⇒ 4.1.5.2-4 Labels should include the unit of measure for the data in the table; units of measurement should be part of row or column labels.

If individual cells have differing units to correspond to traditional usage (e.g., some measures in feet, others in inches), the units may appear in the body of the table.

⇒ 4.1.5.2-5 Consistent column and row spacing should be maintained within a table, and from one table to another. Similarly, spacing between rows should be consistent within a table and between related tables.

As an exception, when columns are grouped under superheadings, extra space between superheadings may help, in order to emphasize that the columns under any single superheading are related.

⇒ 4.1.5.2-6 The spacing between columns should be greater than any internal spaces that might be displayed within a tabulated data item.

The columns in a table should be separated by enough blank spaces, dots, or by some other distinctive feature, to ensure separation of entries in the rows. When columns are not separated by vertical lines, the columns should be separated by at least two character widths.

⇒ 4.1.5.2-7 In dense tables with many rows, a blank line, dots, or some other distinctive feature (to aid horizontal scanning) should be inserted after a group of rows at regular intervals.

For many applications, it will suffice to insert a blank line after every five rows.

⇒ 4.1.5.2-8 The font and size of alphanumeric characters should be consistent within a table and between related tables.

An exception to this guideline is when a word or set of characters is highlighted by varying the typeface, for example, through the use of italics or a bold font.

⇒ 4.1.5.2-9 Columns of alphabetic data should be displayed with left justification to permit rapid scanning.

As an exception, indentation can be used to indicate subordinate elements in hierarchic lists.
In addition, a short list (of just four or five items) could be displayed horizontally on a single line, in the interest of compact display format, if that is done consistently.

⇒ 4.1.5.2-10 Columns of numeric data should be justified with respect to a fixed decimal point; if there is no decimal point, then numbers should be right justified.

⇒ 4.1.5.2-11 Arabic rather than Roman numerals should be used when listed items are numbered.

Arabic numbers are more familiar to most users, and require less interpretation than Roman numerals do. The advantage of Arabic numbers becomes greater when large numbers are used. Exception should only be made in those rare cases when it is conventional to designate the items by Roman numerals.

⇒ 4.1.5.2-12 Item numbers should begin with one rather than zero.

An exception may be made when zero is used in a coding scheme or hierarchical designation.

⇒ 4.1.5.2-13 When a list of numbered items exceeds one display page, the items should be numbered continuously in relation to the first item on the first page.

For example, items continued on the next page should be numbered relative to the last item on the previous page.

⇒ 4.1.5.2-14 Complete numbers should be displayed for hierarchic lists with compound numbers, i.e., repeated elements should not be omitted.

Implicit numbering may be acceptable for tasks involving perception of list structure. Complete numbering is better, however, for tasks requiring search and identification of individual items in the list.

⇒ 4.1.5.2-15 Lists should be formatted so that each item starts on a new line.

⇒ 4.1.5.2-16 When a single item in a list continues for more than one line, items should be marked in some way so that the continuation of an item is obvious.

A continued portion should not appear to be a separate item. Items might be separated by a blank space, or continuing lines within an item might be indented, or each item might be numbered or marked by a special symbol such as an arrow or bullet. Multiline items should ordinarily not be separated across pages.

⇒ 4.1.5.2-17 Where lists of items extend over more than one display page, the last line of one page should be the first line on the succeeding page.

This guidance applies to lists of items, not to lists of actions (as would be found in a procedure), where there is a possibility that repeating an instruction might result in it being done twice. Lists shown in computer-based procedures will have a 'check-off' capability.

⇒ 4.1.5.2-18 For a long list, extending more than one displayed page, a hierarchic structure should be used to permit its logical partitioning into related shorter lists.

⇒ 4.1.5.2-19 If a list is displayed in multiple columns, the items should be ordered vertically within each column rather than horizontally within rows and across columns.

⇒ 4.1.5.2-20 When lists or tables are of variable length and may extend beyond the limits of one display page, the user should be informed when data are continued on another page and when data are concluded on the present page.

For example, incomplete lists might be marked 'continued on next page,' 'continued,' or 'more.' Concluding lists might display a note such as 'end of list' or 'end.' (The notation 'page x of y' can also be used for this purpose.) As an exception, short lists whose conclusion is evident from the display format need not be annotated in this way.

4.1.5.3 Data Forms and Fields

A field is a space in a display containing data (e.g., the current value of a variable). Data fields are usually accompanied by and identifying captions or labels. A data form typically consists of a collection of fields and labels that are related in some way. For example, a form might contain all of the parameter values and other information associated with the status of a given system or with the carrying out of a task, labeled and arranged to be easily scanned.

Some forms contain data fields that accept input entered by the user; this style of interaction is addressed in Section 4.2.5.1.5, Forms.

⇒ 4.1.5.3-1 Data fields to be compared on a character-by-character basis should be positioned one above the other.

⇒ 4.1.5.3-2 The ordering and layout of corresponding data fields across displays should be consistent from one display to another.

⇒ 4.1.5.3-3 The format of a VDU data form should be similar to that of commonly used hardcopy source documents.

⇒ 4.1.5.3-4 When forms are used for data entry as well as for data display, the formats of these forms should be compatible.

⇒ 4.1.5.3-5 Clear visual definition of data fields should be provided so that the data are distinct from labels and other display features.

Distinctive visual characteristics such as borders and background colors should be used to delineate data fields.

⇒ 4.1.5.3-6 The label and the data display area should be separated by at least one character space.

⇒ 4.1.5.3-7 At least three spaces should appear between the longest data field in one column and the rightmost label in an adjacent column.

Where space constraints exist, vertical lines may be substituted for spaces for separation of columns of fields.

⇒ 4.1.5.3-8 When label sizes are relatively equal, both labels and data fields should be left justified. One space should be left between the longest label and the data field column.

⇒ 4.1.5.3-9 When label sizes vary greatly, labels should be right justified and the data fields should be left justified. One space should be left between each label and the data field.

⇒ 4.1.5.3-10 If appropriate, labels should be used to help the user interpret the data displayed in a field.

For example, “DATE (MMM/DD/YYYY): __/__/__.”

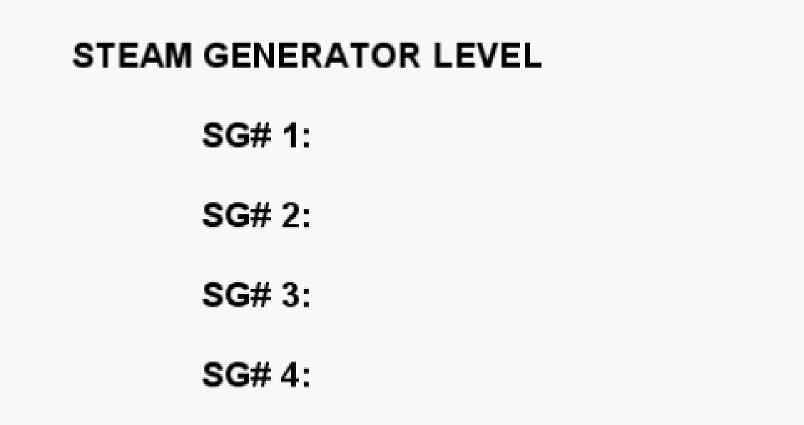
⇒ 4.1.5.3-11 A field group heading should be centered above the labels to which it applies.

⇒ 4.1.5.3-12 At least five spaces should appear between groups of data fields.

Groups of fields may be placed closer together if other means of separating them (e.g., lines or shading) are used.

⇒ 4.1.5.3-13 When headings are located on the line above related screen fields, the labels should be indented a minimum of five spaces from the start of the heading.

Scanning an inquiry screen will be aided if logical groupings of fields are identified by headings (see Figure 4-11). This permits scanning of headings until the correct one is located, at which point the visual search steps down one level to the items within the grouping itself.



STEAM GENERATOR LEVEL

SG# 1:

SG# 2:

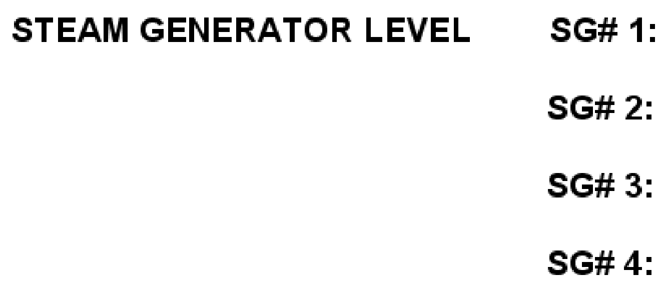
SG# 3:

SG# 4:

Figure 4-11
Placement of Heading Above Data Fields

⇒ 4.1.5.3-14 When headings are placed adjacent to the related fields, they should be located to the left of the topmost row of related fields. The column of labels should be separated from the longest heading by a minimum of three blank spaces.

Scanning a form will be aided if logical groupings of fields are identified by headings (see Figure 4-12). This permits scanning of headings until the correct one is located, at which point the visual search steps down one level to the items within the grouping itself.



STEAM GENERATOR LEVEL SG# 1:

SG# 2:

SG# 3:

SG# 4:

Figure 4-12
Placement of Heading Adjacent to Data Fields

⇒ 4.1.5.3-15 A data form should have a logical organization.

Logical bases for organizing fields include: conventional order (a generally accepted or customary ordering), sequence of use, frequency of use, data comparison (values that must be compared are grouped together), functional grouping (related functions are grouped together), importance (task-critical items are located prominently), and general to specific (detailed fields proceed from more general topics, as in a hierarchical organization). Logical organizations can support user comprehension of the layout of the form and facilitate its use.

⇒ 4.1.5.3-16 The number of pages in a data form required to complete an activity should be minimized to reduce the amount of navigation.

Movement among individual display pages delays the activity and causes the user to divert attention from entering data to navigating the forms.

4.1.5.4 Numeric Readouts

A numeric readout presents data as a string of numerals (digits). While such displays are sometimes used unaccompanied, they are more commonly used in combination with other elements or within another display format. For example groups of numeric readouts, combined with labels, comprise a data form display. Accordingly, guidelines for numeric readouts are given in Section 4.1.6.3.

4.1.5.5 Bar Charts and Histograms

A bar chart is graphic figure in which numeric quantities are represented by the linear extent of parallel lines (or bars), either horizontally or vertically. This type of chart is used to compare the magnitudes of a limited number of items on a single scale.

In a segmented bar chart, the bars are subdivided to show the contributions of component quantities to the total (indicated by the overall extent of the bar) and to allow comparisons among the components.

A deviation bar chart has bars extending to the left or right of (or above and below) a common baseline and is used to indicate the degree of divergence from some ‘normal’ value. When the task calls for the difference between the displayed value and a standard to be evaluated, it may be useful to display that difference directly (as in a deviation chart).

A histogram is a type of bar chart used to depict the frequency distribution for a continuous variable, which may be grouped into classes. The bars in a histogram are typically vertical and contiguous; the lines separating the bars from one another may be omitted.

⇒ 4.1.5.5-1 Each bar on the display should have a unique identification label.

The label provides a positive identification of the parameter each bar represents. A user should not have to memorize the position of each parameter on the display.

⇒ 4.1.5.5-2 When bars are displayed in groups, they should be labeled as a unit, with individual distinguishing labels for each bar.

Direct labeling of bars will make the information easier to use. If the user has to refer to a separately displayed legend, interpretation of the chart will be slower and more subject to error.

⇒ 4.1.5.5-3 When data must be compared, bars should be adjacent to one another and spaced such that a direct visual comparison can be made without eye movement.

A horizontal bar chart is illustrated in Figure 4-13. The spacing between bars should be less than the bar width. If many bars are displayed, then spacing may produce an alternating pattern of bright and dark bands that could prove visually disturbing. In this case, it is preferable to arrange the bars contiguously (i.e., without spaces).

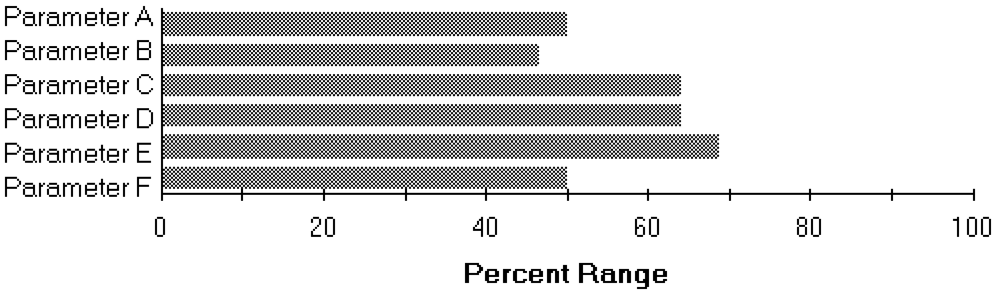


Figure 4-13
Example of a Horizontal Bar Chart

⇒ 4.1.5.5-4 In a related series of bar charts, a consistent orientation of the bars (vertical or horizontal) should be adopted.

If bar length is used to represent duration, then it might be more appropriate to orient the bars horizontally, in accord with the general convention of plotting time on the horizontal axis of a graph. Vertical bars can be used to display frequency counts or a large variety of other measured attributes.

⇒ 4.1.5.5-5 If one bar represents data of particular significance, then that bar should be highlighted.

If one bar represents critical/discrepant data, then that bar might be coded differently. However, if bar coding is already used for other purposes, such as to distinguish among different sets of grouped bars, then no additional highlighting code should be superimposed on the bars themselves; some other means of highlighting (e.g., an arrow) might be adopted.

⇒ 4.1.5.5-6 The zero reference should be the center of the deviation bar chart.

An example of a deviation bar chart appears in Figure 4-14.

⇒ 4.1.5.5-7 On a deviation bar chart, the range of normal conditions for positive or negative deviations should represent no more than 10 percent of the total range.

An example of a deviation bar chart appears in Figure 4-14.

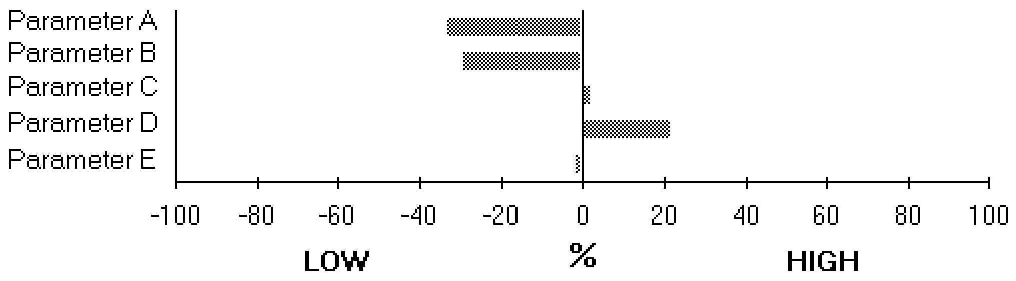


Figure 4-14
Example of a Deviation Bar Chart

⇒ 4.1.5.5-8 The magnitude of each variable should be displayed when a deviation bar display is used as a main display format for safety function parameters.

The actual values of critical parameters should appear on the deviation bar display in addition to percent deviation.

⇒ 4.1.5.5-9 Segmented bars, in which differently coded segments are shown cumulatively within a bar, should be used when both the total measures and the portions represented by the segments are of interest.

An example of a segmented bar chart appears in Figure 4-15.

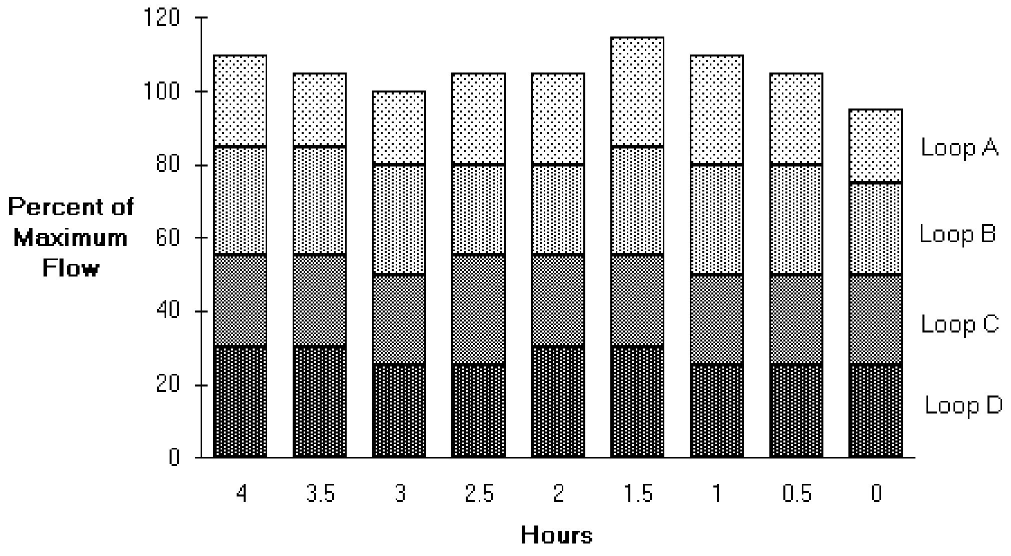


Figure 4-15
Example of a Segmented Bar Chart

⇒ 4.1.5.5-10 The data categories should be ordered within each segmented bar in the same sequence, with the least variable categories displayed at the bottom and the most variable at the top.

Sometimes there are independent logical grounds for the ordering of data categories. If a segmented bar graph that is constructed on a logical basis produces confusing irregularity of segments, then it might be better to display the data in some other graphic format. Any irregularity in the bottom segment will 'propagate' throughout the segments above it, which will make it difficult for a user to examine irregularities in the upper segments.

4.1.5.6 Graphs

A graph is a display that represents values of one or more variables with respect to another variable. In a simple line graph, connected points representing a series of values on the vertical axis are shown as a function of values on the horizontal axis (which often indicates time). This type of presentation is used when many values (a series) are to be shown, and/or when interpolation may be necessary. It is better for showing trends than for giving specific values. The ability to show rate of change is especially useful when operators must anticipate and control parameter deviations. Graphs are not appropriate when there are relatively few items in the series or when the data are extremely irregular.

In a linear profile chart, the line connecting the points forms the upper boundary of a polygon; i.e., the area between the line and the horizontal axis is shaded or otherwise made visually distinct from the rest of the graph area. The contours of the polygon show the relationships among the variables on the horizontal axis. This purpose may be better served by a simple bar chart, unless recognizable contours can be associated with specific relationships or conditions (e.g., by scaling the variables so that a flat contour represents normal conditions).

In a scatterplot, the points are typically not connected, and the horizontal axis does not indicate time. For example, pressure may be plotted as a function of temperature. This format is used to analyze the relationship between the variables.

Certain other types of graphs (e.g., integral and configural displays) use emergent features to portray higher-level information; guidelines for such displays are given in Section 4.1.5.11.

⇒ 4.1.5.6-1 Graphs should convey enough information to allow the user to interpret the data without referring to additional sources.

⇒ 4.1.5.6-2 When multiple curves are included in a single graph, each curve should be identified directly by an adjacent label, rather than by a separate legend.

In the case of multiple curves representing multiple dimension (e.g., pressure, temperature), the dimension and unit of each parameter should be labeled on the curve. As an exception, where displayed curves are too close for direct labeling, an acceptable alternative might be to distinguish the various curves in some way, perhaps by color coding or line coding, and identify their codes in a separate legend. Direct labeling will permit users to assimilate information more rapidly than displaying a separate legend.

⇒ 4.1.5.6-3 If a legend must be displayed, the codes in the legend should be ordered to match the expected or typical spatial order of their corresponding curves in the graph itself.

In cases where curves can be expected to cross and/or when there is a logical ordering of the variables shown (e.g., Loop A, B, C, and D), then allowing the ordering of the legend to remain constant would be preferred.

⇒ 4.1.5.6-4 Coding should be used when multiple variables are displayed in a single graph.

Coding should be provided particularly if curves approach and/or intersect one another; see Section 4.1.4.4. Coding is required to distinguish one curve from another.

⇒ 4.1.5.6-5 Line coding should be used consistently across graphs.

When line coding is used to distinguish among curves representing variables that appear in a series of graphs, the same codes should be used to indicate the corresponding data in all of the graphs.

⇒ 4.1.5.6-6 In displays of multiple curves, if one curve represents data of particular significance, then that curve should be highlighted (see section 4.1.4.4)

If one curve represents critical/discrepant data, for example, that curve might be displayed with a noticeably thicker line stroke or in a different color. If line coding is already used to distinguish among multiple curves, then the means of highlighting any particular curve should be selected so that it will not be confused with coding for visual separation. For example, if displayed curves are distinguished by line codes (solid, dashed, or dotted), then some other means of highlighting (e.g., addition of symbol indicating the significant line) might be adopted.

⇒ 4.1.5.6-7 Trend displays should be capable of showing data collected during time intervals of different lengths.

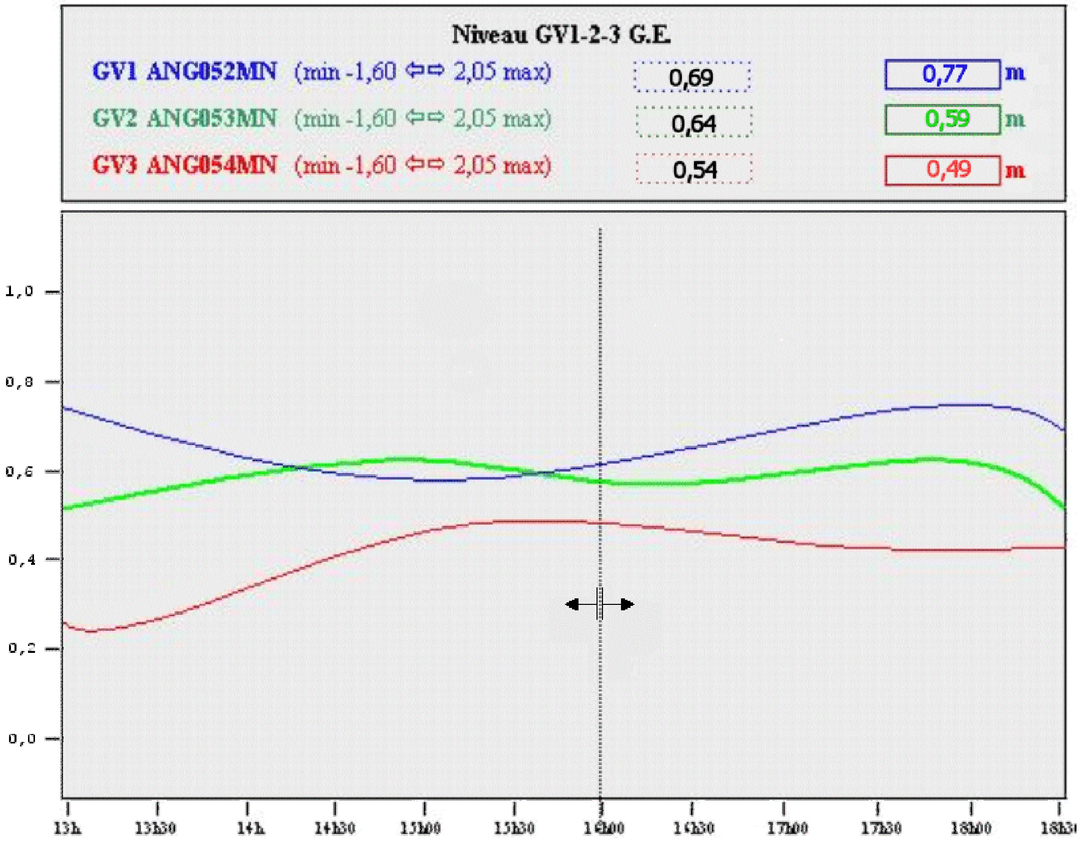
A short time base of just a few minutes is needed to study fast changing trends, while other trends may not show significant changes for several hours.

⇒ 4.1.5.6-8 When the user must compare trend data represented by separate curves, the curves should be displayed in one combined graph.

Combined plots should be related, so the user can correlate changes in one variable with changes in other key variables. Only those curves requiring comparison should be combined, since, as the number of curves on a graph increases, the user’s task of comparison will become more difficult.

⇒ 4.1.5.6-9 If operators must read exact parameter values from displayed curves, features should be provided to support this.

For example, in Figure 4-16, operators can show the exact values of the displayed parameters at a chosen time by positioning a vertical line at the point corresponding to the time; a readout of the values appears in the upper part of the display.



Niveau GV1-2-3 G.E.

GV1 ANG052MN (min -1,60 ⇦⇨ 2,05 max) 0,69 0,77 m

GV2 ANG053MN (min -1,60 ⇦⇨ 2,05 max) 0,64 0,59 m

GV3 ANG054MN (min -1,60 ⇦⇨ 2,05 max) 0,54 0,49 m

Figure 4-16
Example of an Aid for Reading Exact Values from a Line Graph

⇒ 4.1.5.6-10 Curves representing planned, projected, or extrapolated trend data should be distinctive from curves representing actual data.

Curves representing projected data, for example, could be depicted as broken, dashed, or dotted lines, while curves representing actual data could be represented as solid lines.

⇒ 4.1.5.6-11 Combining several individual curves into a single average curve should only be done when users do not need to know the pattern of individual curves or when curves differ on the basis of minor irregularities.

Curve averaging should be performed with caution since averages tend to ‘wash out’ local variations.

⇒ 4.1.5.6-12 Where curves represent cyclic data, the scale should be selected so that at least one complete cycle is shown.

This will allow users to scan any critical portion of the displayed cycle without having to adjust the presentation. The optimal number of cycles to show will depend on the particular application.

⇒ 4.1.5.6-13 The target area, preferred combination of X- and Y-axis values, should be graphically defined.

Monitoring a pressure-temperature display, which presents a saturation curve that indicates the subcooled water region and the superheated steam region, is an example of a task situation where graphic depiction of a target area should be provided. This sort of display is best used for detecting deviations from normal if a target area can be defined. By plotting a brief time history, one may be able to predict where the values are headed. Care should be taken to distinguish the current value from past values, especially when the values change slowly. This can be done by placing a symbol or code for the current value.

⇒ 4.1.5.6-14 Old data points should be removed after some fixed period of time to prevent clutter.

Ideally, as one new point is plotted, the oldest point should be removed, thereby maintaining a constant number of displayed points.

⇒ 4.1.5.6-15 A linear profile chart should form recognizable geometric patterns for specific abnormal conditions.

An example of a linear profile chart appears in Figure 4-17. The irregular profile is indicative of abnormal operating conditions.

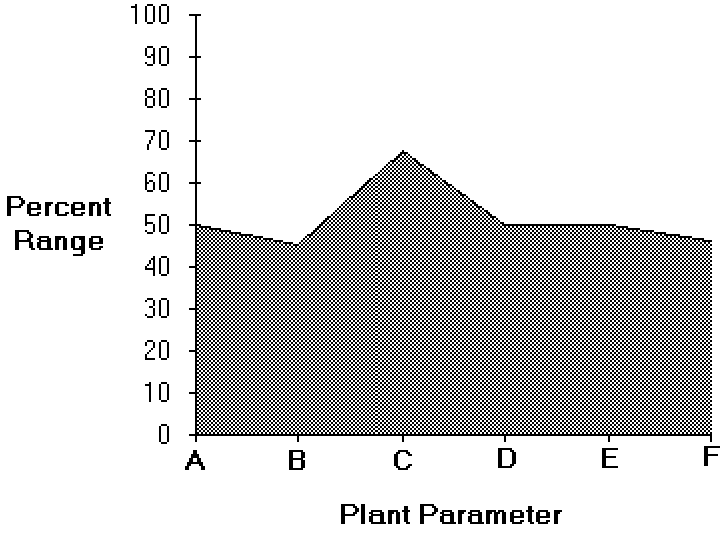


Figure 4-17
Example of a Linear Profile Chart

⇒ 4.1.5.6-16 The area below the profile line should be shaded to provide a more distinguishable profile.

⇒ 4.1.5.6-17 Labels should be provided along the bottom of a linear profile chart to identify each parameter.

⇒ 4.1.5.6-18 All segments in a segmented curve graph should be related to the total value.

A segmented curve graph contains a series of bands depicting the components of a total series (see Figure 4-18). The values of the bands, segments, or strata are plotted on an X-Y plot. The bands are added to one another so that the topmost boundary represents the sum of all bands. For example, segmented curve graphs can be used to show how much each pump is contributing to total flow. This format is most useful when all elements contribute equally to the total under normal circumstances. Segmented curve graphs should not be used when changes in the movement of a series are abrupt, or where accurate reading of a component is of paramount importance.

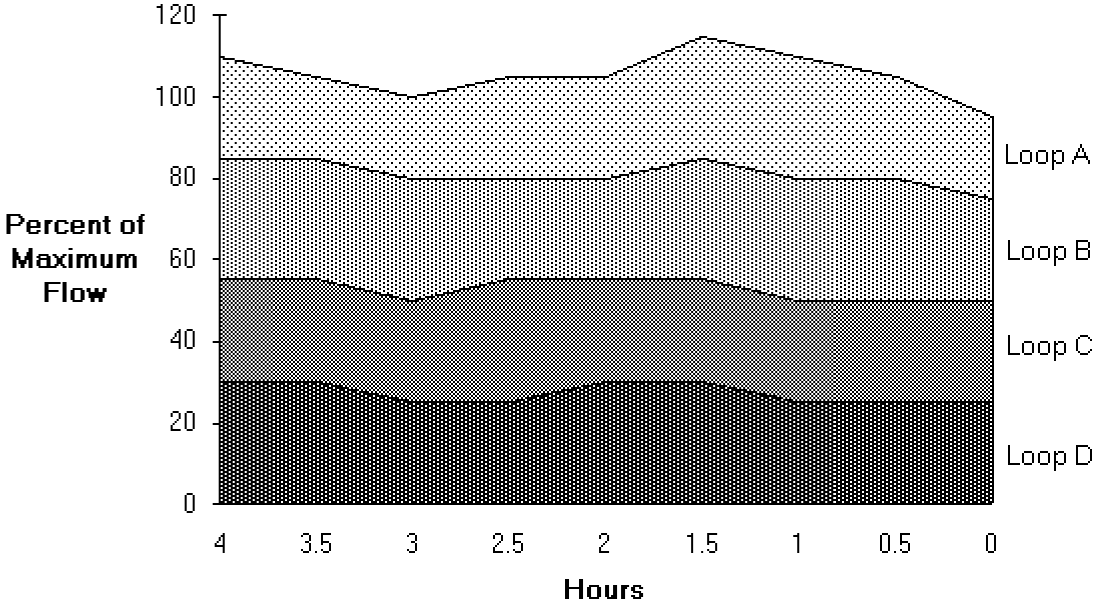


Figure 4-18
Example of a Segmented Curve Graph

⇒ 4.1.5.6-19 The data categories in a segmented curve graph should be ordered so that the least variable curves are displayed at the bottom and the most variable at the top.

Sometimes there are independent logical grounds for the ordering of data categories. If a segmented curve graph that is constructed on a logical basis produces confusing irregularity of curves, then it might be better to display the data in some other graphic format. Any irregularity in the bottom curve will 'propagate' throughout the curves above it, which will make it difficult for a user to evaluate irregularities in the upper curves.

⇒ 4.1.5.6-20 The different bands of segmented curve graphs should be made visually distinctive by coding, such as by the texturing or shading of bands (see Patterns)

⇒ 4.1.5.6-21 Where space permits, the different bands of segmented curve graphs should be labeled directly within the textured or shaded bands.

⇒ 4.1.5.6-22 If some plotted points represent data of particular significance, they should be highlighted to make them visually distinctive from others.

Significant data points might be highlighted by bolding, color, blinking, shape coding, or other means, or might be designated by supplementary display annotation (see Section 4.1.6.8).

⇒ 4.1.5.6-23 When relations among several variables must be examined in scatterplots, an ordered group (matrix) of plots should be displayed, each showing the relation between just two variables.

The ordering of several scatterplots in a single display might help a user discern relations among interacting variables.

⇒ 4.1.5.6-24 When scatterplots are grouped in a single display to show relations among several variables, an interactive aid should be provided for analysis so that if a user selects a set of data in one plot then the corresponding data points in other plots will be highlighted.

Data selection might be accomplished with a superimposed box of controllable size to define the data set of interest. That technique can exploit the capabilities of interactive graphics to permit a range of data analysis not possible when using printed graphs.

4.1.5.7 Pie Charts

A pie chart (also called a sector chart) is a circular chart divided into sections (as pieces of a pie) to represent graphically the relative proportions of different parts of a whole. The segments may represent magnitudes or frequencies. This format is better for indicating approximate proportions than for analysis, for which a simple bar chart would be preferable). It has been recommended (Galitz, 1993) that pie charts be used with caution because

- they provide no means of absolute measurement
- they cannot represent totals greater than 100 percent
- they can only represent a fixed point in time
- users' estimates of relationships are more accurate with linear the with angular representations

⇒ 4.1.5.7-1 There should be no more than five partitions in a pie chart.

⇒ 4.1.5.7-2 Pie chart segments should be labeled directly rather than by a separate legend. If a segment is too small to contain the label, the label should be placed outside the segment with a line from it to the segment.

The label should be in a normal orientation for reading text.

⇒ 4.1.5.7-3 If the task requires precise values, numbers should be added to pie chart segment labels to indicate the percentage and/or absolute values.

Alternative display formats are preferred when users require precise data.

⇒ 4.1.5.7-4 If a particular segment of a pie chart requires emphasis, it should be highlighted by special hatching or displaced slightly from the remainder of the pie.

4.1.5.8 Flowcharts

A flowchart is a diagram that illustrates sequential relations among elements or events. Flowcharts are often shown as boxes connected by arrows.

⇒ 4.1.5.8-1 The available decision options should be displayed in logical order.

For example, if options represent stages of a process, those stages should be listed in the order in which they would actually occur. The ordering of options should not be determined merely by the amount of space that is conveniently available to display them.

⇒ 4.1.5.8-2 Only a single decision should be required at each step.

Decisions should not be combined to reduce flowchart size.

⇒ 4.1.5.8-3 When a flowchart is designed so that a user must make decisions at various steps, the available options should be displayed in some consistent order from step to step.

For example, ‘yes’ might always be on the left and ‘no’ on the right. Another scheme is always to have the desirable path lead downward and the ‘problem’ paths lead out to the side. Consistent ordering will permit a user to review a flowchart more quickly.

⇒ 4.1.5.8-4 While flowcharts should display only the data immediately required by the user, more detailed data should be available by means of a simple action.

⇒ 4.1.5.8-5 Flowcharts should be designed so that the path of the logical sequence is consistent with familiar orientation conventions.

For example, from left to right and from top to bottom.

⇒ 4.1.5.8-6 There should be a standard set of flowchart symbols.

4.1.5.9 Mimics and Diagrams

A mimic is a display format combining graphics and alphanumerics used to integrate system components into functionally oriented diagrams that reflect component relationships. For example, a mimic display may be used to provide a schematic representation of a system.

A diagram is a special form of a picture in which details are only shown if they are necessary for a task. For example, an electrical wiring diagram for a facility would show wiring but not necessarily furniture or plumbing.

⇒ 4.1.5.9-1 Mimics and diagrams should contain the minimum amount of detail needed for the task they were designed to support.

An example of a mimic display is shown in Figure 4-19. Unnecessary graphic detail (such as shadowed symbols or very detailed icons) should be avoided.

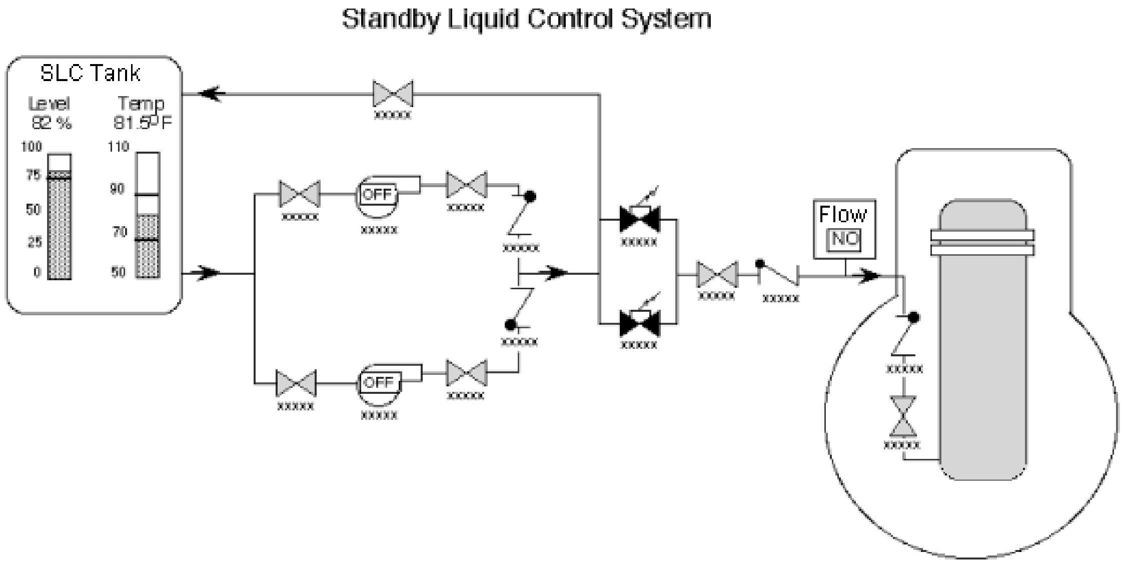


Figure 4-19
Example of a Mimic Display

⇒ 4.1.5.9-2 Plant components represented on mimic lines should be identified.

Symbols used on mimic displays should conform to the guidelines in Section 4.1.6.4.

⇒ 4.1.5.9-3 Indications of the actual status of plant systems and equipment, as opposed to demand status, should be provided when required by the task.

Demand information shows that equipment has been commanded (by control settings or otherwise) to a particular state or level. It shows only what is demanded, not what is actually being realized. Status information shows the state or level actually in effect. To prevent confusion, it is essential that displays be identified as to whether they reflect demand or actual status.

⇒ 4.1.5.9-4 All flow path line origin points should be labeled or begin at labeled components.

⇒ 4.1.5.9-5 All flow path line destination or terminal points should be labeled or end at labeled components.

⇒ 4.1.5.9-6 Flow directions should be clearly indicated by distinctive arrowheads.

⇒ 4.1.5.9-7 Flow paths should be coded (e.g., by color and/or width) to indicate important information (see Color).

For example, color can be used to differentiate process flow paths: blue may be used to code water lines; white, steam lines; and yellow, oil lines. In general, features of the flow path that change (e.g., the open/close status of valves) should be coded so as to be more salient than static features.

⇒ 4.1.5.9-8 Overlapping of flow path lines should be avoided.

Cross-overs should be clearly indicated so that they do not appear as connections.

⇒ 4.1.5.9-9 Where symbols are used to represent equipment components and process flow or signal paths, numerical data should be presented reflecting inputs and outputs associated with equipment.

⇒ 4.1.5.9-10 When a graphic display contains some outstanding or discrepant feature that merits attention by a user, supplementary text should be displayed to emphasize that feature.

For example, a flow diagram for process control might include a current advisory message, POSSIBLE PRESSURE VALVE FAILURE, as well as appropriate graphic indications of the problem.

⇒ 4.1.5.9-11 When users must evaluate information in detail, computer aids for calculation and visual analysis should be provided.

For examining the internal structure of a depicted object, for example, it might be helpful to allow a user to request auxiliary displays of specified cross-sections or transect diagrams. For more detailed structural analysis of depicted objects, it might be necessary to provide computer aids for calculating area, volume, stresses, and heat transfer.

4.1.5.10 Maps

A map is a graphical representation of an area or a space, such as the layout of a room or a facility.

⇒ 4.1.5.10-1 Significant features of a map should be labeled directly on the display unless cluttering or obscuring of other information would result.

Labels on a map should be positioned consistently in relation to the displayed features they designate. For example, equipment names might always be placed immediately above the corresponding symbols showing their locations. As a practical matter, map displays can get very crowded. It may not always prove feasible to maintain a consistent placement for labels, with the result that designers will be tempted to put labels wherever they will fit. In such a crowded display, labels may obscure map features, and vice versa. Locating and reading labels will be slowed, particularly when map features are displayed closely adjacent to the beginning of labels. Under these circumstances, some other approach to map labeling should be considered to avoid crowding.

⇒ 4.1.5.10-2 When several different maps will be displayed, a consistent orientation should be used so that the top of each map will always represent the same direction.

In common use, most maps are oriented so that North is upward.

⇒ 4.1.5.10-3 The user should be able to select different map orientations and reference points.

The system should provide the user with a listing of the common orientations and reference points. If the map display can be displayed at other workstations, only the display at the user's workstation should be affected by the selection. The selected orientation should be clearly indicated, e.g., with a label.

⇒ 4.1.5.10-4 If the map orientation can be changed, the map labels and symbols should remain oriented to the user's position.

⇒ 4.1.5.10-5 When a map exceeds the capacity of a single display frame, users should be able to change the display in order to show different areas of current interest.

Panning is preferred to breaking map displays into discrete pages. Some graphic indicator of the position in the overall display of the visible section should be provided when a user views different sections of an extended display.

⇒ 4.1.5.10-6 Codes, such as texture patterns, color, or tonal variations, should be used when different areas of a map must be defined, or when geographic distribution of a particular variable must be indicated.

It may be desirable to limit area coding to one variable in order to assure effective information assimilation. Another approach might be to allow a user to specify which variable will be coded on a map and to change that selection at will depending upon current task requirements. In some special applications, however, it may be feasible to superimpose several kinds of area coding to permit multivariate data analysis by skilled users.

⇒ 4.1.5.10-7 Tonal codes (different shades of one color) rather than spectral codes (different colors) should be used when users must make relative judgments for different colored areas of a display.

People can order categories along a continuous dimension to match tonal variations in one color, whereas people do not have a natural means of ordering different colors. This recommendation represents an exception to other guidelines advocating distinctive code values. Coding by tonal variation should be considered only for applications where perception of relative differences along a single dimension is more important than perception of absolute values.

⇒ 4.1.5.10-8 Where different areas of a map are coded by texture patterns or tonal variation, the darkest or lightest shades correspond to the extreme values of the coded variable.

Orderly assignment of code values will help users perceive and remember the categories represented by the code.

⇒ 4.1.5.10-9 In applications where the geographic distribution of nongeographic data must be displayed, other graphic elements should be added to a map for that purpose.

A display for radioactive control, for example, might superimpose plume tracks on a background of geographic coordinates, with supplementary annotation and/or coding to indicate track identification, speed, heading, altitude, etc. Alphanumeric characters might be added to a map to show data, but those will not aid a direct visual comparison across areas in the same way that graphic symbols can do. Moreover, alphanumeric data may be confused with labels and other kinds of annotation. For example, a symbol might be displayed in different sizes to indicate a particular measure in different localities, or small stacked bars might be superimposed on the different areas of a map to indicate the local distribution of some data measure.

⇒ 4.1.5.10-10 When changes in mapped data are significant for a user’s task, auxiliary graphic elements should be included to highlight those changes.

For example, auxiliary coding might be used to indicate the expected direction of movement of plume tracks on a background of geographic coordinates.

⇒ 4.1.5.10-11 When the use of mapped data may be complex, computer aids should be provided for data analysis.

Computer aids should be provided when a user must judge distances accurately on a map or other graphic display. For exact measurement, it might be better to allow a user to select (point at) any two points and have the computer read out their separation distance directly. The same technique might be used to determine the direction (bearing) between two points.

⇒ 4.1.5.10-12 The user should be able to rapidly remove non-critical information from a map or map overlay display.

For example, it should be possible by a simple action to remove or temporarily suppress any overlays, non-essential labels, or user annotations from a display, leaving only the critical information.

4.1.5.11 Integral and Configural Displays

The quantity of data presented by information systems can, at times, overload the user. To lower the workload associated with extracting meaningful information from data, displays may be designed to help integrate data into more meaningful units of information. These displays map low-level data, process constraints, and relevant performance goals into the appearance and dynamic behavior of a graphical element so that this information is readily available. There are two types of these displays, integral and configural, which differ in how the relationships among data are represented.

Integral displays show information in such a way that the individual parameters used to generate the display are not represented in it. For example, a display might provide information on overall system status by the appearance of an icon. The icon may change appearance based on computations involving lower-level parameters, but the parameter values themselves are not presented.

In configural displays, the relationships among parameters are represented as emergent features of a graphical element. (An emergent feature is a global perceptual feature that is produced by the interactions among individual lines, contours, and shapes). In contrast to integral displays, information about the individual parameters is also available in the display. Configural displays often use simple graphic forms, such as a polygon (see Figure 4-20). Information that could be presented by separate display formats is integrated into a single format in which each of the separate pieces of information is represented, for example, by the distance of a polygon's vertex from its center. In addition, the geometric shape of the polygon provides a high-level summary (the emergent feature).

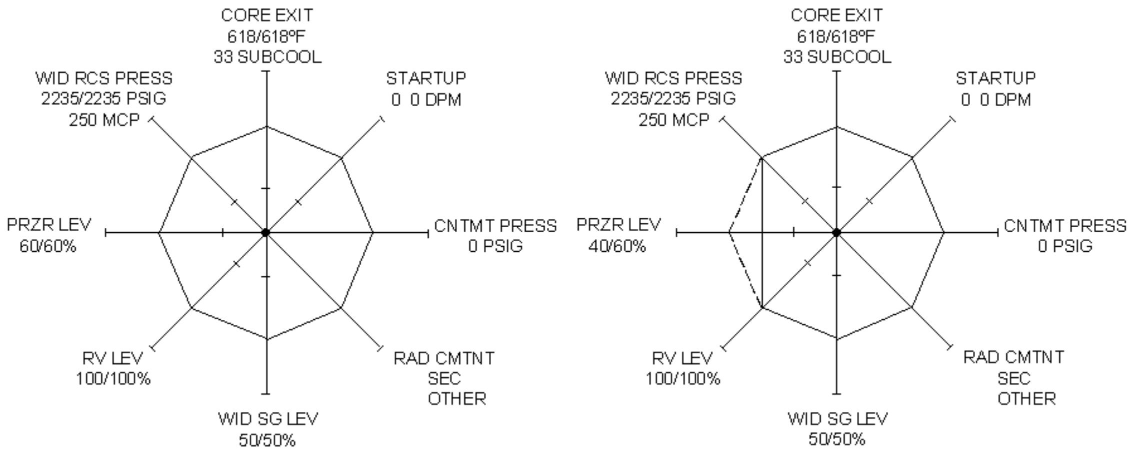


Figure 4-20
Examples of Configural Displays for Normal (Left) and Abnormal (Right) Conditions

⇒ 4.1.5.11-1 Integral displays should be used to communicate high-level, status-at-a-glance information where users may not need information on individual parameters to interpret the display.

Since integral displays do not display individual parameters, they are most appropriate for general status monitoring.

⇒ 4.1.5.11-2 Configural displays should be used when users must rapidly transition between high-level functional information and specific parameter values.

Configural displays provide lower-level information, such as parameter values, and higher-level information conveyed through emergent features. Since both are present in a single display, users can easily move between them.

⇒ 4.1.5.11-3 The methods by which lower-level data are analyzed to produce higher-level information and graphical elements should be understandable to users.

Users must be able to judge the acceptability of higher-level information and how it relates to lower-level information. Operators should be able to access the lower-level information (i.e., parameter displays) with minimal effort so that they can readily investigate any deviations from normal conditions indicated by the integral display.

⇒ 4.1.5.11-4 Users should have access to the rules or computations that link process parameters and graphical features, and to an explanation of how the information system produces higher-level information.

When graphical features change in ways not completely understood by users, they should be able to access the rules that produce the graphic forms. Users should be able to review any analysis performed by the information system.

⇒ 4.1.5.11-5 A perceptually distinct reference aid should be provided in an object display to support users in recognizing abnormalities in the object's characteristics.

When a change in an object's characteristics (e.g., its shape) is the perceptual feature that indicates a fault or abnormal condition, perceptual cues can assist users in detecting the change. If shape is used, the display graphic should include a reference point against which users can compare the current one. Reference points are especially useful when the abnormality is slow to evolve, and the integral object is slowly changing. Recognition of abnormalities can also be aiding by having normal conditions represented by regular, symmetrical shapes and abnormal conditions indicated by asymmetrical shapes.

⇒ 4.1.5.11-6 The display elements should be organized so that the emergent features that arise from their interaction correspond to meaningful information about the process or system, e.g., when the aspect of the system represented by the emergent is disturbed, the disturbance is visible in the emergent feature.

An emergent feature is a high-level, global perceptual feature generated by interactions among individual parts or graphical elements of a display (e.g., lines, contours, and shapes) to produce perceptual properties, such as symmetries, closure, and parallelism. Displays cannot always be organized to provide emergent features, but they should be considered where feasible.

⇒ 4.1.5.11-7 The emergent features or patterns within the display should be nested (from global to local) in a way that reflects the hierarchical structure of the process.

High-order aspects of the process (e.g., at the level of functional purpose or abstract function) should be reflected in global display features; lower-order aspects of the process (e.g., functional organization) should be reflected in local display features.

⇒ 4.1.5.11-8 Each emergent feature should be clearly distinguishable from other emergent features and from information on individual parameters.

For example, users' perception of plant status can be enhanced by shading the area within a feature.

⇒ 4.1.5.11-9 Each relevant process parameter should be represented by a perceptually distinct element within the display.

⇒ 4.1.5.11-10 The display should support the user in performing tasks requiring lower-level information.

When the user must perform tasks using lower level information, the display should provide such support. For example, if precise information about a variable is desirable, then a scale or numeric information should be provided. Scales should be labeled with the names of the displayed parameters.

⇒ 4.1.5.11-11 The emergent features and their interactions should not be so complex as to be susceptible to misinterpretation.

The value of emergent features is that they can provide direct perception of higher-level information, which would otherwise be gained by inference or calculation. Users should be involved in the design (e.g., in testing preliminary mock-ups) to insure that they perceive the displays in the way the designers expect, and to avoid developing displays that actually require more mental effort to interpret than convention ones.

4.1.5.12 Graphic Instrument Panels

These are formats in which graphical objects are arranged to resemble instruments in a control panel. For example, an individual indicator may appear as a circular meter containing a numerical scale and an indicating needle. Such displays are most useful for displaying the values of parameters that users must verify to be within an acceptable range. Normal operation of a system might be indicated by the pointers on series of meters all being oriented vertically, for example. When specific parameter values must be compared to each other or to a standard, other techniques (e.g., bar charts) are preferred. When tasks require exact parameter values, a numeric readout with the appropriate precision should be provided in addition to or instead of the graphical indicator.

⇒ 4.1.5.12-1 Zones indicating operating ranges should be color coded by edge lines or wedges for circular scales.

Zones can be used to indicate operating ranges, off-normal levels, and dangerous levels.

⇒ 4.1.5.12-2 When check-reading positive and negative values on rotary meters (circular displays), the zero or null position should be at 12 o'clock or 9 o'clock.

With a matrix of circular displays, deviations from a 9 o'clock null position are easily detected in check reading. Zero should appear at the 12 o'clock position on multi-revolution dials.

⇒ 4.1.5.12-3 The pointer on fixed scales should extend from the right of vertical scales and from the bottom of horizontal scales.

⇒ 4.1.5.12-4 The pointer on fixed scales should extend to but not obscure the shortest graduation marks.

⇒ 4.1.5.12-5 Tick marks should be separated by at least 0.07 inches (1.75 millimeters) for a viewing distance of 28 inches (71 centimeters) under low illumination.

Low illumination is less than 1.0 ft-L (3.5 cd/m²).

⇒ *4.1.5.12-6 Scales should not be cluttered with more marks than necessary for the precision needed the tasks for which the scale is used.*

4.1.5.13 Speech Displays

These are displays that provide information in the form of speech (either computer-generated or a recorded human voice). Messages are conveyed to the user through audio devices, such as speakers and headsets. Providing information by means of speech is most useful in settings in which users are engaged in tasks requiring constant visual attention. However, users will typically be able to read and comprehend written material faster and with less effort than is required to listen to and understand spoken messages. Thus speech is most appropriate for brief messages. Other means should be considered for transmitting large amounts of information.

⇒ *4.1.5.13-1 Speech should be limited to provide only a few messages.*

Speech messages would not be useful, for example, if many messages might be given at one time, or for conveying a lengthy list of menu options.

⇒ *4.1.5.13-2 The user should be able to have speech messages repeated.*

⇒ *4.1.5.13-3 Messages should be short and simple.*

If a user does not understand a written message, it can be reread. That is not as easy with spoken messages, even though a REPEAT function should be provided. A better approach is to restrict use of speech outputs to short and simple messages. If a user who may not be watching a display must be given long or complex messages, it is probably better to provide a simple auditory signal such as a chime, and then display the messages visually for the user to read. In general, users will understand complex messages better when they see them displayed than when they hear them.

⇒ *4.1.5.13-4 A distinctive and mature voice should be used.*

⇒ *4.1.5.13-5 Spoken messages should be presented in a formal, impersonal manner.*

⇒ *4.1.5.13-6 Words in a speech message should be concise, intelligible, and appropriate for the information presented.*

Where possible, words that rhyme or may confuse message interpretation should not be part of the spoken lexicon, or should not be presented within the same message. Use of slang should be avoided. Words with more than one syllable should be used. Alphanumeric data should be presented using phonetic alphabets, e.g., ‘Whiskey Zulu three two seven’ should be used in preference to ‘WZ327’ where the ‘Z’ and ‘3’ are too phonetically similar.

⇒ 4.1.5.13-7 A speech message priority system should be established such that more critical messages override the presentation of messages having lower priority.

If two or more incidents or malfunctions occur simultaneously, the message having the higher priority should be given first. The remaining messages should follow in order of priority. In the event of a complete subsystem failure, the system should integrate previous messages via electronic gating and report the system rather than the component failure.

⇒ 4.1.5.13-8 If speech is used to provide warnings as well as other forms of user guidance, spoken warnings should be easily distinguishable from routine messages.

For example, speech output used to identify emergency conditions might use some distinctive voice and/or preface each warning message with some other distinctive auditory alert signal. In some applications, computer- generated speech might be useful for providing a few short and simple warnings. However, if speech output is also used for other purposes, then the warning messages must be distinctive.

⇒ 4.1.5.13-9 Speech signal intensity should be clearly audible for the expected ambient noise environment.

For critical messages, speech should be at least 20 dB above the speech interference level at the operating position of the intended receiver. Signal to noise ratios should be at least 5:1. Audio signal power should be approximately 300 milliwatts at the listener ear. Speech signals should fall within the range of 200 to 6100 Hz.

4.1.6 Display Elements

4.1.6.1 Alphanumeric Characters

These include letters, digits, and usually other symbols, such as punctuation marks. Guidelines for text used as an information display format are given under 'Display Formats.' Here, text is considered at the level of display elements.

⇒ 4.1.6.1-1 Text to be read (except labels) should be presented using upper and lower case characters.

Reading text is easier and faster when capitalization is used conventionally to start sentences and to indicate proper nouns and acronyms. There are several exceptions, however. An item intended to attract the user's attention, such as a label or title, can be displayed in upper case. In addition, upper case should be used when lower case letters will have decreased legibility, e.g., on a display terminal that cannot show true descenders for lower case letters.

⇒ 4.1.6.1-2 A clearly legible font should be utilized. Fonts should have true ascenders and descenders, uniform stroke width, and uniform aspect ratio.

Preference should be given to simple styles. Script and other highly stylized fonts (e.g., shadow, calligraphy) should be avoided. Avoid typefaces that: have extended serifs, internal patterns, or stripes; are italicized, stenciled, shadowed or 3-dimensional; appear like handwritten script or like Old English script; or are distorted to look tall and thin or wide and fat. The basic evaluation criterion for font selection should be legibility.

⇒ 4.1.6.1-3 For a given font, it should be possible to clearly distinguish between the following characters: X and K, T and Y, I and L, I and 1, O and Q, O and 0, S and 5, and U and V.

⇒ 4.1.6.1-4 The height of characters in displayed text or labels should be at least 16 minutes of arc (4.7 mrad) and the maximum character height should be 24 minutes of arc (7 mrad).

Character heights of 20 to 22 minutes of arc (5.5 to 6.5 mrad) are preferred for reading tasks. Slightly smaller characters are acceptable in high-contrast panel labels. Characters should not be larger than 45 minutes of arc (13 mrad) when groups of characters are displayed. Minutes of arc can be converted into height as follows:

Height = 6.283D(MA)/21600

where MA is minutes of arc, and D is the distance from the user to the screen.

⇒ 4.1.6.1-5 For fixed (as opposed to proportionally spaced) presentations, the height-to-width ratio should be between 1:0.7 to 1:0.9.

For proportionally spaced presentations, a height-to-width ratio closer to 1:1 should be permitted for some characters, for example, the capital letters M and W. The height-to-width ratio of a given character is the vertical distance between the top and bottom edges, and the left and right edges of a nonaccented capital letter. Some letters, however, are customarily seen as narrower than are others. For example, in a given character set, the letter I, and sometimes the letter J, appear narrower than M and 2. Lowercase letters may similarly vary in width. Accordingly, the height-to-width ratio of a given character set should be the modal character width - that is, the width that occurs most often - in the set of capital letters. These measurements are to be made at the same luminance level as the resolution measurement (see 1.5.1.1).

⇒ 4.1.6.1-6 A 4x5 (width-to-height) character matrix should be the minimum matrix used for superscripts and for numerators and denominators of fractions that are to be displayed in a single character position.

A 5x7 (width-to-height) character matrix should be the minimum matrix used for numeric and uppercase-only presentations. The vertical height should be increased upward by two dot positions if diacritical marks are used. A 7x9 (width-to-height) character matrix should be the minimum matrix for tasks that require continuous reading for context, or when individual alphabetic character legibility is important, such as in proofreading. The vertical height should be increased upward by two dot (pixel) positions if diacritical marks are used. If lower case is used, the vertical height should be increased downward by at least one dot (pixel) position, preferably two or more, to accommodate descenders of lower case letters. stroke width should be greater than 1/12 of the character height. A stroke width may be more than one pixel wide.

⇒ 4.1.6.1-7 Horizontal separation between characters or symbols should be between 10 and 65 percent of character or symbol height.

Separation should not be less than 25 percent of character height when any of the following degraded conditions exists: (1) when character width is less than 85 percent of height; (2) when character luminance in less than 12 ft-L; (3) when luminance contrast is less than 88 percent; (4) when display is more than 35 degrees left or right of the straight-ahead line of sight; and (5) when the visual angle subtended by the character or symbol height is less than 15 minutes of arc.

4.1.6.2 Abbreviations and Acronyms

An abbreviation is a shortened form of a word or phrase (e.g., the word “pressure” might be abbreviated as “press”). An acronym is a word formed from the initial letter(s) of each of the successive or major parts of a compound term. For example, the acronym SART is sometimes used to represent the alarm system control operations: silence, acknowledge, reset, and test.

⇒ 4.1.6.2-1 Abbreviations should be avoided (except when terms are commonly referred to by their initialisms, e.g., SPDS).

When abbreviation is necessary due to space constraints, the words chosen for abbreviation should be those that are commonly known in their abbreviated form, and/or those words whose abbreviations can be unambiguously interpreted. To indicate that there is low pressure in the condensate storage tank, the use of ‘CST Pressure Low’ would be acceptable, but ‘Condensate Storage Tank Prssr Lw’ is not a good abbreviation. If the user enters an abbreviation for a command name, the system should use the same abbreviation when referring to that command in messages or prompts. The use of abbreviations or contractions in output text should be avoided.

⇒ 4.1.6.2-2 When defining abbreviations that are not common to the user population, a simple rule should be used that users understand and recognize.

Abbreviation by truncation is the best method, except when word endings convey important information. When a truncation rule is used, abbreviations are easy to derive and easy for a user to decode. If an abbreviation deviates from the consistent rule, it may be helpful to give it some special mark whenever it is displayed.

⇒ 4.1.6.2-3 Abbreviations should be distinctive so that abbreviations for different words are distinguishable.

⇒ 4.1.6.2-4 Abbreviations and acronyms should not include punctuation.

For example, SPDS is preferred over S.P.D.S. Punctuation should be retained when needed for clarity, e.g., ‘4-inch diameter pipe’ rather than ‘4 in diameter pipe.’

⇒ 4.1.6.2-5 When arbitrary codes must be remembered by the user, characters should be grouped in blocks of three to five characters, separated by a minimum of one blank space or other separating character such as a hyphen or slash.

Arbitrary codes are alphanumeric characters without natural organization. When a code is meaningful, such as a mnemonic abbreviation or a word, it can be longer.

⇒ 4.1.6.2-6 The use of the letters O and I in a non-meaningful code should be avoided since they are easily confused with the numbers 0 (zero) and 1 (one), respectively.

⇒ 4.1.6.2-7 When codes combine letters and numbers, letters should be grouped together and numbers grouped together rather than interspersing letters with numbers.

For example, letter-letter-number (‘HW5’) will be read and remembered somewhat more accurately than letter-number-letter (‘H5W’).

4.1.6.3 Numeric Data

These are data represented in numerical form (as opposed to text form). Examples include numerical representations of plant variables or control setpoints. Numeric displays should be designed to be legible, and should present information in a form that is directly useable and appropriate for the user’s task.

⇒ 4.1.6.3-1 Numeric values should ordinarily be displayed in the decimal number system.

Maintenance, troubleshooting, or configuration tasks may use other systems (e.g., binary, octal, or hexadecimal).

⇒ 4.1.6.3-2 Leading zeros in numeric entries for whole numbers should be suppressed.

For example, 28 should be displayed rather than 0028. A leading zero should be provided if the number is a decimal with no preceding integer (i.e., 0.43 rather than .43).

⇒ 4.1.6.3-3 A number should be displayed at the number of significant digits required by users to perform their tasks; displays should not imply precision beyond the capabilities of the underlying sensors.

Arbitrary conventions should not require that displays present more (or fewer) significant digits than necessary. The number of significant digits must be supported by the accuracy of the underlying sensors, instruments, and electronics; this applies to synthesized or calculated variables as well as measured ones

⇒ 4.1.6.3-4 Numeric displays should accommodate the variable's full range.

The full range of the variable means highest and lowest values that the variable is expected to take on, under any conditions (normal or emergency operations) for the tasks the display is designed to support.

⇒ 4.1.6.3-5 Numeric displays should change slowly enough to be readable.

Numerals should not follow each other faster than one per second when the user is expected to read the numerals consecutively.

⇒ 4.1.6.3-6 If users must rapidly discern directional change, numeric displays should be provided with arrows to indicate the direction of change.

Rapidly changing digits are difficult to read, and directional indicators will help the user interpret the direction of trend.

⇒ 4.1.6.3-7 If users must evaluate the difference between two sets of data, the difference should be presented on the display.

If it is important for the user to be aware of a discrepancy between two sets of data, the difference should be highlighted on the display.

⇒ 4.1.6.3-8 All numbers should be oriented upright.

⇒ 4.1.6.3-9 If more than four digits are required, they should be grouped and the groupings separated as appropriate by commas, by a decimal point, or by additional space.

4.1.6.4 Icons and Symbols

Icons and symbols are graphical, non-verbal representations of objects, characteristics, states, or actions. In common usage, icons are distinguished from other symbols in that they resemble or depict the thing being represented. However, in the context of computer interfaces, the term icon is often used to connote a graphical symbol that is interacted with in order to produce some action in a graphical interface environment.

Icons and symbols are commonly used in computerized interfaces for two reasons. First, they may be used (in place of text) to save space, by concisely representing actions, objects, or states. Second, they may be used to help the users process a visual presentation by making it easier to find information or recognize patterns. To succeed in either purpose, they must be distinctive and easily recognizable. If used in lieu of text, they must also immediately and unambiguously evoke the concept they stand for.

In deciding when or whether to include icons or symbols in an interface, designers should critically consider the advantages claimed for their use. For example, while symbolic representations have the potential to use less space than the corresponding words, the symbols must still be made large enough so that recognition is not slowed. Furthermore, there are practical limits to how small the buttons on which symbols are shown can be made without impairing usability – so the potential space savings may be limited. Similarly, while distinctive, unique symbols or icons may be and located and comprehended more easily and quickly than text labels, this is not always the case. Symbols used in P&IDs are well learned and their meanings are effortlessly called to mind, and their use as interface elements would likely benefit usability and the users' performance. However, using symbols that are less well known to the user population (or those with less concrete referents) may, at least initially, make an interface more difficult to use as compared to one based on text. It is often pointed out that words are easily recognized, very specific symbols, and for this reason text labels are frequently presented along with symbols or icons. That having been said, it is important to note that users of NPP interfaces will be very experienced with them (through training and routine use) so that well designed and consistently used symbols will be rapidly learned. Concerns about novice users' difficulties with abstract symbols probably are less of a concern in the present context than they are in other domains.

⇒ 4.1.6.4-1 Symbols and icons should be simple and immediately recognizable.

Symbols and icons should

- be easily discriminable from all other icons and symbols – e.g., simple, distinctive figures with continuous outside borders will be recognized more reliably
- always be displayed 'right-side-up' and should be large enough for users to perceive their distinguishing features; use symbols size in coding is addressed in Size.

⇒ 4.1.6.4-2 The meanings of icons and symbols should be obvious.

The following considerations are usually involved in selecting symbols that are adequately familiar to the users.

- Symbols that represent abstract concepts, especially those that were not previously used in a plant, should be used only after testing by typical users has confirmed that they can be readily understood after some simple training.
- Where new symbols are being introduced which may not be particularly familiar or involve an abstract concept, consider including some minimal text with the symbol.

- For symbols used on VDU screens, consider adding “pop-up” text screens where the symbol represents a complicated or abstract idea. Note that it is generally not good practice to have the “pop-up” menus for only a few of the symbols. The difference violates the user’s expectation that all symbols of the same type behave the same.

⇒ 4.1.6.4-3 Icons and symbols used in interfaces should conform to existing conventions and users’ expectations.

The appearance and meanings of symbols should not conflict with

- formal plant conventions or guides
- industry or international standards (e.g. ANSI/ISA-S5.5 and ISO/IEC 11581)
- users’ expectations based on experience with consumer software and electronics

⇒ 4.1.6.4-4 The use and meanings of symbols should be consistent throughout the plant as well as within a given interface.

The following application steps are usually needed to achieve a consistent set of symbols:

- Establish or augment plant symbology conventions. This may require a detailed survey of sources such as plant documents, control stations, and existing digital displays. The survey may require user interviews (e.g., operators and maintenance technicians) to determine awareness of the symbols that are already in use. Ensure that the symbol conventions include complete information on the style (e.g., size, look, borders, etc.) of the symbols.
- Identify problems with current symbols. It would not be unusual to find that there are some particular symbols that have existing meanings that are somewhat ambiguous. In those cases, it may be best to avoid that symbol so that no connection to other uses is implied.
- Ensure that symbols are equally effective regardless of the medium by which they are presented (e.g., in text, labels, or on VDU screens). It may be necessary to create and test actual samples to confirm that all symbols that are intended to have the same meaning have the same “look.”
- Test new symbols and innovative uses of existing symbols to assure that users’ responses are as expected. As with any coding convention, however, users must first be trained on the coding convention before testing and implementation. Any test environments should replicate the ambient conditions of the actual control room as closely as possible. If degraded lighting conditions are a design condition, those conditions should be included in the testing.

⇒ 4.1.6.4-5 Icons or symbols that can be interacted with (e.g., that cause an action when clicked) should be readily distinguishable from those the have no such function.

If objects that are not associated with actions resemble those that are, users’ interaction with the interface will be disrupted; their actions may be slowed, or they may conclude that the system operates inconsistently or has malfunctioned.

⇒ 4.1.6.4-6 Changes in the 'look' of icons or symbols that are intended to convey the state of equipment or status of control systems should be conspicuous.

The symbol changes could involve change in such attributes as color, shape, size, orientation, texture, or brightness. It is important that the two states contrast each other sufficiently to detect reliably the change in function or meaning. Symbols that look like buttons and switches can often be made to mimic the action of real-world counterparts. That is, symbols of a button that are pressed can remain in what looks to be a pressed state. This is usually accomplished with graphic effects such as shadowing on the button that changes from the *IN* and *OUT* positions. Similarly, representations of toggle switches can be designed to move from one position to the other. Related guidance can be found in Section 4.3.6, Feedback and Monitoring (Soft Controls).

⇒ 4.1.6.4-7 The layout and arrangement of groups of symbols should follow a consistent and defined logic.

The following considerations are usually involved in establishing the layout and arrangement of symbols.

- Layouts or arrangements of symbols that appear in a group should normally follow conventions similar to those expected for other controls and displays, e.g., numerical and alphabetical progressions, or correspond to physical component or plant arrangements.
- Ensure that where it is intended to use a symbol as part of a group of symbols, confirmation testing is performed of representative groupings, in addition to testing of individual symbols.

⇒ 4.1.6.4-8 The primary use of icons in graphic displays should be to represent actual objects or actions.

Icons may be used to graphically represent operations, processes, and data structures, and may be used as means of exercising control (e.g., by selecting an icon and commanding operations) over system functions, components, and data structures.

⇒ 4.1.6.4-9 Icons should be designed to look like the objects, processes, or operations they represent, by use of literal, functional, or operational representations.

Some pictorial symbols have conventional meanings within a user population, which must be followed to ensure their correct interpretation. Examples of representations: literal, a figure of a pump; functional, a figure of a file cabinet; and operational, a hand on a switch.

⇒ 4.1.6.4-10 Each icon and symbol should represent a single object or action, and should be easily discriminable from all other icons and symbols.

The distinguishing feature between icons should be the external geometric configuration of the icon.

⇒ 4.1.6.4-11 Special symbols to signal critical conditions should be used exclusively for that purpose.

⇒ 4.1.6.4-12 Words and symbols should not be used alternately.

Alternate use of symbols and words could cause confusion and impair task performance.

⇒ 4.1.6.4-13 Icons and symbols should be large enough for the user to perceive the representation and discriminate it from other icons and symbols.

When a displayed symbol of complex shape is to be distinguished from another symbol shape that is also complex, the symbol should subtend not less than 20 minutes of arc at the required viewing distance. VDU-displayed symbols that must be distinguished from other complex shapes should have a minimum of 10 resolution elements for the longest dimension of the symbol.

⇒ 4.1.6.4-14 An icon or symbol should be highlighted when the user has selected it.

⇒ 4.1.6.4-15 Icons that may not be immediately and unambiguously recognized should be accompanied by a text label.

To the extent that it does not clutter or cause distortion of the icon, the label should be incorporated into the icon itself. When icons are designed such that the label is inside the icon, the number of perceptual objects is reduced, resulting in enhanced processing of the label and the icon. The text label may be omitted for icons having unambiguous meanings to users, e.g., standard P&ID symbology.

⇒ 4.1.6.4-16 If icons are used to represent control action options, a label indicating the action should be associated with the icon.

4.1.6.5 Labels

A label is a descriptive item used to identify displayed screen structures or components. Labels are used for controls, indicators, and other display elements to help users locate and identify these elements. The appropriate and clear use of labels should permit rapid and accurate human performance.

In general, the use of labels with modern information displays is similar to label use with conventional control room equipment.

This section includes guidance on the following topics:

- labeling principles
- label location
- label content
- label lettering

4.1.6.5.1 Labeling Principles

⇒ 4.1.6.5.1-1 Controls, indicators, and other individual display elements that must be located, identified, or manipulated, should contain appropriate, distinct, unique, and descriptive labels.

⇒ 4.1.6.5.1-2 A hierarchical labeling scheme should be used to reduce confusion and search time.

⇒ 4.1.6.5.1-3 Major labels should be used to identify major systems, subordinate labels should be used to identify subsystems or functional groups, and component labels should be used to identify each display element.

If needed for clarity, engineering characteristics or nomenclature may also be described in the label.

⇒ 4.1.6.5.1-4 Labels should be consistent within and across panels in their use of words, acronyms, abbreviations, and part/system numbers.

⇒ 4.1.6.5.1-5 All discrete functional control positions (for example, "ON" and "OFF" positions of a particular controller) should be labeled.

4.1.6.5.2 Label Location

⇒ 4.1.6.5.2-1 Control and indicator labels should be located consistently, either below or above the display element, especially on the same display.

⇒ 4.1.6.5.2-2 Avoid placing adjacent labels together. Labels should be separated one from another by at least two standard character spaces.

⇒ 4.1.6.5.2-3 The labels used to identify a group of controls and or indicators corresponding to major systems or functional groups (subsystems) should be located above that group.

⇒ 4.1.6.5.2.4 Curved patterns should not be used for labeling.

Labels should be positioned along a straight line, even if the corresponding control has a circular shape.

⇒ 4.1.6.5.2-5 Labels should not detract from or obscure any other information displayed on the screen that must be read by the user.

⇒ 4.1.6.5.2-6 Labels should not be obscured by other information displayed on the screen.

⇒ 4.1.6.5.2-7 The label for a specific graphical object (i.e., an icon) should be placed in close proximity to the object.

If multiple graphics or parts of a graphic object are close to a label, a line should point from the label to the associated graphic or part. Otherwise, the user may assume that the label refers to the closest or to all graphics or parts.

⇒ 4.1.6.5.2-8 Labels may be placed directly on certain types of components (e.g., pushbuttons) for the purpose of increasing the utility and efficiency of control identification.

When using these types of labels, the following precautions should be observed:

- The label should not rotate (i.e., when the control rotates),
- The control surface area should be sufficient to apply a full legible label, and
- The label should be fully visible in any position the control image may take on the display screen.

⇒ 4.1.6.5.2-9 Control position information should be visible to the user before, during, and after operation of the control.

⇒ 4.1.6.5.2-10 The user should not be allowed to move or hide labels for any visual display components, excepting graph legends.

A user may choose to relocate a graph legend within predefined limits of proximity to the graph. For more guidance, see Section 4.1.5.6, Graphs.

4.1.6.5.3 Label Content

⇒ 4.1.6.5.3-1 Use common terms that originate form typical language usage and/or from standard terminology for nuclear power plants.

⇒ 4.1.6.5.3-2 Trade names and other irrelevant information should not appear on labels.

⇒ 4.1.6.5.3-3 Use whole words rather than abbreviations whenever space permits.

⇒ 4.1.6.5.3-4 Use standard abbreviations as created and used at the plant.

The list of abbreviations has to be checked for duplicates; the same abbreviations should not be used for multiple labels.

⇒ 4.1.6.5.3-5 Use standard acronyms if they have been well established.

⇒ 4.1.6.5.3-6 Avoid the use of words that may be interpreted as both a noun or adjective and as a verb (e.g., "OPEN" in the case of "OPEN VALVE").

⇒ 4.1.6.5.3-7 Words and abbreviations of similar appearance should be avoided where an error in interpretation could occur.

⇒ 4.1.6.5.3-8 When special precautionary words are required, select ones that provide an appropriate sense of urgency, hazard, or danger.

While precautionary words should imply serious consequences, avoid the use of words that may have a negative psychological effect, for example, "Life-Threatening Condition", etc.

⇒ 4.1.6.5.3-9 All danger, warning, and safety instruction labels should be designed in accordance with appropriate safety standards.

⇒ 4.1.6.5.3-10 The label should briefly and simply express the intended action of controls or the meaning of the given indication.

Words on labels should be concise and still convey the intended meaning. Label text should not be so brief that its meaning isn't clear to operating personnel.

⇒ 4.1.6.5.3-11 Nomenclature printed on labels should be consistent with that used in procedures.

⇒ 4.1.6.5.3-12 When presenting a list of options, labels should reflect the question or decision being posed to the user.

4.1.6.5.4 Label Lettering

⇒ 4.1.6.5.4-1 Labels should be uniquely and consistently highlighted, boxed, or otherwise emphasized to differentiate them from other screen structures and data.

The technique used should be easily distinguished from that used to highlight or code emergency or critical messages.

⇒ 4.1.6.5.4-2 Always use capital letters for labels and not a mix of capital and lowercase letters.

Exception can be made for extended messages, where only acronyms and the first letter of proper nouns and the first word may be capitalized. Periods and commas should be omitted from labels, unless they are indigenous to the item being identified.

⇒ 4.1.6.5.4-3 The lettering for all labels should be oriented so that they read from left to right, not around corners, on their side, or up and down.

Users should be presented with horizontally displayed labels, even for the vertical axis of a graph. A conventional text orientation of labels will permit faster, more accurate reading.

⇒ 4.1.6.5.4-4 Labels should be graduated in size such that the labels used for the group on the higher hierarchy level are about 25 percent larger than the labels used for the group on the preceding level of hierarchy.

⇒ 4.1.6.5.4-5 Absolute label size should be determined starting with the smallest lettering size that will be compatible with the display resolution and the typical average viewing distance.

⇒ 4.1.6.5.4-6 Lettering and background colors should provide high contrast and legibility.

Dark letters on a light background are preferred.

⇒ 4.1.6.5.4-7 Ensure that all numbers and characters are clearly distinguishable.

Numbers such as “0”, “1”, “2”, and “5” can sometimes be confused with the letters “O”, “I”, “Z”, and “S”. Additional problems can arise when numbers or characters are not correctly spaced. Labels with odd spacing can impair reading speed and comprehension.

4.1.6.6 Scales, Axes, and Grids

Scales, axes, and grids are used to graphically represent data. Axes are the graphical representation of orthogonal dimensions in the form of lines (e.g., the horizontal and vertical axes of a plot may be the X and Y dimensions, respectively). A scale is a graduated series of demarcations indicating the divisions of an axis. A grid is a network of uniformly spaced horizontal and vertical lines for locating points by means of coordinates.

⇒ 4.1.6.6-1 Numbers on a scale should increase clockwise, left to right, or bottom to top.

⇒ 4.1.6.6-2 Nine should be the maximum number of tick marks between numbers.

Major and minor graduations should be used if there are up to four graduations between numerals. Major, intermediate, and minor graduations should be used if there are five or more graduations between numerals.

⇒ 4.1.6.6-3 Scales should have tick marks at a standard interval of 1, 2, 5, or 10 (or multiples of 10) for labeled divisions; intervening tick marks to aid visual interpolation should be consistent with the labeled scale interval.

Users will find it difficult to interpret scales based on odd intervals. It is not advisable to let the computer divide available scale space automatically if that results in a scale labeled in unfamiliar intervals such as 6 or 13. In special instances, the X-axis might be scaled in odd intervals to show customary divisions, such as the 12 months in a year.

⇒ 4.1.6.6-4 For one-revolution circular scales, zero should be at 7 o'clock and the maximum value should be at 5 o'clock.

⇒ 4.1.6.6-5 Axes should be clearly labeled with a description of what parameter is represented by the axis.

Labels should be displayed in upright orientation on both the X- and Y-axis for ease of reading.

⇒ 4.1.6.6-6 The units of measurement represented by the scale should be included in the axis label.

⇒ 4.1.6.6-7 Conventional scaling practice should be followed, in which the horizontal X-axis is used to plot time or the postulated cause of an event, and the vertical Y-axis is used to plot the effect.

When the X-axis represents time intervals, the labeled scale points should represent the end of each time interval. This consistent usage will aid interpretation of all data plots, including scatterplots, line graphs, and bar charts.

⇒ 4.1.6.6-8 If users must compare graphic data across a series of displays, the same scale should be used for each.

Note that in many applications it may prove more effective to display data for comparison in a single combined chart, rather than requiring users to compare data across a series of charts. Users will find it difficult to compare data sets that are scaled differently. Moreover, users may overlook differences in labeling, and assume that the same scale has been used even when displayed scales are actually different from one another.

⇒ 4.1.6.6-9 The scales should be consistent with the intended functional use of the data.

Scales should be selected to (1) span the expected range of operational parameters, (2) employ appropriate scale ranging techniques, or (3) be supported by auxiliary wide-range instruments. For example, the monitoring of neutron flux at reactor trip must have a variable scale of 0 to 100 percent of the design value and a time scale resolution of seconds. However, post-trip monitoring may have a variable scale of 0 to 10 percent with a time scale resolution of minutes. Finally, operational log data of neutron flux may have a time scale resolution of hours.

⇒ 4.1.6.6-10 A linear scale should be used for displayed data, in preference to logarithmic or other non-linear methods of scaling, unless it can be demonstrated that non-linear scaling will facilitate user interpretation of the information.

Most users are more familiar with linear scales and will interpret linear scales more accurately than other methods of scaling. However, since logarithmic scales show percentage change rather than arithmetic change; they may be appropriate for some special applications.

⇒ 4.1.6.6-11 When users must compare aggregate quantities within a display, or within a series of displays, scaling of numeric data should begin with zero.

Numerical scales generally should have zero at the bottom as the first number on a vertical scale or at the left as the first number on a horizontal scale. The exceptions to this organization would be: (1) if the numbers are used for naming categories, (2) if zero is not a plausible number on the scale, or (3) if the scale contains negative numbers. If for any reason the zero point is omitted, the display should include a clear indication of that omission, and the scales on which quantities are to be compared should be the same.

⇒ 4.1.6.6-12 When graphed data represent positive numbers, the graph should be displayed with the origin at the lower left, such that values on an axis increase as they move away from the origin of the graph.

When the data include negative values and the axes must extend in both directions from a zero point, that origin should be displayed in the center of the graph.

⇒ 4.1.6.6-13 Only a single scale should be shown on each axis, rather than including different scales for different curves in the graph.

Single-scale graphs will generally permit more accurate reading than graphs displaying several scales. Many users will be confused by multiple-scale graphs and make errors when interpreting them. Moreover, by changing the relative scale factors of multiple-scale graphs, it is possible to change radically their apparent meaning and bias interpretation by users.

⇒ 4.1.6.6-14 If different variables on a single graph require different scales, they should be scaled against a common baseline index, rather than showing multiple scales.

Rather than showing power in megawatts and profits in dollars, both might be graphed in terms of percent change from a baseline. An indexed chart can permit comparisons among different variables when multiple scales would otherwise be needed. However, care should be taken in selecting an appropriate baseline against which to index, in order to ensure that comparisons will not be biased. Index scaling may also be appropriate for showing the effect of a single variable whose units of measurement change in real value with time.

⇒ 4.1.6.6-15 When a graphic display has been expanded from its normal coverage, some scale indicator of the expansion factor should be provided.

Scale ranges may be expanded (or contracted) by multiplying or dividing indicated scale values by powers of ten. All such scales should be clearly marked as to whether the indicated values should be multiplied or divided, and the factor to be used (e.g., 10, 100, or 1000).

⇒ 4.1.6.6-16 Users should be able to manually change the scale to maintain an undistorted display under different operating conditions.

⇒ 4.1.6.6-17 If the system is designed to automatically change scale, an alert should be given to the user that the change is being made.

Automatic rescaling can lead to confusion if the change in scale is not recognized.

⇒ 4.1.6.6-18 If interpolation must be made or where accuracy of reading graphic data is required, computer aids should be provided for exact interpolation.

It might suffice, for example, to allow users to request a fine grid as an optional display feature. It might be better to display vertical and horizontal rules that a user could move to intersect the axes of a chart. It might prove best simply to let a user point at any data item and have the computer label that item with a readout of its exact value(s).

⇒ 4.1.6.6-19 When grid lines are displayed, they should be unobtrusive and not obscure data elements (e.g., curves and plotted points).

Grid lines should be thinner than data curves, and should be invisible behind depicted objects and areas. Heavy grid lines may conceal details of plotted data. Electronic displays offer more flexibility than printed graphs. Grids can be displayed or suppressed by user selection. For reading the value of a particular data point, perhaps no grid is needed at all. A user might simply ask the computer to display the value of any selected point.

⇒ 4.1.6.6-20 Graphs should be constructed so that the numbered grids are bolder than unnumbered grids.

If 10-grid intervals are used, the fifth intermediate grid should be less bold than the numbered grid, but bolder than the unnumbered grids.

⇒ 4.1.6.6-21 When data comparisons of interest fall within a limited range, the scaled axis should emphasize that range, with a break in the displayed axis to indicate discontinuity with the scale origin.

Note, however, that a broken axis distorts the displayed value in relation to a base value and so risks confusing users. In effect, a user will expect that a scale marked in regular intervals will continue in a consistent fashion. If an axis must be broken, the break should be labeled clearly, perhaps with some indicator that extends across the displayed graph.

⇒ 4.1.6.6-22 When scaled data will contain extreme values, duplicate axes should be displayed, so that the X-axis appears at both the top and bottom, and the Y-axis at both the left and right sides of the graph.

Extreme data values may be located far from conventionally placed axes. When duplicate axes are displayed at the top and right side, users will find it easier to read the extreme values.

⇒ 4.1.6.6-23 Unless required, use of three-dimensional scales (i.e., where a Z-axis is added to the display) should be avoided.

Showing a Z-axis on a VDU display that is limited to two actual dimensions will confuse many users. If three-dimensional scaling is employed, a consistent method of representation (e.g., isometric or orthographic projection, perspective drawing, or triangular coordinate grid) should be used. It is often possible in graphic display to show a third dimension through use of auxiliary coding (e.g., color or shape coding, or supplementary annotation), which may prove more effective than trying to represent a third spatial dimension pictorially.

4.1.6.7 Borders, Lines, and Arrows

Borders, lines, and arrows are basic elements used to present information graphically. Lines are used to connect objects or to provide a demarcation between objects. A border is a set of demarcation lines that frame an object or group of objects. Arrows are lines that indicate direction.

These elements should not be included in an interface design solely for purposes of ornamentation. Because adding lines or borders can increase the level of visual 'noise' or clutter in a display (making it more difficult to read), it is often preferable to separate or group information using 'white space,' i.e., to indicate the relatedness of sets of data by using spatial proximity and alignment. In a dense data display, when using spacing is not an option, careful use of borders and lines can improve the readability of the display. In some cases the same result can be achieved by using colored backgrounds to separate or group data.

⇒ 4.1.6.7-1 Meaningful differences between lines appearing in graphic displays, such as flow paths, should be depicted by using various line types, e.g., solid, dashed, dotted, and widths.

Three or four line types may be readily distinguished, and two or three line widths may be readily distinguished. A line displayed on a VDU will appear continuous if the separation between resolution elements is less than one minute of arc. To provide the illusion of continuity, graphic lines should contain a minimum of 50 resolution elements per inch.

⇒ 4.1.6.7-2 In flow charts and other graphics displays, arrowheads should be used in a conventional fashion to indicate directional relations in the sequential links between various elements.

⇒ 4.1.6.7-3 Unnecessary borders should not be used in the display.

⇒ 4.1.6.7-4 A border should be used to improve the readability of a single block of numbers or letters.

⇒ 4.1.6.7-5 If several labels or messages are clustered in the same area, distinctive borders should be placed around the critical ones only.

4.1.6.8 Visual Characteristics

As discussed in the general treatment of coding and highlighting (Section 4.1.4.4), variations in the visual characteristics of display elements are often used for

- showing the relatedness of a group of elements (e.g., those pertaining to a given system)
- emphasizing particular elements (e.g., data that are not validated)
- conveying information about displayed data (e.g., relationships of values to setpoints)

Among the characteristics are available for use are:

- color
- size
- shape
- pattern
- brightness
- flashing.

Each method has its own advantages and drawbacks, which will be discussed briefly in their respective subsections. General guidance on coding is given in Section 4.1.4.4. Coding of the relatedness of information by its spatial location is treated in the context of organizing information on display pages (Section 4.1.4.2). Use of spatial position to code priority is discussed in the context of alarms (Section 4.4, Alarms).

4.1.6.8.1 Color

Modifications of the human system interface often involve the use of colors. If the digital upgrade does not change the methods of displaying information and the controls provided for the users, it is unlikely that color usage will be a significant consideration in the design process. Note, however, that it will be necessary to ensure that existing plant color usage and conventions are maintained. For this reason, the consistency with existing color usage will be important even though the modification itself is quite minor. The following application steps are usually needed to achieve consistent color use.

- identify and document existing color usage in the particular plant – survey plant documents, control stations, and existing digital displays, interview users on their awareness of the existing conventions.
- identify potentially confusing or inconsistent uses of color in different contexts – choose colors to be used in digital upgrades to avoid conflicts with current practices.
- test new and innovative use of colors on users to assure that their response is as expected and desired –test environments should replicate the colors and ambient conditions of the actual control station as closely as possible.

Changing a color code for a specific part of the plant (or the entire plant, for that matter) could result in confusion and lead to errors. Users should not have to keep track of what system they are concerned with or where they are physically located in the plant to understand the meaning of a color code. However, the same colors may be employed for several primary uses (e.g., equipment status, alarm category, parameter range, equipment group, etc.), as long as the user can readily distinguish the context. For example, the color red can be used on mimic displays to indicate operating equipment, on alarm displays to indicate high priority alarms, and on individual parameter displays to indicate that a value is outside of its allowable range, on an electric mimic to indicate a voltage level without confusing the user. Color coding within a primary use should be consistent throughout a facility.

If the modification is limited in scope, it us usually best to avoid changes in any established uses of colors. As the extent and scope of a modification becomes larger, changes from past practices may become more practical. Note that introducing a new color is generally relatively easy, introducing an additional meaning to an existing color is more difficult, and totally changing the meaning of an existing color may be impractical.

When a modification results in changes to the way information is displayed, for example, the additions of VDUs, the addition of group displays, changes in alarm presentations, or adds soft controls (and their related displays); color selection and utilization can become a part of the design activities. In this case respecting existing color use becomes more complicated. The search for existing color usage and conventions will need to be widened to include color use in portions of the plant beyond the control areas. The ease with which color can be changed in some digital displays, especially VDUs, provides the opportunity to use color much more extensively than could be done with conventional controls and displays. Complicated color uses are, therefore, much more practical. In particular, color coding to indicate status of systems or components can be more complicated than simply indication whether “running” or “not running.” With proper supporting software logic colors can be used to indicate “normal” and “abnormal.” It should be recognized that these more complicated color usages often involve substantial engineering effort and additional programming. For example, a normal/abnormal color code must be unambiguous and be correct for all plant conditions, otherwise it has the potential to mislead the operators.

⇒ 4.1.6.8.1-1 Color use and the meanings attached to colors should be consistent throughout the plant as well as within a specific upgrade project.

Colors for coding should be based on user conventions with particular colors. Some examples of typical color meanings are summarized in Table 4-7.

These are not intended to be recommendations. They are only examples of color uses over a number of plants. Because there are a variety of practices throughout the nuclear industry, it is not practical to establish a color code that is compatible with all plants. As discussed previously, color codes should be established on a plant-specific basis with consideration of the existing practices at the particular plant. In the case of the examples it is important to note that some meanings clearly cannot be used in the same context. An example of that conflict would be an attempt to use the red/green color pair to mean off-normal/normal as well as using the same color pair to mean on/off. That is, it could well be that the normal condition is on, which would lead to need to make the same indication both green and red. There are many other obvious potential conflicting color examples, such as the use of blue to represent both “bypassed” and “normal.” There could easily be a system where bypassed was, in fact, abnormal. The potential for conflicting meanings coupled with the inherent limits on the number of colors that can be used, make extensive use of color coding difficult.

⇒ 4.1.6.8.1-2 Color should be utilized as part of the overall labeling and demarcation strategy.

The following is a listing of some specific uses of color for labeling and demarcation that may be applicable to digital upgrades:

- On individual parameter displays, such as bar charts, colors can be used to code by parameter type, e.g., red for temperature indications, blue for level indications, green for pressure indications, etc.

- Colors may be used to identify information that is of a different character than provided by other similar labels. For example, on conventional labels, labels that define power sources for components may be a distinctive color.
- For mimic-type displays, color can be used to distinguish components and flow paths of different systems. On large, complex displays, it is often impractical to color-code down to the individual systems, but it may be useful to capture the broader groupings, such as steam, reactor coolant, air, and cooling water systems.
- Colored lines or blocks of background color can be used to segregate (demarcate) groups of controls or indicators. A separate color can be used for each identified group. It is sometimes necessary to choose these colors to maximize the contrast of adjacent colors, similar to the way a cartographer chooses map colors.

Because color perception is complicated and can be affected by many factors, it is usually best to mock up the uses of color in prototypic circumstances, especially lighting and the presence of adjacent displays. It is especially important to mockup the use of color for demarcation purposes. Where different ambient lighting level may be present, the testing should include those different levels.

⇒ 4.1.6.8.1-3 Color should be used as part of the overall strategy to emphasize particular items of information.

Use of color for this purpose should follow guidance on highlighting (Section 4.1.4.4), especially the recommendations that it should be used sparingly and should not interfere with the displayed information.

Bright colors (i.e., high salience) should be used only where essential for emphasis or recognition. Such uses should be tested under conditions that simulate the actual application to ensure that they do not distract the users from their intended meaning. Some of the more aggressive, unnatural colors may detract from their intended meaning. Extremely vibrant colors can induce eyestrain, which will affect human performance. For example, saturated green and red seem to vibrate when they are placed next to each other.

⇒ 4.1.6.8.1-4 Colors should be considered for use as part of the overall strategy to identify the status of components or systems.

The following is a listing of some specific uses of color to indicate status that may be applicable to digital upgrades. In all cases it is particularly important to maintain existing plant practices and standards.

- Color coding can be used to indicate the operational status (e.g., whether they are OFF or ON) of components
- Status color-coding can be used to distinguish between control modes (e.g., MANUAL or AUTOMATIC).
- Color can be used to indicate when a system or component is selected for STANDBY operation, or to distinguish other states, such as unavailable, tagged out, locked out, or being tested.

Color has been extensively used on conventional controls and displays to indicate the status of components, e.g., ON or OFF. That is, one color (often red in power plants) is used to indicate running motors and pumps, open valves, and closed breakers, and a contrasting color (often green in power plants) is used to indicate that the same component is in the opposite state. The use of color for status indication in a digital upgrade must be carefully matched to such existing color stereotypes and conventions, including those at local control stations.

⇒ 4.1.6.8.1-5 Color should be considered for use as part of the overall strategy to convey the magnitude of measured quantities.

Figure 4-21 shows the use of colors to the core power distribution. Note that the colors used to represent power ranges are not arbitrary; most people will assume an ordering corresponding to the visible light spectrum and draw appropriate inferences about the relative magnitudes in different parts of the core. However, the color depiction can nevertheless be confusing or misleading. Users might make incorrect judgments about the sizes of the differences based on the judged similarity between colors (e.g., areas coded with red and orange being more similar in magnitude than those coded with yellow and green). This underscores the importance of including a legend in coded displays.

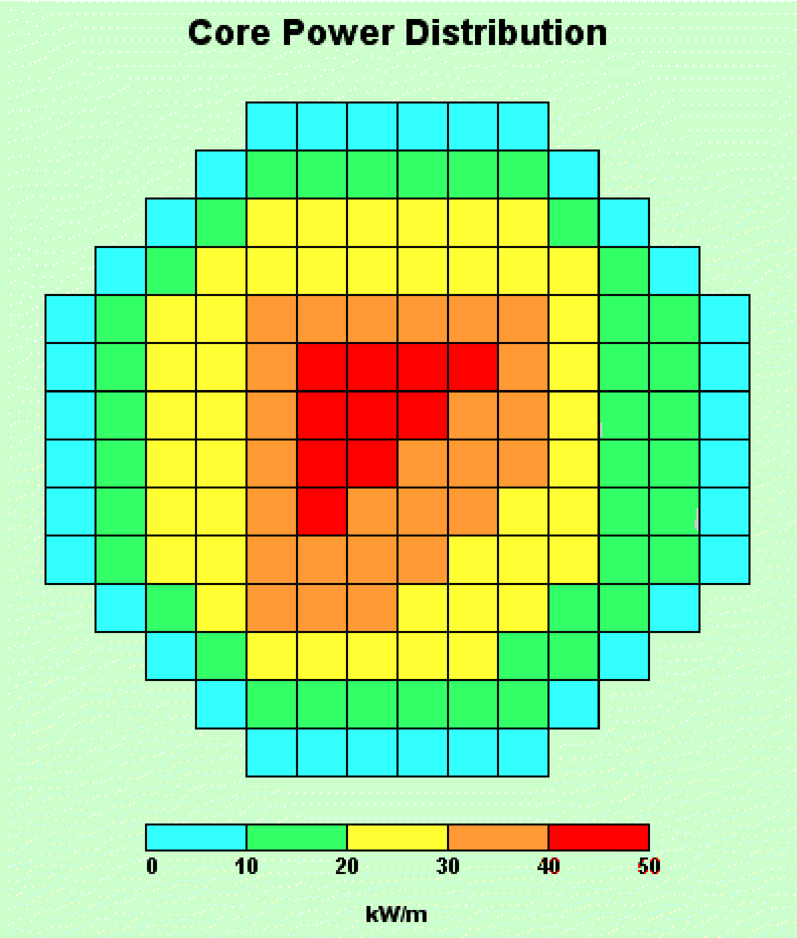


Figure 4-21
Use of Color to Code the Magnitude of a Parameter

The tendency for people to perceive colors categorically might also lead to confusion. For example, the red section may indicate a dangerous situation, or it may just be one increment beyond orange. To avoid such an inference, the required range of magnitude may be coded using only lightness or density, as shown in (Figure 4-22), which uses varying shades of gray to show incremental changes in core power levels. Color added to such a display to indicate values above limits would be unambiguous and very salient.

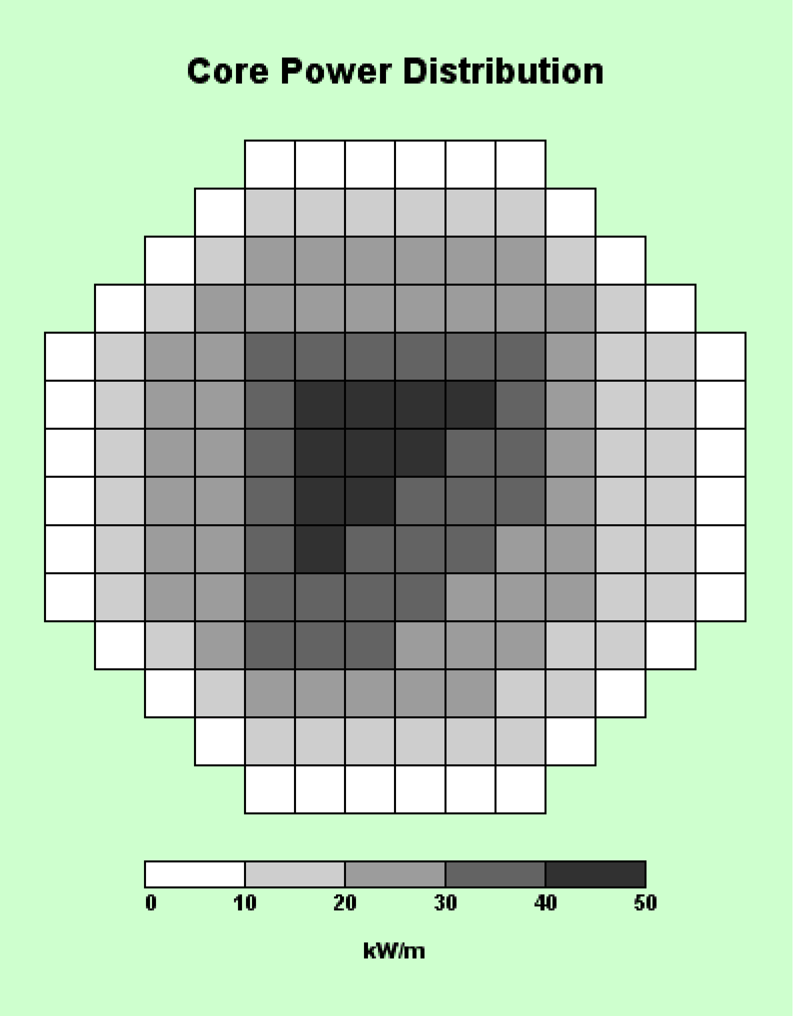


Figure 4-22
Use of Monochromatic Variations ('Density') to Code the Magnitude of a Parameter

(Note that the monochromatic presentation is not immune to misinterpretation. It depends on a natural tendency to see darker shades as "more" of something, in this case more power. However, in this particular case, there is a potential conflict with the natural tendency to see brighter colors as "hotter," which works against the desired representation. This demonstrates the importance of taking users' expectations into account in designing information displays.)

Such a presentation is appropriate when the relative rather than the absolute values of a variable are important For example, in displaying tank depth, a saturated blue might be used to show the deepest point, with gradually desaturated blues to show decreasing depth. Gradual color changes should not be used when absolute values are important, or to code data into discrete categories. For example, gradual color changes should not be used to indicate the level of a storage tank as it is drained or filled. Instead, a set of discrete codes indicating dangerous and acceptable levels may be more appropriate.

⇒ 4.1.6.8.1-6 The number of colors should be limited to those that can be easily distinguished.

The following guidance applies to the selection of colors:

- The requirement for reliable recognition limits the set of colors that may be assigned different meanings to approximately six.
- Fewer than six colors may have to be used where the viewing environment involves low lighting or other distractions. Additional colors may be practical under more favorable conditions.
- Typical users should test actual colors for adequate discrimination under conditions that closely simulate the actual application. It is especially important to test all ambient lighting conditions.

Designers must also be cautious in the use of colors because some members of the population have difficulty distinguishing between certain colors. This leads to the practice of not counting entirely on color to convey a meaning. (See also the discussion of redundant coding.)

⇒ 4.1.6.8.1-7 Colors should have adequate contrast and luminance with respect to the surroundings.

While humans can identify thousands of different colors from one another, it may be difficult for users to read information unless there is contrast between adjacent colors. For example, the colors blue and purple may seem to blend together if they are put next to one another. When a user must be able to read detailed information, contrasting colors should be used, e.g., blue and yellow, or simply black and white. Contrast and luminance will have an affect on the number of different colors that can be used. (See the previous discussion on color selection.) Consequently, the selection of the number of colors needs to be considered considering the conditions of contrast and luminance.

Care needs to be taken to be sure that tests to confirm color selections involve prototypic conditions of contrast and luminance. This involves considerations of the colors of surroundings, adjacent displays, and ambient lighting levels and character. Colors that are used in applications that depend on discrimination from other colors should be tested under conditions that accurately simulate the actual application especially if there is a wide range of possible levels of ambient illumination. These tests also need to be on a scale large enough and with enough complexity to detect color effects that are distracting when applied to a full sized display. Sometimes, colors that appear suitable in isolation or at a small scale can result in garish and confusing effects when viewed in a more prototypic context.

⇒ 4.1.6.8.1-8 The uses of color as a coding should normally be backed up with another coding method.

If color alone is used as a coding method, there is a chance that the indication may be ambiguous. Consequently, some other means to code the indication should be provided. This approach can help to reduce errors in that it tends to require multiple errors for a user to misinterpret the information. Possible error modes may include deficiencies in users' color perception, equipment failures or limitations (e.g., failure that results in a monochrome display), and characteristics of ambient lighting. This is the reason that many warning notices usually involve both text and colors. Coding schemes that would be redundant to color include flashing, reverse video, size or shape changes, changes in font, changes in location or alignment, or the addition of text labels or symbols. For example, showing the change in state of a component in a display should not be done by only changing its color, another redundant scheme should be provided.

⇒ 4.1.6.8.1-9 When a user must distinguish rapidly among several discrete categories of data, a unique color should be used to display the data in each category.

Color coding of discrete categories (e.g., setpoint values and actual values) is particularly useful when data items are dispersed on a display. With some display equipment now providing a wide range of different colors, designers may be tempted to exploit that capability by using many different colors for coding. However, such a capability is not useful for coding discrete categories, except that it may allow a designer to select more carefully the particular colors to be used as codes.

⇒ 4.1.6.8.1-10 When color coding is used, each color should represent only one category of displayed data.

Color will prove the dominant coding dimension on a display. If several different categories of data are displayed, for example, in red, they will have an unwanted visual coherence that may hinder proper assimilation of information by a user.

⇒ 4.1.6.8.1-11 Color coding should not create unplanned or obvious new patterns on the screen.

The tendency for users to see similarly colored elements as related or grouped is strong. Designers should be alert to the possibility

⇒ 4.1.6.8.1-12 Colors and color combinations that may cause problems owing to the workings of color vision should be avoided.

Examples of potentially troublesome application of color include:

- combinations of vivid red and bright green colors (especially red symbols on a green background)
- simultaneous presentation of both pure red and pure blue on a dark background (this may result in chromostereopsis (an uncomfortable three-dimensional effect)

- dominant wavelengths above 650 nanometers
- pure blue on a dark background (especially for text, for thin lines, or for high-resolution information)

4.1.6.8.2 Size

Size coding is achieved by varying the size of displayed object. A larger size is often used to infer larger values, higher priority, more importance, etc.

⇒ 4.1.6.8.2-1 Use of size coding should be limited to avoid crowded displays.

If too many items on the screen can change in size, there is a possibility that they will begin to encroach on each another or even overlap if they all get larger.

⇒ 4.1.6.8.2-2 No more than three size levels should be used to represent for discrete information.

While people can compare two adjacent items and recognize very small variations in size, two or three item sizes are the most that will be recognized alone.

⇒ 4.1.6.8.2-3 Each discrete size should be between 50% and 100% larger than the smaller size.

The design of a control board or VDU usually limits the minimum viewable size and the maximum usable size used.

⇒ 4.1.6.8.2-4 Image proportions should be maintained when varying an image's size.

To ensure that an image is still recognizable, the image's proportions should remain the same.

⇒ 4.1.6.8.2-5 If size is used to convey quantitative information, the area should vary in proportion to the measurement.

People associate the area of an object (as opposed to its length or diameter) with its value.

4.1.6.8.3 Shape

⇒ 4.1.6.8.3-1 Shape coding should be used to represent discrete, nominal information, as opposed to relative values.

Shapes cannot be used to describe relative values or increments because they are not easily prioritized. For example, a triangle, a star, a circle, and a square do not have inherent relative value.

Coding with geometric shapes can be used (much like symbols) to help users discriminate different categories of data on graphic displays. Controls or indicators frequently have specific shapes to indicate their categories. For example, soft controls may be designed as circles, to imitate pushbuttons, while new software alarm indicators may be rectangular, like traditional light panels. Similarly, different controls may have specific shapes depending on;

- the system they control (e.g., residual heat removal, control rod drive, etc.),
- their control action (e.g., activate a pump, control a valve, or operate a control rod), or
- their physical function (e.g., pushbuttons versus rotating controls).

Some shape codes may have inherent meaning and others can be mnemonic in form. However, their interpretation usually relies on learned associations as well as immediate perception.

⇒ 4.1.6.8.3-2 No more than 15 distinct and clearly identifiable shapes should be used.

Approximately 15 different shapes can be readily distinguished, provided the shapes are properly designed. Under adverse viewing conditions, no more than 6 shapes should be used.

4.1.6.8.4 Pattern

Pattern coding is used in many of the same instances as color coding, especially when color coding is not possible, or when a redundant coding technique is needed. Figure 4-23 shows a pattern code (none, horizontal, and diagonal) used for redundancy with conventional color coding of normal, marginal, and abnormal conditions. Patterns can also be used to demarcate groups of items, to identify particular items, or to indicate the status of items.

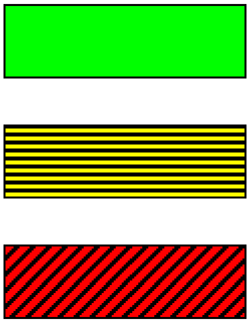


Figure 4-23
Example of Redundant Pattern Coding With Color Coded Indicators

⇒ 4.1.6.8.4-1 Pattern codes should be simple.

Simple patterns are easier to recognize and interpret, especially when they are varied (e.g., by density).

⇒ 4.1.6.8.4-2 When using pattern density to convey quantity, the least dense pattern should represent the lower extreme, and the densest pattern should represent the higher extreme.

This conforms to a ‘natural’ mapping that users will assume; see Figure 4-22.

4.1.6.8.5 Brightness

Brightness coding is often used to indicate priority, importance or status. However, people find it difficult to differentiate between many different brightness levels, so it is normally only used to describe binary (i.e., two-valued) conditions.

⇒ 4.1.6.8.5-1 No more than two levels of brightness coding should be used on VDUs.

Traditional light panels can use three levels (i.e., off, dim and bright), but these three levels are not as discriminable on VDUs. In particular, the “off” level is hard to implement on a VDU. Brightness coding should not be used in conjunction with shape or size coding since increasing a symbol’s brightness on a VDU may change its perceived shape or size.

⇒ 4.1.6.8.5-2 Higher brightness levels should signify more importance and higher priority.

4.1.6.8.6 Flashing

Flash coding is normally used to draw the users’ attention to an item of unusually high importance or priority, such as the highest priority alarms. Users generally associate flashing with something that they must look at or attend to immediately, and it can reduce the time a user spends searching through a block of text. When used improperly, flashing can detract from user comprehension and cause visual fatigue.

⇒ 4.1.6.8.6-1 Flash coding should be used very sparingly.

Only the most important information should use flash coding, in order to preserve the urgency of this coding method and to prevent visual fatigue.

⇒ 4.1.6.8.6-2 Flash coding should not be used on text or detailed data that must be read.

When flashing is used to attract attention to detailed information, flash a separate symbol near that information as opposed to the information itself.

⇒ 4.1.6.8.6-3 Only small area of the screen should flash at any time.

⇒ 4.1.6.8.6-4 No more than two flash rates should be used to ensure that the rates are clearly distinguishable.

The flash rate should be between 0.8 Hz and 5 Hz, and the light should be “on” for half of the time, if not more. When two blink rates are used, separate their rates by at least 2 Hz.

⇒ 4.1.6.8.6-5 Faster flashing rates should correspond to more critical information.

⇒ 4.1.6.8.6-6 Some method of flash suppression or acknowledgement should be provided.

⇒ 4.1.6.8.6-7 Flashing should not be used with long-persistence phosphor displays.

4.1.6.9 Auditory Coding

Auditory codes convey meaning through the use of sounds, such as tones. Current technology allows a wide variety of sounds to be generated and provides an opportunity to use audio coding to lessen the load on the visual 'channel' and to take advantage of the unique aspects of auditory perception (i.e., effectiveness of auditory signals does not depend on the user being oriented toward the interface or device, yet they can be localized if properly designed and presented).

Sounds are frequently used in computer-based systems to provide feedback for users' actions (e.g., acknowledging a selection or indicating an out-of-range input has been refused) or to make them aware of changes in the system (signaling the completion of a requested process or the updating of a display). Designers must be careful to ensure that sounds associated with the user interfaces of digital systems are compatible with existing uses of sound to convey information in the areas into which these systems are introduced. For example, interface-related signals should not be confusable with sounds used to alert users to changes in the plant (i.e., alarm signals), nor should there be any possibility of these interface-related sounds interfering with the audibility of sounds signaling plant conditions.

Furthermore, the characteristics of audio signals should be appropriate for the information they convey. For example, a sound signaling the selection of an unavailable display should not have a perceived urgency (intensity, harshness, or persistence) approaching that of a sound associated with an important and change in the plant.

In addition, when multiple computerized systems or devices are introduced into the same area, designers should ensure that audio signals they produce do not interfere with each other. For example, if several interfaces all use similar-sounding, difficult-to-locate, high-pitched beeps to convey information, a user will probably find the signals more distracting than informative. Similarly, signals should be designed and presented so that multiple users working in the same area are not distracted or confused by signals associated with others' workstations.

Note however that the aim may not always be to keep users from hearing sounds associated with other workstations. For example, operators' awareness of the audio feedback generated by others' interface actions may restore some 'openness' to a crew's interaction with a VDU-based interface, increasing their awareness of each other's actions and improving coordination.

⇒ 4.1.6.9-1 Auditory signals should be provided to alert the user to situations that require attention, such as an incorrect input action or a failure of the HSI to process an input from the user.

An auditory signal should provide users with a greater probability of detecting the triggering condition than their normal observations would provide in the absence of the auditory signal.

⇒ 4.1.6.9-2 Systems used to transmit non-verbal auditory signals should be used only for that purpose.

⇒ 4.1.6.9-3 Auditory signals should provide localization cues that direct users to those control room workstations where attention is required.

⇒ 4.1.6.9-4 Auditory signals should be selected to avoid interference with other auditory sources, including verbal communication.

⇒ 4.1.6.9-5 Advisory or caution signals should be readily distinguishable from warning signals and used to indicate conditions requiring awareness, but not necessarily immediate action.

⇒ 4.1.6.9-6 Auditory alerts, as well as caution and warning sounds, should accompany visual displays.

The audio signal should be used to alert and direct attention to the appropriate visual display.

⇒ 4.1.6.9-7 Once a particular auditory signal code is established for a given operating situation, the same signal should not be designated for some other display.

The meaning of each auditory signal should be clear and unambiguous.

⇒ 4.1.6.9-8 If the audio signal varies on one dimension only (such as frequency), the number of signals to be identified should not exceed four.

⇒ 4.1.6.9-9 One audio signal may be used in conjunction with several visual displays, provided that immediate discrimination is not critical to personnel safety or system performance.

⇒ 4.1.6.9-10 Audio warning signals that might be confused with routine signals or with other sounds in the operating environment should not be used.

Auditory signals intended to alert the user to a malfunction or failure must be different from routine signals such as bells, buzzers, and normal operating noises. Examples of such signals include trains of impulses that resemble electrical interference, or signals similar to noise generated by air conditioning or other equipment. The frequency of a warning tone should be different from that of the electric power employed in the system, to preclude the possibility that a minor equipment failure may generate a spurious signal.

⇒ 4.1.6.9-11 The intensity, duration, and source location of the signal should be compatible with the acoustical environment of the intended receiver as well as with the requirements of other personnel in the signal area.

Audio signals should not startle listeners, add significantly to overall noise levels, or prevent communication among users.

⇒ 4.1.6.9-12 Noncritical auditory signals should be capable of being turned off at the discretion of the user.

A simple, consistent means of acknowledging and turning off warning signals should be provided.

⇒ 4.1.6.9-13 When the signal must indicate which user (of a group of users) is to respond, a simple repetition code should be used.

⇒ 4.1.6.9-14 Sound sources (speakers or buzzers) should direct sound toward the center of the main operating area.

⇒ 4.1.6.9-15 When an audio signal must bend around major obstacles or pass through partitions, its frequency should be less than 500 Hz.

⇒ 4.1.6.9-16 Auditory alert and warning signals should be audible in all parts of the control room.

The guideline applies to warnings that need to be heard by all members of the operating crew. Some signals may be pertinent to a particular functional role and therefore may need to be heard only at workstations supporting that function. Where there is a concern that important information might be missed if the workstation is temporary not staffed, a general alert can be added if there is no response at the workstation for a specified period.

⇒ 4.1.6.9-17 The intensity of auditory signals should be set to unmistakably alert and get a user's attention.

A signal should generally yield a 20dB signal-to-noise ratio in at least one octave band between 200 and 5000 Hz. This level should apply throughout the main operating area. (A 20dB differential may not be necessary for all signals and all environments.) Auditory signal intensity should not cause discomfort or 'ringing' in the ears. Auditory signal intensities should not exceed 90 dB(A), except for evacuation signals, which may be up to 115 dB(A).

⇒ 4.1.6.9-18 When an audio signal must travel over 1000 feet, its frequency should be less than 1000 Hz.

⇒ 4.1.6.9-19 When the noise environment is unknown or expected to be difficult to penetrate, audio signals should have a shifting frequency that passes through the entire noise spectrum and/or be combined with a visual signal.

⇒ 4.1.6.9-20 Audio warning signals should not interfere with any other critical functions or warning signals, or mask any other critical audio signals.

⇒ 4.1.6.9-21 The audio display device and circuit should be designed to preclude warning signal failure in the event of system or equipment failure and vice versa.

Failure of auditory signal circuitry should not adversely affect plant equipment.

⇒ 4.1.6.9-22 Auditory alarm systems should be designed so that false alarms are avoided.

⇒ 4.1.6.9-23 Coding methods should be distinct and unambiguous, and should not conflict with other auditory signals.

⇒ 4.1.6.9-24 Similar auditory signals must not be contradictory in meaning with one another.

⇒ 4.1.6.9-25 Auditory signals may be pulse coded by repetition rate. Repetition rates should be sufficiently separated to ensure discrimination.

⇒ 4.1.6.9-26 If modulation of the frequency (Hz) of a signal denotes information, center frequencies should be between 500 and 1000 Hz.

⇒ 4.1.6.9-27 If discrete-frequency codes are used for audible signal coding, frequencies should be broad band and widely spaced within the 200 to 5000 Hz range (preferably between 500 and 3000 Hz).

The signal frequency of auditory displays should be compatible with the midrange of the ear's response curve, i.e., the use of signals with frequencies to which the ear is less sensitive should be avoided. No more than 4 separate frequencies should be used.

⇒ 4.1.6.9-28 Using the intensity of a sound to convey information is not recommended.

⇒ 4.1.6.9-29 It should be possible to test the auditory signal system.

4.1.7 Data Quality and Update Rate

The ability of personnel to use information depends to a great degree upon the quality of the data presented, including the frequency with which it is updated. Data quality considerations include the ways in which data from plant sensors are processed and checked for accuracy (e.g., analytical redundancy and data verification). It also includes the ways in which data quality (i.e., accuracy) is communicated to the user. Data update rate refers to the frequency with which data sensors are sampled and the contents of a display are refreshed.

⇒ 4.1.7-1 The maximum update rate should be determined by the time required for the user to identify and process the changed feature of the display.

The minimum and maximum update rate should be determined by the rate of change in the data, the requirements of the task, and the user's ability to process the information.

⇒ 4.1.7-2 The user should be capable of controlling the rate of information update on the display, but the allowable rate should not exceed that capable of being met by the information source and the processing equipment.

⇒ 4.1.7-3 Changing alphanumeric values that the user must reliably read should not be updated more often than once per second.

Changing values which the viewer uses to identify rate of change or to read gross values should not be updated faster than 5 times per second, nor slower than 2 per second, when the display is to be considered as real-time.

⇒ 4.1.7-4 When the computer generates a display to update changed data, the old items should be erased before adding new data items to the display.

This practice will avoid any momentary user confusion that might result from seeing portions of old data being overwritten and partially overlapped by new data.

⇒ 4.1.7-5 Items on a graphic display should not move faster than 60 degrees of visual angle per second, with 20 degrees per second preferred.

During motion, gross visual attributes and spatial orientation are usually preserved while small details may be lost or processing slowed. Perception of fast moving stimuli may be incomplete.

⇒ 4.1.7-6 The timeliness of displayed data should be such that, for the purposes of their tasks, users can consider it to represent current conditions at the time it is viewed.

The through-put capacity of the computer network should allow sampling and update rates that prevent any meaningful loss of information in the data presented. Any time delay from when the sensor signal is sampled to when it is displayed should be insignificant in the context of the user's task performance requirements.

⇒ 4.1.7-7 Data values displayed in any part of the workspace should be able to be considered, for purposes of users' tasks, consistent in time with all other displayed data.

⇒ 4.1.7-8 Each variable should be displayed with an accuracy sufficient for the users to perform their tasks.

The required accuracy should be determined by means of task analysis or through discussions with users.

⇒ 4.1.7-9 Variables that are subject to validation (e.g., checks for accuracy) should be identified and an indication should be provided when these data are invalid.

When data fails to meet the specified criteria for validity and thus is suspected of being of poor quality, an indication of validation failure should be provided.

⇒ 4.1.7-10 When checks for accuracy could not be performed, the unvalidated status of the data should be clearly indicated.

When checks for accuracy cannot be performed (e.g., a processor or redundant sensors are not available) the data is unvalidated. (Unvalidated data may be determined to be either valid or invalid as a result of the data validation process.) Under some conditions, unvalidated data may be useful to trained users in determining the status of the plant and determining whether human intervention is needed. Clear indications of the data's unvalidated status should be provided so the user can exercise judgment in interpreting it.

⇒ 4.1.7-11 Data entered by personnel should be identified such that it is easily distinguished from validated data.

⇒ 4.1.7-12 Analytical redundancy should be considered to help ensure the appropriateness of displayed values.

Analytical redundancy is the calculation of expected parameter values using a model of system performance. The expected value is then represented in the display, along with the actual value. Deviations between the two indicate some disturbance or abnormality of the system.

⇒ 4.1.7-13 A display feature should be provided to indicate to the user that the system is operating properly (or that a system failure has occurred).

Display of calendar date and time can allow users to determine whether a computer display is functioning. A programmed “heartbeat” indicator – a symbol or graphic element that flashes continuously as long as the display system is operational and the information is being updated on the display – also can be used. The heartbeat indicator must be actively programmed to create the flashing so that failure of the processor or display software will cause flashing to cease (as opposed to a flashing cursor or text element that may continue to flash under local hardware control even if the display processor or software is not functioning). A built-in testing feature that is activated either automatically or by the user may be used to assess operability of the display system.

⇒ 4.1.7-14 Information system failures (due to sensors, instruments, and components) should result in distinct display changes that directly indicate that depicted plant conditions are invalid.

The information system should be designed so that failures in instrumentation are readily recognized by operators. When panel instruments, such as meters, fail or become inoperative, the failure should be apparent to the user (e.g., through off-scale indication). This may be more difficult to determine in complex graphics, and thus, should be carefully evaluated.

⇒ 4.1.7-15 When task performance requires or implies the need to assess currency of information within a display, the information should be annotated with time information.

⇒ 4.1.7-16 When task requirements dictate that current information changes be continuously viewed and the display is changing so rapidly that the information is difficult to read, the user should have the capability of simultaneously viewing the information in a supplemental ‘snapshot’ display (i.e., a display frozen to enhance readability) along with the continuous display.

For example, if a numeric data display is changing rapidly and the user finds it difficult to read, it should be possible to display a frozen, unchanging value representing the data at the point of the request. The original display should continue to be presented.

⇒ 4.1.7-17 If a display has a freeze capability, the display should have an obvious reminder that it is in the freeze mode.

It is desirable to provide this information to the user in an attention-grabbing mode, such as with a flashing message.

4.1.8 Sources of Additional Information

ANSI/HFES-100, American National Standard for Human Factors Engineering of Visual Display Terminal Work Stations, The Human Factors Society, 1988.

ANSI/ISA-S5.5, Graphic Symbols for Process Displays, Instrument Society of America, 1985.

Danchak, M.M. (1981). Techniques for Displaying Multivariate Data on Cathode Ray Tubes with Applications to Nuclear Process Control. NUREG/CR-1994. Washington, DC: U.S. Nuclear Regulatory Commission.

Human Factors Guide for Nuclear Power Plant Control Room Development, Electric Power Research Institute, Palo Alto, August 1984. EPRI NP-3659.

Frey, P.R., Sides, W.H., Hunt, R.M., and Rouse, W.B. *Computer-Generated Display System Guidelines – Volume 1: Display Design*. EPRI, Palo Alto, CA: 1984. EPRI NP-3701.

Galitz, W.O. (1993). User Interface Screen Design. Wellesley, MA: QED Publishing Group.

IEC-964, Design for Control Rooms of Nuclear Power Plants. International Electrotechnical Commission, Geneva, 1989.

IEEE 1289, IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations, Institute of Electrical and Electronic Engineers, New York, May 27, 1998.

ISO/IEC 11581-1:2000(E), Information technology – User system interfaces and symbols – Icon symbols and function – Part 1: Icons – General, International Organization for Standardization, First edition, 2000.

MIL-HDBK-759C, Department of Defense Handbook for Human Engineering Design Guidelines, Revision C, U.S. Department of Defense, Washington, D. C. July 31, 1995.

MIL-STD-1472F, Department of Defense Design Criteria Standard - Human Engineering. U.S. Department of Defense, August 23, 1999.

Mulley, Raymond, Control System Documentation Applying Symbols and Identification, Instrument Society of America, 1994.

NUREG-0700, Human-System Interface Review Guidelines, Revision 2. U.S. Nuclear Regulatory Commission, Washington, D.C., March 2002.

________, Draft Human-Computer Interface Style Guide, Version 4.0, U.S. Department of Defense, Washington, D. C., December 21, 2000.

Tullis, T.S. (1988). Screen Design. In M Helander, ed., Handbook of Human-Computer Interaction. New York: Elsevier.

[ADDED re: Critical Data].

NRC (1984). Safety Parameter Display System (SPDS), Section 18.2 of the Standard Review Plan (NUREG-0800). Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (1984). Human Factors Review Guidelines for the Safety Parameter Display System (SPDS), Appendix A (formerly draft NUREG-0835) to Section 18.2 of the *Standard Review Plan* (NUREG-0800). Washington, DC: U.S. Nuclear Regulatory Commission.

Table 4-3
Information Grouping Principles

Grouping Method	Conditions for Appropriate Use
Task	Information necessary to support a user's task should be grouped together. See Section 4.1.3, Display Functions.
Sequence of Use	Where displayed information is used in spatial or temporal order, the information should be grouped by sequence of use to preserve that order. For example, data in a VDU display should match the order of steps in an associated paper procedure referencing the data. Information should be arranged sequentially from left to right or top to bottom.
Frequency	Where some information is used more frequently than others, the frequently used information should be grouped at the top or some other predefined location of the display.
Data Comparison	When users must analyze sets of data to discern similarities, differences, trends, and relationships, the display format should be structured so that the data are consistently grouped. Grouping similar items together in a display format improves their readability and can highlight relationships between different groups of data. Grouping can be used to provide structure in the display and aid in the recognition and identification of specific items of information.
Importance	Information that is particularly important should be grouped at the top or some other predefined location of the display.
Function	Where a set of information has strong functional relationships such as lower-level status indications that are related to a higher-level plant system (e.g., main feedwater) or function (e.g., core heat removal), the information should be grouped together to help illustrate those relationships.
Alphanumeric or Chronological Sequence	When items or data must be selected from a list or where there is no appropriate logic for grouping data according to some other principle, alphabetical or chronological grouping should be employed.

Table 4-4
Formats for Displaying Verbal Information

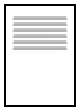
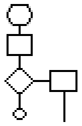
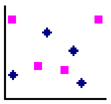
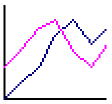
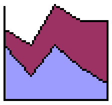
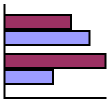
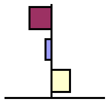
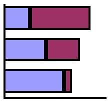
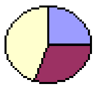
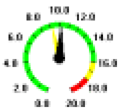
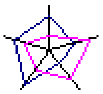
Display Format	Example	Usage Notes
Continuous Text		Present general descriptions, instructions, or procedures. Lists are preferred when a series of items are being presented.
Lists		Visual grouping of a series of related items is preferred over in-line (i.e., continuous text) presentation.
Flowcharts		Illustrate or guide a sequence of conditional judgments or decisions based on yes-no logic; not suited to decision processes involving tradeoffs.
Speech Displays		Transmit information when user's visual attention may not be direct at text displays. Best suited to brief messages. Not appropriate for supporting quantitative tasks.

Table 4-5
Data Display Formats and Usage Notes

Display Format	Example	Usage Notes
Scatterplots (4.1.5.6)		Show how two continuous variables are correlated (or not), or show the distribution of points in 2-dimensional space. Lines or curves may be superimposed to indicate functions relating the variables.
Line Graphs or Curves (4.1.5.6)		Show how two continuous variables are related to each other, especially changes in one variable over time. If time is included, it is typically plotted on the horizontal axis. A third, discrete, variable can be included using line-type or color coding.
Segmented Curve Charts (4.1.5.6)		Used when several line graphs or curves represent all the portions of a whole. The shaded areas stacked on top of each other represent each category's contribution to the whole.
Bar Charts and Histograms (4.1.5.5)		Show values of a single continuous variable for multiple separate entities, or for a variable sampled at discrete intervals.
Deviation Bar Charts (4.1.5.5)		A variation of the bar chart in which bars are constructed so that, under normal conditions, the bar ends lie in a straight line.
Segmented Bars or Columns (4.1.5.5)		A type of bar or column graph that can be used when several bars represent all the portions of a whole (analogous to segmented curve charts).
Pie Charts (4.1.5.7)		Show the relative distribution of data among parts that make up a whole. However, a bar or column chart will usually permit more accurate interpretation.
Graphic Instrument Panels (4.1.5.12)		Show one value of one continuous variable, When showing multiple variables (i.e., multiple meters) that must be compared to each other, it is probably more effective to use other techniques, such as bar or column charts to show values for separate variables, or line graphs to show values changing over time.
Circular or Pattern Charts (4.1.5.11)		Show values of a continuous variable for multiple related entities. Values are displayed along spokes emanating from the origin. Different continuous variables may be represented if they are indexed so that the normal values of each variable can be connected to form an easily recognized polygon, Useful for detecting patterns, but not for determining precise values or making accurate comparisons among values.

(Adapted from TULLIS, 1988)

Table 4-6
Suitability of Data Display Formats by Data and Use

1 Good	Data Characteristics									Uses					
2 Workable	Dimensions			Variables			Samples			Quantitative			Qualitative		
3 Not Recommended	Unidimensional	Duodimensional	Multidimensional	Univariate	Limited Multivariate	Multivariate	Discrete	Limited Series	Series	Exact	Approximate	Relative	Status	Prediction	Pattern Recognition
Continuous Text	1	2	2	1	2	2	1	2	2	2	2	3	2	3	3
Tables and Lists	1	1	2	1	2	2	1	1	2	1	2	3	1	2	3
Bar Charts and Histograms	1	2	3	2	2	1	1	3	3	2	1	1	2	3	2
Segmented Bar	1	2	3	2	2	1	1	3	3	2	1	1	2	3	2
Trend Plots	1	2	3	1	2	3	2	1	1	2	1	1	2	1	2
Scatterplots	3	1	3	1	2	3	2	1	2	2	1	1	2	2	2
Segmented Curves	1	3	3	2	1	3	3	2	1	2	1	2	3	2	2
Pie Charts	1	3	3	3	1	3	1	3	3	3	1	1	3	3	3
Flow Charts															
Mimics and Diagrams	3	2	1	3	2	1	1	3	3	2	2	2	2	2	1
Maps	3	2	1	3	2	1	1	3	3	2	2	2	2	2	1
Integral and Configural Formats	1*	1*	1	1*	2	1	1	3	3	3	2	2	1	3	1
Graphic Instruments	1	3	3	1	2	3	1	3	3	2	1	2	2	2	2
Speech Displays															

(adapted from Frey et al., 1984)

Table 4-7
Examples of Typical Color Meanings

Color	Typical Meaning
Red	• Fire protection equipment and apparatus • Danger • Stop or Trip (for a control) • Running or “ON” • Valve Open • Breaker Closed • Alarm of High Priority • Abnormal Condition
Orange	• Dangerous parts of machinery or equipment, such as open breaker boxes • Alarms of Intermediate priority
Yellow	• Physical hazards, such as falling or tripping • Caution • Alarm of Intermediate Priority • Abnormal Condition • In manual mode • In standby • Not in desired postESFAS initiation status
Green	• Personnel Health or Safety • Location of first aid equipment • Not Running or “OFF” • Valve Closed • Breaker Open • Normal Condition • Alarm Cleared
Blue	• Caution against starting, using or moving equipment in use • Bypassed • In standby • Selected • Normal Condition • In desired post ESFAS initiation state • Water • Secondary water • Primary water (cyan)
Magenta	• Radiation hazards (used in combination with yellow) • Abnormal Condition
Black and/or White	• Traffic and housekeeping markings • Status Indication • Neutral Information • In automatic mode • A non-priority alarm • Text • Steam (gray)

4.2 User Interface Interaction and Management

4.2.1 Section Overview

4.2.2 Description of User Interface Interaction and Management

4.2.3 Interface Management Guidelines Checklist

4.2.4 General Interface Design Objectives

- 4.2.4.1 Simplifying Input
- 4.2.4.2 Ensuring User Control of the Interaction
- 4.2.4.3 Establishing Consistency of Interface and Interaction
- 4.2.4.4 Minimizing Demands on the User
- 4.2.4.5 Maintaining Awareness of Context and Options
- 4.2.4.6 Guiding and Assisting Users
- 4.2.4.7 Allowing Flexibility

4.2.5 Interface Management Functions

- 4.2.5.1 Entry of Commands and Information
- 4.2.5.2 Supporting Use of Individual Display Pages
- 4.2.5.3 Supporting Navigation in Systems of Displays
- 4.2.5.4 Controlling Displays
- 4.2.5.5 Providing Feedback
- 4.2.5.6 Protecting Information
- 4.2.5.7 Managing Information

4.2.6 Interacting with Interface Components

- 4.2.6.1 Windows
- 4.2.6.2 Cursors

4.2.7 Sources of Additional Information

4.2.1 Section Overview

This section contains guidance for designing the means by which users interact with the features and resources of the user interface. Figure 4-24 illustrates the aspects of user interface interaction and management for which guidance is provided. The detailed guidance begins with Section 4.2.4.

As suggested in Section 4.1.3, Display Functions, much of interface management involves accessing displays. It may be useful, therefore, to review the high-level design information and considerations presented in that section while addressing user-interface interaction and management. The section contains detailed treatments of the characteristics of display hierarchies, navigation within hierarchies, and support for teamwork.

4.2.2 Description of User Interface Interaction and Management

User-interface interaction and management refer to the means by which personnel provide inputs to an interface, receive information from it, and manage the tasks associated with access and control of information. User-interface interaction and management comprise a wide range of tasks users undertake when accessing information and controls needed to operate or maintain the plant. Because the design characteristics of the human-system interface determine the specific mechanisms of these tasks, there is no simple link between them and design characteristics. Just as a single interface management task may be performed via many different user interfaces, a single user interface may be used to perform many types of interface management tasks.

Nevertheless, several design objectives can be identified that apply regardless of the particular function to be performed or specific interface feature to be employed. The guidance begins with these general interface design objectives (Section 4.2.4), which include simplicity, consistency, and minimization of demands on the user. Interfaces, however varied the tasks they are designed to support, tend to serve one or more general functions; design guidance for these basic functions (e.g., mediating user input, controlling displays, providing feedback) is presented in Section 4.2.5. Finally, interfaces also contain certain basic components. Guidance for the most common of these, windows and cursors, is in Section 4.2.6.

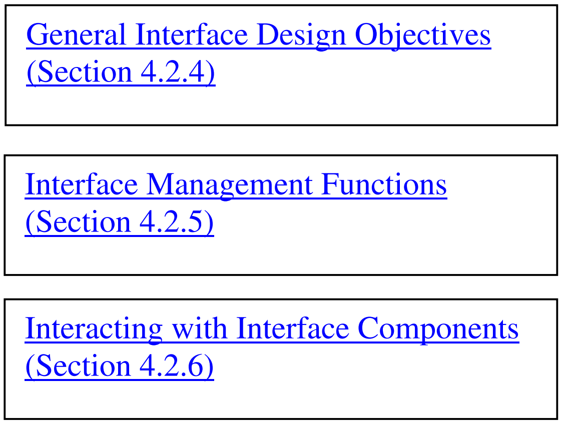

General Interface Design Objectives (Section 4.2.4)
Interface Management Functions (Section 4.2.5)
Interacting with Interface Components (Section 4.2.6)

Figure 4-24
User Interface Interaction and Management

4.2.3 Interface Management Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining sections. For additional information, please consult the sections and guidelines referenced.

Guidelines					**Complies**	**Does not Comply, but with Justification**	**Does not Comply, but without Justification**	**Not Applicable**
4.2.4	General Interface Design Objectives							
	4.2.4.1	Simplifying Input						
		=>	4.2.4.1-1	User input actions should be simple, particularly for real-time tasks requiring fast user response.				
		=>	4.2.4.1-2	Input transactions and associated displays should be designed so that a user can stay with one method of entry, and not have to shift to another.				
		=>	4.2.4.1-3	For interpreting user-composed control entries, upper and lower case letters should be treated as equivalent.				
		=>	4.2.4.1-4	Unless otherwise required by processing or display requirements, alphabetic input should be left justified, and numeric input should be right justified for integer data or decimal point justified for decimal data.				
		=>	4.2.4.1-5	Automatic justification of tabular data entries should be provided.				
		=>	4.2.4.1-6	When a user must enter numeric values that will later be displayed, all significant zeros should be maintained.				
		=>	4.2.4.1-7	Numeric values should be displayed to the level of significance required of the data, regardless of the value of individual input data.				
		=>	4.2.4.1-8	Data entry by overwriting a set of characters within a field should be avoided.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.4.1-9	The user should not be required to enter data separators or delimiters, such as dashes and slashes.				
		=>	4.2.4.1-10	The user should not be required to enter units of measure.				
		=>	4.2.4.1-11	When data entry is a significant part of a user’s task, entered data should appear on the user’s main display.				
		=>	4.2.4.1-12	The same explicit ENTER action should be required for entry of corrections as used for the original entry.				
		=>	4.2.4.1-13	Users should be able to perform simple editing during text entry without having to invoke a separate edit mode.				
		=>	4.2.4.1-14	When appropriate (e.g., in menu-based systems where system response may be slow), the system should allow users to easily enter a sequence of commands or option codes as a single ‘stacked’ entry.				
		=>	4.2.4.1-15	All displays should be designed so that features relevant to user entries are distinctive in position and/or format.				
		=>	4.2.4.1-16	The means of entering information or commands should be compatible with user skills, permitting simple step-by-step actions by beginners, but permitting more complex entries by experienced users.				
	4.2.4.2		Ensuring User Control of the Interaction					
		=>	4.2.4.2-1	Users should be allowed to control the processing of information or execution of commands.				
		=>	4.2.4.2-2	If different kinds of user interrupts are provided, each interrupt function should be designed as a separate control option with a distinct name.				
		=>	4.2.4.2-3	User interrupts and aborts should not modify or remove stored or entered data.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.4.2-4	Users should be allowed to control the pace and sequence of their entry of information or commands.				
		=>	4.2.4.2-5	If PAUSE or SUSPEND options are provided, some indication of the status should be displayed whenever a user selects such an option.				
		=>	4.2.4.2-6	The HSI should provide visual and/or auditory reminders for interrupted tasks.				
		=>	4.2.4.2-7	The HSI should provide simple mechanisms for retrieving displays and controls for tasks that have been suspended.				
		=>	4.2.4.2-8	At any step in a defined transaction sequence, if there is only a single appropriate next step, then a consistent control option to continue to the next transaction should be provided.				
		=>	4.2.4.2-9	Transactions should never leave the user without further available action and should provide next steps or alternatives.				
	4.2.4.3		Establishing Consistency of Interface and Interaction					
		=>	4.2.4.3-1	Procedures for entering commands or information should be consistent in form and consequences.				
		=>	4.2.4.3-2	All terms employed in the user-system interface, and their abbreviations, should be consistent in meaning from one transaction to another, and from one task to another.				
		=>	4.2.4.3-3	The wording and required format of information or command entry functions should be consistently reflected in the wording of user guidance, including all operating procedures, labels, messages, and training material.				
		=>	4.2.4.3-4	Controls used for interface management tasks should have consistent locations.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.2.4.4		Minimizing Demands on the User					
	=>	4.2.4.4-1	Entry of information or commands should not require the user to remember special codes or sequences or to perform translations or conversions.				
	=>	4.2.4.4-2	A user should not be required to re-enter information already available to the system.				
	=>	4.2.4.4-3	Information necessary to accomplish a specific entry (e.g., labels, annotations, prompts, or options lists) should be available to the user when that transaction action is appropriate.				
	=>	4.2.4.4-4	An information entry sequence should be designed so that its organization reflects the user's view of the task, and should provide all control options that may be required.				
	=>	4.2.4.4-5	Flexible means of entering information or commands should be provided so that users can accomplish necessary transactions, and can obtain guidance as needed in connection with any transaction.				
	=>	4.2.4.4-6	The results of any entry should be compatible with user expectations, so that the system changes in a 'natural' way in response to user actions.				
	=>	4.2.4.4-7	If entries are made by keying onto the display, such as by keyed menu selections or commands, they should be distinguishable from displayed text.				
	=>	4.2.4.4-8	Annotations added by users to displayed text should be distinguishable from the text itself.				
	=>	4.2.4.4-9	Travel distance for cursors across and between display pages and windows on a display screen should be minimized.				
	=>	4.2.4.4-10	Displays that can provide decluttering capabilities should also provide a means for the user to rapidly return the display to its original configuration.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.4.4-11	The user should be able to manipulate information without concern for internal storage and retrieval mechanisms of the system.				
		=>	4.2.4.4-12	When likely default values can be defined for the information to be entered in a particular task, those default values should be offered to speed entry.				
		=>	4.2.4.4-13	Preset and automated set-up features should be used to ensure that users do not have to perform these functions while operating the plant.				
		=>	4.2.4.4-14	When users must select options by code entry, the code associated with each option should be displayed in a consistent and distinctive manner.				
		=>	4.2.4.4-15	When several users must interact with the system simultaneously, control entries by one user should not interfere with those of another.				
	4.2.4.5		Maintaining Awareness of Context and Operations					
		=>	4.2.4.5-1	If the consequences of a user entry will differ depending upon context established by a prior action, then some continuous indication of current context should be displayed for reference by the user.				
		=>	4.2.4.5-2	Information displayed to provide context for user entries should be distinctive in location and format, and consistently displayed from one transaction to the next.				
		=>	4.2.4.5-3	Users should be permitted to request a summary of prior entries to help determine present status, and should be allowed to review the entries currently in effect.				
		=>	4.2.4.5-4	A general list of basic options should be provided and always be available to serve as a ‘home base’ or consistent starting point for user input.				
		=>	4.2.4.5-5	When a user is performing an operation on some selected display item, that item should be highlighted.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.2.4.5-6	The general options list should show control entry options grouped, labeled, and ordered in terms of their logical function, frequency, and criticality of use, following the general guidelines for menu design.				
	=>	4.2.4.5-7	Users should be provided with a list of the control options that are specifically relevant and available for any transaction.				
	=>	4.2.4.5-8	Only control options that are actually available for the current transaction should be offered to users.				
4.2.4.6	Guiding and Assisting Users						
	4.2.4.6.1	General					
	=>	4.2.4.6.1-1	System messages should appear in standard locations.				
	=>	4.2.4.6.1-2	Consistent grammatical construction should be used in system messages.				
	=>	4.2.4.6.1-3	System messages should use familiar terminology.				
	=>	4.2.4.6.1-4	System messages should be concise and clearly worded.				
	=>	4.2.4.6.1-5	Wording for system messages should be directed at the user.				
	=>	4.2.4.6.1-6	No extraneous information should be displayed.				
	=>	4.2.4.6.1-7	Presenting the system as a person should be avoided.				
	=>	4.2.4.6.1-8	Experienced users should be able to define when and how guidance will be provided by automated guidance/help systems.				
	=>	4.2.4.6.1-9	The content of help information should be oriented toward users' completion of their tasks; i.e., the information should be procedural.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.1-10	The display of online help should not obscure important information.				
			=>	4.2.4.6.1-11	Online help should accommodate users' differing levels of expertise and preferred interaction styles.				
			=>	4.2.4.6.1-12	Users should be able to request guidance information regarding requirements for information or command entry (e.g., syntax, parameters, and options).				
			=>	4.2.4.6.1-13	Users should be provided with whatever information may be needed to guide command entries at any point in a sequence of transactions, by incorporating prompts in a display and/or by providing prompts in response to requests for HELP.				
		4.2.4.6.2		Prompts					
			=>	4.2.4.6.2-1	Users should be provided with clear and specific information to guide entries during logon/logoff or command or information entry.				
			=>	4.2.4.6.2-2	When a user must specify the address for a message, prompting should be provided.				
			=>	4.2.4.6.2-3	Standard symbols should be used for input prompting.				
			=>	4.2.4.6.2-4	When a command entry is not recognized or is inappropriate, users should be prompted to correct, rather than re-enter the command.				
			=>	4.2.4.6.2-5	Cues should be provided to indicate the size of a fixed-length data entry field.				
			=>	4.2.4.6.2-6	Additional cuing of data format should be included in a field label when that seems helpful.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.2-7	Users should be able to request computer generated prompts to determine required parameters or available options for a command.				
			=>	4.2.4.6.2-8	Prompting should be provided for required formats and acceptable values for data entries.				
			=>	4.2.4.6.2-9	Graphic means may be provided for displaying prompting aids and other guidance pertaining to current control actions.				
		4.2.4.6.3		Advisory Messages					
			=>	4.2.4.6.3-1	Advisory messages should be distinctive.				
			=>	4.2.4.6.3-2	Information requiring prompt attention should be presented through both visual and auditory means.				
			=>	4.2.4.6.3-3	Protection against data loss should be provided.				
			=>	4.2.4.6.3-4	Users should be informed when a command will be time-consuming to process.				
		4.2.4.6.4		Error Messages					
			=>	4.2.4.6.4-1	When the computer detects an entry error, an error message should be displayed stating the error and possible subsequent operations.				
			=>	4.2.4.6.4-2	Error messages should be clearly worded, informative, and appropriate to the task.				
			=>	4.2.4.6.4-3	The computer should display an error message only after completion of an entry.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.4-4	Where an entry is invalid or inoperative at the time of selection, no action should result except a display of an advisory message indicating the error and the appropriate functions, options, or commands.				
			=>	4.2.4.6.4-5	Error messages should facilitate correction of the error.				
			=>	4.2.4.6.4-6	The means of notifying users of errors should remain effective when there are multiple errors.				
			=>	4.2.4.6.4-7	If an error is detected in a group of entries, the system should process correct commands until the error is displayed.				
			=>	4.2.4.6.4-8	Following the output of a simple error message, users should be able to request a more detailed explanation of the error.				
			=>	4.2.4.6.4-9	Error messages should be presented at the point of the error or in a consistent area of the display.				
		4.2.4.6.5		Validating User Input					
			=>	4.2.4.6.5-1	Displays and transactions associated with information entry should be designed so that users can review and confirm entries before they are processed by the system.				
			=>	4.2.4.6.5-2	The system should validate any item whose entry and/or correct format or content is required for subsequent data processing.				
			=>	4.2.4.6.5-3	In a repetitive data entry task, the data for each transaction should be validated as it is completed, and the user should be allowed to correct errors before beginning another transaction.				
			=>	4.2.4.6.5-4	Optional item-by-item data validation within a multiple-entry transaction should be provided.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.5-5	Validation features should accommodate deferred entries				
			=>	4.2.4.6.5-6	If data validation detects a probable error, an error message should be displayed to the user at the completion of data entry.				
			=>	4.2.4.6.5-7	When a data or command entry error is suspected but cannot be determined (in terms of system error logic), a cautionary message asking for confirmation should be displayed.				
		4.2.4.6.6		Correcting Information/Command Entries					
			=>	4.2.4.6.6-1	All error corrections by the user should be acknowledged by the system, either by indicating a correct entry has been made or by another error message.				
			=>	4.2.4.6.6-2	Any user action should be immediately reversible by an UNDO command.				
			=>	4.2.4.6.6-3	For all inputs, whether data entries or commands, users should be allowed to edit composed material before requesting computer processing.				
			=>	4.2.4.6.6-4	When the system detects an error in a user input, the user should be allowed to make an immediate correction.				
			=>	4.2.4.6.6-5	Following error detection, users should be allowed to edit entries by rekeying only those portions that were in error.				
			=>	4.2.4.6.6-6	Users should be required to take an explicit ENTER action for computer processing of error corrections.				
			=>	4.2.4.6.6-7	When inappropriate or unrecognized commands are detected, a list should be provided to the user showing permissible commands, anticipating the command intended.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.6-8	Users should be allowed to BACKUP easily to previous steps in a transaction sequence in order to correct an error or make any other desired change.				
			=>	4.2.4.6.6-9	If an error is detected in a stacked series of command entries, the computer should either consistently execute to the point of error, or else consistently require users to correct errors before executing any command.				
			=>	4.2.4.6.6-10	If only a portion of a stacked command can be executed, the user should be notified and provided appropriate guidance to permit correction, completion, or cancellation of the stacked command.				
			=>	4.2.4.6.6-11	If a user makes a command entry error, after the error message has been displayed, the user should be allowed to enter a new command.				
			=>	4.2.4.6.6-12	If a command entry is not recognized, the user should be allowed to revise the command rather than rejecting the command outright.				
		4.2.4.6.7		User Guidance/Help					
			=>	4.2.4.6.7-1	Reference material describing system capabilities, procedures, and commands and abbreviations should be available and easily accessed on-line.				
			=>	4.2.4.6.7-2	When a user requests HELP on a topic, the computer should accept synonyms and abbreviations.				
			=>	4.2.4.6.7-3	The information presented in response to a HELP request should be tailored to the task context.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.2.4.6.7-4	When a request for HELP is ambiguous in context, the computer should initiate a dialogue to specify what data, message, or command requires explanation.				
	=>	4.2.4.6.7-5	When a HELP display provides summary information, more detailed explanations should be available.				
	=>	4.2.4.6.7-6	A complete hardcopy set of computer system operating procedures and contingency procedures should be available in the control room.				
	=>	4.2.4.6.7-7	Procedures should be prepared from the point of view of the user.				
	=>	4.2.4.6.7-8	Cross-indices of the available data displays should be available in the control room in hardcopy form.				
4.2.4.7	Allowing Flexibility						
	=>	4.2.4.7-1	Flexible HSI features should be provided when they provide specific benefits to user tasks and their use does not impair user performance.				
	=>	4.2.4.7-2	Users should not have to use flexible interface features to support tasks and circumstances that could have been anticipated and designed for.				
	=>	4.2.4.7-3	The system should be sufficiently flexible to enable users to respond to unanticipated situations or where personal preference can positively impact performance.				
	=>	4.2.4.7-4	Users’ flexibility in configuring the interface should not be unlimited.				
	=>	4.2.4.7-5	Displays that can be modified by users should provide a means for the user to rapidly return the display to its default configuration.				
	=>	4.2.4.7-6	The design of flexible HSI features should provide capabilities that are consistent with the levels of expertise of the users.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.4.7-7	When information or command entry requirements may change, some means for the user (or a system administrator) to make necessary changes to available functions should be provided.					
4.2.5	Interface Management Functions								
	4.2.5.1	Entry of Commands and Information							
		4.2.5.1.1	Command Language						
			=>	4.2.5.1.1-1	The system should be designed to help users learn and remember the commands.				
			=>	4.2.5.1.1-2	The interaction should be designed to minimize the effort involved in entering the commands.				
			=>	4.2.5.1.1-3	A command language should be designed to minimize errors, and the system should tolerate types of errors that can be anticipated.				
		4.2.5.1.2	Menus						
			=>	4.2.5.1.2-1	User requested menus should be used whenever possible; the use of permanent menus should be minimized.				
			=>	4.2.5.1.2-2	If menu options are included in a display that is intended also for data review and/or data entry, the menu options should be distinct from other displayed information.				
			=>	4.2.5.1.2-3	When permanent menus are used, there should be one standard design for the input prompt that is used across all tasks.				
			=>	4.2.5.1.2-4	A menu should be designed to display all options appropriate to any particular transaction.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.2-5	Menus should display as selectable only those options that are actually available in the current context.				
			=>	4.2.5.1.2-6	Menus should be designed so that the function of the menu is evident to the user.				
			=>	4.2.5.1.2-7	When equivalent keyboard commands are provided, they should be displayed as part of the menu option label.				
			=>	4.2.5.1.2-8	If one option on a menu is selected more often than the others, then it should be highlighted.				
			=>	4.2.5.1.2-9	Where discrimination among options may be difficult for users, menus can provide a preview of options.				
			=>	4.2.5.1.2-10	Options that are critical or frequently chosen should be quickly accessible using as few steps as possible.				
			=>	4.2.5.1.2-11	Users should be able to select a menu or submenu directly, without going through intermediate selection steps.				
			=>	4.2.5.1.2-12	Users should have to take only one simple action to return to the next higher level in hierarchic menus.				
			=>	4.2.5.1.2-13	Users should have to take only one simple action to return to the general menu at the top level in hierarchic menus.				
			=>	4.2.5.1.2-14	When menu selection is accomplished by code entry, users should be able to combine a series of selections into a single “stacked” entry.				
			=>	4.2.5.1.2-15	Experienced users should be able to bypass a series of menu selections and make an equivalent command entry directly.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.2-16	When a menu is first displayed, the cursor should be positioned so that it may be readily located and used.				
			=>	4.2.5.1.2-17	A menu macro capability should be provided if it produces faster access.				
			=>	4.2.5.1.2-18	Multiple navigation paths should be provided to items in the display system.				
			=>	4.2.5.1.2-19	A visual representation of the menu structure should be provided.				
			=>	4.2.5.1.2-20	Menu options should be ordered and grouped logically.				
			=>	4.2.5.1.2-21	Where ordering cannot be determined by the above, alphabetic ordering should be used.				
			=>	4.2.5.1.2-22	The order of options on menus should be fixed.				
			=>	4.2.5.1.2-23	If meaningful categories cannot be developed for menu options then visual groups should be created for long menus.				
			=>	4.2.5.1.2-24	All menu items should be visible to the user without scrolling.				
			=>	4.2.5.1.2-25	When multiple menu options are displayed in a list, each option should be displayed on a new line, i.e., format the list as a single column.				
			=>	4.2.5.1.2-26	When menu selection must be made from a long list, and not all options can be displayed at once, a hierarchic sequence of menu selections should be provided rather than one long multipage menu.				
			=>	4.2.5.1.2-27	Menus should have a limited number of items in breadth and in depth.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.2-28	If menu options are grouped in logical subunits, each group should have a descriptive label that is distinctive in format from the option labels themselves.				
			=>	4.2.5.1.2-29	If menu options are grouped in logical subunits, the same color should be used for menus within the same group.				
			=>	4.2.5.1.2-30	The display format and selection logic of hierarchic menus should be consistent at every level.				
			=>	4.2.5.1.2-31	Hierarchic menus should be organized and labeled to guide users within the hierarchic structure.				
			=>	4.2.5.1.2-32	Users should be able to access a visual representation of their paths through a hierarchy of menus.				
			=>	4.2.5.1.2-33	When users must step through a sequence of menus to make a selection, the hierarchic menu structure should be designed to minimize the number of steps required.				
			=>	4.2.5.1.2-34	When hierarchic menus are used, the user should have some indication of current position in the menu structure.				
			=>	4.2.5.1.2-35	If hierarchical branching is used, each subordinate menu should be visually distinct from each previous superordinate menu.				
			=>	4.2.5.1.2-36	The display of hierarchic menus should be formatted so that options that actually accomplish actions can be distinguished from options that merely branch to other menu frames.				
			=>	4.2.5.1.2-37	The categories listed across the menu bar should be organized systematically.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.2-38	Category labels on menu bars should be centered in the vertical dimension. Horizontally, category labels on the menu bar should be separated by enough space to be distinguishable as separate items, i.e., by at least two standard character widths.				
			=>	4.2.5.1.2-39	The height of a menu bar should be sufficient to contain standard text characters that serve as menu category labels, as well as space above and below the text characters.				
			=>	4.2.5.1.2-40	Pull-down and pop-up menus should be activated only by a specific user action that requests the display of the menu.				
			=>	4.2.5.1.2-41	When a pull-down or pop-up menu item(s) has/have been selected, the menu should revert to its hidden state as the selected command is carried out.				
			=>	4.2.5.1.2-42	If menu items are selectable via activation of programmable function keys, the arrangement of the menu list should be compatible with the arrangement of the keys to the greatest degree possible.				
			=>	4.2.5.1.2-43	An explanatory title should be provided for each menu that reflects the nature of the choice to be made.				
			=>	4.2.5.1.2-44	Menus should be displayed in consistent screen locations for all modes, transactions, and sequences.				
			=>	4.2.5.1.2-45	When menu selection is accomplished by code entry, a standard command entry area (window) should be provided where users enter the selected code.				
			=>	4.2.5.1.2-46	Users should not be able to select menu items that are in conflict.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.2-47	If menu selection is accomplished by pointing, dual activation should be provided, in which the first action designates the selected option, followed by a separate second action that makes an explicit control entry.				
			=>	4.2.5.1.2-48	If menu selection is accomplished by pointing, the sensitive area for pointing should be as large as consistently possible, including at least the area of the displayed option label plus a half-character distance around that label.				
			=>	4.2.5.1.2-49	The system should provide feedback as users interact with menus.				
			=>	4.2.5.1.2-50	When menus are provided in different displays, they should be designed so that option lists are consistent in wording-				
			=>	4.2.5.1.2-51	Menu options should be consistently worded as commands.				
			=>	4.2.5.1.2-52	Letter codes used to designate menu options should be meaningful and should be used consistently.				
		4.2.5.1.3		Function Keys					
			=>	4.2.5.1.3-1	Function keys should be provided for interim command entries, i.e., for actions taken before the completion of a transaction.				
			=>	4.2.5.1.3-2	Each function key should be labeled informatively to designate the function it performs.				
			=>	4.2.5.1.3-3	Function keys should be grouped in distinctive locations on the keyboard to facilitate their learning and use.				
			=>	4.2.5.1.3-4	A function assigned to a particular key in a given task context should be assigned to the same key in other contexts.				

					Guidelines	Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.3-5	When a function is continuously available, its function should be assigned to a single key.				
			=>	4.2.5.1.3-6	Frequently used functions should be executed by means of a single key action and should not require chord-keying (e.g., use of the shift key).				
			=>	4.2.5.1.3-7	When a function key performs different functions in different operational modes, equivalent or similar functions should be assigned to the same key.				
			=>	4.2.5.1.3-8	If chord-keying is used, the functions paired on one key should be logically related.				
			=>	4.2.5.1.3-9	If chord (e.g., control/shift) keying is used, the logical relation between shifted and unshifted functions should be consistent from one key to another.				
			=>	4.2.5.1.3-10	If a key is used for more than one function, the function currently available should always be indicated to the user.				
			=>	4.2.5.1.3-11	If the functions assigned to a set of keys change as a result of user selection, the user should be provided with an easy means to return to the initial, base-level functions.				
			=>	4.2.5.1.3-12	When function key activation does not result in any immediately observable natural response, users should be provided with some other form of computer acknowledgment.				
			=>	4.2.5.1.3-13	Function keys are not needed for a current transaction should be temporarily disabled.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.3-14	If some function keys are active and some are not, the current subset of active keys should be indicated in some noticeable way, such as by brighter illumination.				
			=>	4.2.5.1.3-15	The system should prompt the user for confirmation if a function key is pressed in a context unrelated to the function.				
			=>	4.2.5.1.3-16	The layout of function keys should be compatible with their use.				
		4.2.5.1.4		Macros/Programmable Function Keys					
			=>	4.2.5.1.4-1	Users should be allowed to assign a single name to a defined series of entries, and then to use that named “macro” for subsequent command entry.				
			=>	4.2.5.1.4-2	Users should have access to an index of their macros and programmable function keys with their respective composition of commands.				
			=>	4.2.5.1.4-3	The use of user definable macros and programmable function keys should be limited.				
			=>	4.2.5.1.4-4	A user should be restricted from modifying a macro or programmable function key as defined by a different originating user.				
			=>	4.2.5.1.4-5	Users should not be allowed to duplicate macro names.				
		4.2.5.1.5		Forms					
			=>	4.2.5.1.5-1	Form filling should be provided as an aid for composing complex command entries.				
			=>	4.2.5.1.5-2	Appropriate and readily modified default parameters should be displayed in forms used for composing complex command entries.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.5-3	Forms for command entry should be consistent in format.				
			=>	4.2.5.1.5-4	Form filling should be used for tasks where some flexibility in information entry is needed, such as the inclusion of optional as well as required items, and/or where computer response may be slow.				
			=>	4.2.5.1.5-5	Where no source documents or forms exist to support information entry, then fields should be logically grouped, by sequence and frequency of use, importance, and functional associations.				
			=>	4.2.5.1.5-6	Just one explicit entry action at the end of the transaction sequence should be required, rather than separate entry of each item.				
			=>	4.2.5.1.5-7	For each data field, an associated label should be displayed to help users understand what entries can be made.				
			=>	4.2.5.1.5-8	Whenever possible, entry of multiple data items should be allowed without keying special separator or delimiter characters.				
			=>	4.2.5.1.5-9	When a field delimiter must be used for data entry, a standard character should be employed consistently for that purpose.				
			=>	4.2.5.1.5-10	When multiple data items are entered as a single transaction, as in form filling, the user should be allowed to review, modify, or cancel the items before entering the form.				
			=>	4.2.5.1.5-11	When entry of information in a field is deferred or omitted, the system should identify the field by highlighting or other means. Before the information is filed or accessed, the user should be reminded that information has not been entered, if such entry is required.				
			=>	4.2.5.1.5-12	When sets of data items must be entered sequentially, in a repetitive series, a tabular display format should be provided where data sets can be keyed row by row.				

					Guidelines	Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.5-13	Users should not have to remove unused underscores or otherwise enter keystrokes for each position within a variable length entry area.				
			=>	4.2.5.1.5-14	Optional versus required data entries within fields on input forms should be distinct.				
			=>	4.2.5.1.5-15	Distinctive formats should be provided for column headers and row labels, so that users can distinguish them from data entries.				
			=>	4.2.5.1.5-16	For entry of tabular data, when entries are frequently repeated, users should be provided with some easy means to copy duplicated data.				
			=>	4.2.5.1.5-17	Where the number of fields is limited, screen traversal distances are short, and when data fields will be accessed sequentially, users should be allowed to tab directly from one data field to the next, so that the cursor can move freely back and forth across rows or columns.				
			=>	4.2.5.1.5-18	Direct pointing devices, such as a mouse or light pen, should be available (1) for selecting fields in complicated forms, or (2) when field entry will be less predictable (as in database update).				
			=>	4.2.5.1.5-19	For long forms, those with many rows, some extra visual cue should be provided to help a user scan a row accurately across columns.				
			=>	4.2.5.1.5-20	If certain information is used frequently, then it should be automatically entered into the form as a default; see guidance on defaults in Section 4.2.4.4.				
		4.2.5.1.6		Direct Manipulation					

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.6-1	Direct manipulation should be used primarily in tasks with actions and objects that lend themselves to pictographic representation, and in which the actions and objects need not be modified for the successful interpretation of the command by the system.				
			=>	4.2.5.1.6-2	When user input involves frequent pointing on a display surface, the interface should be designed so that other actions (e.g., display control) are also accomplished by pointing, in order to minimize shifts from one entry device to another.				
			=>	4.2.5.1.6-3	Selection of an icon, menu, or application-specific capability from a function area should be acknowledged by highlighting the selected item.				
			=>	4.2.5.1.6-4	The direct manipulation interface should include (1) windows for containing the data files, (2) menus for additional objects and actions that are not easily represented by pictographic icons.				
			=>	4.2.5.1.6-5	Direct manipulation should not be used when the computer response is slow.				
			=>	4.2.5.1.6-6	If icons are used to represent control actions in menus, a text label should be displayed with each icon to help assure that its intended meaning will be understood.				
			=>	4.2.5.1.6-7	Graphic means should be provided for displaying the context of current control actions to users.				
			=>	4.2.5.1.6-8	Prompting aids and other guidance pertaining to current control actions should be displayed graphically to the user.				
			=>	4.2.5.1.6-9	A user should be able to “open” an icon with a simple, explicit action.				

					Guidelines	Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.6-10	The size and separation of items on the screen that are displayed for selection should allow them to be pointed to easily (i.e., without requiring precise positioning of the pointer).				
			=>	4.2.5.1.6-11	When exact placement of graphic elements is required, users should be allowed to expand (“zoom”) the critical display area to make the positioning task easier.				
			=>	4.2.5.1.6-12	Users should be provided some means for designating and selecting displayed graphic elements for manipulation.				
			=>	4.2.5.1.6-13	All items currently selected should be highlighted in some way to minimize uncertainty about the objects or files to which subsequent actions will be applied.				
			=>	4.2.5.1.6-14	During graphic data entry/editing, the selected attributes that will affect current actions should be displayed for ready reference by the user.				
			=>	4.2.5.1.6-15	Automatic registration or alignment of computer-generated graphic data should be provided, so that variable data are shown properly with respect to fixed background or map data at any display scale.				
			=>	4.2.5.1.6-16	When complex graphic data must be entered quickly, computer aids should be provided to automate that process.				
			=>	4.2.5.1.6-17	Automated plotting of computer-stored data should be provided at user request, with provision for subsequent editing by a user.				
			=>	4.2.5.1.6-18	When graphic data must be plotted in predefined standard formats, templates or skeletal displays for those formats should be provided to aid data entry.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.6-19	When graphs must be constructed for data plotting, computer aids should be provided for that purpose.				
			=>	4.2.5.1.6-20	Computer aids should be provided to help users specify appropriate scales for graphic data entry.				
			=>	4.2.5.1.6-21	Users should be allowed to designate a group of elements to which graphic editing operations will be applied in common.				
			=>	4.2.5.1.6-22	The effects of operations performed on direct manipulation interfaces should be immediately visible.				
			=>	4.2.5.1.6-23	Explicit error messages should be provided for incorrect actions related to the process (as opposed to the interface).				
			=>	4.2.5.1.6-24	Representations used as icons should require minimal interpretation.				
		4.2.5.1.7		Natural Language					
			=>	4.2.5.1.7-1	A natural language interface should not be the sole means of taking actions that may have to be done very quickly or reliably.				
			=>	4.2.5.1.7-2	The outputs of a natural language system should be consistent with the types of entries required of users.				
		4.2.5.1.8		Query Language					
			=>	4.2.5.1.8-1	A query language should reflect a single, natural data structure or organization.				
			=>	4.2.5.1.8-2	The wording of a query should simply specify what data are requested.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.8-3	Users should be allowed to employ alternative forms when composing queries, corresponding to common alternatives in natural language.				
			=>	4.2.5.1.8-4	A query language should minimize the need for quantifiers in query formulation.				
			=>	4.2.5.1.8-5	A query language should include logic elements that permit users to link sequential queries as a single entry.				
			=>	4.2.5.1.8-6	If a query will result in a large-scale data retrieval, the user should be informed and required to confirm the transaction or to narrow the query before processing.				
			=>	4.2.5.1.8-7	A query language interface should not be the sole means of taking actions that may have to be done very quickly or reliably.				
		4.2.5.1.9		Question and Answer					
			=>	4.2.5.1.9-1	The system should provide the user with a specific request for information.				
			=>	4.2.5.1.9-2	Each question should be displayed separately.				
			=>	4.2.5.1.9-3	The system should indicate any constraints that apply to the user's response.				
			=>	4.2.5.1.9-4	The system should accept as much data as the user is willing to provide in an answer.				
			=>	4.2.5.1.9-5	When a series of computer-posed questions are interrelated, answers to previous questions should be displayed when those will provide context to help a user answer the current question.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.9-6	The user should have the ability to remove a question and answer from the screen or recall a question and answer to the screen.				
			=>	4.2.5.1.9-7	When questions prompt entry of data from a source document, the question sequence should match the data sequence in the source document.				
			=>	4.2.5.1.9-8	A question mark should be the delimiter of the question and answer dialogue.				
		4.2.5.1.10		Speech					
			=>	4.2.5.1.10-1	Spoken input should be used together with alternative methods such as keyed entry or pointing.				
			=>	4.2.5.1.10-2	The characteristics of the speech recognition function should be appropriate for the tasks it is intended to support.				
			=>	4.2.5.1.10-3	Feedback and simple error correction procedures should be provided for speech input, so that when a spoken entry has not been correctly recognized by the computer, the user can cancel that entry and speak again.				
			=>	4.2.5.1.10-4	When speech input is the preferred means of input, alternatives forms for critical entries should be allowed, so that if the system cannot recognize an entry after repeated attempts, another entry form can be substituted.				
			=>	4.2.5.1.10-5	Speech recognition systems should have a means of activation and deactivation (e.g., PAUSE and CONTINUE options) so that conversation between users is not taken as command input.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.5.1.10-6	The vocabulary items should (1) consist of words that are meaningful and familiar to the user, (2) be phonetically distinct from one another; and (3) consist of 2-5 syllables.				
		=>	4.2.5.1.10-7	Application vocabularies should be divided into sets based on the hierarchy of the application and recognition accuracy requirements.				
		=>	4.2.5.1.10-8	The user should be able to test the recognition of any individual vocabulary item without the entire interactive system being on-line. Feedback on the word recognized and the corresponding confidence score should be available immediately after each use of a word.				
		=>	4.2.5.1.10-9	When the consequences of errors are not significant, the speech amplitude and rejection levels required for input should be user-adjustable.				
		=>	4.2.5.1.10-10	Where word boundaries (pauses between words) are required for system interpretation, boundaries of 100 milliseconds or more should be allowed by the system.				
		=>	4.2.5.1.10-11	An indication of the similarity of each spoken command to the recorded template should be available to the user.				
		=>	4.2.5.1.10-12	If an application functions with a speaker-dependent voice recognizer, the user should be able to retrain or update any or all vocabulary templates at any time.				
4.2.5.2	Supporting Use of Individual Display Pages							
	=>	4.2.5.2-1	When requested data exceeds the capacity of a single display frame, users should be given some easy means to move (vertically, horizontally, or both, as needed) over displayed material by paging or scrolling.					

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.5.2-2	When users are required to integrate information across a large display, the HSI should be designed to minimize the effort associated with scrolling, paging, and zooming, and to maintain the users' orientation.				
		=>	4.2.5.2-3	The design of display pages should take into account limitation in users' abilities to effectively process visual information presented in a scrolling frame.				
		=>	4.2.5.2-4	Displays should be designed to avoid the need for excessive scrolling.				
		=>	4.2.5.2-5	An appropriate orientation for display framing should be chosen and used consistently throughout the interface.				
		=>	4.2.5.2-6	Display framing should be described (e.g., in user instructions and key labels) in functional terms, and wording that implies spatial orientation should be avoided.				
		=>	4.2.5.2-7	Display framing should be described (e.g., in user instructions and key labels) in functional terms, and wording that implies spatial orientation should be avoided.				
		=>	4.2.5.2-8	In addition to scrolling continuously or line-by-line, users should have the option of moving in larger increments (e.g., a display frame or 'page' at a time).				
		=>	4.2.5.2-9	Users should have the ability to scroll or page using different techniques.				
		=>	4.2.5.2-10	Users should be able to expand the size of (i.e., 'zoom') any selected area of the display.				
		=>	4.2.5.2-11	The interface should have features that help user remain oriented when 'zooming' displays.				
		=>	4.2.5.2-12	When users zoom a display, the system should compensate for changes in the size of symbols, labels, and other graphical objects.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.2.5.3		Supporting Navigation in Systems of Displays					
	=>	4.2.5.3-1	The organization of the display network should be readily understood by users.				
	=>	4.2.5.3-2	The display system should be represented so that the user's perception of the relatedness of displays is consistent with distance in the structure of the display hierarchy.				
	=>	4.2.5.3-3	Cues should be provided to help the user retain a sense of location within the information structure.				
	=>	4.2.5.3-4	Easily discernable features should appear in successive views and provide a frame of reference for establishing relationships across views.				
	=>	4.2.5.3-5	There should be physical or functional overlaps between displays that prevent the displays from appearing as disjointed views.				
	=>	4.2.5.3-6	A hypertext information system should show how a destination node is related to the point of departure.				
	=>	4.2.5.3-7	If the interpretation of displayed data depends on its context (i.e., the location in the display network), an explicit indication of the context should appear in the display.				
	=>	4.2.5.3-8	In spatial representations (such as maps or P&IDs), features should be included to help operators understand the depiction and to assist in way finding and maintaining orientation (especially when the representation is larger than a display page).				
	=>	4.2.5.3-9	During navigation, displays should support users' comprehension of the relationships between successive views or destinations.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.5.3-10	Wherever possible, the time and effort associated with navigation among display pages (especially those that are often used in succession) should be minimized.				
		=>	4.2.5.3-11	Use of various navigation strategies should be supported.				
		=>	4.2.5.3-12	The display network should provide more than one way to access displays.				
		=>	4.2.5.3-13	When multiple methods are provided for navigating in a hypertext system, they should function similarly.				
		=>	4.2.5.3-14	Backtrack capabilities should always be available in hypertext interfaces and should function in the same way.				
		=>	4.2.5.3-15	Selection points (e.g., navigation targets or links) should be easily detectable and readily distinguished from other displayed text or objects.				
	4.2.5.4		Controlling Displays					
		=>	4.2.5.4-1	Users should be able to specify the information to be displayed and select the format in which it is presented.				
		=>	4.2.5.4-2	Screen control locations and control options should be clearly and appropriately indicated.				
		=>	4.2.5.4-3	The rate at which displayed values are updated should be appropriate for the users' tasks.				
		=>	4.2.5.4-4	If a display can be frozen, it should contain features to ensure that users' remain aware of its state, and of the ongoing situation.				
		=>	4.2.5.4-5	If a display is suppressed, the interface should contain features to ensure that users' remain aware of its absence, and of the ongoing situation.				
		=>	4.2.5.4-6	Automated window management should be coordinated with the user's tasks.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.5.4-7	Automated interface management features should be designed such that their operation can be anticipated by users.				
		=>	4.2.5.4-8	The operation of automated interface management features should be apparent to the user.				
		=>	4.2.5.4-9	The operation of automated interface management features should not draw excessive attention from the user.				
4.2.5.5			Providing Feedback					
		=>	4.2.5.5-1	The computer should acknowledge every entry immediately.				
		=>	4.2.5.5-2	Actions requested by users should be completed within an appropriate time.				
		=>	4.2.5.5-3	If processing time requires delay of concurrent user inputs (and no keyboard buffer is available), users should be kept aware of the status of processing.				
		=>	4.2.5.5-4	When slower-than-typical response time can be anticipated (e.g., owing to unusual demands on the system) the users should be given information that will allow them to adjust their interaction with the system.				
		=>	4.2.5.5-5	Response time deviations should not exceed more than half the mean response time.				
4.2.5.6			Protecting Information					
	4.2.5.6.1		User Identification					
		=>	4.2.5.6.1-1	The logon process and procedures for user identification should be as simple as possible, consistent with protecting the system and associated data.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.6.1-2	When system security requires more stringent user identification than is provided by password entry, auxiliary tests should be devised that authenticate user identity without imposing impractical demands on users.				
			=>	4.2.5.6.1-3	Messages or signals should be provided in order to notify users (and system administrators) of potential threats to data security.				
			=>	4.2.5.6.1-4	If there are pending actions and the user requests a logoff, the system should inform the user that these actions will be lost and allow the user to cancel either the pending actions or the logoff.				
			=>	4.2.5.6.1-5	Where possible, in the event of automatic logoff, open files should be saved to some defined file name.				
			=>	4.2.5.6.1-6	Interactive timesharing systems should allow some specified time between keyboard actions before automatic logoff unless a longer period is requested by the user.				
			=>	4.2.5.6.1-7	An audible signal should be presented at specified intervals prior to automatic logoff.				
			=>	4.2.5.6.1-8	As required for security, procedures to control access to printed data should be established, rather than simply prohibiting the printing of sensitive data.				
		4.2.5.6.2		Data Integrity					
			=>	4.2.5.6.2-1	Measures should be provided to minimize data loss from failures or errors in the data processing system.				
			=>	4.2.5.6.2-2	Data should be protected from damage as result of inadvertent or mistaken actions by the user.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.6.2-3	Display formatting features, such as field labels and delimiters, should be protected from accidental change by users.				
			=>	4.2.5.6.2-4	When users are not authorized to change displayed data, “read-only” status should be indicated on the display.				
			=>	4.2.5.6.2-5	Data should be protected from inadvertent loss caused by the actions of other users.				
			=>	4.2.5.6.2-6	When simulated data and system functions are displayed or provided (perhaps for user training), real data should be protected and real system use should be clearly distinguished from simulated operations.				
			=>	4.2.5.6.2-7	In situations where mistaken or unwanted data changes may be possible, users (or a system administrator) should be able to request a record of data entry/change transactions.				
			=>	4.2.5.6.2-8	When a control entry will cause any extensive change in stored information, particularly if that change cannot be easily reversed, the user should be notified and confirmation of the action should be required before implementing it.				
			=>	4.2.5.6.2-9	For conditions that may require special user attention to protect against information loss, an explicit alert and/or advisory message should be provided to prompt appropriate user action.				
			=>	4.2.5.6.2-10	When a user requests logoff, pending transactions should be checked and if any pending transaction will not be completed, or if data will be lost, an advisory message requesting user confirmation should be displayed.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.6.2-11	If a user requests change (or deletion) of a stored data item that is not currently being displayed, both the old and new values should be displayed so that the user can confirm or nullify the change before the transaction is completed.				
			=>	4.2.5.6.2-12	When records of data access are necessary, the records should be maintained automatically.				
	4.2.5.7		Managing Information						
		4.2.5.7.1		Editing Documents					
			=>	4.2.5.7.1-1	Users should be allowed to specify segments of text in whatever units are natural for entry/editing.				
			=>	4.2.5.7.1-2	Users should be allowed to display text exactly as it will be printed.				
			=>	4.2.5.7.1-3	Easy means should be provided for users to specify required format control features (e.g., margin and tab settings) during text entry/editing.				
			=>	4.2.5.7.1-4	Text entered by users should be formatted automatically.				
			=>	4.2.5.7.1-5	Users should be able to modify the formatting of text as needed.				
			=>	4.2.5.7.1-6	A tab function should be available for paragraph indentation and for moving the cursor to a preselected location.				
			=>	4.2.5.7.1-7	For editing programs or tabular data, cursor tab controls or other provisions for establishing and moving readily from field to field should be provided.				
			=>	4.2.5.7.1-8	The means should be provided to readily move the cursor to the head (beginning) or the foot (end) of the file.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.7.1-9	When inserting words or phrases, items to be inserted should be displayed as the final copy will appear.				
			=>	4.2.5.7.1-10	Users should be allowed to specify a string of text and request the computer to advance (or back up) the cursor automatically to the next (or last previous) occurrence of that string.				
			=>	4.2.5.7.1-11	When systematic editing changes will be made throughout a long document, a “global search and replace” capability should be provided.				
			=>	4.2.5.7.1-12	Users should be allowed to select and move text segments from one place to another within a document.				
			=>	4.2.5.7.1-13	Users should be allowed to label and store frequently used text segments, and to later recall (copy into current text) stored segments identified by their assigned labels.				
			=>	4.2.5.7.1-14	If the selected text, table, or graphics area extends beyond the bottom of the displayed page, the screen should automatically scroll until the user stops selecting or when the end of the display page is reached.				
			=>	4.2.5.7.1-15	Users should not be able to select non-contiguous blocks of text when copying, cutting, or pasting.				
		4.2.5.7.2		Saving Files					
			=>	4.2.5.7.2-1	The user should be able to save the information entered into a file by a single action that will permit the user to continue interacting with that file.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.7.2-2	After finishing the interaction with any type of file, the user should be able to save the information and stop interacting with the file by a single action.				
			=>	4.2.5.7.2-3	After finishing the interaction with any type of file, the user should be able to stop interacting with the file by a single action (e.g., selecting a menu item) without saving the changes to the file.				
			=>	4.2.5.7.2-4	The command used to “exit with save” should differ from the commands for “save” (without exit) and for “exit without save.”				
			=>	4.2.5.7.2-5	Processing of files should be designed to prevent the lost of input or changes.				
		4.2.5.7.3		Temporary Editing Buffer					
			=>	4.2.5.7.3-1	When selected data is cut or copied from a text file, tabular file, and/or graphics file and placed in a temporary editing buffer, the data should be placed in the buffer automatically, with the only specific action required by the user being the cut or copy action.				
			=>	4.2.5.7.3-2	The contents of the temporary editing buffer should remain intact after the application from which the contents were taken is closed.				
			=>	4.2.5.7.3-3	The default condition should be that additions to the temporary editing buffer are not cumulative.				
			=>	4.2.5.7.3-4	The user should be able to access the contents of the temporary editing buffer in a window with a single action.				
		4.2.5.7.4		Excerpt File					

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.7.4-1	The capability to accept and maintain information, independent of application, should be provided for holding relevant information across displays or applications.				
			=>	4.2.5.7.4-2	Users should have the capability to create multiple excerpt files.				
			=>	4.2.5.7.4-3	The user should have the capability to integrate new data with data already in the excerpt file.				
			=>	4.2.5.7.4-4	The user should be able to cut or copy data from the excerpt file and paste it to any other file.				
			=>	4.2.5.7.4-5	The user should be able to save the excerpt file.				
4.2.6		Interacting with Interface Components							
	4.2.6.1		Windows						
		4.2.6.1.1		General					
			=>	4.2.6.1.1-1	As appropriate to the user task, windows should be capable of the following operations: scrolling/panning, resizing, moving, hiding, activating, deactivating, copying to/from, zooming in/out, tabbing, and undo-last.				
			=>	4.2.6.1.1-2	User control of windows should operate consistently from one display to another for each type of window.				
			=>	4.2.6.1.1-3	When control actions such as command entry may be taken by a user working within a window, those control actions should be consistent from one window to another.				
		4.2.6.1.2		Labeling and Appearance					

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.1.2-1	Windows should be identified by a label consistently located at the top of the window's border.				
			=>	4.2.6.1.2-2	Window objects, dialog boxes, and subordinate windows should be labeled.				
			=>	4.2.6.1.2-3	The titles of subordinate windows should match the menu selection items of the menus from which they are selected.				
			=>	4.2.6.1.2-4	Windows should be visually separated from each other and from their background, preferably by borders or similar demarcation.				
			=>	4.2.6.1.2-5	Window types should be perceptually distinct (see Figure 4-26).				
		4.2.6.1.3		Multiple Windows					
			=>	4.2.6.1.3-1	If separate display pages contain information that the user must compare, combine, or otherwise mentally process, then they should be presented simultaneously.				
			=>	4.2.6.1.3-2	Users should be able to select separate data windows that will share a single display screen.				
			=>	4.2.6.1.3-3	When multiple windows are open simultaneously, the user should have the capability to easily tile, layer, or sequentially view the windows (see Figure 4-26).				
			=>	4.2.6.1.3-4	The system should keep track of the windows that are open (but not necessarily active or displayed), and provide a means of displaying the list of open windows to the user.				
			=>	4.2.6.1.3-5	An upper limit on the number of windows allowed to be open at one time should be defined to ensure that system response time is not compromised.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.1.3-6	If several windows are displayed at once, the window(s) in which action can be taken should be indicated.				
			=>	4.2.6.1.3-7	A separate menu bar should be provided for each application window, where different applications are operating concurrently in open windows (e.g., multi-tasking).				
		4.2.6.1.4		Active and Inactive Windows					
			=>	4.2.6.1.4-1	The user should be able to activate a window by performing any of a set of simple actions in that window or related to that window.				
			=>	4.2.6.1.4-2	The action that activates a window should automatically position the place-holding cursor in that window so that the user can provide inputs through that window.				
			=>	4.2.6.1.4-3	If windows are capable of different modes, the system should provide immediate and unambiguous feedback concerning which mode is in effect.				
			=>	4.2.6.1.4-4	A window that is not displayed should be capable of receiving information from the system.				
			=>	4.2.6.1.4-5	The system should alert the user to critical information that becomes available in an inactive or non-displayed window.				
			=>	4.2.6.1.4-6	Under normal operating conditions, active windows should be frontmost on the display.				
			=>	4.2.6.1.4-7	Caution and warning windows should be frontmost on the display.				
		4.2.6.1.5		Size and Location of Windows: Defaults					

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.1.5-1	The size and shape of the initial presentation of a window should be consistent with its contents (amount of information, number of menus, and data fields).				
			=>	4.2.6.1.5-2	The default dimensions of text windows should be large enough so that the readability of the information is not impaired.				
			=>	4.2.6.1.5-3	The amount of resizing, placement, and manipulation of windows required for using the HSI should be minimized.				
			=>	4.2.6.1.5-4	The system should not allow the user to move or resize a window containing non-critical information such that it obscures critical information.				
			=>	4.2.6.1.5-5	A temporary window object should not obscure critical control information and command entry interfaces of the active window.				
			=>	4.2.6.1.5-6	The system should not allow the user to move a window containing critical information off the display screen.				
			=>	4.2.6.1.5-7	Windows should have a default location on the display screen.				
			=>	4.2.6.1.5-8	Display data that is temporarily obscured by a window object should reappear when the object is removed.				
		4.2.6.1.6		Size and Location of Windows: Adjusting					
			=>	4.2.6.1.6-1	Window movement capability should be provided such that the user can move windows to different areas of the display.				
			=>	4.2.6.1.6-2	It should not be possible to position windows in such a way that menu bars, access to the command area, or caution and warning messages are obscured.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.1.6-3	Movement of a window should appear to be smooth and continuous to the user.				
			=>	4.2.6.1.6-4	Windows partially moved off the display should be made readily accessible with a single action.				
			=>	4.2.6.1.6-5	Users should be able to change the horizontal and vertical dimensions of a window independently or together.				
		4.2.6.1.7		Opening and Closing Windows					
			=>	4.2.6.1.7-1	The user should be able to open a window by performing any of a set of simple actions.				
			=>	4.2.6.1.7-2	Users should be able to close a window with a single action.				
			=>	4.2.6.1.7-3	If several windows are open, several easy means should be provided for a user to shift among them.				
			=>	4.2.6.1.7-4	The action that opens a window should automatically make that window active.				
			=>	4.2.6.1.7-5	An easy means for the user to suppress the display of windows should be provided.				
			=>	4.2.6.1.7-6	The window system should convey to the user the relationship between the window, the icon, and the action when a window is opened or closed.				
			=>	4.2.6.1.7-7	When a main application window is closed by the user, all associated subordinate windows and dialog boxes should also close.				
			=>	4.2.6.1.7-8	When a windows are being closed (either by the user or as the result of some other action), the user should be made aware of any pending changes or incomplete interactions.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.2.6.2	Cursors						
4.2.6.2.1	Appearance						
	=>	4.2.6.2.1-1	Cursors should have distinctive visual features (shape, blink, or other means of highlighting).				
	=>	4.2.6.2.1-2	The cursor should not move beyond the display boundaries or disappear from sight.				
	=>	4.2.6.2.1-3	The cursor should not be so distracting as to impair the searching of the display for information unrelated to the cursor.				
	=>	4.2.6.2.1-4	The displayed cursor should be stable.				
	=>	4.2.6.2.1-5	On the initial appearance of a data entry display, the cursor should appear automatically at some consistent and useful location.				
	=>	4.2.6.2.1-6	When there is a predefined HOME position for the cursor, that position should be consistently defined on all displays of a given type.				
	=>	4.2.6.2.1-7	When the user must repeatedly return the cursor to the origin or other specific screen location, automatic return or repositioning of the cursor should be provided.				
4.2.6.2.2	Controls						
	=>	4.2.6.2.2-1	The user should be able to adjust the sensitivity of the cursor movement to be compatible with the required task and user skills.				
	=>	4.2.6.2.2-2	Control actions for cursor positioning should be compatible with movements of the displayed cursor, in terms of control function and labeling.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.2.2-3	Users should be provided with an easy, accurate means of positioning a displayed cursor to point at different display elements and/or display locations.				
			=>	4.2.6.2.2-4	Where cursor positioning is incremental by discrete steps, the step size of cursor movement should be consistent horizontally (i.e., in both right and left directions), and vertically (in both up and down directions).				
			=>	4.2.6.2.2-5	At the minimum, keys for cursor control should allow horizontal and vertical cursor movement.				
			=>	4.2.6.2.2-6	When position designation is required in a task emphasizing keyed data entry, cursor control should be provided by some device integral to the keyboard (function keys, joystick, and trackball).				
			=>	4.2.6.2.2-7	If cursor movement is accomplished by depressing keys, the keys should be located on the main keyboard.				
		4.2.6.2.3		Movement					
			=>	4.2.6.2.3-1	If the cursor is moved by depressing a key, releasing the key should cause the cursor to stop moving.				
			=>	4.2.6.2.3-2	The cursor control should permit both fast movement and accurate placement.				
			=>	4.2.6.2.3-3	When fine accuracy of positioning is required, as in some forms of graphic interaction, the displayed cursor should include a point designation feature.				
			=>	4.2.6.2.3-4	The user should be able to turn rate aiding of the cursor movement on or off.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.2.3-5	Users should be able to select at least two speeds (normal and fast) for the movement of the cursor when the keys for cursor control are held down.				
			=>	4.2.6.2.3-6	When character size is variable, the incremental cursor positioning should vary correspondingly, with a step size matching the size of currently selected characters.				
			=>	4.2.6.2.3-7	If a cursor must be positioned sequentially in predefined areas, such as displayed data entry fields, this should be accomplished by simple user action.				
			=>	4.2.6.2.3-8	Users should be required to take a separate, explicit action, distinct from cursor positioning, for the actual entry (enabling, activation) of a designated function.				
			=>	4.2.6.2.3-9	When there are areas of a display in which data entries cannot be made (such as in field labels or in blank spaces that are part of data formatting), the cursor should ‘step over’ those areas, and they should be insensitive to pointing actions.				
			=>	4.2.6.2.3-10	For text editing, users should be allowed to move the cursor freely over a displayed page of text to specify items for change, and to make changes directly to the text.				
			=>	4.2.6.2.3-11	If proportional spacing is used for displayed text, computer logic should make necessary adjustments automatically when the cursor is being positioned for data entry or data change.				
			=>	4.2.6.2.3-12	Users should be able to move the cursor by specific units of text, as well as one character at a time.				
			=>	4.2.6.2.3-13	An ENTER action for multiple data items should result in entry of all items, regardless of where the cursor is placed on the display.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		4.2.6.2.4	Multiple Cursors						
			=>	4.2.6.2.4-1	Multiple cursors on a single display should be used only when it can be demonstrated that they are required by the task.				
			=>	4.2.6.2.4-2	In a multitasking environment with multiple monitors, controllers, or cursors, the location of the active cursor should be obvious to the user.				
			=>	4.2.6.2.4-3	If multiple cursors are used, they should be visually distinctive from one another.				
			=>	4.2.6.2.4-4	If multiple cursors are controlled by different devices, their separate controls should be compatible in operation.				
			=>	4.2.6.2.4-5	When multiple cursors are controlled by a single device, the cursor currently being controlled should be clearly indicated.				
			=>	4.2.6.2.4-6	When there are multiple cursor control/pointing devices, a unique pointing cursor shape should be associated with each device.				
			=>	4.2.6.2.4-7	Cursors of different shapes should be used for different purposes.				
		4.2.6.2.5	Pointing Cursors						
			=>	4.2.6.2.5-1	The pointing cursor should be visible to the user at all times and may obscure characters unless it interferes with performance within an application.				
			=>	4.2.6.2.5-2	The pointing cursor should not blink.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.2.5-3	Pointing cursors should maintain image quality throughout an entire range of motion within the display. The position of the pointing cursor should be clearly visible during movement from one screen position to another. Flicker should be minimized.				
			=>	4.2.6.2.5-4	To the greatest degree possible, pointing cursors should be completely graphic and should not contain a label.				
			=>	4.2.6.2.5-5	The pointing cursor should maintain its size across all screen and display locations.				
			=>	4.2.6.2.5-6	The movement of the pointing cursor should appear to the user to be smooth and continuous, with smooth and continuous movement of the cursor control device. The pointing cursor should not move in the absence of any input from the user.				
		4.2.6.2.6		Text Entry Cursors					
			=>	4.2.6.2.6-1	The text entry cursor should only be visible when text entry is possible.				
			=>	4.2.6.2.6-2	At the initiation of a task, an application, or a new display, the user should be able to immediately determine the location of the text entry cursor. Following the initial placement of the text entry cursor, the position of the cursor should be under the user’s control.				
			=>	4.2.6.2.6-3	If text entry cursor blinking is to be used to direct the user’s attention, the default blink rate should be 3 Hz.				
			=>	4.2.6.2.6-4	The place-holding cursor should not obscure any other character displayed in the position designated by the cursor.				
			=>	4.2.6.2.6-5	There should be only one text entry cursor per window.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.2.6-6	The text entry cursor should assume the height and/or width of the text characters adjacent to it.				
		4.2.6.2.7		Multiple Display Devices					
			=>	4.2.6.2.7-1	When displays are the same size and are located adjacent to each other, the cursor should appear to move in a smooth, continuous motion from one display device to the next.				
			=>	4.2.6.2.7-2	When display devices are physically separated, have different orientations, or different sizes, techniques should be employed to help the user keep track of the cursor's position.				

4.2.4 General Interface Design Objectives

The section contains design guidance that applies generally to functions of the HSI supporting user-interface interaction and management, without regard to the particular input format. The guidelines are organized around a number of design objectives reflecting general principles of human-system interaction and good interface design practices:

- Simplifying Input
- Ensuring User Control of the Interaction
- Establishing Consistency of Interface and Interaction
- Minimizing Demands on the User
- Maintaining Awareness of Context and Options
- Guiding and Assisting Users
- Allowing Flexibility

The overall goal is to minimize interface management tasks and associated workload so the user can focus on primary tasks.

4.2.4.1 Simplifying Input

The user interface should permit completion of tasks with the minimum number of actions. For example, it should be possible to print a display by simple request, without having to take a series of other actions first, such as first calling for the display to be written to a file, then specifying a file name, and then calling for a print of that named file. Similarly it should be possible to display a particular page of a long series of pages directly, without having to take repetitive NEXT PAGE or PREV PAGE actions.

Note that the need for simplicity and minimizing the number of actions must be balanced in some situations against the need to guard against inadvertent actions that carry risk to plant equipment or safety. In some cases (for example, executing a control action such as opening a valve or tripping a pump when there is significant risk associated with inadvertent activation of the control), additional confirmatory steps may be needed in the interaction with the interface to ensure that the correct action has been selected and the user is taking a deliberate step to execute the function. See Section 4.2.5.6.2 for additional guidance.

⇒ 4.2.4.1-1 User input actions should be simple, particularly for real-time tasks requiring fast user response.

⇒ 4.2.4.1-2 Input transactions and associated displays should be designed so that a user can stay with one method of entry, and not have to shift to another.

For example, shifts from mouse to keyboard entry and then back again should be minimized. Forcing users to shift from one keyboard to another, or move from one workstation to another, to accomplish different input tasks should also be avoided. Similarly, users should not have to use multiple input devices to interact with multiple VDUs at the same workstation.

⇒ 4.2.4.1-3 For interpreting user-composed control entries, upper and lower case letters should be treated as equivalent.

Users find it difficult to remember whether upper or lower case letters are required, and so the interface design should not try to make such a distinction.

⇒ 4.2.4.1-4 Unless otherwise required by processing or display requirements, alphabetic input should be left justified, and numeric input should be right justified for integer data or decimal point justified for decimal data.

Optional entry or omission of a decimal point at the end of an integer should be allowed as equivalent alternatives.

⇒ 4.2.4.1-5 Automatic justification of tabular data entries should be provided.

A user should not have to enter blanks or other extraneous formatting characters to achieve proper justification. For example, if a user enters "56" in a field four characters long, the system should not interpret "56 __ __" as "5600". For general numeric data, optional entry or omission of leading zeros should be allowed as equivalent alternatives. If a user enters "56" in a field that is four characters long, the system should recognize that entry rather than requiring an entry of "0056". Special cases may represent exceptions to this rule, such as entry of serial numbers or other numeric identifiers.

⇒ 4.2.4.1-6 When a user must enter numeric values that will later be displayed, all significant zeros should be maintained.

Zeros should not be arbitrarily removed after a decimal point if they affect the meaning of the number in terms of significant digits.

⇒ 4.2.4.1-7 Numeric values should be displayed to the level of significance required of the data, regardless of the value of individual input data.

⇒ 4.2.4.1-8 Data entry by overwriting a set of characters within a field should be avoided.

If a user chooses to alter the contents of a field, the displayed previously existing entry (e.g., a default value or label) should be cleared from the input field.

⇒ 4.2.4.1-9 The user should not be required to enter data separators or delimiters, such as dashes and slashes.

The entry of data separators and delimiters can be time consuming and error prone.

⇒ 4.2.4.1-10 The user should not be required to enter units of measure.

The entry of dimensional units (e.g., 'gpm') can be time consuming and error prone. However, the unit of measure should be shown so that the user can verify that the entry is correct, e.g., gpm rather than liters per minute.

⇒ 4.2.4.1-11 When data entry is a significant part of a user's task, entered data should appear on the user's main display.

When the main display is basically formatted for other purposes, such as a graphic display for process control, a separate window or area on the display may have to be reserved for data entry. The window should appear in a predictable location (e.g., always at the same place on the display, or as close as possible to the graphic element to which it is related); see Section 4.2.6.1.5.

⇒ 4.2.4.1-12 The same explicit ENTER action should be required for entry of corrections as used for the original entry.

⇒ 4.2.4.1-13 Users should be able to perform simple editing during text entry without having to invoke a separate edit mode.

While entering text, users should have some capability for text selection (by cursor movement) and deletion (e.g., by use of destructive backspace).

⇒ 4.2.4.1-14 When appropriate (e.g., in menu-based systems where system response may be slow), the system should allow users to easily enter a sequence of commands or option codes as a single 'stacked' entry.

Implementation of stacking should be simple and straightforward; for example:

- entries should be required to be in the same order as they would normally be made in a succession of separate control entry actions
- command names, their abbreviations, or option codes should be accepted just as if those control entries had been made separately
- the computer should display its interpretation of a stacked entry in circumstances in which user review and confirmation is desirable
- users should be allowed to stack control entries without any punctuation other than spaces between words or option codes
- if punctuation other than spaces is needed to separate entries in a stacked control entry, a single standard symbol (e.g., a slash) should be used for that purpose
- the delimiter for control entries should preferably be the same as any delimiter that might be used when making data entries

For example, suppose that users bring up particular screens by selecting the type of presentation, the content, and the configuration from a series of menus. The system might allow a user needing a full screen view of a data overview page to enter ‘dof’ rather than selecting data, overview, full screen from three successive menus. If the menu system could not be designed so that single letters would suffice to uniquely represent all the choices, it would be necessary to separate the entries (preferably using spaces).

⇒ 4.2.4.1-15 All displays should be designed so that features relevant to user entries are distinctive in position and/or format.

Relevant features include displayed options, command entry areas, prompts, advisory messages, and other displayed items (such as titles and time signals) whose changes signal the results of user entries. Interaction is simplified if the features that operators interact with have a predictable appearance and location.

⇒ 4.2.4.1-16 The means of entering information or commands should be compatible with user skills, permitting simple step-by-step actions by beginners, but permitting more complex entries by experienced users.

Most systems will have users with varying levels of experience. Any particular user may become more expert with increasing experience, or perhaps less expert after a long period of disuse. Accommodating users of varying expertise requires a mixture of different dialogue types, with some means for smooth transition from one mode of dialogue to another. For instance, as users come to learn menu codes, they might be allowed to enter those codes without necessarily displaying a menu; see below.

4.2.4.2 Ensuring User Control of the Interaction

Users should be able to specify when a requested transaction should start or be completed, or to schedule the periodic transactions. In many applications, users will wish specified transactions be performed as quickly as possible. In some applications, however, users may have good reasons to delay initiation (or completion) of transactions. For example, a user might wish to specify that a requested data analysis routine be deferred until some later time, to ensure that interim updates to the data will be taken into account.

⇒ 4.2.4.2-1 Users should be allowed to control the processing of information or execution of commands.

In most applications, a user should be able to interrupt or terminate processing once it has been initiated. The functions in Table 4-8 should be provided (as appropriate to task requirements).

Table 4-8
Functions for the Control of Processing Commands

Function	Result	Application Example
END	conclude a repetitive sequence of actions	in a repetitive sequence of data entries, where completing one transaction cycles automatically to begin the next, END might break the cycle and permit the user to select other transactions
PAUSE/CONTINUE	interrupt and later resume a sequence of transactions without any change to data entries for the interrupted transaction	a user might interrupt a current task to read an incoming message
SUSPEND	preserve current status when a user leaves the system, and permit resumption at that point when the user later logs back onto the system	a user might postpone completion of a task until needed data become available

The processing of an entry or the cancellation of an ongoing process should not occur as a side effect of some other action. For example,

- the system should not interrupt an extended data entry to require immediate correction of any entry error, but instead should wait for the user's ENTER action
- when a user is composing a command to accomplish some transaction, the computer should not interrupt the user by responding as soon as it recognizes a partial entry, but instead should wait for the user's ENTER action

In automated process control applications, emergency conditions may take precedence over current user transactions, and a computer-generated warning might interrupt user actions. In routine, repetitive data entry transactions, successful completion of one entry may lead automatically to initiation of the next. Computer detection of problems with current user entries can usually be negotiated at the conclusion of a transaction, before it is implemented. Nondisruptive alarms or advisory messages can be displayed to report computer monitoring of external events so that the user can choose when to deal with them.

⇒ 4.2.4.2-2 If different kinds of user interrupts are provided, each interrupt function should be designed as a separate control option with a distinct name.

The means of invoking interrupt functions should be clear to the user. For example, it is undesirable to have a single INTERRUPT key that has different effects depending upon whether it is pushed once (causing processing to pause) or twice (causing processing to be terminated). Users would be confused by such an expedient, and uncertain about what action has been taken and its consequences. Separate options (keys or menu choices) designated PAUSE and END would be preferable.

⇒ 4.2.4.2-3 User interrupts and aborts should not modify or remove stored or entered data.

⇒ 4.2.4.2-4 Users should be allowed to control the pace and sequence of their entry of information or commands.

The functions in Table 4-9 should be provided (as appropriate to task requirements).

Table 4-9
Functions for the Control of Entering Information

Function	Result	Application Example
CANCEL	erase any changes just made by the user and restore the current display to its previous version	correction of erroneous input prior to actually entering the information in a data file
BACK	return to the display for the last previous transaction	in a sequence of related data entries, on several display frames, return to the previous frame, where data items could then be erased or could be edited individually
REVIEW	return to the first display in a defined transaction sequence, permit the user to review a sequence of entries and make necessary changes	in a sequence of related data entries, on several display frames, return to the first frame, from which data could be reviewed and edited as needed throughout the sequence of frames
RESTART	canceling any entries that have been made in a series of entries and returning to the beginning of the sequence	in a sequence of related data entries on a form-filling display, erase all data entries and return to the first field on the form

⇒ 4.2.4.2-5 If PAUSE or SUSPEND options are provided, some indication of the status should be displayed whenever a user selects such an option.

When a transaction is time consuming or resource intensive, users may be given the option of pausing or suspending it so that other tasks can be completed promptly. If appropriate (i.e., for a paused transaction), the action that will permit resumption of the interrupted transaction should be indicated to the user.

⇒ 4.2.4.2-6 The HSI should provide visual and/or auditory reminders for interrupted tasks.

The interface should indicate that tasks are pending, but the reminders should not unnecessarily disrupt ongoing tasks, since the user will typically have suspended a task in order to attend to something that is more urgent. More conspicuous reminders may be warranted when tasks currently being initiated might depend on input from the suspended task, when windows related to the suspended tasks are being closed, or when user input has ceased for a time (indicating that the more urgent task has been completed).

⇒ 4.2.4.2-7 The HSI should provide simple mechanisms for retrieving displays and controls for tasks that have been suspended.

Extensive effort should not be required to either retrieve the display or reconfigure the display so that work may resume on a suspended task.

⇒ 4.2.4.2-8 At any step in a defined transaction sequence, if there is only a single appropriate next step, then a consistent control option to continue to the next transaction should be provided.

CONTINUE or NEXT or STEP are all suitable names for this option. If data entry is involved, then users should be required to take an explicit ENTER action to signal data entry, rather than simply selecting CONTINUE.

⇒ 4.2.4.2-9 Transactions should never leave the user without further available action and should provide next steps or alternatives.

A number of basic actions (e.g., “Continue,” “Abort,” and “Go to Main directory”) should be available to users at any point in their interaction with the system.

4.2.4.3 Establishing Consistency of Interface and Interaction

⇒ 4.2.4.3-1 Procedures for entering commands or information should be consistent in form and consequences.

Menu selection techniques, user input procedures, editing and error correction procedures are examples of user actions for which conventions are required. Consistent procedures will help users develop consistent habits of operation, can reduce the likelihood of user confusion and error, and are especially important for any transaction that risks data loss.

⇒ 4.2.4.3-2 All terms employed in the user-system interface, and their abbreviations, should be consistent in meaning from one transaction to another, and from one task to another.

The same kind of action should be referred to by the same word in any context. For example, EDIT should not be used in one place, MODIFY in another, UPDATE in a third, all referring to the same kind of action. Commands should be congruent with one another, following natural language patterns; if one command is UP, its complement should be DOWN. Other natural complements include OPEN-CLOSE, RUN-STOP, ON-OFF, IN-OUT, and RAISE-LOWER. For instructional material, such as display labeling, on-line guidance, and other messages to users, consistent terminology should be used to refer to entry of commands or information.

⇒ 4.2.4.3-3 The wording and required format of information or command entry functions should be consistently reflected in the wording of user guidance, including all operating procedures, labels, messages, and training material.

For example, if user guidance mentions a file name, that name should be shown in a format that would be acceptable if the name were included in a command entry; if a user must complete a control form to specify printer settings, the words used as labels on that form should also be used in any error messages and HELP displays which may guide that process.

⇒ 4.2.4.3-4 Controls used for interface management tasks should have consistent locations.

Interface management controls include user interfaces for selecting displays and navigating within displays. Examples include command fields, function buttons, and scroll bars. Consistent locations are one way to uniquely identify interface management controls to support users in identifying and accessing them. Controls for navigating within a display page should be separate from the main body of the display screen; they should remain in fixed locations as the page is navigated.

4.2.4.4 Minimizing Demands on the User

⇒ 4.2.4.4-1 Entry of information or commands should not require the user to remember special codes or sequences or to perform translations or conversions.

Command names should specifically describe the functions being implemented and should reflect the vocabulary and syntax of the user's operational language. The user should not have to transform units at time of data entry. For example, user entries should be in the same units that are used in control room displays and procedures; the user should not be required to convert from gallons per minute to gallons per hour.

⇒ 4.2.4.4-2 A user should not be required to re-enter information already available to the system.

A user should need to enter any particular information only once, and the computer should access that information if needed thereafter for the same task or for different tasks. That is, if users enter a series of values in the course of carrying out a task, they should not be required to enter these same values again during subsequent activities. Requiring re-entry of data requires unnecessary effort on the part of users and increases the possibility of entry errors. The computer should automatically access or compute information that can be derived from existing computer records. Such information should be displayed to users so that they can verify that it is correct for the current situation.

⇒ 4.2.4.4-3 Information necessary to accomplish a specific entry (e.g., labels, annotations, prompts, or options lists) should be available to the user when that transaction action is appropriate.

Required annotation will vary with the application. Some annotation may be so commonly needed that it should be continuously displayed, e.g., document name, page number, and indication of control mode (if any). Other annotation might be displayed only at user request, such as document status (date last changed or last printed), which might be displayed in an optional window overlay, and format control characters, which might be visible in an optional display mode. For example, the user might wish to see format control characters, such as tab and margin settings.

⇒ 4.2.4.4-4 An information entry sequence should be designed so that its organization reflects the user's view of the task, and should provide all control options that may be required.

A logical unit to the user is not necessarily the same as a logical unit of the computer software that mediates the transaction sequence. It might be, for example, that a user should enter ten items of data in a single transaction, because those data all come from one particular paper form, even though the computer will use five of those items for one purpose and five items for another in its subsequent internal processing.

⇒ 4.2.4.4-5 Flexible means of entering information or commands should be provided so that users can accomplish necessary transactions, and can obtain guidance as needed in connection with any transaction

The user should be able to go forward or back at will when scanning a multipage display. If user interface design permits only forward steps, so that the user must cycle through an entire display series to reach a previous page, that design is deficient.

⇒ 4.2.4.4-6 The results of any entry should be compatible with user expectations, so that the system changes in a 'natural' way in response to user actions.

The result of an entry should be consistent with the user's view of the system. For example, a control entry of NEXT PAGE should show the next frame of a current display, and should not jump off to some other internally defined 'page' in the computer's database. When a control entry is completed by pressing a certain key, that key should be labeled ENTER (or some functionally equivalent word) and should result in computer acknowledgment of the entry.

⇒ 4.2.4.4-7 If entries are made by keying onto the display, such as by keyed menu selections or commands, they should be distinguishable from displayed text.

Interfaces should be designed so that keystrokes intended to invoke commands are not taken as text entry, or vice versa. Errors can be avoided by having keyed entries made only in a reserved window in the display, or by using function keys rather than text entry for command selection.

⇒ 4.2.4.4-8 Annotations added by users to displayed text should be distinguishable from the text itself.

For example, continuous annotation might be displayed in the top and/or bottom lines of a page, separated from the text by blank lines, or in an adjacent window. Temporary pop-up windows with a distinctive border or background color (e.g., computerized 'post-it' notes) might also be used. To reduce clutter, such windows might be displayed automatically when the cursor is moved to a symbol indicating the presence of a note, and closed when the cursor is moved away.

⇒ 4.2.4.4-9 Travel distance for cursors across and between display pages and windows on a display screen should be minimized.

Unnecessary cursor movement can increase information access cost and divert mental resources from more important tasks by requiring the user's attention and time for execution.

⇒ 4.2.4.4-10 Displays that can provide decluttering capabilities should also provide a means for the user to rapidly return the display to its original configuration.

When users are given the option of easily removing material such as labels and annotations from a display so that essential data can be viewed without interference, it should be possible just as easily to return the display to its original condition.

⇒ 4.2.4.4-11 The user should be able to manipulate information without concern for internal storage and retrieval mechanisms of the system.

The system should contain sufficient memory to accommodate the user's requirements.

⇒ 4.2.4.4-12 When likely default values can be defined for the information to be entered in a particular task, those default values should be offered to speed entry.

Interactions involving defaults should have the following characteristics:

- At the start of an input transaction, currently defined default values should be displayed in their appropriate data fields. It may be helpful to mark default values in some way to distinguish them from new data entries.
- Users should be provided with some simple means to confirm acceptance of displayed default values (e.g., pressing the ENTER key without entering any value). Similar techniques, e.g., tabbing past the default field, should be used when a user must review the accuracy of previously entered data.
- When keyed command or option code entries are used and a default is defined for a null control entry, the default should be indicated to the user.
- When designers do not define default values, users (perhaps system administrators) should be permitted to define or remove default values for any input field.
- Users should be allowed to replace a displayed default with a different entry, without thereby changing the default definition for subsequent sessions. The direct replacement of a default value in a data field with a new value should not change the definition of the default value.

⇒ 4.2.4.4-13 Preset and automated set-up features should be used to ensure that users do not have to perform these functions while operating the plant.

Preset features are ready to use without a separate set-up operation. Automated set-up features are performed by the system rather than by personnel. The demands associated with setting up a computer-based system prior to its use can distract the user from primary tasks. Preset and automated set-up features should be used to minimize system set-up demands that may interfere with primary tasks. For example, the interface might offer the capability to automatically show (by opening and sizing the associated windows) all of the controls and displays needed to line up a given system for a specific purpose.

⇒ 4.2.4.4-14 When users must select options by code entry, the code associated with each option should be displayed in a consistent and distinctive manner.

In many applications, an equal sign is used to designate option codes, such as N = Next page and P = Previous page.

⇒ 4.2.4.4-15 When several users must interact with the system simultaneously, control entries by one user should not interfere with those of another.

This requires careful interface design for applications where joint, coordinated actions must be made by a group of users. See Section 4.1.3.3 for more information on crew coordination.

4.2.4.5 Maintaining Awareness of Context and Options

At any point in their interaction with the interface, users should be aware of what actions are available to them, and what effect those actions will have.

⇒ 4.2.4.5-1 If the consequences of a user entry will differ depending upon context established by a prior action, then some continuous indication of current context should be displayed for reference by the user.

The user should not have to query the system to determine the current mode. For example, if activating a DELETE key establishes a mode, so that subsequent selection of a PAGE key will erase a page of data rather than simply advancing to display the next page, then some indication of that established DELETE mode should be displayed to the user. (In this example, the design should also require the user to take a second action to confirm that DELETE is really wanted; see Section 4.2.5.6.)

⇒ 4.2.4.5-2 Information displayed to provide context for user entries should be distinctive in location and format, and consistently displayed from one transaction to the next.

The system should indicate current position within a sequence.

⇒ 4.2.4.5-3 Users should be permitted to request a summary of prior entries to help determine present status, and should be allowed to review the entries currently in effect.

Summarizing prior entries will be particularly helpful in tasks where the sequence of user actions is variable, where a user must know what was done in order to decide what to do next. Summarizing prior entries may not be needed for routine transactions if each step identifies its predecessors explicitly, although even in those circumstances, a user may be distracted and at least momentarily become confused.

⇒ 4.2.4.5-4 A general list of basic options should be provided and always be available to serve as a 'home base' or consistent starting point for user input.

There should be a simple means of calling up the basic set of commands that are appropriate at any point during the use of a system or application. Methods for doing this might include an option shown on every screen, an OPTIONS function key, or a generally available implicit option (i.e., by an action that is always available and has the same effect regardless of the context). For example, a system might be designed so that keying CONTROL-H at any point during its use will cause a menu of basic options (e.g., save, close, open new, print screen, or clear entries) to be displayed.

⇒ 4.2.4.5-5 When a user is performing an operation on some selected display item, that item should be highlighted.

This practice will help avoid error, if a user has misunderstood or perhaps forgotten which item was selected.

⇒ 4.2.4.5-6 The general options list should show control entry options grouped, labeled, and ordered in terms of their logical function, frequency, and criticality of use, following the general guidelines for menu design.

In systems in which selection is made by use of a cursor, formats should be organized to minimize positioning movements of the cursor.

⇒ 4.2.4.5-7 Users should be provided with a list of the control options that are specifically relevant and available for any transaction.

Transaction-specific options might be listed in the working display if there is space for them. Otherwise, they might be displayed in an overlay window at user request. Control options that are available for almost any transaction should be treated as implicit options, which need not be included in a list of transaction-specific options, unless they are particularly relevant to the current transaction.

⇒ 4.2.4.5-8 Only control options that are actually available for the current transaction should be offered to users.

If certain options are not yet implemented, as during system development, or are not available for any other reason, they should not be presented as available to users. Options used only in special circumstances (e.g., by systems programmers or maintenance personnel) should not appear on interfaces used during typical operations. Options that are typically used, but are not available (e.g., disabled) in the current context should be distinctively coded (e.g., 'grayed'). For example, a trend plot will typically include controls for expanding or contracting the time scale. When the limit of such adjustment is reached, the corresponding control should change in appearance to indicate that no further expansion or compression of the time scale is possible.

4.2.4.6 Guiding and Assisting Users

Systems typically include various features intended to guide or assist the user. Transactions typically include prompts that alert the user to the need for input and/or suggest the appropriate means or format for providing it. Computer-based guidance/help may be presented automatically (e.g., after an incorrect entry has been detected) or at the user's request.

Online help may be provided in a variety of computer-based formats ranging from online manuals to brief messages. In some systems, the guidance information appears in a display page that completely replaces the existing task display. Window-based systems can present guidance information within the same display screen as the task display, allowing the task and the guidance to be viewed simultaneously. The presentation of this guidance may be initiated by the user or the system. The user may actively access guidance (e.g., by entering a help command or opening an online guidance document). The guidance system may retrieve a help document, issue a message, or prompt the user to take a particular action.

General guidelines for designing user assistance features are given in Section 4.2.4.6.1. Guidelines for specific types of user assistance are given in later subsections.

4.2.4.6.1 General

⇒ 4.2.4.6.1-1 System messages should appear in standard locations.

Messages may be provided in window overlays.

⇒ 4.2.4.6.1-2 Consistent grammatical construction should be used in system messages.

⇒ 4.2.4.6.1-3 System messages should use familiar terminology.

For example, "Data requires special access code; call Data Base Admin, X 9999 for access" is preferable to "IMS/VS DBMS private data; see OP-DBSA-0/99-99."

⇒ 4.2.4.6.1-4 System messages should be concise and clearly worded.

⇒ 4.2.4.6.1-5 Wording for system messages should be directed at the user.

For example, “Press ENTER to continue” is preferable to “The operator should press ENTER to continue.”

⇒ 4.2.4.6.1-6 No extraneous information should be displayed.

Only relevant data to a task or operation should be displayed.

⇒ 4.2.4.6.1-7 Presenting the system as a person should be avoided.

System messages such as, “I AM LOADING YOUR FILE NOW. I’LL TELL YOU WHEN I’M DONE” should not be used.

⇒ 4.2.4.6.1-8 Experienced users should be able to define when and how guidance will be provided by automated guidance/help systems.

The type and degree of guidance needed from guidance/help systems varies with the level of expertise of the user. Less experienced users of the HSI should be provided with only limited options for controlling the presentation of guidance/help. Regardless of the user’s level of experience, it should not be possible to ‘turn off’ guidance/help functions.

⇒ 4.2.4.6.1-9 The content of help information should be oriented toward users’ completion of their tasks; i.e., the information should be procedural.

⇒ 4.2.4.6.1-10 The display of online help should not obscure important information.

Online help systems that are window-based can be beneficial because they present help information directly on the task display, allowing users to glance between the help and the task rather than referring to a separate manual or display. However, if multiple windows are already open, the presence of an additional help window may obscure important information.

⇒ 4.2.4.6.1-11 Online help should accommodate users’ differing levels of expertise and preferred interaction styles.

Users may vary in their proficiency and preferences in using some interface management techniques.

⇒ 4.2.4.6.1-12 Users should be able to request guidance information regarding requirements for information or command entry (e.g., syntax, parameters, and options).

⇒ 4.2.4.6.1-13 Users should be provided with whatever information may be needed to guide command entries at any point in a sequence of transactions, by incorporating prompts in a display and/or by providing prompts in response to requests for HELP.

4.2.4.6.2 Prompts

These are cues the computer system gives the user that suggest the type of response that the user should provide. Prompts can support users in selecting the proper operation for an interface management task.

⇒ 4.2.4.6.2-1 Users should be provided with clear and specific information to guide entries during logon/logoff or command or information entry.

Prompts may be incorporated in a display and/or provided in response to requests for HELP. Where six or fewer control options exist, they should be listed. Where more input options exist, an example of the type of entry that is required should be presented. If a default value has been defined for null entry, that value should be included in the prompting information.

⇒ 4.2.4.6.2-2 When a user must specify the address for a message, prompting should be provided.

Prompting might consist of a series of questions to be answered, an address form to be completed by the user, or reminders of command entries required.

⇒ 4.2.4.6.2-3 Standard symbols should be used for input prompting.

The symbol(s) chosen should be reserved for that use. For example, a colon is often used to distinguish an input prompt from a label.

⇒ 4.2.4.6.2-4 When a command entry is not recognized or is inappropriate, users should be prompted to correct, rather than re-enter the command.

A faulty command should be able to be retained in the command entry area of the display, with the cursor automatically positioned at the incorrect item, with an advisory message describing the problem. It should be possible for the user to correct individual errors without affecting adjacent valid entries.

⇒ 4.2.4.6.2-5 Cues should be provided to indicate the size of a fixed-length data entry field.

Underscoring gives a direct visual cue as to the number of characters to be entered, and the user does not have to count them. For example, “Enter ID: _____________________” is preferable to “Enter ID (9 characters).”

⇒ 4.2.4.6.2-6 Additional cuing of data format should be included in a field label when that seems helpful.

For example, “DATE (MM/DD/YYYY) : __ __/__ __/__ __ __ __.”

⇒ 4.2.4.6.2-7 Users should be able to request computer generated prompts to determine required parameters or available options for a command.

Using a HELP function key, or perhaps simply keying a question mark in the command entry area, are satisfactory methods to request prompting.

⇒ 4.2.4.6.2-8 Prompting should be provided for required formats and acceptable values for data entries.

⇒ 4.2.4.6.2-9 Graphic means may be provided for displaying prompting aids and other guidance pertaining to current control actions.

For example, a guidance display providing a graphic representation of keypad layout with notes explaining the various key functions can help a user to learn the control options available via function keys.

4.2.4.6.3 Advisory Messages

These are messages from the computer system indicating conditions that may require the user's attention.

⇒ 4.2.4.6.3-1 Advisory Messages should be Distinctive

The salience of the message presentation should be appropriate to its content. For example, messages regarding potential data loss might be marked with a blinking symbol and/or displayed in red, and be accompanied by a distinct auditory signal (see next). Error messages might be marked with a different special symbol and/or displayed in yellow.

⇒ 4.2.4.6.3-2 Information requiring prompt attention should be presented through both visual and auditory means.

For example, if a user attempted to change the scale of a parameter plot but entered a scale value that was beyond the allowable range, the visual indication that the change had not been accomplished (perhaps a message) might be accompanied by a brief tone; this would prevent the user from misinterpreting the displayed information based on the assumption that the attempted change had been made. Note that the audio signals referred to here call attention to information about the interface; detailed guidance on alarms, which alert users to important information about plant processes, is in Section 4.4.

⇒ 4.2.4.6.3-3 Protection against data loss should be provided.

During logoff, the system should check pending transactions to determine if data loss seems probable. If so, the computer should prompt for confirmation before the logoff command is executed.

⇒ 4.2.4.6.3-4 Users should be informed when a command will be time-consuming to process.

Typical response times for various types of commands are given in Section 4.2.5.5. Advisory messages may be provided when response time will exceed the maximum amounts given.

4.2.4.6.4 Error Messages

These are messages from the computer system to the user indicating that an error or potential error has been made.

⇒ 4.2.4.6.4-1 When the computer detects an entry error, an error message should be displayed stating the error and possible subsequent operations.

Error messages should explicitly provide as much diagnostic information and remedial direction as can be inferred reliably from the error condition. Where clear inference is not possible, probable helpful inference(s) may be offered. For example, “Code format not recognized; enter two letters, then three digits” is preferable to “Invalid input.” Users should not have to search through reference information to translate error messages.

⇒ 4.2.4.6.4-2 Error messages should be clearly worded, informative, and appropriate to the task.

Messages should

- describe the error and available remedies in language that reflects the user’s point of view, not the programmer’s
- use neutral wording, i.e., they should not imply blame, personalize the computer, or attempt to make a message humorous.

⇒ 4.2.4.6.4-3 The computer should display an error message only after completion of an entry.

An error message should not be generated as wrong data are keyed, but only after an explicit ENTER action has been taken.

⇒ 4.2.4.6.4-4 Where an entry is invalid or inoperative at the time of selection, no action should result except a display of an advisory message indicating the error and the appropriate functions, options, or commands.

For example, no action should occur when attempting to print a document from within an edit mode.

⇒ 4.2.4.6.4-5 Error messages should facilitate correction of the error.

Users’ are better able to handle errors if

- the erroneous entry remains displayed until the error has been corrected
- the location of a detected error is marked by positioning the cursor at that point on the display, i.e., at that data field or command word

- error messages indicate the correct alternatives
- error messages are removed after the error has been corrected

⇒ 4.2.4.6.4-6 The means of notifying users of errors should remain effective when there are multiple errors.

The user may not be aware that there are multiple errors if there is no distinctive change in the display. To ensure that users are aware of multiple errors

- notification should be made for each error when multiple errors are detected.
- if a user repeats the same error, a noticeable change should exist in the displayed error message, e.g., the system might display the same verbal message but with a changing label.

⇒ 4.2.4.6.4-7 If an error is detected in a group of entries, the system should process correct commands until the error is displayed.

⇒ 4.2.4.6.4-8 Following the output of a simple error message, users should be able to request a more detailed explanation of the error.

A more complete discussion of each error should be made available on-line. As a supplement to on line guidance, system documentation should include a listing and explanation of all error messages

The user should be made aware of the detection of multiple entries in order to facilitate corrections. For example, “DATE should be numeric [+ 2 other errors].” The computer should place the cursor in the data field referred to by the displayed error message, with other error fields highlighted. There should also be means to request sequential display of the other error messages.

⇒ 4.2.4.6.4-9 Error messages should be presented at the point of the error or in a consistent area of the display.

4.2.4.6.5 Validating User Input

These are capabilities that check the user’s inputs, according to defined software logic, and indicate that it is acceptable to the computer system. Users are often able to notice and correct errors given the opportunity to do so. If invalid input is submitted, the system should trap the error before further processing is attempted. For example, a validating capability may inform the user that a command or query is improperly formatted.

⇒ 4.2.4.6.5-1 Displays and transactions associated with information entry should be designed so that users can review and confirm entries before they are processed by the system.

The following characteristics can make user confirmation more effective:

- Data being entered through a keyboard should be echoed on the screen on a stroke-by-stroke basis, except when applied to passwords or other security measures.
- When verification of prior data entries is required, users should be allowed to review and confirm the data, rather than re-entering the data.
- Currently operative default values should be displayed during data entry; acceptance of default values should not require re-entry of values.
- The user should be able to obtain a paper copy (i.e., a printout) of the contents of alphanumeric or graphic displays.

⇒ 4.2.4.6.5-2 The system should validate any item whose entry and/or correct format or content is required for subsequent data processing.

The validation process should

- be automatic, i.e., not require user the user to initiate it
- be completed before another transaction can begin
- check for correct format, legal value, or range of values
- cross-check related entries to ensure that the data set is logically consistent

⇒ 4.2.4.6.5-3 In a repetitive data entry task, the data for each transaction should be validated as it is completed, and the user should be allowed to correct errors before beginning another transaction.

This is particularly important when the task requires transcription from source documents, so that a user can detect and correct entry errors while the relevant document is still at hand.

⇒ 4.2.4.6.5-4 Optional item-by-item data validation within a multiple-entry transaction should be provided.

This capability, which might be termed an “interim ENTER,” may sometimes help a novice user who is uncertain about the requirements imposed on each data item.

⇒ 4.2.4.6.5-5 Validation features should accommodate deferred entries

Validation should not interfere with the users’ control of the interaction by forcing entry of data in a predetermined sequence. For example:

- The user should be able to enter a special symbol in the data field to indicate that the item has been temporarily omitted rather than ignored.
- When the requests require processing of entries, the presence of deferred items should be signaled to the user, and immediate entry (or perhaps further deferral) of missing items should be allowed.

⇒ 4.2.4.6.5-6 If data validation detects a probable error, an error message should be displayed to the user at the completion of data entry.

Error messages returned by validation processing should

- not interrupt an ongoing transaction
- be specific as to the discrepancies detected

For example, during reactivity control, the following type message may be displayed: "A negative value has been entered in the field 'Control Rods'. Enter a positive number between 1 and 32."

⇒ 4.2.4.6.5-7 When a data or command entry error is suspected but cannot be determined (in terms of system error logic), a cautionary message asking for confirmation should be displayed.

The user should be alerted to entries that may be in error. For example, "Cooldown rate of 200 degrees per hour is outside the normal range; confirm or change entry."

4.2.4.6.6 Correcting Information/Command Entries

These are capabilities that, after checking data or command inputs entered by the user, either automatically put them in the correct form or supply corrections that the user can either accept or reject.

⇒ 4.2.4.6.6-1 All error corrections by the user should be acknowledged by the system, either by indicating a correct entry has been made or by another error message.

⇒ 4.2.4.6.6-2 Any user action should be immediately reversible by an UNDO command.

UNDO itself should be reversible (e.g., by means of a REDO command). Even with an UNDO capability, however, a user may make an irretrievable mistake, if succeeding actions intervene before a prior destructive action is noticed. If a user is too hasty in confirming a destructive action, and realizes the mistake right away (i.e., before taking another action), then an UNDO action should be available to reverse the potential damage.

⇒ 4.2.4.6.6-3 For all inputs, whether data entries or commands, users should be allowed to edit composed material before requesting computer processing.

Input editing will allow users to correct many errors before computer processing. When an error is detected, a user will be able to fix it by editing, i.e., without having to retype any correct items (which might introduce further errors).

⇒ 4.2.4.6.6-4 When the system detects an error in a user input, the user should be allowed to make an immediate correction.

It is helpful to correct data entry errors at the source, i.e., while a user still has the entry in mind and/or source documents at hand. When a user cannot correct an entry, as when transcribing from a source document that itself contains an error, it may help to allow the user to defer entry of the wrong item. Alternatively, the user might wish to cancel the transaction.

⇒ 4.2.4.6.6-5 Following error detection, users should be allowed to edit entries by rekeying only those portions that were in error.

If a user must re-enter an entire data set to correct one wrong item, new errors may be made in previously correct items.

⇒ 4.2.4.6.6-6 Users should be required to take an explicit ENTER action for computer processing of error corrections.

The action taken to accomplish corrections should be the same action that was taken to enter the data originally.

⇒ 4.2.4.6.6-7 When inappropriate or unrecognized commands are detected, a list should be provided to the user showing permissible commands, anticipating the command intended.

⇒ 4.2.4.6.6-8 Users should be allowed to BACKUP easily to previous steps in a transaction sequence in order to correct an error or make any other desired change.

For example, a user might wish to BACKUP through the defined sequence of a question-and-answer dialogue in order to change a previous answer.

⇒ 4.2.4.6.6-9 If an error is detected in a stacked series of command entries, the computer should either consistently execute to the point of error, or else consistently require users to correct errors before executing any command.

In most applications, partial execution will probably prove desirable. The point here is that an interface design decision should be made and then followed consistently.

⇒ 4.2.4.6.6-10 If only a portion of a stacked command can be executed, the user should be notified and provided appropriate guidance to permit correction, completion, or cancellation of the stacked command.

Note that stacked commands can fail because of error in their composition, or for other reasons such as unavailability of required data.

⇒ 4.2.4.6.6-11 If a user makes a command entry error, after the error message has been displayed, the user should be allowed to enter a new command.

A user should not be forced to correct and complete an erroneous command. In considering a command entry error message, a user may decide that the wrong command was chosen in the first place, and wish to substitute another command instead.

⇒ 4.2.4.6.6-12 If a command entry is not recognized, the user should be allowed to revise the command rather than rejecting the command outright.

Misstated commands should not simply be rejected. Instead, software logic should guide users toward proper command formulation. Note that this guidance refers to checking whether an entry is part of the command set, not to the process of validating entries against plausible or permissible values; see Section 4.2.4.6.5.

4.2.4.6.7 User Guidance/Help

⇒ 4.2.4.6.7-1 Reference material describing system capabilities, procedures, and commands and abbreviations should be available and easily accessed on-line.

Features that facilitate users' access to help information include:

- ability to access on-line user guidance by means of a simple action that is consistent throughout the interface
- advisory messages or prompts to guide users to help resources
- an on-line HELP index
- ability to browse on-line HELP
- help based on task context
- acceptance of synonyms and abbreviations in help requests
- easy return to the task after accessing HELP

Explicit actions should be required to access or suppress user guidance.

⇒ 4.2.4.6.7-2 When a user requests HELP on a topic, the computer should accept synonyms and abbreviations.

⇒ 4.2.4.6.7-3 The information presented in response to a HELP request should be tailored to the task context.

If an error in command entry is made, HELP should display information concerning that command, its function, its proper structure and wording, and required and optional parameters.

⇒ 4.2.4.6.7-4 When a request for HELP is ambiguous in context, the computer should initiate a dialogue to specify what data, message, or command requires explanation.

In order to define the needed information, the user might be allowed to point, or position a special symbol, such as a question mark, at a displayed item about which HELP then would be provided.

⇒ 4.2.4.6.7-5 When a HELP display provides summary information, more detailed explanations should be available.

⇒ 4.2.4.6.7-6 A complete hardcopy set of computer system operating procedures and contingency procedures should be available in the control room.

Operating procedures should describe the overall computer system, the components with which the user can interface, and the specific procedures necessary to accomplish all of the user-computer interface functions. Contingency procedures should describe indications available to the user that identify failure or malfunctioning of the computer system and necessary actions to be performed by the user if the computer fails or malfunctions.

⇒ 4.2.4.6.7-7 Procedures should be prepared from the point of view of the user.

The organization, content, and wording of procedures should reflect the users' conceptualization of the system, their training, and their experience.

⇒ 4.2.4.6.7-8 Cross-indices of the available data displays should be available in the control room in hardcopy form.

The specific codes, or addresses, by which data displays can be called up by a user should be cross-indexed by alphanumeric or numeric code, program name, system/subsystem identification, and functional group identification.

4.2.4.7 Allowing Flexibility

Flexibility is built into most interfaces to enable users to tailor their HSIs to meet current task demands and to adjust them to their personal preferences. For example, user needs are typically different for different levels of expertise. Users who have limited exposure to the advanced capabilities of computer-based HSI components may require a high degree of support for interface management actions, such as through the use of menu-based systems and computer-based help features. Users who are highly proficient in the use of the HSI may require features that limit the number of steps required to complete an action, such as via a command-based interface rather than a menu-based interface.

User performance may be impaired by an excessive number of flexibility features or inadequately designed flexibility features that create demands that compete with primary tasks. Inadequately designed flexibility features can also expose the user to HSI configurations that violate human factors engineering principles and may increase the likelihood of errors and poorer task performance. Table 4-10 lists some uses of HSI flexibility that may enhance performance.

The flexible user interface features provided should be the result of careful analyses of user requirements; they should address the need to optimize performance under specific conditions. They should not be a substitute for analyses of user requirements. Flexibility should be constrained so that working with the system does not become a complex decision-making task. Flexibility without proper analysis can expose the user to configurations that may impair performance, such as by increasing the likelihood of errors or delays.

⇒ 4.2.4.7-1 Flexible HSI features should be provided when they provide specific benefits to user tasks and their use does not impair user performance.

For example, the capability for users to add annotations to displayed information might be provided.

⇒ 4.2.4.7-2 Users should not have to use flexible interface features to support tasks and circumstances that could have been anticipated and designed for.

⇒ 4.2.4.7-3 The system should be sufficiently flexible to enable users to respond to unanticipated situations or where personal preference can positively impact performance.

Table 4-10
Users of HSI Flexibility

Reduce the Cost of Accessing Information – Flexible HSI capabilities can reduce the attention and effort required for accessing information. The flexibility of computer-based technologies can enhance operator performance by allowing the HSI to provide the right information for the operator's current work methods and work objectives, while removing unneeded information that may become a nuisance. Examples include: automated information retrieval features; programmable function keys for accessing particular displays; capabilities for organizing information (i.e., display window management, spatial arrangement of icons); and capabilities for introducing labels, markers, or landmarks to support operators in locating information in displays that require visual scanning.

Reduce the Cost of Processing and Integrating Information – Flexible HSI capabilities can support operators in mentally processing and integrating information presented by the HSI. Examples of HSI features for arranging the spatial proximity of information to aid mental integration include: the physical movement of display devices, the movement of display pages to particular display devices, and the movement of display pages within display windows. Examples of HSI features for supporting users interpreting information include reconfigurable displays, such as graphical plots in which an operator may plot one variable as a function of another or as a function of time, and features that perform calculations requested by the operator.

Reduce the Cost of Executing Control Actions – Flexible HSI capabilities can reduce the effort and attention required for executing control actions. Examples include HSI features that allow particular control actions to be executed automatically. Other examples include: "escape mechanisms" features, which allow to the operator to promptly terminate and exit complicated human-system interactions, and "workarounds," which allow the user to override automatic responses that may not be beneficial for a particular task.

Enhance Signals – This capability increases the salience of an indication or piece of information to support detection by operators. These changes in salience effectively increase the signal-to-noise ratio for specific information.

Reduce Noise – This capability reduces or removes "noise" from the information environment to support the operator in detecting relevant information. This removal or reduction of noise effectively increases the signal-to-noise ratio for other information that may be more important. Noise may include indications of plant or system changes that do not provide information that is useful to the operator's current tasks.

Document a Baseline or Trend – This capability allows the operator to create a reference for monitoring so that changes can be easily identified without relying upon the operator's memory of the previous state. Examples include capabilities for documenting initial conditions or for establishing a trend over a period of time for comparison at some later time.

Create External Reminders – This capability allows the operator to create reminders for activities involved in monitoring or control execution. Reminders for monitoring activities may identify particular variables requiring close attention. Reminders for control actions may remind operators of special conditions important when carrying-out control actions. For example, operators may create reminders regarding unusual control configurations that should not be changed or to draw attention to unusual indications that are already being addressed in other ways. These reminders may be created through manipulations of the appearance of the HSI component or through the creation of messages.

Users should be able to develop novel information displays for unusual circumstances. However, such displays should not reduce the predictability or consistency of the interface, e.g., by replacing or altering predesigned displays (see below).

⇒ 4.2.4.7-4 Users' flexibility in configuring the interface should not be unlimited.

For example,

- The options provided for configuring the interface should be well defined.
- Users should not be able to make changes to the interface's basic graphical elements and text or to characteristics specifically designed to convey important information (e.g., coding schemes).
- Users should not be able to delete or alter annotations of modifications entered by other users

⇒ 4.2.4.7-5 Displays that can be modified by users should provide a means for the user to rapidly return the display to its default configuration.

⇒ 4.2.4.7-6 The design of flexible HSI features should provide capabilities that are consistent with the levels of expertise of the users.

⇒ 4.2.4.7-7 When information or command entry requirements may change, some means for the user (or a system administrator) to make necessary changes to available functions should be provided.

Entry functions that may need to be changed include the types of dialogue that are provided, procedures for transaction selection and interrupt, methods for context definition and error management, and alarm control.

4.2.5 Interface Management Functions

4.2.5.1 Entry of Commands and Information

User input formats are the types of dialogues through which users interact with the system. A variety of input formats can be used for user-interface interaction and management tasks. The selection of dialogue types should be based on anticipated task requirements, user skills, and anticipated system response time. Dialogue types are related to task requirements in Table 4-11. Guidance for designing specific input formats is given in the sections to follow.

4.2.5.1.1 Command Language

Commands are instructions, entered by users via a keyboard or similar keyed device, that request the computer system to perform specific operations. In a command language dialogue, the user interacts with the computer by entering commands, possibly with minimal prompting from the system. An important aspect of command language interfaces is that users usually must supply the appropriate commands rather than, e.g., choosing them from lists or pointing at an icon.

Table 4-11
Dialogue Formats for Representative User Tasks

Task/System/User Characteristics	Command Language	Menus	Function Keys	Macros and Progr. Keys	Forms	Direct Manipulation	Natural/Query Language	Question/ Answer	Speech
Arbitrary entry sequences	X					X			
Reduce hands-on control									X
Unpredictable retrieval							X		X
Wide range of control entries	X								
Frequent control/ transactions			X	X					
Small command set		X	X						
Complex control				X	X	X			
Large command set		X		X					
Routine data entry								X	
Entry order constrained								X	
Data entry flexibility needed					X				
Little arbitrary data input		X				X			
Slow computer response time					X				
Fast computer response time		X				X		X	
Highly trained users	X								
Moderately trained users				X	X		X		
Little training		X				X		X	X

Commands used for user-interface interaction and management may be categorized as action and destination commands. Action commands include instructions for specific computer operations such as manipulating information pertaining to interface management and navigating display systems. Some action commands for navigation include Previous/Next Display and Zoom In/Zoom Out; they allow users to move through an information structure in steps. Destination commands include codes for identifying and retrieving specific displays; they allow users to move directly from one location in the display network to another without accessing intervening locations (similar to navigation paths in hypertext systems). The number of destination commands may be high for a display system that contains a large number of selectable display pages.

⇒ 4.2.5.1.1-1 The system should be designed to help users learn and remember the commands.

Some means of doing this include:

- providing a general list of basic commands, with appropriate command format guidance, should be available to the user
- allowing users to request computer-generated prompts as necessary to determine required parameters in a command entry, or to determine available options for an appropriate next command
- allowing users to assign names to commands. This capability may support recall, for example, when users must use more than one display system having differently defined commands. By providing some flexibility in renaming the commands, users can enhance the consistency between the dialogues. However, default names should be easily restored because different users may want to assign different names.
- organizing functions in related groups or layers, with the fundamental layer of the language allowing use of the system by people with limited needs; successive layers of the command language can then accommodate more complex requests.
- accompanying guidance information with graphical illustrations of command content and syntax where possible.

⇒ 4.2.5.1.1-2 The interaction should be designed to minimize the effort involved in entering the commands.

Examples of such features include:

- entries not exceeding 7 characters
- requiring users to enter only as many characters as needed to uniquely identify the desired command; for example, if a “P” uniquely identifies a print command (i.e., no other commands start with “P”), then a user should be able to enter PRINT, or PR, or P to initiate printing
- allowing users to define abbreviations for commands

- accepting commands without any punctuation other than the spaces between words; command entry will be faster and more accurate when spaces are used rather than any other kind of punctuation
- treating single and multiple blanks between words as equivalent when processing command entries; people cannot readily distinguish one blank space from several, and so the computer should not impose such a distinction
- if command punctuation other than spaces is required, using a single standard delimiter symbol (such as a slash) for that purpose

⇒ 4.2.5.1.1-3 A command language should be designed to minimize errors, and the system should tolerate types of errors that can be anticipated.

Techniques for achieving this include:

- making commands distinctive from one another, and emphasizing significant differences in function; in general, commands should not have semantically similar names, such as SUM and COUNT, or ERASE and DELETE, or QUIT and EXIT
- insuring that commands and abbreviations have distinctive spelling, so that simple spelling errors will be recognized as such rather than invoking different commands; for example if one command name is DELETE, abbreviated DEL, then another command should not be named DELIVER, with an abbreviation of DELR. Instead, ERASE could be substituted for DELETE, or SEND for DELIVER
- having the system recognize a variety of synonyms for each word defined in the command language; for example, it may be useful, for the system to accept "UP" as well as "RAISE." The synonyms that are likely to be used can be determined by analysis of error records in prototype testing
- when the set of potential command entries is well defined, having the system recognize and correct common misspellings of commands, rather than requiring re-entry; it may be advisable to have the user verify commands recognized in this way, especially if they refer to the process rather than the interface
- allowing users to enter probable alternative forms of command syntax such as using different punctuation and/or listing command modifiers in different orders; for example, the computer might accept alternative methods of specifying a request, such as "SG3 LVL," "LVL SG3," or "LVL/SG3"

4.2.5.1.2 Menus

A menu is a displayed listing of possible options from which a user can choose. Menu interfaces are widely used in many computer-based systems. Because they present the user with a set of options, the user needs to recognize rather than recall the correct one. A wide variety of menu systems exist. Some important characteristics include the types of menus and their structure, the options to be included and their arrangement, and ease of use.

Permanent vs. On-Demand Menus. Menus may be presented on dedicated pages. This typically results in more paging activity (because the application must return the user to the main menu page at every task change). While there are circumstances in which the approach is tolerable (e.g., when users are making infrequent shifts among very different types of activity, so that disruption is minimal), other styles are generally preferred. When entries for any particular transaction will be selected from a small set of options that are accessed frequently, those options can be displayed in a menu added to the working display, rather than requiring a user to remember them or to access a separate menu display. However, if there are more than a few options, little room may be left for display of data. If an extensive menu must be added to a working data display, that menu should be provided as a separate window that can temporarily overlay displayed data at user request, but can then be hidden again by further user action. Similarly, options associated with particular screen objects can be temporarily presented, e.g., by 'right-clicking' the object.

⇒ 4.2.5.1.2-1 User requested menus should be used whenever possible; the use of permanent menus should be minimized.

⇒ 4.2.5.1.2-2 If menu options are included in a display that is intended also for data review and/or data entry, the menu options should be distinct from other displayed information.

Menu options should be located consistently in the display and incorporate some consistent distinguishing feature to indicate their special function, perhaps beginning with a special symbol such as a plus sign (+NEXT or +BACK). "Embedded menus," in which various items within a working display are highlighted in some way to indicate that they can be selected to obtain further information, may also be used.

⇒ 4.2.5.1.2-3 When permanent menus are used, there should be one standard design for the input prompt that is used across all tasks.

Increasingly, menu selection is done by means of pointing rather than keyed entry. When choices are made via keyed entry, it is important to include a consistent prompt that unambiguously indicates the need for user input. For example, "ENTER CHOICE: __."

Choosing which options to display in menus. Not all options will be available or appropriate in every context; this has implications for designing menus. The designer might decide to show only those options that are appropriate at a given time (thus making selection of an inappropriate option impossible), but the resulting menus would not be consistent from one transaction to the next. This interferes with learning of the locations of options on the menus and can increase option selection time. On the other hand, all options could be shown all the time; however if a user selects a displayed option, and is then told that option is not actually available, an undesirable element of unpredictability has been introduced into the interface design. A third (more typical) approach is to show all options but use a code (usually a lower-contrast presentation) to designate those that are irrelevant or unavailable. This works well for menus that contain a limited number of actions that apply to large numbers of pages.

When the options are not actions but destinations in a large display network, there may be a very large number of options, but only a few that are relevant to a particular location in the network (e.g., the number of parent and descendant nodes that can be accessed from a given node is small compared to the total number of nodes in the network). In this case it would seem practical to present only the relevant options.

⇒ 4.2.5.1.2-4 A menu should be designed to display all options appropriate to any particular transaction.

A familiar set of general control options (i.e., options that are always implicitly available) may be omitted from individual displays. Such general options might be selected by requesting a general menu, or perhaps by function key or command entry. For example, if a function key allows users to produce a paper copy of any screen, the PRINT option, though implicitly available, might not necessarily be shown on every screen.

⇒ 4.2.5.1.2-5 Menus should display as selectable only those options that are actually available in the current context.

The contents of menus (i.e., items and their ordering) can remain consistent in different contexts if the current availability of each of the options is clearly indicated. If non-available options are displayed, they should be visually distinct from the options that are available. For example, options that are temporarily unavailable may be coded (e.g., presented in gray) to indicate their status.

⇒ 4.2.5.1.2-6 Menus should be designed so that the function of the menu is evident to the user.

⇒ 4.2.5.1.2-7 When equivalent keyboard commands are provided, they should be displayed as part of the menu option label.

⇒ 4.2.5.1.2-8 If one option on a menu is selected more often than the others, then it should be highlighted.

Search and selection is enhanced by highlighting and preselecting the default option.
For example, the cursor may be automatically positioned over the default option, or the text string for the default option may automatically appear in the input field.

⇒ 4.2.5.1.2-9 Where discrimination among options may be difficult for users, menus can provide a preview of options.

This will support the user in determining which of the current options should be selected.

Minimizing the number of actions required. Menu dialogues eliminate the need to type commands and can reduce or prevent inappropriate entries. The cost to the user is the interaction with the menu itself; thus menus should be designed to reduce to the extent possible the number of actions the user is forced to take in order to have commands executed (e.g., by providing shortcuts for frequent tasks or by facilitating movement through hierarchical menu structures).

⇒ 4.2.5.1.2-10 Options that are critical or frequently chosen should be quickly accessible using as few steps as possible.

Immediate access may be provided through such approaches as dedicated buttons and placing the option on multiple menus.

⇒ 4.2.5.1.2-11 Users should be able to select a menu or submenu directly, without going through intermediate selection steps.

One method for avoiding intermediate selection steps is to allow users to select nodes directly from a representation of the menu structure. That is, rather than navigating down the through multiple levels of the display hierarchy, the user might be given the option of pointing at the needed display on a map or tree diagram of the display system.

⇒ 4.2.5.1.2-12 Users should have to take only one simple action to return to the next higher level in hierarchic menus.

This action could be considered analogous to the BACK option.

⇒ 4.2.5.1.2-13 Users should have to take only one simple action to return to the general menu at the top level in hierarchic menus.

The user should not have to backtrack to return to the starting level in a hierarchical menu system. This capability can be provided by dedicating a program function key, touch field, or a cursor entry field to display the main menu. This action could be considered analogous to the REVIEW option.

⇒ 4.2.5.1.2-14 When menu selection is accomplished by code entry, users should be able to combine a series of selections into a single "stacked" entry.

If necessary, stacked sequential entries might be separated by some character, such as a space, slash, comma, or semicolon. It would be preferable, however, if they were simply strung together without special punctuation. Computer interpretation of an unpunctuated string will require letter codes (by preference) or fixed-digit number codes for option selection.

⇒ 4.2.5.1.2-15 Experienced users should be able to bypass a series of menu selections and make an equivalent command entry directly.

In effect, a command entry might specify an option anywhere in a hierarchic menu structure, permitting a user to jump down several levels, or to move directly from one branch to another. If a command bypasses only a portion of the complete menu sequence, and so does not yet specify a complete control entry, then the appropriate next menu should be displayed to guide completion of the control entry.

⇒ 4.2.5.1.2-16 When a menu is first displayed, the cursor should be positioned so that it may be readily located and used.

Cursor positioning can reduce unnecessary visual search and cursor movement. If the cursor appears within the menu, then the cursor should be placed beside the option with the highest probability of selection. If the options are about equally likely, then the cursor should be placed beside the first option.

⇒ 4.2.5.1.2-17 A menu macro capability should be provided if it produces faster access.

A menu macro capability allows a navigation path to be recorded. The path can then be executed by the user through a command. This capability can reduce the number of navigation steps, compared to accessing a series of menus in sequence. It may provide faster access to information for experienced users.

⇒ 4.2.5.1.2-18 Multiple navigation paths should be provided to items in the display system.

Multiple navigation paths should accommodate a range of user experience in navigating the display system. Highly experienced users should be allowed to use shortcuts, such as ‘type-ahead’ or ‘jump-ahead’ to reduce the number of interface management actions required to navigate through the display selection system.

⇒ 4.2.5.1.2-19 A visual representation of the menu structure should be provided.

Where space allows, some aspects of the menu structure should be presented visually so the user is not required to remember it. That is, information should be provided in the user interface to augment or substitute for the user’s knowledge of the display navigation structure.

Arrangement of Menu Options. Menus will be more effective if their organization is immediately apparent to the user. Options may be grouped based on conceptual relationships among them, ordered according the sequence in which they are typically used. If no logical basis is available, then the options should be displayed in order of their expected frequency of use, with the most frequent listed first. When applicable, a menu should indicate logically related groups of options, rather than an undifferentiated string of alternatives. For example, in vertical listing of options, subordinate categories might be indented. Logical grouping of menu options will help users learn system capabilities. When logical grouping requires a trade-off against expected frequency of use, that trade-off should be resolved consistently for those functions throughout the menu structure.

One of the strengths of menu dialogues is that the user is shown the available options; they may be less effective when the list of options is large. Scrolling in menus should be avoided. Displaying options in several columns may be used where shortage of display space dictates a compact format. However, it is often preferable to use hierarchic menus, where a high-level menu might be shown in the left column of a display, accompanied by a lower-level menu in the right column whose options change to reflect whatever selection is currently made from the high-level menu. A single column format will aid scanning, especially for novice users.

⇒ 4.2.5.1.2-20 Menu options should be ordered and grouped logically.

⇒ 4.2.5.1.2-21 Where ordering cannot be determined by the above, alphabetic ordering should be used.

⇒ 4.2.5.1.2-22 The order of options on menus should be fixed.

The order of options on a menu should not change automatically, such as based on their frequency of use.

⇒ 4.2.5.1.2-23 If meaningful categories cannot be developed for menu options then visual groups should be created for long menus.

Non-categorized menus may be divided into arbitrary visual groupings through the use of space or lines. The groups should be as equal in size as possible. Each group should consist of four to seven options. The use of visual grouping can facilitate visual search.

⇒ 4.2.5.1.2-24 All menu items should be visible to the user without scrolling.

This guideline applies to permanent menus as well as pop-up or pull-down menus and menu bars. The number of categories listed on the menu bar should not exceed the length of the bar.

⇒ 4.2.5.1.2-25 When multiple menu options are displayed in a list, each option should be displayed on a new line, i.e., format the list as a single column.

⇒ 4.2.5.1.2-26 When menu selection must be made from a long list, and not all options can be displayed at once, a hierarchic sequence of menu selections should be provided rather than one long multipage menu.

Under certain circumstances, it might be reasonable for the user to be required to scan multiple display pages to find a particular item. Even in such cases, however, an imposed structure for sequential access may prove more efficient, as when a user can make preliminary letter choices to access a long alphabetic list.

Design of Hierarchical Menus. Two important aspects of the menu structure are breadth and depth. Menu breadth refers to the number of options on a particular panel. Depth refers to the number of levels in the structure. (As an extreme example, a very shallow structure would include all options on a single level; i.e., all options can be accessed from a single menu panel. At the other extreme, a very deep menu structure would assign each option to a different level; i.e., each option would lead to only one other option.) When designing hierarchical menus, the need to limit their breadth and depth (in order to make navigating them manageable) will trade off against the need to represent large numbers of options that are organized in ways that make sense to the users. The usability of hierarchical menus with many options can be enhanced by having the menus at higher levels remain visible as subsequent selections are made.

⇒ 4.2.5.1.2-27 Menus should have a limited number of items in breadth and in depth.

It is recommended that each menu option list should have between 4 and 8 options. Menus with only two options should be avoided. “Menus” with only one item should not be used. In general, broad and shallow menu structures, rather than narrow and deep menu structures should be used. (Examples of a broad, shallow menu structure and narrow, deep menu structure are provided in Figure 4-25.) Other things being equal, users will find very deep menu structures more difficult to navigate than broad ones. However, providing a large number of menu choices midway in a hierarchical structure should be avoided, since users are more likely to get lost in the middle levels of a menu structure.

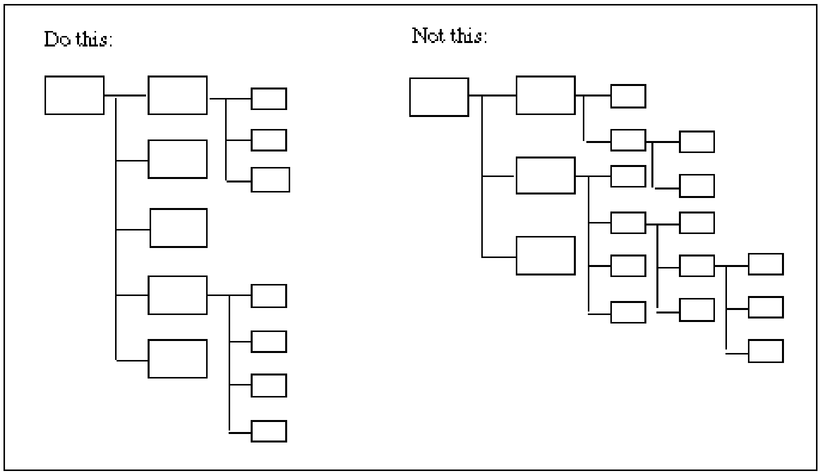


Figure 4-25
Examples of Broad and Shallow Menu Structures

⇒ 4.2.5.1.2-28 If menu options are grouped in logical subunits, each group should have a descriptive label that is distinctive in format from the option labels themselves.

Although this practice uses valuable display space, it will help provide user guidance. Moreover, careful selection of group labels may serve to reduce the number of words needed for individual option labels.

⇒ 4.2.5.1.2-29 If menu options are grouped in logical subunits, the same color should be used for menus within the same group.

⇒ 4.2.5.1.2-30 The display format and selection logic of hierarchic menus should be consistent at every level.

⇒ 4.2.5.1.2-31 Hierarchic menus should be organized and labeled to guide users within the hierarchic structure.

Users will learn menus more quickly if a map of the menu structure is provided as HELP.

⇒ 4.2.5.1.2-32 Users should be able to access a visual representation of their paths through a hierarchy of menus.

How the user's path through the menus is visually represented will depend on the type of menu. For example, if a user progresses through a series of permanent menus, an icon showing the previous menus and current menus, as well as menu selections, might be displayed. If a user progresses through a series of pull down menus, the previous menus might remain displayed with the selected item highlighted, and the association between that item and the subsequent menu would be represented by a close spatial relation (e.g., each successive menu might be displayed immediately alongside the previous one, with its top border vertically aligned with the selected option).

⇒ 4.2.5.1.2-33 When users must step through a sequence of menus to make a selection, the hierarchic menu structure should be designed to minimize the number of steps required.

This represents a trade-off against the need for logical grouping in hierarchic menus. The number of hierarchic levels should be minimized, but not at the expense of display crowding.

⇒ 4.2.5.1.2-34 When hierarchic menus are used, the user should have some indication of current position in the menu structure.

One possible approach would be to show prior (higher) menu selections on the display. If routine display of path information seems to clutter menu formats, then a map of the menu structure might be provided at user request as a HELP display.

⇒ 4.2.5.1.2-35 If hierarchical branching is used, each subordinate menu should be visually distinct from each previous superordinate menu.

Examples include the display of level numbers and a graphical stacking effect. Successful user operations depend on knowledge of context. Users will be better able to navigate the hierarchy if they know the levels from which the current display menu came and how far down in the hierarchy the current menu is.

⇒ 4.2.5.1.2-36 The display of hierarchic menus should be formatted so that options that actually accomplish actions can be distinguished from options that merely branch to other menu frames.

In some applications, it may prove efficient to design "hybrid" menus that display one branch of the menu hierarchy elaborated to include all of its control options, while other branches are simply indicated by summary labels. In such a hybrid menu, it will help orient users if options that accomplish control actions are highlighted in some way to distinguish them from options that will result in display of other frames of the hierarchic menu.

Menu Bars. A menu bar consists of a set of options, usually oriented horizontally at the top of a display area, which is used to initiate actions or, more typically, to invoke pull-down menus. Conventions should govern the organization of the menu bar. For example, on a horizontal menu bar, the categories on the left side of the menu bar might be system functions that apply across all (or most) applications. The categories on the right side of the menu bar might be those that are specific to the currently active application. Within this general spatial layout, both the system-wide and specific categories would be ordered from left (the category containing the most frequently used actions) to right (the category containing the least frequently used).

⇒ 4.2.5.1.2-37 The categories listed across the menu bar should be organized systematically.

⇒ 4.2.5.1.2-38 Category labels on menu bars should be centered in the vertical dimension. Horizontally, category labels on the menu bar should be separated by enough space to be distinguishable as separate items, i.e., by at least two standard character widths.

One standard character width would be required to separate adjacent words in a multiword category. To indicate separate categories, more than one width would be needed.

⇒ 4.2.5.1.2-39 The height of a menu bar should be sufficient to contain standard text characters that serve as menu category labels, as well as space above and below the text characters.

On-Demand Menus (Pull-downs and Pop-ups). Some display systems feature full-page menus, which appear as entire display pages that replace the currently displayed page. More typically, menus are displayed 'over' the page content, which remains mostly visible. The pop-up window appears as a window that overlays the currently presented display page. The pull-down window is displayed when a user chooses an item from a menu bar that extends across one or more borders of the display screen and contains multiple options for selection. The expanding or pop-out menu is a variation of the pull-down menu in which further lower-level options appear after intermediate-level options are selected. For example, when the cursor is positioned over one of the options of the pop-up menu, an additional list of options appears. Individual options of the pop-out menu may have additional pop-out menus.

Among the types of user-requested menus, pull-down menus provide two advantages over pop-up menus: (1) the menu bar serves as a useful mnemonic aid, showing the user the command categories available in the menu; and (2) gaining visual access to the menu items within a category, selecting the item, and removing the menu can be accomplished with a minimal number of actions. The primary advantage of a pop-up menu over a pull-down menu is that, depending on the specific implementations, the user may have immediate access to the menu at the screen location of the selection action. The ideal user-requested menu design would provide the user with a reminder of the menu categories and allow the user to select an item with few actions and little movement of a cursor on the screen.

⇒ 4.2.5.1.2-40 Pull-down and pop-up menus should be activated only by a specific user action that requests the display of the menu.

Menus should not appear simply because the cursor has passed over the menu title.

⇒ 4.2.5.1.2-41 When a pull-down or pop-up menu item(s) has/have been selected, the menu should revert to its hidden state as the selected command is carried out.

⇒ 4.2.5.1.2-42 If menu items are selectable via activation of programmable function keys, the arrangement of the menu list should be compatible with the arrangement of the keys to the greatest degree possible.

⇒ 4.2.5.1.2-43 An explanatory title should be provided for each menu that reflects the nature of the choice to be made.

EXAMPLE: (Good) Organizational Role: r = Responsible, a = Assigned, p = Performing. (Bad) Select: r = Responsible, a = Assigned p = Performing. When instructions to the user accompany a list of options, the instructions should precede presentation of the list.

⇒ 4.2.5.1.2-44 Menus should be displayed in consistent screen locations for all modes, transactions, and sequences.

This applies to pop-up, pull-down, and windowed menus, and to menu bars.

Selection of Menu Options. Menu selections are typically made by pointing with a cursor or by entering codes from a keyboard; function keys and direct pointing (e.g., with a finger or stylus) are also used. Consideration for choosing the means for interacting with menus include

- the style of interaction the user employs for concurrent tasks
- the familiarity of the user with the menu structure and options

General user interaction guidance cautions against forcing users to alternate between different input devices. If a user's tasks are primarily accomplished using a mouse/cursor, menu selection by the same means should be available. If the interaction is mainly via keyboard, the menu selection by means of a cursor controlled by arrow keys or by direct entry of option codes using the keyboard is preferred. The general aim of flexibility would favor providing multiple means for menu selection (e.g., by mouse/cursor and by key entry). If shortcuts were available this would at the same time make the interface accommodate different levels of expertise as well.

⇒ 4.2.5.1.2-45 When menu selection is accomplished by code entry, a standard command entry area (window) should be provided where users enter the selected code.

That entry area should be in a fixed location on all displays. In a customary terminal configuration, where the display is located above the keyboard, command entry should be at the bottom of the display, in order to minimize user head/eye movement between the display and the keyboard. Experienced users might key coded menu selections in a standard area identified only by its consistent location and use. If the system is designed primarily for novice users, however, that entry area should be given an appropriate label, such as "ENTER choice here: ___."

⇒ 4.2.5.1.2-46 Users should not be able to select menu items that are in conflict.

Menu items that are in conflict might be, for example, two different font sizes in a text input task. Users should, however, be able to select multiple menu items that are not in conflict (e.g., a font size and font type in text input). Each menu item selection would be a separate transaction with the system.

⇒ 4.2.5.1.2-47 If menu selection is accomplished by pointing, dual activation should be provided, in which the first action designates the selected option, followed by a separate second action that makes an explicit control entry.

The two actions of cursor placement and entering should be compatible in their design implementation. If the cursor is positioned by keying, then an ENTER key should be used to signal control entry. If the cursor is positioned by light pen, the pen should have a dual-action “trigger” for cursor positioning and control entry. On a touch display, the computer might display a separate ENTER box that can be touched by a user to indicate that the cursor has been properly positioned. This recommendation for dual activation of pointing assumes that accuracy in selection of entries is more important than speed. In some applications, that may not be true.

⇒ 4.2.5.1.2-48 If menu selection is accomplished by pointing, the sensitive area for pointing should be as large as consistently possible, including at least the area of the displayed option label plus a half-character distance around that label.

The larger the effective target area, the easier the pointing action will be, and the less risk of error in selecting a wrong option by mistake.

⇒ 4.2.5.1.2-49 The system should provide feedback as users interact with menus.

For example,

- When a menu item is chosen, the system should display some acknowledgment of that entry (e.g., by highlighting).
- Selection of menu items with “On” and “Off” states should change their state; the “On” state should be indicated by making the item more prominent.
- When multiple options can be selected, menu systems should indicate which options have been selected so far.
- Menu systems should provide feedback indicating when a pointing device has entered the selectable area of an option.
- Menu systems should provide feedback indicating when the selection process is ended.
- Menu items that are available should be highlighted whenever the cursor passes over them.
- As soon as the cursor passes outside the boundaries of the menu item the item should return to its normal state. Unavailable options should not highlight when the cursor passes over them.
- The active menu selection should be indicated to the user.
- More than one method of indication should be used if possible, such as changes in font size and color.

Wording and Coding Menu Options. Labels for menu options should use appropriate and consistent syntax. Wording options as commands will permit logical selection by pointing, facilitate the design of mnemonic codes for keyed entry, and help users learn commands in systems where commands can be used to bypass menus. Furthermore, wording options as commands properly implies that the initiative in command entry lies with the user. Wording options as questions implies initiative by the computer.

When entry is by letter codes, letter codes should also be appropriate and consistent. Meaningful codes are much less error prone than arbitrary ones. For example, L = Left, R = Right is preferable to 1 = Left, 2 = Right. (Numbering of options may be acceptable when a logical order or sequence is implied.). Different codes for the same action will tend to confuse users and impede learning. The same code for different actions will tend to induce user errors, especially if those actions are frequently taken. However, this practice may be tolerable when selections are seldom taken, and then always taken from labeled alternatives. The same action should not be given different names (and hence different codes) at different places in a transaction sequence (e.g., f = Forward and n = Next). The same code should not be given to different actions, e.g., q = Quit and q = Queue.

⇒ 4.2.5.1.2-50 When menus are provided in different displays, they should be designed so that option lists are consistent in wording.

⇒ 4.2.5.1.2-51 Menu options should be consistently worded as commands.

- *The wording of menu options should consistently represent commands to the computer, rather than questions to the user.*
- *If menu selection is used in conjunction with or as an alternative to command language, the wording and organization of displayed menu options should correspond consistently to defined elements and structure of the command language.*

Where appropriate, cumulative sequences of menu selections should be displayed in a command entry area until the user signals entry of a completely composed command.

⇒ 4.2.5.1.2-52 Letter codes used to designate menu options should be meaningful and should be used consistently.

- *If letter codes are used for menu selection, those letters should be consistently used in designating options from one transaction to another.*
- *The code associated with each option should be displayed in a consistent and distinctive manner; e.g., displayed in boldface, followed by a period or dash, separated by a space or tab.*
- *If menu selections are made by keyed codes, each code should be the initial letter or letters of the displayed option label, rather than assigning arbitrary letter or number codes.*
- *Meaningful (as opposed to arbitrary) codes should be used to facilitate learning and reduce errors.*

4.2.5.1.3 Function Keys

Function keys are individual keys on a keyboard or pad that are dedicated to particular predefined operations, such as to call up a predefined display. When a function key is pressed, an instruction is sent to the computer system to perform that operation. An important consideration for function-key dialogues is the relationship between the keying operation and the functions executed. Single keying requires pressing an individual key. Chord keying requires multiple keys to be pressed at once, such as when a function key must be pressed in combination with SHIFT, ALT, or CONTROL key. In addition, a function-key dialogue may have multiple modes, and, in each mode, a particular function key may perform a different operation.

⇒ 4.2.5.1.3-1 Function keys should be provided for interim command entries, i.e., for actions taken before the completion of a transaction.

Function keys will aid such interim actions as DITTO, CONFIRM, and requests for PRINT, or HELP, and also interrupts such as BACKUP and CANCEL. Interim control refers to an action taken by a user while working with displayed data, e.g., while still keying data entries or changes. Function keys will aid interim control entries partly because those entries may be frequent.

⇒ 4.2.5.1.3-2 Each function key should be labeled informatively to designate the function it performs.

Labels should be sufficiently different from one another to prevent user confusion. For example, two keys should not be labeled ON and DN.

⇒ 4.2.5.1.3-3 Function keys should be grouped in distinctive locations on the keyboard to facilitate their learning and use.

Frequently used or important function keys should be placed in the most convenient or prominent locations.

⇒ 4.2.5.1.3-4 A function assigned to a particular key in a given task context should be assigned to the same key in other contexts.

A particular function should be accessed in the same manner in any context in which it is used. For example, the SAVE function should be invoked using the same key whether the user is saving edited information or new information.

⇒ 4.2.5.1.3-5 When a function is continuously available, its function should be assigned to a single key.

⇒ 4.2.5.1.3-6 Frequently used functions should be executed by means of a single key action and should not require chord-keying (e.g., use of the shift key).

⇒ 4.2.5.1.3-7 When a function key performs different functions in different operational modes, equivalent or similar functions should be assigned to the same key.

Functions assigned to a given key in different modes should be related. For example, a particular key might be used to confirm data changes in one mode, and confirm message transmission in another. As a negative example, a key labeled RESET should not be used to save data in one mode, dump data in another, and signal task completion in a third.

⇒ 4.2.5.1.3-8 If chord-keying is used, the functions paired on one key should be logically related.

Functions assigned to a given key should be related. For example, if a particular function key moves the cursor to the upper left corner of a display screen, then that same key when shifted might be used to move the cursor to the bottom right corner of the screen. As a negative example, a function key that moves the cursor should not be used when shifted to delete displayed data.

⇒ 4.2.5.1.3-9 If chord (e.g., control/shift) keying is used, the logical relation between shifted and unshifted functions should be consistent from one key to another.

Consistency in the underlying logic for chord keying will help a user to learn the functions associated with different keys. For example, one consistent logic might be that shifted and unshifted functions are opposite, so that if a particular key moves the cursor forward, then that key, when shifted, would move the cursor backward. Another possible logic might be that shifted and unshifted functions are related by degree, so that if a particular key deletes a single displayed character, then that key, when shifted, would delete a word.

⇒ 4.2.5.1.3-10 If a key is used for more than one function, the function currently available should always be indicated to the user.

If a key is used for just two functions, depending upon defined operational mode, then alternate illuminated labels might be provided on the key to indicate which function is current. In those circumstances, it is preferable that only the currently available function is visible, so that the labels on a group of keys will show what can be done at any point. If key function is specific to a particular transaction, an appropriate guidance message on the user’s display should be provided to indicate the current function.

⇒ 4.2.5.1.3-11 If the functions assigned to a set of keys change as a result of user selection, the user should be provided with an easy means to return to the initial, base-level functions.

In effect, multifunction keys can provide hierarchic levels of options much like menu selection dialogues, with the same need for rapid return to the highest-level menu. For some applications, it may be desirable to automate the return to base-level assignment of multifunction keys, to occur immediately on completion of a transaction and/or by time-out following a period of user inaction.

⇒ 4.2.5.1.3-12 When function key activation does not result in any immediately observable natural response, users should be provided with some other form of computer acknowledgment.

Temporary illumination of the function key will suffice, if key illumination is not used for other purposes such as indicating available options. Otherwise, an advisory message should be displayed.

⇒ 4.2.5.1.3-13 Function keys are not needed for a current transaction should be temporarily disabled.

Users should not be required to apply mechanical overlays to indicate that functions are not to be used. If a user selects a function key that is invalid for the current transaction, no action should result except display of an advisory message indicating what functions are available at that point.

⇒ 4.2.5.1.3-14 If some function keys are active and some are not, the current subset of active keys should be indicated in some noticeable way, such as by brighter illumination.

This practice will speed user selection of function keys.

⇒ 4.2.5.1.3-15 The system should prompt the user for confirmation if a function key is pressed in a context unrelated to the function.

The function should not be executed unless the action is confirmed.

⇒ 4.2.5.1.3-16 The layout of function keys should be compatible with their use.

Key arrangement should reflect the general principles of organization, such as importance, frequency, and order of use. For example, keys for emergency functions should be given a prominent location.

4.2.5.1.4 Macros/Programmable Function Keys

A macro-command consists of a series of commands that have been grouped and redefined as a single command. When the function key assigned to a particular macro-command is pressed, the series of commands is executed. A programmable function key is a key to which the user can assign functions; it can be assigned to a single function or a macro-command. Macro-commands and programmable function keys are special cases of the function-key dialogue. Their use enables a user to automate aspects of the interface management task.

⇒ 4.2.5.1.4-1 Users should be allowed to assign a single name to a defined series of entries, and then to use that named "macro" for subsequent command entry.

In this way, users can make frequently required but complicated tasks easier to accomplish, when the interface designer has failed to anticipate a particular need. The system should not accept a user designated macro name that is the same as an existing command name. Similarly, when a system may be operated by more than one user and it is not practical or desirable to maintain unique configurations or workspaces for individual users, the system should not accept a macro name that has already been defined by another user.

⇒ 4.2.5.1.4-2 Users should have access to an index of their macros and programmable function keys with their respective composition of commands.

Users should have a means of providing a list of their macro names and functions to other users with whom they will communicate.

⇒ 4.2.5.1.4-3 The use of user definable macros and programmable function keys should be limited.

The advantages may outweigh the disadvantages for some tasks (e.g., software development or modification), whereas for other tasks (e.g., application specific software) the disadvantages may outweigh the advantages.

⇒ 4.2.5.1.4-4 A user should be restricted from modifying a macro or programmable function key as defined by a different originating user.

⇒ 4.2.5.1.4-5 Users should not be allowed to duplicate macro names.

An error message should be provided if the user attempts to assign a previously used name to a macro.

4.2.5.1.5 Forms

A form is a display containing category labels and blank spaces where users enter data. In a form-filling dialogue, the user enters commands or information into the data fields. Forms facilitate the interface management task by reducing the need for the operator to memorize the types of information needed and the permissible entries for each. Command-entry forms are used to aid the user in composing commands. Information-entry forms are used for tasks requiring the user to specify information. Forms may have error checking features, which check entries to determine if they are in the permissible range. Forms may have default information already entered into data fields to facilitate their use.

⇒ 4.2.5.1.5-1 Form filling should be provided as an aid for composing complex command entries.

For example, for a complex data retrieval request, a displayed form might indicate the various parameters that could be specified. For a print request, a displayed form might help a user invoke the various format options that are available.

⇒ 4.2.5.1.5-2 Appropriate and readily modified default parameters should be displayed in forms used for composing complex command entries.

Default parameters permit users to compose potentially complicated entries by relatively simple actions. If defaults have been defined, they should be indicated to users. A displayed form permits a user to review (and confirm or change) default values, just as a user might review displayed defaults for data entry. When only a few parameters are involved, it may be feasible simply to prompt users with guidance messages rather than by displaying a form.

⇒ 4.2.5.1.5-3 Forms for command entry should be consistent in format.

The design of such forms should generally conform to guidelines for the design of information entry forms.

⇒ 4.2.5.1.5-4 Form filling should be used for tasks where some flexibility in information entry is needed, such as the inclusion of optional as well as required items, and/or where computer response may be slow.

Form-filling is often preferred when entering a set of values serially, one at a time, in response to a series of prompts would be inconvenient.

⇒ 4.2.5.1.5-5 Where no source documents or forms exist to support information entry, then fields should be logically grouped, by sequence and frequency of use, importance, and functional associations.

⇒ 4.2.5.1.5-6 Just one explicit entry action at the end of the transaction sequence should be required, rather than separate entry of each item.

Depending on form design, this practice might involve entering the entire form, or entry by page or section of a longer form. Form design should indicate to users just where explicit entry is required. Single entry of grouped data will generally permit faster input than item-by-item entry, and should prove more accurate as well. This practice permits user review and possible data correction prior to entry, and also helps the user understand at what point grouped data are processed. It will also permit efficient cross validation of related data items by the computer.

⇒ 4.2.5.1.5-7 For each data field, an associated label should be displayed to help users understand what entries can be made.

⇒ 4.2.5.1.5-8 Whenever possible, entry of multiple data items should be allowed without keying special separator or delimiter characters.

Formatting characters such as hyphens should be provided by the system. This can be accomplished either by keying into predefined entry fields or by separating sequentially keyed items with blank spaces. In this context, tabbing from field to field is not considered to be keying a special delimiter character. When data items contain internal blanks, the entry fields with a predefined structure should be designed so that users will not have to key any internal delimiters.

⇒ 4.2.5.1.5-9 When a field delimiter must be used for data entry, a standard character should be employed consistently for that purpose.

A special delimiter character that does not require shift keying should be used. A character that does not occur as part of any data entry (except possibly for entry of running text where its occurrence would not be ambiguous) should be used. For example, a slash (/) may be a good choice.

⇒ 4.2.5.1.5-10 When multiple data items are entered as a single transaction, as in form filling, the user should be allowed to review, modify, or cancel the items before entering the form.

⇒ 4.2.5.1.5-11 When entry of information in a field is deferred or omitted, the system should identify the field by highlighting or other means. Before the information is filed or accessed, the user should be reminded that information has not been entered, if such entry is required.

Fields requiring an entry might be made more conspicuous (i.e., coded) in some way to make omissions less likely and avoid having to provide reminders or error messages.

⇒ 4.2.5.1.5-12 When sets of data items must be entered sequentially, in a repetitive series, a tabular display format should be provided where data sets can be keyed row by row.

Row-by-row entry facilitates comparison of related data items, and permits potential use of a DITTO key for easy duplication of repeated entries. When the items in each data set exceed the capacity of a single row, tabular entry will usually not be desirable, unless there is a simple means for horizontal scrolling.

⇒ 4.2.5.1.5-13 Users should not have to remove unused underscores or otherwise enter keystrokes for each position within a variable length entry area.

⇒ 4.2.5.1.5-14 Optional versus required data entries within fields on input forms should be distinct.

⇒ 4.2.5.1.5-15 Distinctive formats should be provided for column headers and row labels, so that users can distinguish them from data entries.

⇒ 4.2.5.1.5-16 For entry of tabular data, when entries are frequently repeated, users should be provided with some easy means to copy duplicated data.

For example, a DITTO capability will speed data entry, and should prove more accurate than requiring users to re-key duplicated data.

⇒ 4.2.5.1.5-17 Where the number of fields is limited, screen traversal distances are short, and when data fields will be accessed sequentially, users should be allowed to tab directly from one data field to the next, so that the cursor can move freely back and forth across rows or columns.

⇒ 4.2.5.1.5-18 Direct pointing devices, such as a mouse or light pen, should be available (1) for selecting fields in complicated forms, or (2) when field entry will be less predictable (as in database update).

When input is not predictably structured, it may be preferable to move among fields by direct pointing rather than tabbing.

⇒ 4.2.5.1.5-19 For long forms, those with many rows, some extra visual cue should be provided to help a user scan a row accurately across columns.

Visual aids for scanning rows are probably needed more when a user is reviewing and changing displayed data than for initial data entry. Such aids should be provided consistently, however, so that display formats for both data entry and review will be compatible. For example, a blank line might be inserted after every fifth row, or dots might be placed between columns in every fifth row. As an alternative, a displayed ruler that a user can move from one row to another may be used.

⇒ 4.2.5.1.5-20 If certain information is used frequently, then it should be automatically entered into the form as a default; see guidance on defaults in Section 4.2.4.4.

4.2.5.1.6 Direct Manipulation

Direct manipulation interfaces allow users to act on visible objects to accomplish tasks, e.g., opening a display by clicking on its icon. A variety of icons may be used to manipulate plant displays. Icons shown on mimic displays represent specific plant components, systems, or functions. Clicking on them may provide access to information about these components and systems, or display an interface for their operation. Displays may contain a variety of computer-based interfaces, such as buttons and sliders, for performing interface management tasks. For example, interfaces for manipulating the presentation of display windows on display screens often contain buttons, sliders, and ‘grab and drag’ points; these are used for opening/closing, resizing, and moving windows and scrolling and paging the window’s contents.

Input is usually provided by using a pointing device to manipulate the graphical object, causing the computer operations to be performed on the object or information it represents. Feedback is represented by a change in the graphic object. For example, when deleting a file, the document icon may disappear into a trashcan icon.

⇒ 4.2.5.1.6-1 Direct manipulation should be used primarily in tasks with actions and objects that lend themselves to pictographic representation, and in which the actions and objects need not be modified for the successful interpretation of the command by the system.

In command entry by direct manipulation, the techniques for selecting and moving displayed objects would be similar to those described in guidelines for graphic data entry. For example, rather than compose a command or select a function key to file a document, a user might move a displayed icon representing the document to superimpose it on another icon representing a file. An extension of this idea is the use of “embedded menus” in which various items within a working display are highlighted in some way to indicate that they can be selected to obtain further information.

⇒ 4.2.5.1.6-2 When user input involves frequent pointing on a display surface, the interface should be designed so that other actions (e.g., display control) are also accomplished by pointing, in order to minimize shifts from one entry device to another.

This recommendation implies extensive use of menus in the margins of a graphic display to permit direct selection of control options by pointing. If screen capacity is too limited to permit simultaneous display of both graphic data and menus, then the designer might provide temporary superposition of menu windows on displayed data, or might provide some separate display device to show current options for control entry. Control entry via keyboard and/or function keys will be less satisfactory. If pointing is performed on some separate input device, such as a stylus on a digitizing tablet, then associated control actions should also be implemented via that device. For graphics software, a pointing action by a user can accomplish several different logical functions: specifying a displayed element ("pick" function); selecting a system-defined object, attribute, or action ("button" or "choice" function); or indicating a location in the conceptual drawing space ("locator" function). A designer must distinguish among these functions, although most users will not. Alphabetic entry for titles, labels, and other annotation of graphic displays will be accomplished more quickly by conventional keyboard input than by pointing.

⇒ 4.2.5.1.6-3 Selection of an icon, menu, or application-specific capability from a function area should be acknowledged by highlighting the selected item.

⇒ 4.2.5.1.6-4 The direct manipulation interface should include (1) windows for containing the data files, (2) menus for additional objects and actions that are not easily represented by pictographic icons.

⇒ 4.2.5.1.6-5 Direct manipulation should not be used when the computer response is slow.

Other modes of interaction should be considered if the system is unable to respond immediately (i.e., within 0.25 second) to direct manipulation input.

⇒ 4.2.5.1.6-6 If icons are used to represent control actions in menus, a text label should be displayed with each icon to help assure that its intended meaning will be understood.

A redundant text label might help make the meaning clear to a user who is uncertain just what a displayed icon means.

⇒ 4.2.5.1.6-7 Graphic means should be provided for displaying the context of current control actions to users.

A graphic representation of the currently selected values of functions, elements, and attributes affecting control actions might help reduce user errors in command entry. Graphic techniques might be used to display the scope of a proposed control action, such as outlining a group of display elements that will be affected by the action.

⇒ 4.2.5.1.6-8 Prompting aids and other guidance pertaining to current control actions should be displayed graphically to the user.

A graphic representation of keypad layout with notes explaining the various key functions might help a novice user to learn the control options available via function keys. A graphic representation of logical combinations specified in query formulation might help reduce errors in the use of query language.

⇒ 4.2.5.1.6-9 A user should be able to "open" an icon with a simple, explicit action.

The action or information represented by an icon is invoked or accessed by “opening” the icon. This should involve two steps: (1) indicating the object or action to be selected (e.g., moving a pointing cursor to an icon or function area) and (2) invoking the function through the performance of a specific, well-defined selection action, e.g., a “double click” on the cursor control device button. Note: A “double click” is defined by two clicks within 700 milliseconds of each other.

⇒ 4.2.5.1.6-10 The size and separation of items on the screen that are displayed for selection should allow them to be pointed to easily (i.e., without requiring precise positioning of the pointer).

It is recommended that target be a minimum of 0.2 inch (5 millimeters) on a side and separated by at least 0.1 inch (3 millimeters). When functions are represented by text labels, a large area for pointing should be provided, typically including the area of the displayed label, plus a half-character distance around the label. When selection is by touch screen, larger sizes and separation are recommended; e.g., a maximum height and width of 1.5 inches (40 mm) and a minimum height and width of 0.6 inches (15 mm), with a maximum separation distance of 0.25 inches (6 mm) and minimum of 0.1 inches (3 mm).

⇒ 4.2.5.1.6-11 When exact placement of graphic elements is required, users should be allowed to expand (“zoom”) the critical display area to make the positioning task easier.

For example, if a pointer must be positioned over a displayed component symbol in order to read or modify the associated parameters, and a number of such symbols are displayed close to one another, it should be possible for the user to “zoom in” to make selecting the desired component easier.

⇒ 4.2.5.1.6-12 Users should be provided some means for designating and selecting displayed graphic elements for manipulation.

Users should have a means of indicating groups of elements (or parts of a complex element) to which an action will be applied. For example, designation might be by pointing, in the case of a discrete element, or might require some sort of outlining action to delineate portions of a complex figure.

⇒ 4.2.5.1.6-13 All items currently selected should be highlighted in some way to minimize uncertainty about the objects or files to which subsequent actions will be applied.

A dotted border might be displayed around a selected element, or perhaps a selected element might be displayed with video inversion to distinguish it from other elements.

⇒ 4.2.5.1.6-14 During graphic data entry/editing, the selected attributes that will affect current actions should be displayed for ready reference by the user.

Users may forget what options have been chosen. Displayed reminders will be particularly important in situations where the consequences of a mistaken user action are difficult to reverse, e.g., where it may be hard to erase an incorrectly drawn line. For example, when graphic attributes – plotting symbols, character size, line type, or color – are chosen from displayed menus, it might suffice to highlight the currently selected menu options; alternatively, current selections might be shown in some sort of "reminder" window. A few attributes might be shown by the displayed cursor, i.e., by changing cursor shape, size, or color depending upon current attribute selections. If lines are drawn by rubberbanding (i.e., if the length and orientation of a line are adjusted by pulling on the ends), then that process itself would show the currently selected line type. In some applications, display cues may not be adequate to convey attribute information completely. There may not be sufficient room on the display, or the attributes may derive from underlying models whose characteristics are too complex for simple display representation. In such cases, users should be able to request auxiliary display of such information to determine the operative context for current actions.

⇒ 4.2.5.1.6-15 Automatic registration or alignment of computer-generated graphic data should be provided, so that variable data are shown properly with respect to fixed background or map data at any display scale.

The computer-prompted registration procedures required when devices such as graphics tablets are used to enter data are often error-prone. The design should therefore either permit direct entry of properly registered data on the display surface or have an accurate and easy-to-use registration procedure.

⇒ 4.2.5.1.6-16 When complex graphic data must be entered quickly, computer aids should be provided to automate that process.

Users can create simple graphics or edit stored graphic material fairly quickly, but creating complex graphic displays takes more time. A variety of computer aids can be provided to help enter graphic data. For example, entry of detailed drawings and/or photographic imagery can be accomplished via a video camera and high-resolution digitizer, with facilities provided for a user to edit the result.

⇒ 4.2.5.1.6-17 Automated plotting of computer-stored data should be provided at user request, with provision for subsequent editing by a user.

In many applications, data intended for graphic display will already be stored in the computer. In such cases, a user might specify the graphic format required (e.g., a line graph, or, for three-dimensional data, an XYZ plot), and edit elements in the resulting display output, without actually having to re-enter the data. When users do have to enter data for graphic display, they might choose form filling or tabular entry for efficiency in the initial input of data and then invoke graphic capabilities for subsequent data editing. In either case, it is important that previously entered data should be accessible for graphic processing.

⇒ 4.2.5.1.6-18 When graphic data must be plotted in predefined standard formats, templates or skeletal displays for those formats should be provided to aid data entry.

In many applications, it may help to provide flexibility so that general prestored formats can be modified by a user and then saved for subsequent use. For example, sample displays might be stored in the computer to aid in creating standard graphs such as bar graphs, or standard diagrams such as organization charts, or page layouts for typesetting, or maps drawn to different scales or with different projections.

⇒ 4.2.5.1.6-19 When graphs must be constructed for data plotting, computer aids should be provided for that purpose.

Construction aids might include stored templates of different kinds of graphs, prompts to guide users in the definition of scale axes, and aids for format control such as automatic centering of axis labels if requested by a user. Computer aids for graph construction should be designed to allow flexibility in their use. A user should be allowed to position labels and other graphic elements at will, except where operational requirements may impose fixed formats.

⇒ 4.2.5.1.6-20 Computer aids should be provided to help users specify appropriate scales for graphic data entry.

The computer should handle scaling automatically, subject to review and change by a user. The computer might provide a general template for the plotting scale and prompt the user as necessary to define the scale more exactly, including specification of the origin, linear or logarithmic axes, scale intervals, minimum and maximum values, and labels for axes. In the process of defining scales, the computer might impose rules to ensure that the resulting graphic displays are designed to permit effective information assimilation by their users, e.g., displaying scales with conventional direction, so that numbers increase in value from left to right, or from bottom to top.

⇒ 4.2.5.1.6-21 Users should be allowed to designate a group of elements to which graphic editing operations will be applied in common.

For example, a user might carefully position two elements with respect to each other, and then wish to move both of them together while preserving their relative positions. Grouping elements might be a temporary action, intended for just a few successive editing operations, or it might be specified more permanently via some sort of “make group” command.

⇒ 4.2.5.1.6-22 The effects of operations performed on direct manipulation interfaces should be immediately visible.

In direct manipulation interfaces (where users ‘drag and drop’ displayed icons), immediate responses to actions are essential to the user having a sense of acting on the objects of the task domain themselves, rather than upon a representation of the objects through some intermediary.

⇒ 4.2.5.1.6-23 Explicit error messages should be provided for incorrect actions related to the process (as opposed to the interface).

In some cases, error messages may not be needed in direct manipulation interfaces because results of actions are immediately visible or because some types of errors may be eliminated. However, the design strategy of relying on the ability of users to detect errors from the behavior of the user interface, rather than providing error messages, has some potential problems. Direct manipulation interfaces have their own problems, which may lead to new types of errors. Some of these errors may be difficult to detect if they are legal operations with respect to the user interface but undesirable actions with respect to the task domain (e.g., plant operation). For example, an interface might allow users to toggle options on and off by clicking icons, the appearance of which would change to indicate the state of the option. If a user attempted to select an option that was not available at the time, the failure of the action might be indicated only by the absence of a change in the icon. However, if a user were attempting change the state of a plant component and the action could not be carried out, an explicit error message would be displayed to indicate that no action had been taken.

⇒ 4.2.5.1.6-24 Representations used as icons should require minimal interpretation.

4.2.5.1.7 Natural Language

In natural language dialogues, users compose entries using a restricted subset of their natural language. The intent is to take advantage of the highly developed skills that people already have in using their own language, and to avoid the need for users to learn artificial dialogues for communicating with computer.

⇒ 4.2.5.1.7-1 A natural language interface should not be the sole means of taking actions that may have to be done very quickly or reliably.

⇒ 4.2.5.1.7-2 The outputs of a natural language system should be consistent with the types of entries required of users.

Users of natural language interfaces may model their entries after the system's outputs.

4.2.5.1.8 Query Language

A query language is a special-purpose language designed to allow the user to direct questions to the computer, usually to interrogate a database. Query languages are artificial in the sense that they contain terms and grammar that are specifically developed for interacting with the computer. Most queries are entered as text strings via keyboards and are often constructed using keywords (e.g., Select, From, and Where). Then a mapping function uses the keywords to examine the database and find all cases that satisfy the query's criteria. A query language may be limited in size to facilitate learning, but they are generally intended for experienced users.

⇒ 4.2.5.1.8-1 A query language should reflect a single, natural data structure or organization.

The query language should be congruent with the user's perception of how the data are organized. For example, if a user supposes that all data about a particular person are stored in one place, then the query language should permit such data to be retrieved by a single query, even though actual computer storage might carry data of interest in different files.

⇒ 4.2.5.1.8-2 The wording of a query should simply specify what data are requested.

A user should not have to tell the computer how to find the data. This objective has been called "nonprocedurality," meaning that a user should not have to understand computer procedures for finding data.

⇒ 4.2.5.1.8-3 Users should be allowed to employ alternative forms when composing queries, corresponding to common alternatives in natural language.

There are typically a number of equally precise ways of specifying a given condition. Therefore, when quantifying a query, a user should be able to employ equivalent forms, such as "over 50," "more than 50," or "51 or more."

⇒ 4.2.5.1.8-4 A query language should minimize the need for quantifiers in query formulation.

People have difficulty in using quantifiers. Negative quantifiers ("no," "none," or "zero") are particularly difficult for users to deal with. Other potentially confusing quantifiers include indefinite ("some" or "any") and interrogative ("how many") forms. If a query language does require quantifiers, it may be helpful to allow a user to select the desired quantifier from a set of sample queries worded to maximize their distinctiveness.

⇒ 4.2.5.1.8-5 A query language should include logic elements that permit users to link sequential queries as a single entry.

Common links for query formulation include 'and' and 'or'. However, a query language should be designed so that it does not require logical links. Some logical quantifiers ('greater than' or 'less than') may confuse users.

⇒ 4.2.5.1.8-6 If a query will result in a large-scale data retrieval, the user should be informed and required to confirm the transaction or to narrow the query before processing.

In this regard, it may be helpful to permit a user to set some upper bound for data output, in effect to define what constitutes a "large-scale" retrieval. It may help a user to decide whether to confirm or modify a pending query, if the user can request a partial display of the currently specified data output.

⇒ 4.2.5.1.8-7 A query language interface should not be the sole means of taking actions that may have to be done very quickly or reliably.

Query language dialogues are usually used for retrieving data from databases and, as a result, may have fewer applications in nuclear power plants than other interaction formats that may be used for a broader range of activities. The use of query languages can be a difficult task since users must apply a specially developed grammar to construct queries. Consequently, query languages have decreased in popularity as human-computer interfaces for non-programmers. Other types of user interfaces, such as menus and direct manipulation interfaces, are considered easier to use.

4.2.5.1.9 Question and Answer

Question and answer is a type of dialogue in which a computer presents one question at a time for a user to answer. While many computer dialogues pose questions in some form, to which the user must reply, the question and answer dialogue is distinguished by its explicit structure. At each step of the human-computer interaction, the system issues a single explicit question as a prompt, to which the user responds with a single answer. Answers are usually alphanumeric text strings entered via a keyboard. They may be terms from predefined dialogues (e.g., Yes/No, Increase/Decrease) from a limited grammar, or an arbitrary data item (e.g., a numerical value for a control setpoint). Question and answer systems may allow abbreviations in responses to reduce the number of keystrokes needed. Based upon the answer received, the system may determine which question to ask next. If the user enters an inappropriate answer, the system may issue an error message and then present the question again. This process may be repeated until the user gives an acceptable response.

⇒ 4.2.5.1.9-1 The system should provide the user with a specific request for information.

⇒ 4.2.5.1.9-2 Each question should be displayed separately.

Users should not be required to answer several questions at once. A user may become confused in trying to deal with several questions at once, particularly if the number of questions is variable from one transaction to another.

⇒ 4.2.5.1.9-3 The system should indicate any constraints that apply to the user's response.

For example, if the only answer that the system would accept were a percentage, the question should be followed by "(%)". The answer area should follow the contextual information.

⇒ 4.2.5.1.9-4 The system should accept as much data as the user is willing to provide in an answer.

If the information that the system requests is constrained, a data form should be used.

⇒ 4.2.5.1.9-5 When a series of computer-posed questions are interrelated, answers to previous questions should be displayed when those will provide context to help a user answer the current question.

Another way to request a related series of user entries is to use a form-filling dialogue rather than question-and-answer.

⇒ 4.2.5.1.9-6 The user should have the ability to remove a question and answer from the screen or recall a question and answer to the screen.

⇒ 4.2.5.1.9-7 When questions prompt entry of data from a source document, the question sequence should match the data sequence in the source document.

⇒ 4.2.5.1.9-8 A question mark should be the delimiter of the question and answer dialogue.

In general, space for answering the question should be provided closely following the question mark. However, when additional information needed for the answer follows the question, the space for answering the question should be placed after the additional information.

4.2.5.1.10 Speech

Speech input allows users to use spoken commands for tasks that would otherwise require manual actions; this is a potentially useful feature in computer-based control rooms. For example, it might allow operators to make control inputs using a keyboard or pointing device, while using speech for interface management (e.g., calling up or closing display windows). A potential limitation is that, at times, a high degree of verbal interaction with others may be required, lessening the opportunity to use speech in this way.

Speech commands are interpreted by speech recognition systems, which can be either speaker dependent or independent. The latter have the advantage of allowing anyone to enter a command. The tradeoff is that the percentage of utterances misunderstood or not recognized is typically higher. (Speaker-dependent systems tend to be more accurate because they are trained on the unique characteristics of individual user’s voices). There are also tradeoffs involving the nature of the speech to be recognized. Systems for recognizing discrete utterances taken from a limited set of words or phrases tend to be more accurate than system that must recognize continuous speech employing an unrestricted vocabulary. Speech recognition capabilities are changing rapidly with technological advances, and these tradeoffs may be less significant in the future. The capabilities available at the time the system is being designed should be evaluated.

⇒ 4.2.5.1.10-1 Spoken input should be used together with alternative methods such as keyed entry or pointing.

Task demands, operating circumstances, or personal preference may cause users to prefer one of another means for input.

⇒ 4.2.5.1.10-2 The characteristics of the speech recognition function should be appropriate for the tasks it is intended to support.

For example, a system designed to mediate control inputs might be optimized for recognition of discrete words or phrases from a limited set of commands, uttered by any user. In this application error would be disruptive, but because the set of commands to be recognized is finite, high reliability can be achieved by limiting the vocabulary. On the other hand, a system intended to assist in preparing procedures or incident reports might be tuned for recognition of continuous, unrestricted speech by specific users. In this case, recognition of natural speech is needed, and errors would be more tolerable; reliability is increased by training on individual users' voices.

⇒ 4.2.5.1.10-3 Feedback and simple error correction procedures should be provided for speech input, so that when a spoken entry has not been correctly recognized by the computer, the user can cancel that entry and speak again.

As with other input modalities, the system should make the user aware of a failed input and provide a simple means of correcting the error.

⇒ 4.2.5.1.10-4 When speech input is the preferred means of input, alternatives forms for critical entries should be allowed, so that if the system cannot recognize an entry after repeated attempts, another entry form can be substituted.

Because speech recognition systems are affected by normal variations in a user's voice, and by changes in the acoustic environment, a spoken entry that was accepted yesterday might not be accepted today. Thus, for important entries a user should be able to use an alternative word. For example, "Exit" might be defined as an acceptable substitute for "Finished." Spelling a word letter-by-letter is not an acceptable alternative, since speech recognition systems may have trouble correctly identifying similar sounding letters.

⇒ 4.2.5.1.10-5 Speech recognition systems should have a means of activation and deactivation (e.g., PAUSE and CONTINUE options) so that conversation between users is not taken as command input.

For example, the speech recognition function might be activated and deactivated by means of a function key or by spoken commands (e.g., distinctive words or phrases).

⇒ 4.2.5.1.10-6 The vocabulary items should (1) consist of words that are meaningful and familiar to the user, (2) be phonetically distinct from one another; and (3) consist of 2-5 syllables.

Items of 2-5 syllables in length are generally better recognized than one-syllable items.

⇒ 4.2.5.1.10-7 Application vocabularies should be divided into sets based on the hierarchy of the application and recognition accuracy requirements.

This improves recognition by reducing the number of choices that the system has to evaluate.

⇒ 4.2.5.1.10-8 The user should be able to test the recognition of any individual vocabulary item without the entire interactive system being on-line. Feedback on the word recognized and the corresponding confidence score should be available immediately after each use of a word.

⇒ 4.2.5.1.10-9 When the consequences of errors are not significant, the speech amplitude and rejection levels required for input should be user-adjustable.

⇒ 4.2.5.1.10-10 Where word boundaries (pauses between words) are required for system interpretation, boundaries of 100 milliseconds or more should be allowed by the system.

⇒ 4.2.5.1.10-11 An indication of the similarity of each spoken command to the recorded template should be available to the user.

⇒ 4.2.5.1.10-12 If an application functions with a speaker-dependent voice recognizer, the user should be able to retrain or update any or all vocabulary templates at any time.

A user's voice changes over time, even in the course of an hour of continuous use. Several factors have the ability to alter the voice temporarily. To maintain good performance under these conditions, the user must have the ability to modify the template set.

4.2.5.2 Supporting Use of Individual Display Pages

Ideally, information needed to perform tasks is contained on display pages that can be shown entirely within the area available for displaying them. However, when the information fills an area larger than the display frame, the user may have to scroll, pan, or zoom to view it. On the other hand, if the information is divided among two or more smaller pages, the user must navigate the display system (see Section 4.2.5.3) to collect it. Limited guidance exists on the tradeoff between the demands of manipulating large pages and accessing multiple pages. The approach chosen should take into account such factors as how navigation functions are implemented, the system's response to navigation inputs, and the ways in which links are defined. It should aim to reduce the effort required of the user to access the information.

In nuclear power plants, large displays with graphical information may include mimic displays (e.g., representations of plant systems), flowcharts (e.g., representations of procedure steps), overviews of the display network, and maps (e.g., a representation of the physical arrangement of equipment in the containment building). Large displays with non-graphical data may include text displays, such as tables of data with many columns and rows (e.g., alarm lists). Users typically interact with such pages by the following means:

- Scrolling – Scrolling allows users to adjust the relative positions of a large page and the frame through which it is viewed in order to display the part of the page needed for the present task. The users' means of making the adjustment can be designed from either of two perspectives: that of moving the frame over a fixed display page, or that of moving the display page behind a fixed frame. Displays may be scrolled in the top-bottom direction, the left-right direction, or both.

- Note: Some sources make a distinction between scrolling and panning such that ‘scrolling’ refers to the orientation in which the display page is conceived of as moving behind a fixed frame, and ‘panning’ refers to the opposite (more common) orientation, in which the viewing area is conceived of as moving over a fixed page. The analogy in the former case is with a scroll of paper; in the latter, with a camera. Continuing the camera analogy, ‘panning’ is sometimes used to refer only to horizontal adjustments, while vertical adjustment is called ‘tilt.’ However, this distinction is not commonly made. In addition, ‘panning’ has recently begun to be used to refer to movements that appear smooth (as opposed to discrete line-by-line or frame-by-frame adjustments). Accordingly, in this document, the term ‘scrolling’ is used generally, referring to vertical and horizontal adjustments, regardless of orientation.
- Paging – Paging is a display framing technique that allows the user to view a display as a set of (typically) display-size units that are accessed in sequence. Thus, the display page is shown as a succession of discrete larger units, rather than being revealed line-by-line or in a continuous fashion.
- Zooming – Zooming is also based on a camera analogy; the action is analogous to changing the focal length of a camera lens. Zooming-in is similar to moving closer to an object while zooming-out is similar to moving further away from it. Because the size of the display screen is fixed, the effect of zooming-in is to show a smaller area of the display page at a higher magnification; the effect of zooming-out is to show a larger area at lower magnification. Scrolling capabilities are often provided in conjunction with zooming capabilities.
- Hierarchical Paging – With this approach, the large display page is divided into a set of smaller pages organized in a hierarchy. The pages vary in the amount of material included from the large display page and the degree of magnification. As the user moves down the hierarchy, more detailed information is accessed from smaller areas of the large display page.
- Distortion-Oriented Techniques – Distorted views can be presented to facilitate user recognition of location. These techniques allow a user to view details of an area of a large display page while keeping the rest of the page in view. This is accomplished by presenting the focus area at a higher magnification than the rest of the display page. The result is a distorted view of the large display page because different parts of it give the user contextual information. Key features of the unmagnified global structure inform the user of the existence and location of other parts of the information structure and support the interpretation of local details.

⇒ 4.2.5.2-1 When requested data exceeds the capacity of a single display frame, users should be given some easy means to move (vertically, horizontally, or both, as needed) over displayed material by paging or scrolling.

Dedicated function keys can provide for paging (i.e., movement by large increments).

⇒ 4.2.5.2-2 When users are required to integrate information across a large display, the HSI should be designed to minimize the effort associated with scrolling, paging, and zooming, and to maintain the users’ orientation.

Minimizing the burdens associated with moving around the page leaves more attention for integrating the information. Table 4-12 provides examples of how these burdens can be reduced.

The following features will help to users to remain oriented while moving through large display pages:

- Large display outputs that are viewed by continuous scrolling should be provided with a graphic indicator inset at the margin of the display frame to indicate current location.
- Prior to executing a zoom or scroll operation, the user should be able to select a particular position on the display to become the center for that operation.
- Displays that can be navigated via zoom or scroll operations should provide a means for the user to rapidly return the display to the default or starting configuration.
- Framing functions should consistently present scrolling and zooming operations so that the same area of the display remains in view when switching between zoom and scroll modes.
- Displayed elements should maintain their relative positions during scrolling and zooming; For example, when a mimic display is scrolled, background items (such as representations of piping and components), component labels, and overlaid "active" data (i.e., parameter displays) should all move together, maintaining the same spatial relationships.

Table 4-12
Reducing Navigation Demands in Large Displays

Minimize the complexity of the navigation moves – Simplifying the navigation action may reduce the demands imposed on cognitive resources, especially central cognitive processes (e.g., determining relationships between the current and desired locations) and response processes (e.g., manipulating the navigation control). The least demands are associated with displays that require no panning, scrolling, or zooming. More demands are associated with displays that require motion in one dimension (e.g., panning in either the vertical or horizontal direction, but not both). Still more demands may be associated with displays that require motion in multiple dimensions (e.g., panning in both the vertical and horizontal directions or panning plus zooming). Therefore, displays should be designed to minimize the number of dimensions that must be manipulated to access the information.
Support comprehension of navigation moves – The central processing demands associated with the move may be greater when the current and target positions cannot be seen at the same time on the display page. In such cases, cognitive demands may be imposed for developing a mental representation of the display page and for determining the relationship between the starting and target locations. If the navigation moves proceed as a series of discrete steps, then additional demands may be imposed for developing an understanding of the relationships between each of these discrete views. These processing demands may interfere with the cognitive task involved with information integration. The use of design approaches for supporting visual momentum can be applied to large displays to support the user's understanding of the relationships of information items in a display space and reduce information access costs.
Minimize the amount of time needed to complete a display navigation move – Moving from one location to another on the display page requires time. It may be affected by such factors as the number of steps in a navigation move, the length of the navigation moves, and the display system's response time. As the length of time increases there is an increased likelihood that the information held in working memory will be lost. Therefore, the amount of time needed to complete a navigation move should be minimized. This may be accomplished by reducing the response time of the display system and reducing the number of actions required to complete a navigation move.
Minimize the difficulty of target detection – When moving from one location to another on the display page, cognitive demands are imposed on perceptual processes for detecting the target information item. These demands may increase the amount of time required to complete the navigation move and, therefore, increase the likelihood that the information held in working memory will be lost. Therefore, the HSI should be designed to facilitate target detection. For example, the targets should be visually distinct from the background. In addition, the scrolling, panning, or zooming motions should be sufficiently slow when approaching the target so the operator can recognize the target.

⇒ 4.2.5.2-3 The design of display pages should take into account limitation in users' abilities to effectively process visual information presented in a scrolling frame.

If text is meant to be scanned while it is scrolled, the column width should be 35 or fewer characters across. This value pertains to text that the user must scan while it is scrolled. Text displays in which the user alternates between scrolling and reading may have wider columns.

⇒ 4.2.5.2-4 Displays should be designed to avoid the need for excessive scrolling.

For example, the user should have the ability (by a single action) to shift the relative positions of the display frame and page when the longer lines of content may exceed the width of the display frame. However, frequent scrolling to view the ends of lines will disrupt reading, e.g., of text passages, and should be avoided by either setting display frame size and line length appropriately or by causing text to 'wrap' within the display frame.

⇒ 4.2.5.2-5 An appropriate orientation for display framing should be chosen and used consistently throughout the interface.

As described above, the perspective for scrolling action may be to (1) conceive the display frame as a window moving over a fixed array of data or (2) conceive data as moving behind a fixed display frame. The former approach is recommended. Users' interaction with contemporary computer applications typically includes moving a cursor freely over a displayed page. This tends to result in users thinking of the page as fixed, and therefore the perspective in which the frame moves over the page will seem 'natural'.

In terms of the actual interaction, this means that scrolling is presented as a movement of the display frame, not of the display page, and thus scrolling commands should refer to the frame, not to the displayed text of data. For example, a command to scroll up (i.e., clicking an 'up' arrow, or pushing a scroll handle up) should result in the display frame moving up relative to the displayed page, so that data or text above the current position becomes visible.

⇒ 4.2.5.2-6 Display framing should be described (e.g., in user instructions and key labels) in functional terms, and wording that implies spatial orientation should be avoided.

Examples of framing in functional terms are: "forward" and "back" or "next" and "previous." Control of display framing functions might be implemented by keys marked with arrows, to avoid verbal labels altogether.

⇒ 4.2.5.2-7 The purpose and means of interacting with scrolling structures (i.e., the display elements, such as 'scroll bars,' used to control scrolling) should be obvious, and the structures should give some indication of the relative positions of the display frame and the entire display page.

Users' recognition of the scrolling structures and the effects they produce should be enhanced by

- including either a textual or graphic label (e.g., a ‘scroll’ icon or arrows)
- using the same display structure throughout the interface
- clearly indicating the direction of the motion an input (e.g., a click) will produce

The functions of the structures associated with scrolling should be made apparent by

- displaying structures only when the corresponding movement is possible
- displaying only a single scrolling structure for each (i.e., vertical, horizontal) direction
- placing the structures appropriately (e.g., a vertically oriented scroll bar might be placed along one of the side borders of the display frame for vertical scrolling and a horizontally oriented scroll bar might be placed along the top or bottom of the display frame for horizontal scrolling.

Scrolling/paging structures should indicate both the absolute and relative positions of the user in the data file. For example, the scroll bar might indicate

- the absolute position by displaying a page number on the scroll icon or handle
- the relative position by the location of the icon or handle within the scroll bar

⇒ 4.2.5.2-8 In addition to scrolling continuously or line-by-line, users should have the option of moving in larger increments (e.g., a display frame or ‘page’ at a time).

Users will be able to get to needed information more quickly if the interface includes features to support moving through large pages efficiently:

- If the information displayed on a large page is separated into smaller units (e.g., based on its content or the size of the display frame), users should be able to step through the displayed information by jumping from one unit or ‘page’ to the next.
- Users should be able to move in single or multiple-unit increments. For example, the user might advance multiple ‘pages’ through a displayed file directly by moving the icon on the scroll bar, at which time the display might move to the location in the file that corresponds to the page number on the scroll icon.
- When moving over multiple pages, the movement should be discrete with no display of intermediate pages between the starting page and the selected page.
- For display pages showing continuous data, users should be able to view frame-sized portions of the page in succession, i.e., to move through the displayed data a frame at a time.

For guidance on navigation of system or networks of discrete pages, see Section 4.2.5.3.

⇒ 4.2.5.2-9 Users should have the ability to scroll or page using different techniques.

For example, in an interface that includes both a pointing device and a keyboard, it should be possible to scroll by means of a scroll bar on the display, or by using arrow keys on the keyboard. For applications in which the user is expected to scroll the display frequently, scroll controls may be built into the pointing device.

⇒ 4.2.5.2-10 Users should be able to expand the size of (i.e., 'zoom') any selected area of the display.

⇒ 4.2.5.2-11 The interface should have features that help user remain oriented when 'zooming' displays.

For example, the interface should

- provide a scale indicator of the expansion factor
- include a graphic indicator of the position in the overall display of the currently visible section
- provide an easy means for the user to return to normal display coverage

⇒ 4.2.5.2-12 When users zoom a display, the system should compensate for changes in the size of symbols, labels, and other graphical objects.

This compensation should maintain these objects at a legible size without allowing them to become unnecessarily large and, thus, cluttering the display. When zooming out on a display page, symbols may be aggregated and presented as a single object to reduce visual clutter, if it is not necessary for users to act on them individually while viewing the display at this level of magnification.

4.2.5.3 Supporting Navigation in Systems of Displays

Display navigation refers to the operation of searching or moving through a system or network of displays for the purpose of finding or retrieving a needed display or item of information. Supporting this activity involves providing interface features that orient the user and means for moving through the display system to retrieve particular display pages. Each of these is described below.

Orientation features help the user understand the relationship between currently accessed information and the rest of the information structure. These features are important because users of large information systems can have a sense of feeling lost in the information space. Orientation features minimize this problem; they may be present in both the display network and in the individual display pages. For example, the display network may contain features showing which display page is currently selected. Display pages that exceed the size of display windows may contain features identifying which portions are currently within view and out of view. A variety of features that support orientation are described below. These include overview displays, spatial references, contextual cues, text-based descriptions, and titles and identification codes.

Perhaps the simplest means of supporting the user's orientation is to include titles or other identifying information that indicates the position of a display in a larger information space. For example, if a group of display pages is functionally related, their titles may be designed to reflect this relationship. Some process control display systems assign a unique numerical or alphanumerical code to each display page. The coding scheme may include prefixes and suffixes to indicate relationships between displays. The prefix identifies the major branch of the menu system (e.g., a major plant system), while the suffix indicates the level in the branch. For example, if a four-digit numerical coding scheme is used, the first digit might indicate major branches (e.g., 1000, 2000, 3000), and the second digit the next lower level of branch (i.e., the second level of branches within the 2000 branch would be 2100, 2200, 2300); this pattern would continue for the remaining digits of the coding scheme.

Overview displays (sometimes called ‘long-shot views’ or system ‘maps’) support the user in understanding the overall organization of information, visualizing portions of the organization that are not currently in view, and understanding the relationships between current and target positions relative to each other and the overall organization. For example, such a display might depict the arrangement of a display network and important display pages within the network. Overview displays, as used in this context, should not be confused with displays that summarize important plant status information.

Some important characteristics of overview displays are described below:

- Format – overview displays may be presented in many formats, such as a separate page, a window within a display screen, and as stand-alone reference material.
- Parallel presentation – display systems may vary in the availability of the overview display. The display may be retrievable upon demand or continuously presented.
- Indication of current location – overview displays may indicate of the user’s current location within the information structure.
- Amount of information structure shown and degree of resolution – overview displays may show the entire structure of the display network or page, or portions of it. The amount of the structure presented and the size of the presentation will affect the users’ ability to resolve details. Viewing techniques such as pan and zoom allow selected portions of a display to be viewed. Window resizing may be used to adjust the size of the presentation.

Spatial references are visual features that convey information about the relationship of currently viewed information to the rest of the information structure. When the entire structure cannot be viewed at once, spatial references may help the user identify the current location and to understand where adjacent items may be found. Some techniques include:

- Scales, axes, and grids – Scales, axes, and grids are sometimes used to provide spatial references for graphical displays. Axes are the graphical representation of orthogonal dimensions in the form of lines (e.g., horizontal and vertical axes). A scale is a graduated series of demarcations indicating the divisions of an axis. A grid is a network of uniformly spaced horizontal and vertical lines for locating points by means of coordinates. Grids may be applied to large displays to divide them into discrete sections, such as those used in geographical maps. If the grid uses a sequential coordinate system such as numbers or letters, then the user may use the coordinates of the current position to determine how much of the display structure lies in each direction around it. Grids are especially compatible with spatially organized information such as maps and mimic displays.
- Perceptual landmarks – These are easily discernable display features that can support the user’s understanding of the arrangement of information within a display. Once a landmark

is recognized, patterns are quickly activated to guide subsequent searches in its vicinity. When they appear in successive displays, landmarks can provide a frame of reference for establishing relationships between the displays. In graphical displays, major pieces of equipment, such as the reactor vessel or turbine, may serve as landmarks. Labels and headings provide important landmarks for aiding navigation in displays of tabular data or text (e.g., computer-based procedures).

- Display overlap – A single display that is too large to be shown as a single view on a display device may be divided into sections in which some portions repeat (overlap) across successive views. These repeated features establish across-display relationships (e.g., interfacing piping systems may be depicted on another display) and may call attention to other display frames (e.g., the edge of one display may identify the beginning of an adjacent display containing related information). The overlap may present physical or functional relationships between successive views.

Orientation coding, such as different background colors and patterns, may be applied to some display pages to differentiate them from displays in other parts of the display network. These cues may be used to overcome the homogeneity of displays and convey a sense of location. However, care is warranted when using color for orientation coding in interfaces that already use color extensively for other purposes; for example, use of color-coded backgrounds may produce poor color combinations (i.e., poor contrast or legibility). Using colored borders (rather than backgrounds) can lessen such problems.

Structure of Display Systems. The structure of the interface and its associated navigation aids should make it easy for users to recognize where they are in the data space and should enable them to get rapid access to data not currently visible (e.g., on other display pages). The way the system works and is structured should be clear to the user. One way of providing a logical, explicit structure for the display network is by providing a consistent hierarchical organization. When each major branch of the network has the same, corresponding set of descendant branches, users can apply their understanding of the layout of one branch to predict how information is organized in similar branches of the network.

By understanding how information is organized in the display network, the user is better able to determine where to look to find needed information. Examples of cues that support comprehension of the structure of a network of displays include: a view of the overall structure of the display network, navigational landmarks that identify key nodes of the display network, and representations of the display network that spatially distribute the nodes in a consistent, predictable manner. An information space that has no explicit structure is difficult, if not impossible, to search exhaustively. If an organized exhaustive search of the information space is to be attempted, an organizing structure must be imposed on it. An indication of structure such as a grid should be provided, especially when the space does not contain inherent regular features to define it.

Overview displays can support visualizing portions of the organization that are not currently in view and help users to understand the relationships between current and target positions relative to each other and the overall organization. For example, the overview may depict the arrangement of a display network and important display pages within the network. Overview displays, as used in this context, should not be confused with displays that provide summarize important plant status information.

⇒ 4.2.5.3-1 The organization of the display network should be readily understood by users.

Specifically, the structure of the display system should:

- reflect an obvious, consistent logic
- be based on task requirements
- be available for display in the form of an overview

⇒ 4.2.5.3-2 The display system should be represented so that the user's perception of the relatedness of displays is consistent with distance in the structure of the display hierarchy.

Designers should strive for compatibility between cognitive (i.e., the user's perception) and organizational distance (as defined by the structure of the display network). For example, locations that are close to one another in the display structure should be spatially contiguous in the representation of the display structure.

Location Within Structure. Information structures often have links that are based on conceptual relationships between the information content (relational links) rather than on structural relationships (e.g., relationships that result from a regular hierarchical structure). Therefore, users may arrive at a point in the information structure without having been oriented by traversing a series of hierarchically arranged links. Nevertheless, features can be included in display pages to help users recognize where they are.

⇒ 4.2.5.3-3 Cues should be provided to help the user retain a sense of location within the information structure.

In order to help users recognize the relationship between the displayed pages and the rest of the display system, pages should

- include information that will allow the user to rely on the familiar structure of the document for orientation – for example, volume, chapter, section, etc.
- show page title and identifying information to communicate the position of a display in a larger information space – for example, if display pages are functionally related, their names may be designed to reflect this relationship; unique numerical or alphanumeric codes may indicate relationships between displays
- be coded to differentiate them from displays in other parts of the display network – for example, by using color coded backgrounds or borders, or different patterns

Relationships Among Display Pages. Disorientation can occur when users do not understand the relationships between successive views of a display system. Designers can protect against disorientation by incorporating features that indicate how the currently displayed page is related to other parts of the display system or network. Such features are analogous to finding information in the physical environment (e.g., recognizing one's previous location and the direction and distance to other related destinations). Users will be better able to remain oriented if successive views contain common features or indications of relationships to other displays (e.g., if there is some overlap with the previous display, or if there are signs showing the how the displayed page relates to other pages with similar functions).

⇒ 4.2.5.3-4 Easily discernable features should appear in successive views and provide a frame of reference for establishing relationships across views.

⇒ 4.2.5.3-5 There should be physical or functional overlaps between displays that prevent the displays from appearing as disjointed views.

To achieve physical overlap, some portions of a display page may be repeated on other displays. This overlap should include only those features needed to establish across-display relationships and to call attention to other data and display frames. Functional overlap may be achieved by providing pointers to data on related displays. For example, a flowchart or mimic display may include pointers to relevant items on other displays. As another example, displays that present the same plant data at different levels of abstraction can include functionally overlapping information that connects the displays.

⇒ 4.2.5.3-6 A hypertext information system should show how a destination node is related to the point of departure.

⇒ 4.2.5.3-7 If the interpretation of displayed data depends on its context (i.e., the location in the display network), an explicit indication of the context should appear in the display.

Knowing one’s location in the display network may not be necessary for accessing the next desired location, but it may be important for interpreting the displayed information.

⇒ 4.2.5.3-8 In spatial representations (such as maps or P&IDs), features should be included to help operators understand the depiction and to assist in way finding and maintaining orientation (especially when the representation is larger than a display page).

Specific features used to enhance understanding and use of spatially organized information include:

- Axes and scales
- Grids
- Directional cues

⇒ 4.2.5.3-9 During navigation, displays should support users’ comprehension of the relationships between successive views or destinations.

The central processing demands associated with the move may be greater when the current and target positions cannot be seen at the same time on the display page. In such cases, cognitive demands may be imposed for developing a mental representation of the display page and for determining the relationship between the starting and target locations. If the navigation moves proceed as a series of discrete steps, then additional demands may be imposed in developing an understanding of the relationships between each of these discrete views. These processing demands may interfere with the cognitive task involved with information integration.

Minimizing Navigation Costs. Moving from one location to another in a display system requires time and attention. The 'cost' of navigation may be affected by such factors as the number of steps required, the distance to the destination, and the display system's response time. When navigation demands are high there is an increased likelihood that the information held in working memory will be lost or that attention will not be available for other tasks. Therefore, the amount of effort needed to complete a navigation move should be minimized. This may be accomplished by reducing the response time of the display system, by making navigation targets or links easier to locate, or by reducing the number of actions required to complete a navigation move.

⇒ 4.2.5.3-10 Wherever possible, the time and effort associated with navigation among display pages (especially those that are often used in succession) should be minimized.

A variety of methods can be used to minimize the effort associated with moving among pages in a system of displays:

- using broad, shallow menu structures rather than narrow, deep ones
- allowing direct access to specific displays via keyword entry (e.g., 'bookmarks')
- providing shortcuts to, for example, the top of the hierarchy, major branches, previously accessed displays (i.e., a 'history' list), or displays often accessed in succession
- indicating the contents of destination pages, thus allowing users to 'preview' the information and avoid the need to backtrack

⇒ 4.2.5.3-11 Use of various navigation strategies should be supported.

The approaches used by operators to navigate a display structure will vary based on factors such as their degree of familiarity with the structure and their current position within the structure. Accordingly, the interface should support different strategies:

- top-down – navigating downward through a hierarchy from the top level is easier if a single-action shortcut is provided to return to the highest level
- bottom-up – navigation that begins at lower levels of a hierarchy can be facilitated if a single-action shortcut is provided to return to the lowest level
- lateral transitions – users needing to sequentially access displays at a given level of the hierarchy will be helped if 'next'/'previous' functions are provided

Direct navigation to a destination selected from a list or map should also be supported (see below).

⇒ 4.2.5.3-12 The display network should provide more than one way to access displays.

The range of methods available for interacting with the display network should not increase the level of mental workload of the user, such as through multiple methods that are inconsistent.

⇒ 4.2.5.3-13 When multiple methods are provided for navigating in a hypertext system, they should function similarly.

Users should not have to apply different strategies to accomplish the same task.

⇒ 4.2.5.3-14 Backtrack capabilities should always be available in hypertext interfaces and should function in the same way.

Backtrack capabilities, which almost all hypertext systems feature, are vital for allowing users to become reoriented. Some hypertext systems use this capability inconsistently, especially where multiple means are provided for accessing information. This inconsistency can cause problems.

⇒ 4.2.5.3-15 Selection points (e.g., navigation targets or links) should be easily detectable and readily distinguished from other displayed text or objects.

The following can help minimize the demands associated with locating links or targets:

- selection points targets should be visually distinct from the background
- codes such as bold, italics, and underline should not be used to identify selection points if other conventional uses of these codes occur in the text, such as to emphasize certain words, since using one code for multiple purposes is likely to confuse the user
- visual coding of selectable items should not add visual clutter or decrease the overall effectiveness of the coding scheme
- scrolling, panning, or zooming motions should be sufficiently slow when approaching the target so the user can recognize the target.
- selection points should not be identified solely by changes in the cursor, since this will increase the attention demands in locating links

4.2.5.4 Controlling Displays

Users are typically given the means to control the information that is presented and the format in which it is displayed.

The update capability of a display system refreshes the data in a display with current values. A display freeze capability prevents a data display from being refreshed with current data values. The freeze capability may be used to provide a view of the status for a specified time or to allow the user to read a rapidly changing display. Display update capabilities are typically initiated automatically; in some cases, the user may be able to adjust the rate of updating. Display freeze capabilities may be initiated automatically or manually. Important characteristics of these capabilities include the degree of user control, the rate of automatic updates, and the designation of the freeze state.

Display suppression features temporarily remove information that is less important, irrelevant, or otherwise unnecessary, and then redisplay it when needed. The intent is to reduce visual clutter. Important characteristics include the user's degree of control over the display suppression capabilities, dedicated keys for this capability, and the designation of the suppressed state.

⇒ 4.2.5.4-1 Users should be able to specify the information to be displayed and select the format in which it is presented.

The user should be able to temporarily suppress standard data displays (see below).

⇒ 4.2.5.4-2 Screen control locations and control options should be clearly and appropriately indicated.

⇒ 4.2.5.4-3 The rate at which displayed values are updated should be appropriate for the users' tasks.

Recommendations for specific circumstances include the following:

- Absent other considerations, displayed values should be automatically updated as more current data become available.
- Changing data values that must be read should be displayed in a fixed position and updated no more than once per second. If users need only to monitor general trends in changing data values, and do not need to take exact readings, faster update rates may be acceptable.
- The user should be able to "freeze" automatically updated data at any point (see below). This is necessary in order for the user to examine changed data more deliberately.
- When a user must visually integrate changing patterns on a graphic display, the data should be updated at a rate appropriate to human perceptual abilities for that kind of data change; e.g., when patterns change very slowly (or very quickly) it may be useful to compress (or expand) the time scale.
- For free-drawn graphics, the refresh rate on the monitor should be high enough to produce the appearance of a continuous track.

⇒ 4.2.5.4-4 If a display can be frozen, it should contain features to ensure that users' remain aware of its state, and of the ongoing situation.

When a display that is ordinarily updated in real time is frozen at the user's request, the following strategies should be used:

- The display should be appropriately labeled to remind users of its "frozen" status.
- The user should be advised if some significant, but not displayed, change is detected in the computer processing of new data.

- When the user elects to resume update of the display, the display should, by default, be positioned at the current real-time point; choice of another point (e.g., to allow a speeded replay of the intervening time) should be conspicuously indicated.

Provisions should also be made to insure that the display defaults to its normal ‘unfrozen’ mode of display. For example, if a frozen display is closed, it should be not be still be frozen when it is next opened. Similarly, it may be advisable to define a period of time after which a frozen display will resume updating.

⇒ 4.2.5.4-5 If a display is suppressed, the interface should contain features to ensure that users’ remain aware of its absence, and of the ongoing situation.

- A data display that has been suppressed should be annotated with an appropriate label to remind users that data have been suppressed.
- Users should be advised if some significant (but not displayed) change is detected in the computer processing of new data when data have been suppressed from a display.
- Data that has been suppressed from a display should be able to be quickly restored to its complete, originally generated form.
- Function keys used to restore suppressed data should have no other use.
- For instance, if a user presses a key to restore suppressed data, that key should only restore the data, and should not also move the cursor to some other position.

Automated Actions. Task performance can be enhanced by interface features that automatically manage windows or present task information, reducing interface management demands for the user. For example, if carrying out a task entails multiple windows being opened in succession, it may be appropriate for all associated windows to be automatically closed upon completion the task (i.e., when the ultimate command is executed or the action is cancelled). However, automated actions may disrupt performance if they are unexpected, require users to redirect their attention, or are difficult for users to understand. A good model of the users’ tasks is required for the system to make selections that are relevant to the users’ needs.

⇒ 4.2.5.4-6 Automated window management should be coordinated with the user’s tasks.

⇒ 4.2.5.4-7 Automated interface management features should be designed such that their operation can be anticipated by users.

⇒ 4.2.5.4-8 The operation of automated interface management features should be apparent to the user.

Automated interface management features that provide little feedback when they act may require the user to divert attention away from current tasks to determine whether the change has occurred. Understanding of automatic actions can be supported by requiring the user to approve actions prior to execution.

⇒ 4.2.5.4-9 The operation of automated interface management features should not draw excessive attention from the user.

4.2.5.5 Providing Feedback

This refers to the behavior of the interface when the user enters data, and indicates whether the data is being received. Feedback can help users determine whether the computer has accepted an input and whether it is having the desired result.

For every entry action by the user, there should be some obvious reaction from the system. The absence of a response is not an acceptable means of indicating that an entry is being processed. In a menu selection context, it may suffice simply to highlight the selected option label (e.g., by brightening or inverse video) when that would provide an unambiguous acknowledgment. In many cases, execution of a requested transaction produces an immediately apparent result, as when a user requests NEXT PAGE and the next page is displayed. In others, a message might indicate completion of the transaction, such as when a user requests a printout at a remote facility and the computer displays a confirming message (e.g., "RAD WASTE file has been sent to printer"). A message might also indicate that execution is in progress or deferred, as when a user enters data and the computer displays an interim message (e.g., "RAD WASTE file is being updated"). A message might indicate that the control entry requires correction or confirmation, as when a user requests a file display and the computer displays an error message "RAD WASTE file not recognized."

When a command may take time to complete, feedback on its progress is needed in addition to the indication that the system has received the command. Completion of the action commanded by the menu item will be sufficient feedback, provided that the action has a result that is visible to the user. However, if the completion of the menu item has no visible result, the additional feedback that the command was completed is needed.

In most applications, users can be allowed to continue work while previous transactions are still being processed. However, in some cases processing delays may require subsequent inputs to be held off (e.g., in situations where processing the current transaction will affect the results of subsequent user actions). In such conditions an explicit, salient indication is needed to prevent users from becoming confused about which commands have been issued or about what the system is doing. Note also, that even if a sequence of inputs is suspended owing to a processing delay, the user should still remain in control of the interaction (e.g., by having the option to cancel the process causing the delay).

System response time refers to the time between the submission of an input to a computer system and the return of results. Important characteristics include the amount of time and the variability between individual responses. The response time may be characterized according to the type of input to which the computer system responds (e.g., control activation, system activation, user requests, error feedback). System response time is important because long delays can detract from primary task performance, especially when the user must remember information while the system is responding.

⇒ 4.2.5.5-1 The computer should acknowledge every entry immediately.

The form of the acknowledgement depends on the nature of the input; for example:

- keyed entries should be displayed stroke by stroke; however, it may not be desirable to display passwords and other secure entries (but a symbol, e.g., asterisk, may be shown as each key stroke is completed)

- completion of a data entry transaction should result in confirmation message if data entry was successful, or else with in error message
- for a repetitive data entry task that is accomplished as a continuing series of transactions, successful entry should be indicated by regenerating the data entry display, automatically removing the just-entered data in preparation for the next entry

⇒ 4.2.5.5-2 Actions requested by users should be completed within an appropriate time.

Examples of appropriate response times for selected activities are shown in Table 4-13. In general, the response should be faster for transactions perceived by a user to be simple. In addition, response time should take into account task requirements:

- When information from different locations must be compared or mentally integrated, the system response time for information retrieval should be minimized; slow response increases the mental effort required to perform such tasks
- System response times should be consistent with operational requirements; the system should respond quickly enough to allow users to complete tasks within process-related time constraints.

Table 4-13
Maximum and Preferred System Response Times

User Activity	Response Time (sec)	
	Maximum	**Preferred**
Control Activation (for example, keyboard entry, cursor controller movement)	0.10	< 0.10
System Activation (system initialization)	3.0	< 0.50
Request for given service: Simple Complex Loading and Restart	2.0 5.0 15-60.0	< 0.25 < 2.0 < 6.0
Error Feedback (following completion of input)	2.0	< 0.25
Response to I.D.	2.0	< 0.25
Information on next procedure	< 5.0	< 2.0
Response to simple inquiry from list	2.0	< 0.25
Response to simple status inquiry	2.0	< 0.25
Response to complex inquiry in table form	2-4.0	< 0.25
Request for next page	0.5-1.0	< 0.25
Response to “execute problem”	< 15.0	< 6.0
Light pen entries	1.0	< 0.25
Drawings with light pens	0.1	< 0.10
Response to complex inquiry in graphic form	2-10.0	< 0.25
Response to dynamic modeling	---	---
Response to graphic manipulation	2.0	< 0.25
Response to user intervention in automatic process	4.0	< 1.50

⇒ 4.2.5.5-3 If processing time requires delay of concurrent user inputs (and no keyboard buffer is available), users should be kept aware of the status of processing.

The following features can make delays less disruptive to the user:

- indicating the delay to the user (e.g., by a change in the appearance of the cursor); an auditory signal may be preferable if user may be looking somewhere other than at the screen while making entries
- presenting a signal when the computer is ready to continue following response time-induced keyboard lockout; for example, the cursor changes back to its normal shape
- providing an auxiliary means of control entry, such as a special function key, to abort a transaction causing extended lockout of the usual entry device; see Section 4.2.4.2
- providing periodic feedback to indicate normal system operation while users are standing by
- giving users some positive indication of completion when processing in response to an entry is lengthy

⇒ 4.2.5.5-4 When slower-than-typical response time can be anticipated (e.g., owing to unusual demands on the system) the users should be given information that will allow them to adjust their interaction with the system.

For example, to allow users to proceed with other tasks during delays, the system should

- acknowledge the data entry immediately and then provide an indication of the delay to the user
- indicate, if possible, the time remaining for the process or of the fraction of the process completed
- clearly indicate subsequent completion and appropriate related information (e.g., a message stating that further user action is required)

⇒ 4.2.5.5-5 Response time deviations should not exceed more than half the mean response time.

For example, if the mean response time is 4 seconds, the variation should be limited to a range of 2 to 6 seconds.

4.2.5.6. Protecting Information

A computer-based system may contain the following features that restrict personnel access to aspects of the computer system to prevent accidental or deliberate damage:

- User Identification – These are capabilities for establishing the identities of authorized users. Important characteristics include password protection, tests to authenticate user identity (e.g., biometric devices), and notifications of potential threats to data security, such as from unauthorized personnel.

- Information Access – These are capabilities that reduce the likelihood of files being accessed and changed. Examples include encryption of sensitive data, indication of the data's security classification, administrative controls regarding access to printed data, automatic records of data access, and the use of read-only files.
- Data Integrity – These are automatic capabilities for minimizing the loss of data that may occur as the result of a computer failure or the user's actions. Capabilities for protecting against computer failures include periodic automatic archiving of data files, maintenance of transaction logs for reconstructing recent data changes, offsite storage of copies of important software, and the provision of backup computing facilities. Capabilities for protecting against user errors include protection from interrupts and data changes, providing safe defaults, and requiring confirmation of potentially destructive entries.

4.2.5.6.1 User Identification

Steps must often be taken to protect systems against unauthorized use. This is typically done by authenticating the identity of legitimate users by means of passwords. However, the development of biometric authentication technology (i.e., verifying a user's identity based on a physiological or behavioral characteristic) has accelerated in recent years, and systems based on this technology (e.g., fingerprint, iris recognition, face recognition) will soon be in widespread use.

For protecting data from unauthorized use, it may not be enough merely to resist intrusion. It may also be helpful if the computer can detect and report any intrusion attempts. In the face of persistent intrusion attempts, it may be desirable to institute countermeasures of some sort, such as changing user passwords or establishing other more stringent user authentication procedures. For example, a maximum limit on the number and rate of unsuccessful logon attempts might be imposed. Such limits typically provide a margin for user error while protecting the system from persistent attempts at illegitimate access. Legitimate users will sometimes have difficulty completing a successful logon, perhaps due to inattention, or a faulty terminal, or faulty communications. Occasional logon failures of that kind should be tolerable to the system, with the user simply invited to try again.

A record of continuing failure by any particular user to complete successful logon procedures, including password entry and other tests of claimed user identity, may indicate persistent intrusion attempts or lack of fitness for duty. Thus, repeated logon failures might be grounds for denying access to that user. Access might be denied temporarily for some computer-imposed time interval, or indefinitely, pending review by a system administrator.

If an identified user is required to take separate actions to authenticate data handling transactions, such as accessing particularly sensitive files or issuing particular commands, the efficiency of system operations may be degraded. Where continuous verification of user identity seems required for data protection, some automatic means of identification might be employed for that purpose.

⇒ 4.2.5.6.1-1 The logon process and procedures for user identification should be as simple as possible, consistent with protecting the system and associated data.

To avoid making logon burdensome, the process should

- display the logon prompts as soon as possible with no additional user involvement
- establish user authorization at initial logon, i.e., it should be completed before a user may select any operational options
- maintain data access/change privileges throughout a work session once a user's identity has been authenticated
- provide prompts for all user entries, including passwords and/or whatever other data are required to confirm user identity and to authorize access to the system
- provide keystroke feedback by special characters (e.g., * or #) or audio rather than by echoing a password entry
- allow users to choose their own passwords and to change their passwords as needed
- not require users to enter routine data that can readily be obtained by other people; if verification of such data is needed, users should be asked to review and confirm currently stored values in a supplementary procedure following logon
- advise users of logon delays, providing information about its current status and when the system will become available
- allow users to start productive work immediately after completing the logon process

⇒ 4.2.5.6.1-2 When system security requires more stringent user identification than is provided by password entry, auxiliary tests should be devised that authenticate user identity without imposing impractical demands on users.

⇒ 4.2.5.6.1-3 Messages or signals should be provided in order to notify users (and system administrators) of potential threats to data security.

⇒ 4.2.5.6.1-4 If there are pending actions and the user requests a logoff, the system should inform the user that these actions will be lost and allow the user to cancel either the pending actions or the logoff.

⇒ 4.2.5.6.1-5 Where possible, in the event of automatic logoff, open files should be saved to some defined file name.

For example, by concatenation of User's Name + Date.

⇒ 4.2.5.6.1-6 Interactive timesharing systems should allow some specified time between keyboard actions before automatic logoff unless a longer period is requested by the user.

⇒ 4.2.5.6.1-7 An audible signal should be presented at specified intervals prior to automatic logoff.

⇒ 4.2.5.6.1-8 As required for security, procedures to control access to printed data should be established, rather than simply prohibiting the printing of sensitive data.

User requirements for printed data are often unpredictable, and printing restrictions may handicap task performance. Rather than restrict printing, establish appropriate procedures for restricting further distribution of data printouts; additional authentication might be required.

4.2.5.6.2 Data Integrity

Automatic data protection features are needed because users cannot be relied upon to remember to take necessary protective measures. Though not strictly a feature of user interface design, reliable data handling by the computer will do much to maintain user confidence in the system. Conversely, data loss resulting from computer failure will weaken user confidence, and reduce user acceptance where system use is optional. For example, depending upon the criticality of the application, different protective measures may be justified, including periodic automatic archiving of data files, maintenance of transaction logs for reconstruction of recent data changes, offsite storage of copies of operating software, or even provision of parallel “backup” computing facilities.

If an action taken by a user may result in loss of data, the user should be informed. Some actions such as BACKUP, CANCEL, or REVIEW, by their definition will cause only limited data change, and so need no special protection. However, if an interrupt action may cause extensive data change (e.g., RESTART, LOGOFF), then the user should be made aware of the potential consequences before processing. If a user interrupts a series of changes to a data file, then the computer might automatically save both the original and the changed versions of that file for subsequent user review and disposition.

The surest way to prevent modification of values that must not be altered (e.g., setpoints specified in plant technical specifications) is to disable or remove from the interface the means for taking the action. Similarly, the means for altering data may be provided only to certain categories of user, or at designated workstations. It is not enough simply to instruct users not to make changes in displayed information.

Destructive modes should not be established automatically. In many applications, it may be better not to provide any destructive mode. For example, in a workspace-based system, data would not really be deleted but only removed or suppressed from the user’s workspace. True deletion would require higher authorization, such as qualified system engineers.

⇒ 4.2.5.6.2-1 Measures should be provided to minimize data loss from failures or errors in the data processing system.

Protection of data should not rely on any action by the user, e.g.,

- creation and maintenance of backup and disaster recover files should be automatic.
- when data files may be deleted (or overwritten) by name, the file names assigned by the system should be distinctive.
- the system's default actions (e.g., in the case of a transaction being terminated) should protect data (e.g., by saving rather than deleting the file being used).

⇒ 4.2.5.6.2-2 Data should be protected from damage as result of inadvertent or mistaken actions by the user.

When protection of displayed data is essential, computer control over the display should be maintained. It is not enough simply to instruct users not to make changes in displayed data. Users may attempt unwanted changes by mistake, or for curiosity, or perhaps even to subvert the system. To protect data, the interface should

- not provide the means to modify values (e.g., setpoints) that must not be changed
- require users to take explicit action to select any mode of interaction that might result in data loss
- reduce the likelihood of accidental activation of controls that may cause data loss, by separating and/or physically protecting them
- temporarily disable controls that may have destructive effects when they are not needed for current task
- continuously indicate the current mode if user inputs in that mode might result in data loss

⇒ 4.2.5.6.2-3 Display formatting features, such as field labels and delimiters, should be protected from accidental change by users.

In many data entry tasks, users will be allowed to change data fields but should be prevented from making any structural changes to the display. In applications where a user may have to create or modify display formats, special control actions should be provided for that purpose.

⇒ 4.2.5.6.2-4 When users are not authorized to change displayed data, "read-only" status should be indicated on the display.

In applications where the use of read-only displays is common, some simple cue in the display header may suffice to indicate that status. In applications where users can usually make additions and/or corrections to displayed data, any exception to that practice may confuse a user and so should be noted more prominently on the display.

⇒ 4.2.5.6.2-5 Data should be protected from inadvertent loss caused by the actions of other users.

When one user's actions can be interrupted by another user

- the interruption should be temporary and nondestructive
- the interrupted user should subsequently be able to resume operation at the point of interruption without data loss.

When multiple users review, enter, or modify data in a system

- they should be made aware of data changes or entries made by other users
- they should not interfere with one another

⇒ 4.2.5.6.2-6 When simulated data and system functions are displayed or provided (perhaps for user training), real data should be protected and real system use should be clearly distinguished from simulated operations.

⇒ 4.2.5.6.2-7 In situations where mistaken or unwanted data changes may be possible, users (or a system administrator) should be able to request a record of data entry/change transactions.

⇒ 4.2.5.6.2-8 When a control entry will cause any extensive change in stored information, particularly if that change cannot be easily reversed, the user should be notified and confirmation of the action should be required before implementing it.

What constitutes an extensive change requires definition in the context of each system operation. As noted above, certain kinds of changes (e.g., to tech spec values) will not be supported by the user interface at all. Others, such as those that will result in changes to procedures and/or system operation, will only be available to authorized users, and subject to confirmation. When user entries or changes will be nullified by an abort action, the user should be requested to confirm the abort. Confirmation messages should be simple, positive, and direct.

⇒ 4.2.5.6.2-9 For conditions that may require special user attention to protect against information loss, an explicit alert and/or advisory message should be provided to prompt appropriate user action.

The prompt for a CONFIRM action should inform users explicitly of any possible data loss. For example, the message, “CONFIRM deletion of entire FEEDWATER file?” is preferable to “CONFIRM DELETE.” If a complete file is to be deleted, sufficient information (e.g., name, description, size, date established, and data last changed), should be displayed to verify the file for deletion.

⇒ 4.2.5.6.2-10 When a user requests logoff, pending transactions should be checked and if any pending transaction will not be completed, or if data will be lost, an advisory message requesting user confirmation should be displayed.

A user may sometimes suppose that a job is done before taking necessary implementing actions.

⇒ 4.2.5.6.2-11 If a user requests change (or deletion) of a stored data item that is not currently being displayed, both the old and new values should be displayed so that the user can confirm or nullify the change before the transaction is completed.

For proposed deletion of significant amounts of data, such as entire files, it probably will not be feasible to display all of the data. In such instances, sufficient information should be provided so that users can identify those files they have selected for deletion. The user should be clearly advised of the potential data loss and required to confirm the destructive action before it will be executed. This practice will tend to prevent inadvertent change, including changes resulting in loss of needed data. User attempts at selective data change without displayed feedback will be prone to error.

⇒ 4.2.5.6.2-12 When records of data access are necessary, the records should be maintained automatically.

Transaction records and logs should be stamped with user identifiers, time, and date. Provisions should be made to control requests for records and logs of data transactions with classified material. Users should be informed concerning the nature and purpose of automated recording of individual actions. Even cooperative, well-intentioned users can forget to keep manual logs of data access, and will resent the time and effort required to keep such logs. Subversive users, of course, cannot be expected to provide accurate records.

4.2.5.7 Managing Information

Computer-based display systems may have capabilities that allow the users to create, change, store, and retrieve documents via the computer. Important characteristics include creating and editing documents, saving documents, temporary editing buffer, and excerpt file. Each of these is covered in a separate subsection.

4.2.5.7.1 Editing Documents

These include features that support the user in creating and changing documents, such as hyphenation, tabs, margins, line breaks, pagination, manipulation of figures and other graphical objects, cutting and pasting, and manipulation of fonts (e.g., font type, underlining, bold).

⇒ 4.2.5.7.1-1 Users should be allowed to specify segments of text in whatever units are natural for entry/editing.

For unformatted (“free”) text, natural units will be characters, words, phrases, sentences, paragraphs, and pages. For specially formatted text, such as computer program listings, other logical units (e.g., lines, procedures, and subprograms) may be used.

⇒ 4.2.5.7.1-2 Users should be allowed to display text exactly as it will be printed.

Accurate display is particularly necessary when the format of printed output is important, as when printing letters and tables. Ideally, text displays should be able to represent all the features that are provided in printed output, including upper and lower case, underlining, bolding, subscripting, superscripting, special symbols, and different styles and sizes of type. When those features are important, the necessary display capability should be provided. For special formatting features that are not frequently used, it may be sufficient to use extra symbols to note text features that cannot be directly displayed. In that case, care should be taken that such annotation does not disturb the spacing of displayed text. This may require two display modes, one to show text spacing as it will be printed, and the other to show annotations to the text. A corollary to this recommendation is that changes made to displayed text should appear as a user makes them. Some line-based editors show changes only after a document has been filed and later recalled for display, which does not represent good user interface design.

⇒ 4.2.5.7.1-3 Easy means should be provided for users to specify required format control features (e.g., margin and tab settings) during text entry/editing.

Required format features will vary depending on the application. The intent of this guideline is that all required format features should be easy to control. Any format features that are provided but are optional for the user's task should not be made easy to use at the expense of required format features. One convenient method of margin and tab control is to allow users to mark settings on a displayed "ruler" that extends the width of a page and is continuously displayed at the top of the screen.

⇒ 4.2.5.7.1-4 Text entered by users should be formatted automatically.

When text formats must follow predefined standards, the standard format should be provided automatically and not rely on users to remember and specify proper formats. When text formats cannot be predicted in advance, users should be able to specify and store for future use the formats that might be needed for particular applications. In the absence of any specific requirements, input should be automatically formatted to be easily readable:

- Unless otherwise specified by the user, entered text should be left-justified to maintain constant spacing between words, leaving right margins ragged if that is the result.
- Automatic pagination for text entry/editing should be provided, allowing users to specify the page size; this may not be needed for short documents.
- In the entry/editing of text, automatic pagination and line breaks by the computer should keep words intact, and hyphenation should only be introduced where specified by users.
- For entry/editing of unformatted text, an automatic line break ("return") should be provided when text reaches the right margin, with provision for user override.
- When a user is inserting text into a document that has already been paginated, no text should be lost if the user inserts more text than a page can hold; i.e., the document should be automatically repaginated.

⇒ 4.2.5.7.1-5 Users should be able to modify the formatting of text as needed.

For example,

- the user should have the ability to change the text's physical characteristics (e.g., typeface and style, capitalization, and tab positions)

- users should be allowed to override automatic pagination in order to specify how many lines stand alone at the bottom or top of a page ("widows" and "orphans"), and to specify text that should not be divided between two pages, such as lists or tables
- users should be allowed to override automatic pagination in order to specify page numbers at any point in a document (e.g., as when parts of large documents are saved as separate files)
- the user should be able to change margins for a text file (e.g., the user may set margins wider than the viewable area in order to prepare information for printing on oversized pages)

⇒ 4.2.5.7.1-6 A tab function should be available for paragraph indentation and for moving the cursor to a preselected location.

The user should be able to set tabs at locations across a display, consistent with the spacing provided by the space bar. The symbols indicating the location of tabs should be invisible to the user by default but should become visible with a single action by the user (for example, by making a screen ruler appear on the display or displaying the tab symbols within the text field).

⇒ 4.2.5.7.1-7 For editing programs or tabular data, cursor tab controls or other provisions for establishing and moving readily from field to field should be provided.

⇒ 4.2.5.7.1-8 The means should be provided to readily move the cursor to the head (beginning) or the foot (end) of the file.

⇒ 4.2.5.7.1-9 When inserting words or phrases, items to be inserted should be displayed as the final copy will appear.

⇒ 4.2.5.7.1-10 Users should be allowed to specify a string of text and request the computer to advance (or back up) the cursor automatically to the next (or last previous) occurrence of that string.

An automatic string search capability will generally speed cursor placement in comparison with incremental positioning, particularly when moving over large portions of a document. The function should be easy to use, yet should support expert users:

- Users should have multiple methods for searching for lines or alphanumeric strings.
- Users should have the ability to search for and move to a specific line number in a file.
- Unless otherwise specified by a user, upper and lower case letters should be treated as equivalent in searching text; the computer should also ignore such other features as bolding, underlining, parentheses, and quotes.
- When case is important, users should be allowed to specify case as a selectable option in string search.
- Users may also wish to specify features such as bolding, underlining, and quotes when searching text (e.g., when searching for a string only when it appears in a heading).

⇒ 4.2.5.7.1-11 When systematic editing changes will be made throughout a long document, a "global search and replace" capability should be provided.

This feature replaces all occurrences of one text string with another. It can operate in two different ways: making all changes automatically, or allowing the user to review and confirm each change. Both options should be available.

The case of the replacement string should match the case of the old string, unless otherwise specified by the user (e.g., if a word is replacing the first word in a sentence, the first letter of the new word should be capitalized).

⇒ 4.2.5.7.1-12 Users should be allowed to select and move text segments from one place to another within a document.

A user should not have to re-enter (i.e., rekey) text that is already available to the computer. One convenient method of allowing the user to both move and copy text is to provide a “cut and paste” facility in which the “cut” text remains in a storage buffer and can be “pasted” more than once. For copying, the user can cut text, paste it back into its original location, and paste it again at a new location.

The cut and paste features should have the following characteristics:

- The user should be able to paste (1) alphanumeric data cut or copied from a text file or table into a graphical display, and (2) graphical data into a text or tabular file.
- Users should be able to cut both graphical objects and areas of a graphical display.
- Users should be able to view text that has been cut or copied prior to pasting.
- Users should be able to insert copied text at any location in the current file or other files created with the same application.
- The pasted text should be inserted at the location immediately before the cursor (in a text file), or at the approximate location of the cursor (in a graphical file).
- Users should be able to paste the most recently cut or copied text as many times as they choose. The text to be pasted is replaced only when new text is cut or copied.
- No gap should be left in the file at the point in the text from which material was removed; the cursor should remain in the same location in the text as it was prior to the cut.

⇒ 4.2.5.7.1-13 Users should be allowed to label and store frequently used text segments, and to later recall (copy into current text) stored segments identified by their assigned labels.

For example, much text processing involves repetitive elements specific to different applications, such as signature blocks, technical terms, long names, formulas, or equations.

⇒ 4.2.5.7.1-14 If the selected text, table, or graphics area extends beyond the bottom of the displayed page, the screen should automatically scroll until the user stops selecting or when the end of the display page is reached.

⇒ 4.2.5.7.1-15 Users should not be able to select non-contiguous blocks of text when copying, cutting, or pasting.

Cutting and pasting (operations which frequently follow selecting) is ambiguous with non-contiguous blocks, especially with respect to the spatial relation between the two non-contiguous blocks when they are pasted into a text file at a new location or into a new text file.

4.2.5.7.2 Saving Files

These include features that allow the user to exit a document and save the changes made when editing it.

⇒ 4.2.5.7.2-1 The user should be able to save the information entered into a file by a single action that will permit the user to continue interacting with that file.

This action replaces the previous information stored in the file with the newly saved information.

⇒ 4.2.5.7.2-2 After finishing the interaction with any type of file, the user should be able to save the information and stop interacting with the file by a single action.

⇒ 4.2.5.7.2-3 After finishing the interaction with any type of file, the user should be able to stop interacting with the file by a single action (e.g., selecting a menu item) without saving the changes to the file.

Commands for exiting are different from those for saving and exiting with a save.

⇒ 4.2.5.7.2-4 The command used to "exit with save" should differ from the commands for "save" (without exit) and for "exit without save."

⇒ 4.2.5.7.2-5 Processing of files should be designed to prevent the lost of input or changes.

File handling features that protect against loss of information include

- preventing users from exiting a file without the opportunity to save the file contents.
- requiring users to verify that they want to exit and lose their most recent inputs.
- making files that were modified and stored with the “save” or “exit with save” actions retrievable with a simple action.
- automatically saving files at frequent intervals while being edited; users should be aware of automatic file saving operations.

- providing the option of invoking an automatic backup function that retains previous versions of files; the specific number of previous versions saved should be selectable by the user.
- making changed files retrievable with a single action even after exiting without saving new input, i.e., changes should be accessible for a period of time after the "exit" actions.

4.2.5.7.3 Temporary Editing Buffer

These include features that allow the computer to temporarily store information while the user edits a document.

⇒ 4.2.5.7.3-1 When selected data is cut or copied from a text file, tabular file, and/or graphics file and placed in a temporary editing buffer, the data should be placed in the buffer automatically, with the only specific action required by the user being the cut or copy action.

If a temporary editing buffer is used, data pasted into a text file, tabular file, and/or graphics file is pasted from that buffer.

⇒ 4.2.5.7.3-2 The contents of the temporary editing buffer should remain intact after the application from which the contents were taken is closed.

⇒ 4.2.5.7.3-3 The default condition should be that additions to the temporary editing buffer are not cumulative.

New data placed in the buffer replaces old data.

⇒ 4.2.5.7.3-4 The user should be able to access the contents of the temporary editing buffer in a window with a single action.

Access to the contents of the temporary editing buffer permits the user to read the contents, but not operate on them.

4.2.5.7.4 Excerpt File

This file allows the user to move data from one location to another. It differs from a temporary editing buffer in that the excerpt file can be saved.

⇒ 4.2.5.7.4-1 The capability to accept and maintain information, independent of application, should be provided for holding relevant information across displays or applications.

An example of this capability is the scrapbook or excerpt file.

⇒ 4.2.5.7.4-2 Users should have the capability to create multiple excerpt files.

⇒ 4.2.5.7.4-3 The user should have the capability to integrate new data with data already in the excerpt file.

Integrating data might include (1) pasting the new data following data already in the file, (2) pasting the new data before data already in the file, and (3) interleaving new data in data already in the file. Each of these capabilities should be available through a single user action.

⇒ 4.2.5.7.4-4 The user should be able to cut or copy data from the excerpt file and paste it to any other file.

⇒ 4.2.5.7.4-5 The user should be able to save the excerpt file.

4.2.6 Interacting with Interface Components

4.2.6.1 Windows

A window is a dedicated geometric area on a display screen within which the system presents information or receives input from the user. In addition to being opened and closed, windows can be moved, resized, and rearranged by the user to adjust the presentation of information in a display screen.

The degree of automation of window management tasks may vary. For some systems, all window management tasks are performed manually; in others, they are performed automatically by the information system. Still other window management systems present windows automatically but allow the operator to make manual adjustments. For example, when an information system opens a window (e.g., in response to a change in the plant or information system or the operator's input), it automatically determines the size and position of the window on the display screen. The operator may then close, move, or resize the window.

4.2.6.1.1 General

⇒ 4.2.6.1.1-1 As appropriate to the user task, windows should be capable of the following operations: scrolling/panning, resizing, moving, hiding, activating, deactivating, copying to/from, zooming in/out, tabbing, and undo-last.

Some tasks will require fewer window operations than others. For example, displays used by operators for monitoring are typically designed so that scrolling is not necessary. Similarly, a window that simply presents a one-line status message from the system that the user will only read and not respond to might need to only have the ability to be closed; it will not need to be movable, or adjustable in size.

⇒ 4.2.6.1.1-2 User control of windows should operate consistently from one display to another for each type of window.

Control of predefined windows may simply involve "opening" and "closing" them, by selection of displayed option labels or function keys. Control of user-defined windows may require user specification of window contents, window size, and positioning on the display. Such window control must be learned by a user, and consistent design of control logic aids that learning.

⇒ 4.2.6.1.1-3 When control actions such as command entry may be taken by a user working within a window, those control actions should be consistent from one window to another.

Cursor positioning controls should operate consistently within all windows. If controls in one window operate differently than in another, user confusion will be unavoidable.

4.2.6.1.2 Labeling and Appearance

⇒ 4.2.6.1.2-1 Windows should be identified by a label consistently located at the top of the window's border.

Labels should remain on the screen while the data changes.

⇒ 4.2.6.1.2-2 Window objects, dialog boxes, and subordinate windows should be labeled.

The labels should convey information important to the use of these items, such as content, purpose, or menu path (e.g., the source or media from which the information originated.)

⇒ 4.2.6.1.2-3 The titles of subordinate windows should match the menu selection items of the menus from which they are selected.

⇒ 4.2.6.1.2-4 Windows should be visually separated from each other and from their background, preferably by borders or similar demarcation.

⇒ 4.2.6.1.2-5 Window types should be perceptually distinct (see Figure 4-26).

For example, active windows in both the tiled and layered window environments should be perceptually distinct from inactive window types.

4.2.6.1.3 Multiple Windows

When multiple windows are being displayed, they can be arranged in various ways. Layering refers to moving one window so it appears to be positioned on top of another one. The overlapping may be partial, such that the top window covers all but a portion of the other window, or total, such that it entirely covers the other window. The degree of overlap of one window relative to the others may be changed to improve the user's view of or increase the ease of interaction with its contents. Tiling refers to a configuration in which windows are positioned beside one another like floor tiles. Windows may be arranged in a tiled format so that they can be viewed without overlaps, and related windows are adjacent to each other.

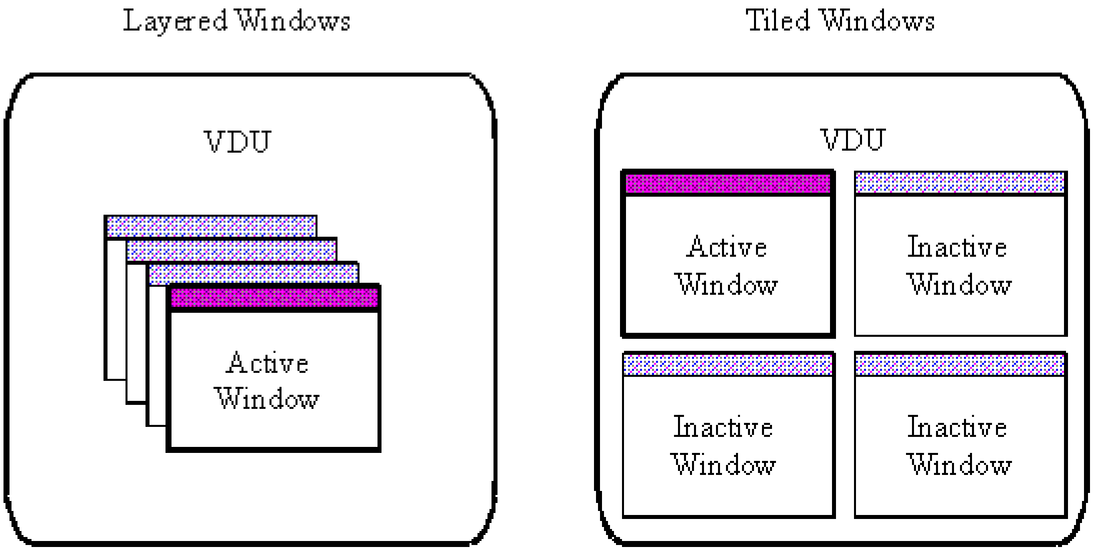


Figure 4-26
Layered and Tiled Windows

⇒ 4.2.6.1.3-1 If separate display pages contain information that the user must compare, combine, or otherwise mentally process, then they should be presented simultaneously.

Multiple displays can reduce the information access costs associated with alternating between the display pages. This may be accomplished via duplicate display devices or via multiple display windows that can be viewed together on the same display screen.

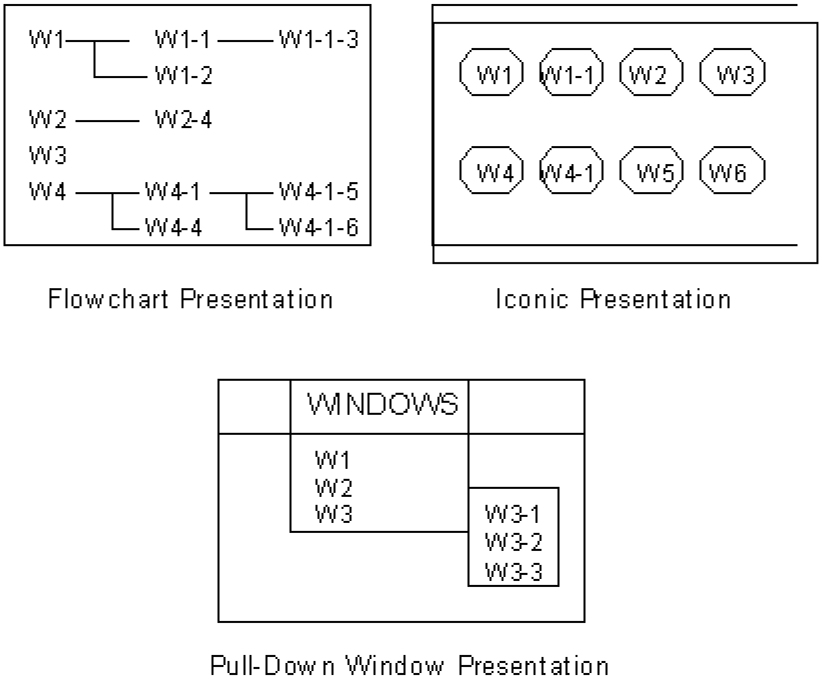
⇒ 4.2.6.1.3-2 Users should be able to select separate data windows that will share a single display screen.

⇒ 4.2.6.1.3-3 When multiple windows are opened simultaneously, the user should have the capability to easily tile, layer, or sequentially view the windows (see Figure 4-26).

Depending upon user needs, data windows might appear simultaneously as segments of a joint display (i.e., tiled), might be overlaid in varying degrees so as to obscure one another (i.e., layered), or might be displayed sequentially at the user's option. In the latter condition, multiple display windows will differ little from multiple display pages, except perhaps in speed of sequential access.

⇒ 4.2.6.1.3-4 The system should keep track of the windows that are open (but not necessarily active or displayed), and provide a means of displaying the list of open windows to the user.

Open windows, for example, could be listed in a menu or as a graphic. This indication should allow the user to easily identify all open windows, including any that are hidden. The indication may be presented at the user's request, rather than being continuously displayed. Possible formats include a list, a menu, iconic representation, and network representation. Examples are shown in Figure 4-27.



Flowchart Presentation

Iconic Presentation

Pull-Down Window Presentation

Figure 4-27
Examples of Open Window Indications

⇒ 4.2.6.1.3-5 An upper limit on the number of windows allowed to be open at one time should be defined to ensure that system response time is not compromised.

⇒ 4.2.6.1.3-6 If several windows are displayed at once, the window(s) in which action can be taken should be indicated.

Adding windows to a display can increase the conceptual complexity of control actions as well as the difficulty of data assimilation. A prominent cursor might be displayed in the currently active window, or perhaps the displayed border of an active window to indicate to a user which window is currently “active;” see discussion of active/inactive windows below.

⇒ 4.2.6.1.3-7 A separate menu bar should be provided for each application window, where different applications are operating concurrently in open windows (e.g., multi-tasking).

An example of separate menu bars is shown in Figure 4-28.

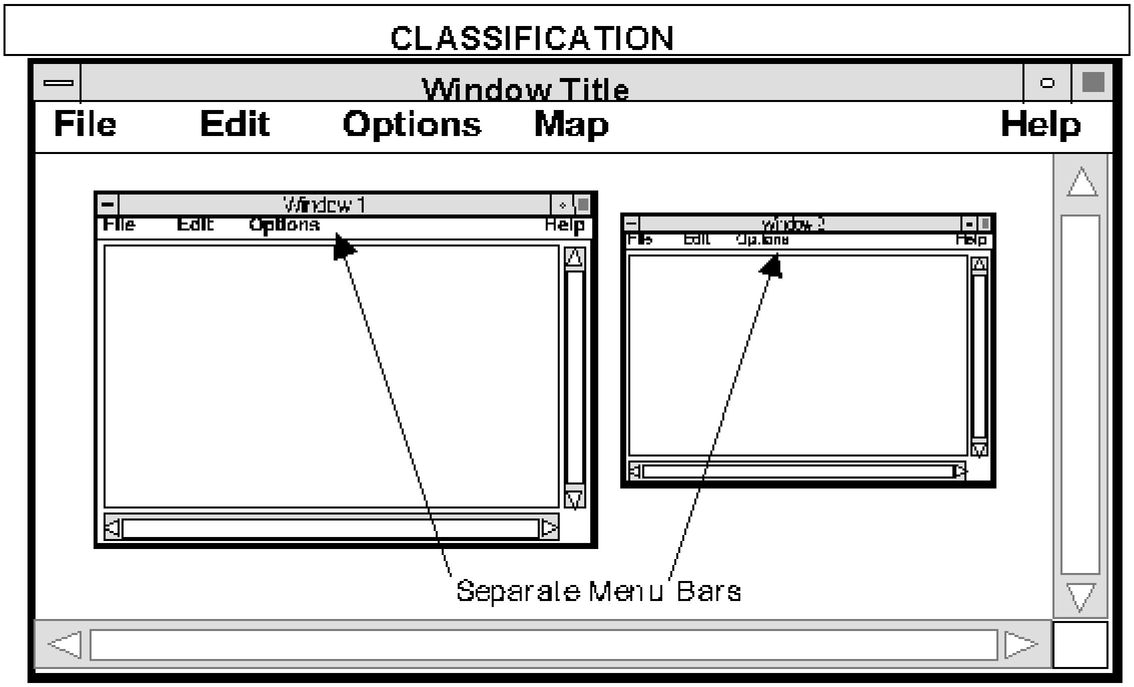


Figure 4-28
Examples of Different Applications with Separate Menu Bars

4.2.6.1.4 Active and Inactive Windows

⇒ 4.2.6.1.4-1 The user should be able to activate a window by performing any of a set of simple actions in that window or related to that window.

A window might be activated by moving the pointing cursor to the window and performing any action, including pressing a key or a button on a cursor control device, issuing a command to open a specific window, selecting a window title from a list on a menu, or selecting an icon representing the window.

⇒ 4.2.6.1.4-2 The action that activates a window should automatically position the place-holding cursor in that window so that the user can provide inputs through that window.

⇒ 4.2.6.1.4-3 If windows are capable of different modes, the system should provide immediate and unambiguous feedback concerning which mode is in effect.

⇒ 4.2.6.1.4-4 A window that is not displayed should be capable of receiving information from the system.

Parameters should continue to be updated whether or not the display page on which they are reported is currently displayed.

⇒ 4.2.6.1.4-5 The system should alert the user to critical information that becomes available in an inactive or non-displayed window.

⇒ 4.2.6.1.4-6 Under normal operating conditions, active windows should be frontmost on the display.

⇒ 4.2.6.1.4-7 Caution and warning windows should be frontmost on the display.

4.2.6.1.5 Size and Location of Windows: Defaults

⇒ 4.2.6.1.5-1 The size and shape of the initial presentation of a window should be consistent with its contents (amount of information, number of menus, and data fields).

When a window temporarily obscures other displayed data, the obscured data should not be permanently erased but should reappear if the overlay is removed.

⇒ 4.2.6.1.5-2 The default dimensions of text windows should be large enough so that the readability of the information is not impaired.

It is typically recommended that windows used for scanning data be no less than four lines high. Window sizes of four lines provide better performance than those with fewer than four lines. Windows with more than four lines show little advantage over windows with four lines. Similarly, windows displaying continuous text are usually wide enough to display about 50 characters. When users read continuously scrolling text (at a rate set by the user), line lengths of 52 to 78 characters provide the fastest performance.

⇒ 4.2.6.1.5-3 The amount of resizing, placement, and manipulation of windows required for using the HSI should be minimized.

Window controls should be provided to allow users to adjust windows for personal needs. However, unnecessary resizing, placement, and manipulation of windows can increase information access cost and divert mental resources from more important tasks by requiring the user's time and attention. Therefore, the window should be initially presented in the most appropriate form for the user's tasks.

⇒ 4.2.6.1.5-4 The system should not allow the user to move or resize a window containing non-critical information such that it obscures critical information.

It may be difficult for the system to anticipate or recognize the relative importance of the information contained in any pair of windows. It may be preferable, whenever practical, to display critical information in a predefined area (e.g., a status bar) that remains 'on top.'

⇒ 4.2.6.1.5-5 A temporary window object should not obscure critical control information and command entry interfaces of the active window.

⇒ 4.2.6.1.5-6 The system should not allow the user to move a window containing critical information off the display screen.

⇒ 4.2.6.1.5-7 Windows should have a default location on the display screen.

⇒ 4.2.6.1.5-8 Display data that is temporarily obscured by a window object should reappear when the object is removed.

If a window object temporarily obscures display data, the data should not be permanently erased.

4.2.6.1.6 Size and Location of Windows: Adjusting

The size of the windows on the display screen may be increased (e.g., to make them easier to view) or decreased (e.g., to reduce clutter). Windows on the screen may also be positioned to improve the user's view or to locate related windows adjacent to one another.

⇒ 4.2.6.1.6-1 Window movement capability should be provided such that the user can move windows to different areas of the display.

⇒ 4.2.6.1.6-2 It should not be possible to position windows in such a way that menu bars, access to the command area, or caution and warning messages are obscured.

⇒ 4.2.6.1.6-3 Movement of a window should appear to be smooth and continuous to the user.

⇒ 4.2.6.1.6-4 Windows partially moved off the display should be made readily accessible with a single action

⇒ 4.2.6.1.6-5 Users should be able to change the horizontal and vertical dimensions of a window independently or together.

4.2.6.1.7 Opening and Closing Windows

Windows that are not in use may be closed to reduce clutter in the display screen or opened to allow the user to view and interact with the display contained in the window.

⇒ 4.2.6.1.7-1 The user should be able to open a window by performing any of a set of simple actions.

Typical methods of opening windows include: issuing a command to open a specific window, selecting a window title from a list on a menu, or selecting an icon for the window.

⇒ 4.2.6.1.7-2 Users should be able to close a window with a single action.

⇒ 4.2.6.1.7-3 If several windows are open, several easy means should be provided for a user to shift among them.

Typical methods of shifting among open windows include: clicking a mouse button, the tab key, cursor keys, or a function key. The most direct method might be to allow a user to select a window by pointing anywhere within its displayed borders, but that action might be confused with the selection of a particular item within the window.

⇒ 4.2.6.1.7-4 The action that opens a window should automatically make that window active.

⇒ 4.2.6.1.7-5 An easy means for the user to suppress the display of windows should be provided.

Two examples include closing a window and reducing the window to an icon.

⇒ 4.2.6.1.7-6 The window system should convey to the user the relationship between the window, the icon, and the action when a window is opened or closed.

For example, an animated depiction of the window closing may portray the window shrinking to an icon, and vice versa when the window opens (see Figure 4-29).

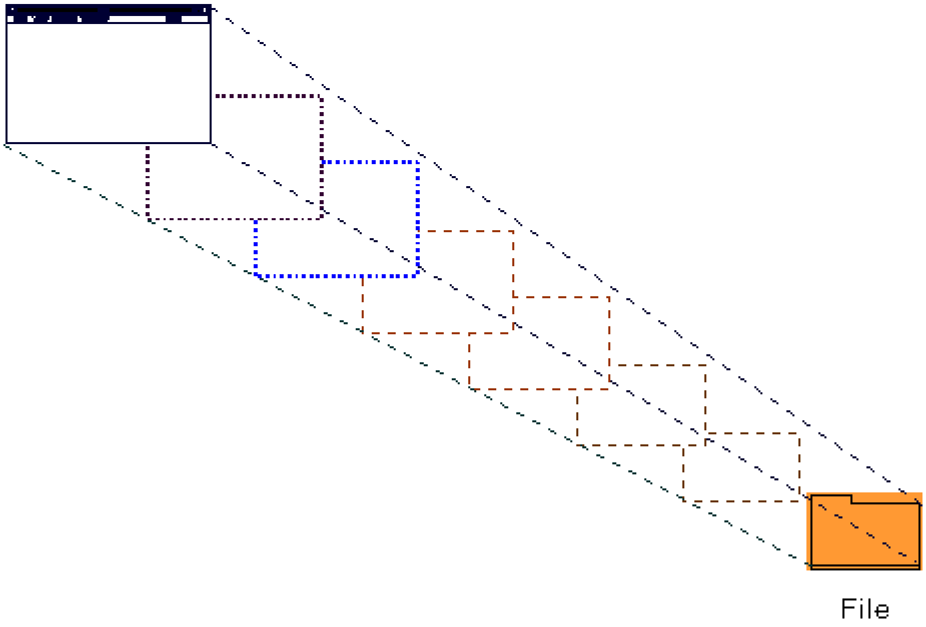


Figure 4-29
Example of Figure Animation

⇒ 4.2.6.1.7-7 When a main application window is closed by the user, all associated subordinate windows and dialog boxes should also close.

⇒ 4.2.6.1.7-8 When a windows are being closed (either by the user or as the result of some other action), the user should be made aware of any pending changes or incomplete interactions.

The process of closing windows (or automatically closing subordinate windows) should be designed to protect against loss of data; see Sections 4.2.5.6.2 and 4.2.5.7.2. Warning messages or confirmation dialogues should be displayed to alert the user to unfinished actions.

4.2.6.2 Cursors

A cursor is an on-screen graphic element that is driven by the user (using a mouse, trackball, or other control device) to move and manipulate on-screen objects. Aspects of cursors that affect their use include: appearance, controls, movement, multiple cursors, pointing cursors, text entry cursors, and multiple display devices. Each of these aspects of cursors is covered in a separate subsection.

4.2.6.2.1 Appearance

This includes the cursor's form (e.g., arrow or bar), salience characteristics (e.g., blinking), and positioning on the display screen.

⇒ 4.2.6.2.1-1 Cursors should have distinctive visual features (shape, blink, or other means of highlighting).

A cursor is the most immediate and continuously available form of user guidance, since it will generally mark the current focus of user attention. Different cursor formats may denote different operational conditions. If that is done, each of those different cursors should be distinctive from other displayed items, and from each other. An underscore cursor would be difficult to see on a display of underscored text, or on a graphical display containing many other lines. If multiple cursors are used on the same display (e.g., one for alphanumeric entry and one for line drawing), then each cursor should be distinguishable from the others.

⇒ 4.2.6.2.1-2 The cursor should not move beyond the display boundaries or disappear from sight.

⇒ 4.2.6.2.1-3 The cursor should not be so distracting as to impair the searching of the display for information unrelated to the cursor.

⇒ 4.2.6.2.1-4 The displayed cursor should be stable.

The cursor should remain where it is placed until moved by the user (or by the computer) to another position. The intent of the recommendation here is to avoid unwanted "drift." Some special applications, such as aided tracking, may benefit from computer-controlled cursor movement.

⇒ 4.2.6.2.1-5 On the initial appearance of a data entry display, the cursor should appear automatically at some consistent and useful location.

In a form-filling display, the cursor should be placed in the first entry field. When menu selection is by pointing, the system should place the cursor automatically at the first listed option. When menu selection is by code entry, the cursor should be automatically placed in the command entry area.

⇒ 4.2.6.2.1-6 When there is a predefined HOME position for the cursor, that position should be consistently defined on all displays of a given type.

The HOME position of the cursor should also be consistent in the different “windows” or sections of a partitioned display. For example, HOME might be in the upper left corner of a text display, or at the first field in a form-filling display, or at the center of a graphic display.

⇒ 4.2.6.2.1-7 When the user must repeatedly return the cursor to the origin or other specific screen location, automatic return or repositioning of the cursor should be provided.

4.2.6.2.2 Controls

These are devices used for positioning the cursor (e.g., mouse or arrow keys) and their characteristics.

⇒ 4.2.6.2.2-1 The user should be able to adjust the sensitivity of the cursor movement to be compatible with the required task and user skills.

⇒ 4.2.6.2.2-2 Control actions for cursor positioning should be compatible with movements of the displayed cursor, in terms of control function and labeling.

For cursor control by key action, a key labeled with a left-pointing arrow should move the cursor leftward on the display. For cursor control by joystick, leftward movement of the control (or leftward pressure) should result in leftward movement of the cursor.

⇒ 4.2.6.2.2-3 User Users should be provided with an easy, accurate means of positioning a displayed cursor to point at different display elements and/or display locations.

Cursor positioning is a frequent user action during graphic data entry. An easy means for controlling cursor movement is essential for efficient performance.

⇒ 4.2.6.2.2-4 Where cursor positioning is incremental by discrete steps, the step size of cursor movement should be consistent horizontally (i.e., in both right and left directions), and vertically (in both up and down directions).

⇒ 4.2.6.2.2-5 At the minimum, keys for cursor control should allow horizontal and vertical cursor movement.

Ideally, keys for cursor control should allow both horizontal and vertical movement, and movement along the diagonals.

⇒ 4.2.6.2.2-6 When position designation is required in a task emphasizing keyed data entry, cursor control should be provided by some device integral to the keyboard (function keys, joystick, and trackball).

Separately manipulated devices (light pen or mouse) will tend to slow the user.

⇒ 4.2.6.2.2-7 If cursor movement is accomplished by depressing keys, the keys should be located on the main keyboard.

4.2.6.2.3 Movement

These are characteristics describing the movement and positioning capabilities of the cursor (e.g., responsiveness, pointing precision, cursor behavior at data entry fields, response adjustable features).

⇒ 4.2.6.2.3-1 If the cursor is moved by depressing a key, releasing the key should cause the cursor to stop moving.

⇒ 4.2.6.2.3-2 The cursor control should permit both fast movement and accurate placement.

Ideally, when the user moves a pointing device, the displayed cursor should appear to move instantly. Rough positioning should take no more than 0.5 seconds for full screen traversal. Fine positioning may require incremental stepping of the cursor, or a control device incorporating a large control/display ratio for small displacements, or a selectable vernier mode of control use. For any given cursor control action, the rate of cursor movement should be constant, i.e., should not change with time. Slow visual feedback of cursor movement can be particularly irritating when a user is repeatedly pressing a cursor control key, or perhaps holding the key down. In that case, slow feedback may cause the user to misjudge location and move the cursor too far.

⇒ 4.2.6.2.3-3 *When Fine Accuracy of Positioning is Required, as in some Forms of Graphic Interaction, the Displayed Cursor should Include a Point Designation Feature*

A cross may suffice (like cross-hairs in a telescope), or perhaps a notched or V-shaped symbol (like a gun sight). Precise pointing will also require a cursor control device capable of precise manipulation. Touch displays, for example, will not permit precise pointing.

⇒ 4.2.6.2.3-4 The user should be able to turn rate aiding of the cursor movement on or off.

With rate aiding, the speed of the pointing cursor’s movement is proportional to the speed of input movement. The default should be to have rate aiding off.

⇒ 4.2.6.2.3-5 Users should be able to select at least two speeds (normal and fast) for the movement of the cursor when the keys for cursor control are held down.

⇒ 4.2.6.2.3-6 When character size is variable, the incremental cursor positioning should vary correspondingly, with a step size matching the size of currently selected characters.

4.2.6.2.3-7 If a cursor must be positioned sequentially in predefined areas, such as displayed data entry fields, this should be accomplished by simple user action.

Automatic cursor advance is generally not desirable. Programmable tab keys are customarily used for this purpose.

⇒ 4.2.6.2.3-8 Users should be required to take a separate, explicit action, distinct from cursor positioning, for the actual entry (enabling, activation) of a designated function.

This guideline may not apply to tasks in which rapid, continuous entry is required (e.g., line drawing or tracking).

⇒ 4.2.6.2.3-9 When there are areas of a display in which data entries cannot be made (such as in field labels or in blank spaces that are part of data formatting), the cursor should 'step over' those areas, and they should be insensitive to pointing actions.

Automatic format protection will generally make cursor positioning easier for a user, since the cursor will not have to be stepped through blank areas, and much routine cursor control can be accomplished with only casual reference to the display. When a user may have to modify display formats, then this automatic format protection can be provided as a general default option subject to user override.

⇒ 4.2.6.2.3-10 For text editing, users should be allowed to move the cursor freely over a displayed page of text to specify items for change, and to make changes directly to the text.

Free cursor movement and changes made directly to the text are characteristics usually associated with so-called screen-based editors and not associated with line- or command-based editors. Screen-based editors are preferred by users and are potentially more efficient.

⇒ 4.2.6.2.3-11 If proportional spacing is used for displayed text, computer logic should make necessary adjustments automatically when the cursor is being positioned for data entry or data change.

Without automatic computer aids, a user probably will not handle proportional spacing accurately.

⇒ 4.2.6.2.3-12 Users should be able to move the cursor by specific units of text, as well as one character at a time.

Cursor positioning will be easier if appropriate function keys can be provided. A SENTENCE key that allows a user to move directly to the next displayed sentence will be more convenient than some chord-keying logic such as CONTROL-S.

⇒ 4.2.6.2.3-13 An ENTER action for multiple data items should result in entry of all items, regardless of where the cursor is placed on the display.

A user may choose to move the cursor back to correct earlier data items, and may not move the cursor forward again. The computer should ignore cursor placement in such cases.

4.2.6.2.4 Multiple Cursors

A computer-based system may feature multiple cursors, such as when multiple personnel interact with a single, group-view display. Important characteristics include the appearance of the cursor (e.g., coding to aid discrimination of multiple cursors), identification of cursor states (e.g., active state), controlling multiple cursors from a single device, and compatibility among multiple cursor control devices.

⇒ 4.2.6.2.4-1 Multiple cursors on a single display should be used only when it can be demonstrated that they are required by the task.

Multiple cursors may confuse a user, and so require special consideration if used in interface design. Multiple cursors might be useful to mark a user's place when manipulating data in multiple display windows. In graphic interaction, one cursor might be used for line drawing and a different cursor for alphanumeric data entry (labels).

⇒ 4.2.6.2.4-2 In a multitasking environment with multiple monitors, controllers, or cursors, the location of the active cursor should be obvious to the user.

If there are two pointing cursors, one on each of two monitors, the active cursor should be apparent to the user. If there is a single cursor that moves between two monitors, its path should be continuously trackable. As the cursor crosses from one monitor to the other, it should either maintain its vertical coordinate for side-by-side monitors and horizontal for stacked monitors, or should jump between uniquely specified locations on each screen.

⇒ 4.2.6.2.4-3 If multiple cursors are used, they should be visually distinctive from one another.

⇒ 4.2.6.2.4-4 If multiple cursors are controlled by different devices, their separate controls should be compatible in operation.

Assume that one cursor is moved upward on a display by forward motion of a joystick. Then a second cursor should also be moved upward by forward motion, perhaps by forward motion of a second joystick or by forward motion of a trackball or other device.

⇒ 4.2.6.2.4-5 When multiple cursors are controlled by a single device, the cursor currently being controlled should be clearly indicated.

⇒ 4.2.6.2.4-6 When there are multiple cursor control/pointing devices, a unique pointing cursor shape should be associated with each device.

⇒ 4.2.6.2.4-7 Cursors of different shapes should be used for different purposes.

The shape of a cursor should reflect the state of the system or processing mode. A specific cursor should be uniquely assigned to a specific purpose to provide state or mode information to the user. A straight-line cursor might be used as the placeholder cursor to indicate entry position in a word processing task, an arrow might be used as a pointing cursor to indicate screen structures, and an X-shaped pointing cursor might be used when the user cannot interact with the system. Within this general framework, the number of cursor shapes used should be kept to a minimum.

4.2.6.2.5 Pointing Cursors

Pointing cursors are the arrows (or other symbols) that move across a display in response to movement of the pointing device. They are used to indicate functions, objects, or locations that the user wishes to select or act on.

⇒ 4.2.6.2.5-1 The pointing cursor should be visible to the user at all times and may obscure characters unless it interferes with performance within an application.

To maintain pointing cursor quality, the cursor should obscure other characters, not vice versa.

⇒ 4.2.6.2.5-2 The pointing cursor should not blink.

⇒ 4.2.6.2.5-3 Pointing cursors should maintain image quality throughout an entire range of motion within the display. The position of the pointing cursor should be clearly visible during movement from one screen position to another. Flicker should be minimized.

⇒ 4.2.6.2.5-4 To the greatest degree possible, pointing cursors should be completely graphic and should not contain a label.

⇒ 4.2.6.2.5-5 The pointing cursor should maintain its size across all screen and display locations.

⇒ 4.2.6.2.5-6 The movement of the pointing cursor should appear to the user to be smooth and continuous, with smooth and continuous movement of the cursor control device. The pointing cursor should not move in the absence of any input from the user.

4.2.6.2.6 Text Entry Cursors

Text entry cursors indicate the point at which typed or copied characters will be inserted. They typically appear as a blinking vertical line or underscore character.

⇒ 4.2.6.2.6-1 The text entry cursor should only be visible when text entry is possible.

⇒ 4.2.6.2.6-2 At the initiation of a task, an application, or a new display, the user should be able to immediately determine the location of the text entry cursor. Following the initial placement of the text entry cursor, the position of the cursor should be under the user's control.

For example, the cursor might be placed initially at the first data field in a data form, at the upper left corner of a blank display in a word processing task, and immediately following the last character of a word processing display containing alphanumeric characters.

⇒ 4.2.6.2.6-3 If text entry cursor blinking is to be used to direct the user's attention, the default blink rate should be 3 Hz.

A blinking cursor need not obscure characters. For example, the blinking cursor may be an underline that does not cover the entire character.

⇒ 4.2.6.2.6-4 The place-holding cursor should not obscure any other character displayed in the position designated by the cursor.

As an example, a block cursor might employ brightness inversion ("reverse video").

⇒ 4.2.6.2.6-5 There should be only one text entry cursor per window.

⇒ 4.2.6.2.6-6 The text entry cursor should assume the height and/or width of the text characters adjacent to it.

4.2.6.2.7 Multiple Display Devices

In some systems, users may interact with multiple display devices by means of a single pointing device. It is important that the user is able to track the movement of the pointing cursor from one device to another. When display devices are physically separated or dissimilar the cursor motion between them may not be perceptually smooth. That is, the user must translate motion on one display into a different motion in the other or follow the cursor as it 'jumps' across the space separating the displays. These factors may cause the user to lose track of the cursor's location. Various techniques can be used to support the user in following the cursor motion between display screens. The cursor can be made to always enter the other display at a uniquely specified entry point. This method allows the user to anticipate the cursor's location on the other display, which may reduce the time associated with finding it. However, the user must first locate the specified entry point. When display screens have different proportions of height and width, then the user may have difficulty understanding how the cursor position on the edge of one display screen corresponds to a position on the other screen. In such cases, computational techniques can be applied that compensate for the differences in screen sizes to make cursor motion appear more continuous. Alternatively, the small-screen display might overlap a smaller portion of the large-screen display, such that a one-to-one relationship in cursor motion is maintained.

⇒ 4.2.6.2.7-1 When displays are the same size and are located adjacent to each other, the cursor should appear to move in a smooth, continuous motion from one display device to the next.

⇒ 4.2.6.2.7-2 When display devices are physically separated, have different orientations, or different sizes, techniques should be employed to help the user keep track of the cursor's position.

4.2.7 Sources of Additional Information

O'Hara, J., Brown, W., Lewis, P., and Persensky, J.J. (2002). Human-system interface design review guidelines [NUREG-0700, Rev.2]. Washington, DC: U.S. Nuclear Regulatory Commission.

Human Factors and Ergonomics Society (2002). Human factors engineering of computer workstations [BSR/HFES 100]. Santa Monica, CA: Human Factors and Ergonomics Society.

DoD (1996) Technical architecture framework for information management – Volume 8: DoD human computer interface style guide.

ISO 9241-10:1996 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 10: Dialogue principles.

ISO 9241-13:1998 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 13: User guidance.

ISO 9241-14:1997 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 14: Menu dialogues.

ISO 9241-15:1997 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 15: Command dialogues.

ISO 9241-16:1999 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 16: Direct manipulation dialogues.

ISO 9241-17:1998 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 17: Form filling dialogues.

4.3 Soft Control Systems

4.3.1 Overview
4.3.2 Soft Controls Guidelines Checklist
4.3.3 Deciding Whether to Use Hard or Soft Controls
4.3.4 Selection Displays
4.3.5 Control Displays
4.3.5.1 Identification and Management of Control Displays
4.3.5.2 Display of Control Modes, Logic, and Constraints
4.3.5.3 Control Input and Commands
4.3.6 Feedback and Monitoring
4.3.7 Sources of Additional Information
4.3.8 Appendix: Error Tolerant Design

4.3.1 Overview

This section provides guidance on deciding on whether to use hard controls or soft controls for specific applications and guidance on the design of soft controls. An overview of the considerations involved in soft control design is illustrated in Figure 4-30. The detailed guidance begins with Section 4.3.3.

Controls are the devices through which personnel interact with plant functions, processes, systems, components, and variables. From a human-system interface (HSI) standpoint, controls can be hard and soft. Hard controls are physical hardware devices, such as j-handles, position switches, and pushbuttons, which are typically mounted on control panels. Soft controls, on the other hand, are user input devices presented as displays on a computer screen.

From an instrumentation and control (I&C) standpoint, hard controls may be either hardwired directly to the equipment being operated or they may provide input through software. Soft controls, on the other hand, only provide input through software and cannot be hardwired to equipment. In the strict sense, when a hard control is linked to software, it is a soft control in that it can be flexibly used to provide different types of control modes and options that are defined based on the current software configuration. Thus it is important to recognize that software control of plant equipment can be implemented using hard or soft interfaces.

Most of the guidance in this section discusses soft controls that are implemented using soft interfaces, i.e., on-screen controls. However, the user may apply many of the same principles when implementing soft control with hard input devices.

Since soft controls can be used to control plant functions, processes, systems, components, and variables, the term “items” will be used to refer to all of them collectively.

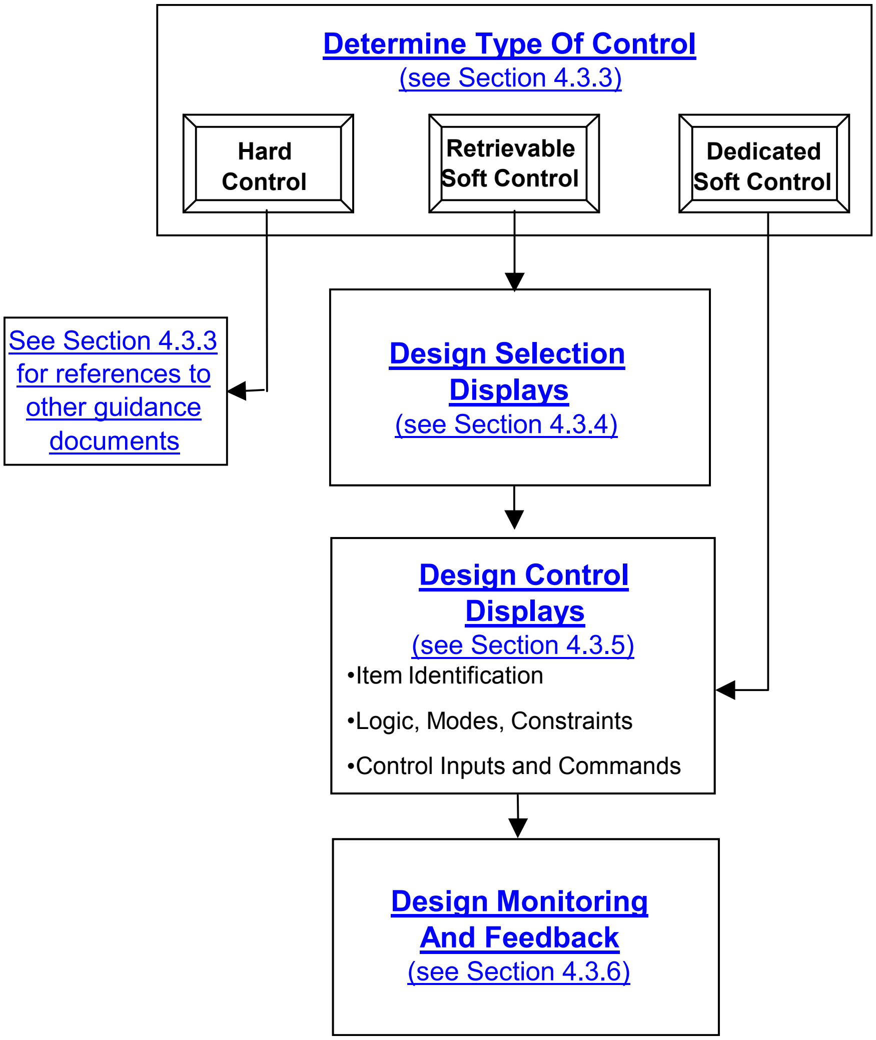

Determine Type Of Control
(see Section 4.3.3)
Hard Control
Retrievable Soft Control
Dedicated Soft Control
See Section 4.3.3 for references to other guidance documents
Design Selection Displays
(see Section 4.3.4)
Design Control Displays
(see Section 4.3.5)
•Item Identification
•Logic, Modes, Constraints
•Control Inputs and Commands
Design Monitoring And Feedback
(see Section 4.3.6)

Figure 4-30
Soft Control Design Considerations Addressed in this Section

The main elements of a soft control are:

- *Selection display* – The display from which a soft control is selected.

- *Control display* – The display with which the control action is taken. In addition to providing for control input, this display may provide information about relevant parameter values, the control logic, constraints, and feedback related to the control actions.

- *Display devices* – The devices on which the soft control display is presented. It may be a video display unit (VDU) or other display device.

- *Input devices* – The devices used to interact with the soft control. Typically theses are computer-input devices, such as a keyboard, mouse, and touch screen.

Since the display devices and input devices for soft controls are the same as for interacting with the computer-system in general, these topics are not addressed in this section. Guidance on display devices and input devices can be found elsewhere.

Some of the benefits of soft controls are summarized below. These features are discussed at greater length in the detailed guidance sections beginning with Section 4.3.3.

Soft controls offer a great deal of flexibility and when properly implemented can greatly enhance the users understanding, execution, and monitoring of the control action. Soft controls are especially attractive when the endpoint vision for the modernization program involves the following types of modifications:

- transition to computer-based workstations with seated operators
- the consolidation of controls
- the integration of controls with relevant displays and other information
- an increased level of automation
- computerized procedures
- increased flexibility in the presentation of controls and displays.

Perhaps the greatest benefit of soft controls is the ability to greatly enhance the information needed to fully understand a control action. A display of the control logic can be made available at the interface. The control display can be designed to indicate any prerequisite conditions for the control action (e.g., the presence of any interlocks or alarm conditions associated with the actions). The soft control display can precisely provide feedback about the effects of the control action so that the user can monitor its progress. Soft controls can be designed to perform different functions, depending on the current control mode, thus providing greater flexibility. They can also provide checks on user inputs and provide more informative feedback to users about the acceptability of their inputs to protect the system against incorrect user control inputs.

Soft control can be integrated into other displays, such as task displays and computerized procedures so that the control is available to the user precisely where it is needed. Soft controls can also be grouped into sets of controls that are needed together (as a set) for user actions.

Soft controls can be used to consolidate a large amount of panel space into a single VDU. Further, new controls can be added to the control room without a need to add additional panel space or to rearrange already existing controls. This feature makes operations from a seated workstation possible. This also enables control to be easily modified.

While the benefits of soft controls are many, their main drawback is that under some circumstances they require additional time and workload to operate. This mainly happens when they have to be retrieved from the computer system. While soft controls can be implemented as spatially dedicated controls, like hard controls, as more controls are consolidated into a single VDU, this becomes impractical. Users must then retrieve them from the computer system before they can be operated. In addition, users can often operate them by touch and the feedback provided from the manipulation of the control makes them easy to use. By contrast, screen based soft controls require more attention to the "manipulation" of the control itself.

As noted above, these tradeoffs are discussed in more detail in the detailed guidance section.

4.3.2 Soft Controls Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining soft control sections. For additional information please consult the sections and guidelines referenced.

4.3.3	Deciding Whether to Use Hard or Soft Controls							
	=>	4.3.3-1	Identify hardwired controls that are required by regulation or needed for diversity from the computer system.					
	=>	4.3.3-2	Determine the need for spatial dedication and continuous availability. Consider using spatially dedicated, continuously available controls (hard or soft) when the user's tasks require rapid action, highly-reliable response, or frequent access to controls.					
	=>	4.3.3-3	Determine whether tradeoffs favor a hard or soft control implementation.					
4.3.4	Selection Displays							
	=>	4.3.4-1	Provide flexible approaches to soft control selection.					
	=>	4.3.4-2	The design of the HSI should clearly distinguish between control actions and interface management actions.					
	=>	4.3.4-3	The selection display should be clearly and prominently labeled to identify the set of items being presented.					
	=>	4.3.4-4	The display should clearly indicate what items can be selected for control and the items themselves should be visually distinct.					
	=>	4.3.4-5	The selection display should support the identification of items based on recognition rather than recall.					
	=>	4.3.4-6	Selection of an item from a display should require simple input actions.					
	=>	4.3.4-7	The selection display should provide feedback to the user of the items that have been selected.					
4.3.5	Control Displays							
	4.3.5.1	Identification and Management of Control Displays						
		=>	4.3.5.1-1	A clear link should be provided between the selection display and the control display.				

		=>	4.3.5.1-2	The item to be controlled should be clearly and prominently identified in the control display.					
		=>	4.3.5.1-3	The control display should not obscure associated information. If this is not possible, a means should be provided for viewing information that may be concealed by the control display					
		=>	4.3.5.1-4	When multiple control displays are opened at the same location, their unique identification should be visible.					
	4.3.5.2	Display of Control Modes, Logic, and Constraints							
		=>	4.3.5.2-1	When the soft control can be operated in more than one mode, the current mode should be clearly and prominently identified and the other mode options should be available.					
		=>	4.3.5.2-2	Higher-level controls should be considered for common operational situations.					
		=>	4.3.5.2-3	Information defining the control logic should be available to help personnel properly perform control functions					
		=>	4.3.5.2-4	Timing requirements should be considered in the design of soft controls					
		=>	4.3.5.2-5	Deadband should be displayed where appropriate and important for the operators' understanding of the control response.					
		=>	4.3.5.2-6	Error signals for control systems should be supplied for selected controls					
		=>	4.3.5.2-7	A soft control display should allow users to quickly assess the status of individual components affected by the control.					
		=>	4.3.5.2-8	Information concerning interlocks, lockouts, and lockins related to the control action should be available to help personnel properly perform control functions. The user should be notified when interlocks, lockouts, and lockins are in effect and which actions are being blocked and what conditions activated the block.					
		=>	4.3.5.2-9	An interlock, lockout, or lockin should not initiate an action that was previously blocked merely because the status of the triggering condition has changed.					
	4.3.5.3	Control Input and Commands							
		4.3.5.3.1	General Control Input Guidance						
			=>	4.3.5.3.1-1	The control display should be labeled and contain clear information to identify the item being controlled.				
			=>	4.3.5.3.1-2	The control input field should clearly and predominantly identify the aspect of the item that is being controlled				

			=>	4.3.5.3.1-3	The control options should be clearly presented and easily distinguished from each other.				
			=>	4.3.5.3.1-4	The user interaction with the control display should minimize the possibility of initiating a control action if the visual display is not working properly.				
			=>	4.3.5.3.1-5	If an input device controls more than one variable, the user should not have to reset the device to match the value of the new variable before executing a control action.				
			=>	4.3.5.3.1-6	If multiple soft controls are needed for a particular task, they should be retrievable as a predefined group.				
			=>	4.3.5.3.1-7	If keyboard input is used for a soft control, the input should be displayed in an input field on the control display and the control should not be acted on until a confirming response is made, such as hitting the return or enter key.				
		4.3.5.3.2		Discrete-Adjustment Controls					
			=>	4.3.5.3.2-1	Discrete-adjustment controls should be used for selecting among a set of individual settings or values.				
			=>	4.3.5.3.2-2	Discrete-adjustment controls should indicate which setting was selected				
			=>	4.3.5.3.2-3	If a discrete-adjustment control initiates continuous operation, it should provide continuous indication on the current state.				
		4.3.5.3.3		Continuous-Adjustment Controls					
			=>	4.3.5.3.3-1	Continuous-adjustment controls should be used when precise adjustments along a continuum are needed or when many discrete settings are present.				
			=>	4.3.5.3.3-2	Reference values should be provided to help users judge the appropriateness of values when entering continuous variable inputs.				
			=>	4.3.5.3.3-3	When part of the range of values depicted by a continuous-adjustment control represents critical information, such as alarm limits, those values should be coded to facilitate recognition.				
			=>	4.3.5.3.3-4	The value to which a continuous-adjustment control is set should be digitally displayed.				
			=>	4.3.5.3.3-5	The physical size of the continuous-adjustment control should allow the user to read the current and target values with the required precision and accuracy.				

			=>	4.3.5.3.3-6	A means of providing incremental increases or decreases in demanded values should be provided when precise inputs are needed. Each press of an arrow button should change the current value uniformly				
			=>	4.3.5.3.3-7	Incremental input devices should provide salient feedback when they are actuated.				
		4.3.5.3.4		Error Tolerance and Correction					
			=>	4.3.5.3.4-1	Where possible, a command entry field should show valid value range and the expected number entry format, e.g. 0XX or XXXXX as well as a default value.				
			=>	4.3.5.3.4-2	Confirmation steps should be considered and, where used, implemented as a separate user input from control actions.				
			=>	4.3.5.3.4-3	User control input verification should be considered.				
			=>	4.3.5.3.4-4	A specific command that produces one action in one mode should not cause a different action in another mode.				
			=>	4.3.5.3.4-5	Unique commands associated with actions that have important consequences should not be easily confused with other commands used in the same or different modes.				
4.3.6	Feedback and Monitoring								
	=>	4.3.6-1	The soft control should display the user's input in a way that allows the user to review it and determine whether it is correct.						
	=>	4.3.6-2	Immediate feedback should be provided that a command was received. Additional feedback should indicate whether the user's command is being acted upon and the current status of the item being controlled relative to the demanded status.						
	=>	4.3.6-3	Feedback should indicate the status of sequential actions that are in progress.						
	=>	4.3.6-4	Systems that can change mode automatically should provide feedback to make the user aware of the current mode.						
	=>	4.3.6-5	Feedback should indicate when the demanded status is achieved.						

4.3.3 Deciding Whether to Use Hard or Soft Controls

One of the first considerations in choosing an approach to the design of controls is whether the controls should be soft controls or hard controls. This decision is not one that can be decided on using human factors criteria alone. I&C criteria for reliability, diversity, isolation, separation, transient response performance requirements, and defense-in-depth must also be considered.

In this section we will address the factors that enter into the decision as to whether to implement controls using hard control or soft control technology. This decision can be broken down into a several step process as discussed below and as illustrated in Figure 4-31.

The process leads to four types of controls:

- *Hardwired controls* – Controls implemented in hardware that are hardwired to plant equipment.
- *Hard controls* – Controls implemented in hardware that may or may not be hardwired to plant equipment.
- *Spatially-dedicated and continuously-available (SDCA) soft controls* - Soft controls that are spatially dedicated on VDUs so that they are always continuously availability to users.
- *Retrievable soft controls* – Soft controls that have to be retrieved from the computer-system and displayed on a VDU so users can operate them.

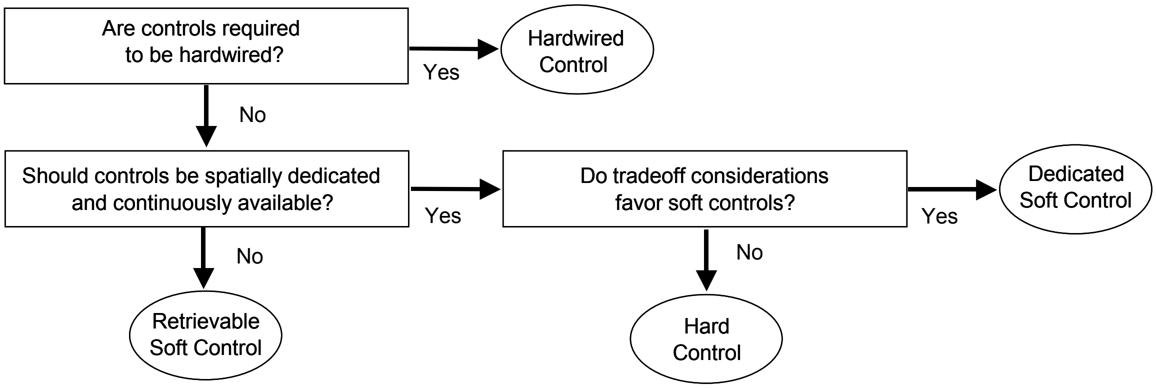


Figure 4-31
Deciding Between Types of Controls

⇒ 4.3.3-1 Identify hardwired controls that are required by regulation or needed for diversity from the computer system.

The Nuclear Regulatory Commission (NRC) has generally taken the position that sufficient hardwired, spatially-dedicated controls and displays should be provided in the main control room of an NPP to supply one train of equipment for each of the five main critical safety functions (CSFs) described for the safety parameter display system (NUREG-1342), namely: reactivity control, core cooling and heat removal, reactor coolant system (RCS) integrity, radioactivity control, and containment conditions. NUREG-0800 Branch Technical Position HICB-19 (Position 4) states that these controls and displays shall provide for manual, system-level actuation of CSFs and monitoring of parameters that support the safety functions. The manual capability should consist of hardwired, system-level controls and displays. Diverse means may be a non-safety system, automatic, or manual action. *Note that the regulatory criteria are modified over time, so the most current requirements should be consulted at the time these decisions are being made.*

There may also be controls that, while not of regulatory concern, should be hardwired so that actions can be taken independent from the computer system. An example may be “kill” or trip switches for important equipment where personnel safety or equipment protection is of concern. These controls may also be soft controls.

⇒ 4.3.3-2 Determine the need for spatial dedication and continuous availability. Consider using spatially dedicated, continuously available controls (hard or soft) when the user’s tasks require rapid action, highly-reliable response, or frequent access to controls.

SDCA controls are always immediately available to the user for either taking control actions. While hard controls are always SDCA, soft controls can be as well. Dedicated VDUs can be used to display a set of soft controls that do not have to be accessed.

When controls are not SDCA, they have the potential to impact user performance in two ways. First, since the controls have to be accessed before they can be used, task time is increased. Second, the actions associated with retrieving the control can be distracting. Therefore, SDCA controls (either hard or soft controls) should be when the following conditions exist:

- The user has to take actions rapidly (within a few seconds). Retrievable soft control access is typically a multi-step process, e.g., accessing the soft control from a selection display, providing the input, and confirming the desired action. When the time it takes to access a soft control in the computer system is unacceptable, then the control should be SDCA. There are very few tasks in a nuclear power plant that are required to be rapid, so this criterion will not apply very often. Examples that may fall under this are: manual reactor scram or immediate actions for an anticipated transient without scram (ATWS) event. The designer should consider not just the time to access a single control, but the time needed to access several controls in rapid succession and its overall effect on task performance. Task in this sense means a series of decisions/actions which together achieve some goal or purpose and need to be considered together.

- The user action must be highly reliable. The human error probability (HEP) may be increased when controls have to be accessed from a computer system. The reasons are that the status of the control may not be immediately monitored, the time to respond may be longer, and the possibility of accessing the wrong control may be increased. The shift of attention from process control tasks to display navigation and retrieval (and then back again) can potentially be a distracting activity. Shifting attention in this way is one of the well-known mechanisms of human error. SDCA controls should be considered for these types of actions. Probabilistic safety assessment (PSA) studies can help in identifying any such actions. For example, those actions that are risk important should be evaluated in terms of the difference in risk between SDCA and retrievable controls. In most cases, the difference in risk will be insignificant.

- The control is frequently used. A SDCA control should be considered when a particular control action is done very often in order to minimize the time it would take to frequently access the control.

Note that the characteristics of rapid action, highly reliable response and frequent action also make tasks candidates for automation, see Section 3.3.3 on Functional Requirements Analysis and Function Allocation. The new I&C system may support such changes in automation.

When controls do not need to be SDCA, then they can be implemented as retrievable soft controls.

For controls that should be SDCA, the decision needs to be made whether to implement the control as a hard control or a dedicated soft control (see Guideline 4.3.3-3). However, even when the analysis indicates that a control should be SDCA, it may be desirable to provide a retrievable control as well for use in other displays, such as procedures or locations remote from the dedicated display.

⇒ 4.3.3-3 Determine whether tradeoffs favor a hard or soft control implementation.

A large number of factors enter into the decision as to whether to implement a control in hard of soft control technology. Some general rules of thumb are summarized below and detailed considerations are presented in Table 4-14. A discussion each consideration follows after the table.

The most significant considerations in determining whether to implement controls in hard and soft technology are endpoint vision, scope of I&C modification, and impact on user tasks. These considerations lead to two fundamental approaches to control. A utility will probably want to use a basically hard control approach when:

- The endpoint vision calls for minimal impact of HSI technology in the control room.
- The HSIs and underlying I&C are not impacted by the modernization program.
- Plant systems and I&C changes have not altered the ways users do their tasks.

By contrast, a utility will probably want to use a basically soft control approach when:

- The endpoint vision calls for extensive modernization of plant HSIs and seated operations.
- The HSIs and underlying I&C are significantly changed by the modernization program.
- Plant systems and I&C have altered the ways users do their tasks.

In the former approach, the utility will stay primarily with hard controls and use soft controls sparingly and only where necessary. In the latter approach, the utility will implement as much as possible in soft controls and will use hard controls only where necessary.

In addition to establishing a basic approach based on the considerations identified above, there are a number of "lower-level" considerations that may lead a utility to favor soft or hard controls. These considerations are summarized in Table 4-14 and discussed further below.

Table 4-14
Typical Profile of Hard and Soft Control Features

Consideration[1]	Hard Control	Soft Control
1. Endpoint vision	Minimal impact on CR	More advanced CR
2. Scope of I&C modifications	Limited and "black box"	Extensive
3. Impact on user tasks	Task not changed much	Tasks changed considerably
4. Panel space	Not an issue	Limited
5. Flexibility of Location	Unnecessary	Desirable
6. Integration of HSI resources	Unnecessary	Desirable
7. Improve related information	Not an issue	Desirable
8. Flexibility of function	Limited	Desirable
9. Enhance error tolerance	Sufficient as is	Improve
10. Modifiability of controls	Unnecessary	Desirable
11. Separate controls and computer input devices	Desirable	Not an issue
12. Importance of tactile feedback	High	Low

[1] The numbers on each of these considerations corresponds to numbered paragraphs below where a discussion the consideration is provided.

1. *Endpoint vision* – Once the required hardwired controls are identified, the next consideration is whether a hard or soft is suggested by general considerations. There are several considerations that may dictate the preference for one or the other, including the endpoint vision of where the utility would like to see their control room finally end up when all modifications are completed. Some options are a control room using mostly soft controls, partial soft controls or a hard control room with selected upgrades. For example, if the endpoint vision is for a primarily seated workstation based control room with a great deal of flexibility, then a soft control approach is suggested.

2. *Scope of I&C modifications* – I&C considerations are important. A utility may be concerned about such considerations as (1) compatibility with existing I&C equipment in the plant or control room, (2) capabilities/functions in the equipment available for selection, and (3) coordinating the phases of soft control implementation in the control room with the digital I&C modernizations in plant systems. These considerations may lead to the selection of hard or soft control approaches for various aspects of the modernization project.

3. *Impact on user tasks* – If the modification has not changed the functions and tasks of the operators, then there may be less incentive to go to a soft control approach (unless required by the new I&C equipment). However, if the systems or components operate differently after the modification, then there is a strong incentive not to use the old hard controls. Of course, this decision will be dependent on overall decisions regarding control system

platforms and the associated impact on concept of operations. One should try to avoid requiring users to operate a mixture of hard and soft controls for the same task. To the greatest extent possible, users should not have to move back and forth between hard controls on panels and soft controls at workstations while performing a single task.

4. *Panel space* – Many soft controls can be made available to users through a single VDU. Thus panel space is not needed for each individual control, as is the case for hard controls. An example of where this can be useful is a modification that results in more controls than the existing panel would accommodate. In that case the use of a soft control interface could be used to avoid awkward and hard to use control arrangements.

5. *Flexibility of Location* – Soft controls can typically be retrieved at different locations, such as from VDUs at different workstations in the control room, or at panels outside the control room. Thus, users can access the controls where they are, rather than having to go to where the control is, as is the case with hard controls.

6. *Integration of HSI resources* – Soft controls provide an opportunity for much better integration of HSI resources. For example, soft controls can be integrated into relevant alarm and procedure displays. Similarly, alarms and other information can be integrated into the soft control display itself. Thus a degree of HSI integration is possible that does not exist with conventional HSIs.

7. *Improve related information* – A soft control display can include information specifically tailored to the specific control actions being taken. For example, the soft control display can show the comparison between a current parameter value and the value the user set using the soft control. In addition, this information is located right where that control action is being taken. This improves the information and feedback to the users that is not easily provided with hard controls. In addition, a soft control display can include information about the control logic and constraints such as interlocks that make it easier for the user to determine when an appropriate action can be taken and to quickly determine why a desired control action was not executed.

8. *Control flexibility* – Hard controls are typically associated with one control action. In this sense they are not flexible. Soft controls, on the other hand, can allow the user to adapt the HSI to changing needs or conditions of use. For example, the user may be able to arrange the presentation of the control and its associated information based on a current need or personal preference. Alternatively, the control and information may be automatically arranged by the computer based on the current situation or plant mode. Soft controls also offer the capability to accommodate different control actions in various modes. They can perform a range of control functions, each representing a different mode (e.g., mode 1 for performing function A, and mode 2 for performing function B). The behavior of these functions is defined by the software. When the user carries out a control action, the software converts the input into a signal for the control system. Hence, a specific action, such as pressing a button, can produce different results depending on such factors as the particular display page currently accessed, the status of the control system, and the status of the plant.

9. *Enhance fault tolerance* – Since digital systems provide enhanced capability to provide smart interlocks, the screen-based control can provide more informative feedback to users about the acceptability of their inputs to protect the system against incorrect user control inputs.

10. *Modifiability of controls* – Since soft controls are implemented in software, it is easier to add a new soft control or to modify any aspect of an existing soft control than is possible with hard controls.

11. *Separate controls and computer input devices* – When hard controls are used, they typically effect plant equipment, e.g., start a pump. When soft controls are used, the same input devices and displays are used for both plant and HSI control. For example, a user may use a mouse and VDU to access a display, and then use the same mouse and VDU to operate a piece of plant equipment (e.g., a pump) from that display. In this case, the mouse and VDU are used to operate both the HSI and the plant. This is both good and bad. It is good because the number of devices in the control room is reduced and the user can transition between plant control and interface management tasks without shifting to different displays and input devices. On the other hand, it forces actions to be serial and can potentially result in errors from inadvertently doing one thing when the other was intended.

12. *Importance of tactile feedback* – Hard control can often be operated by feel (using proprioceptive feedback). Users can feel the movement of the control and can often associate the extent of the movement with the magnitude of the control input. Since users do not need to look on the control itself, they can look at the associated display.

Once it is decided which control will be implemented as soft controls, the guidance included in this section can be used. If guidance is needed on the design and layout of hard controls, it can be found in the many existing guidance documents, including:

- NUREG-0700
- IEC 1227
- EPRI-NP 3659.

For retrievable soft controls, both selection displays and control displays have to be designed. This guidance is provided in the next two sections, 4.3.4 and 4.3.5, respectively. For SDCA soft controls, no selection display is needed since they are always available to users. To design a SDCA display, proceed directly to Section 4.3.6.

4.3.4 Selection Displays

A selection display shows the user the items for which soft controls are available. When the user selects the item to be controlled from the display, a control display for the item is displayed.

Guidelines for selection display design are provided below.

⇒ 4.3.4-1 Provide flexible approaches to soft control selection.

There are many possible ways to enable users to retrieve soft control displays. The choice among them is, to a large degree, related to the design of other aspects of the information system, as will be discussed below. The design can include combinations of these approaches to provide flexibility to users needing to access soft controls.

Two common approaches are to provide access to soft controls through mimic displays and through menus. Mimic displays are good because the item to be controlled can be seen in the context of the other components it is related to. Menus are good because groups of components can be accessed in one convenient place. When selecting controls from mimic displays, for example, the user can place a cursor on the component's icon and click to open the component's control window. The left side of Figure 4-32 illustrates this approach. (Note that the figure is simplified and only meant to illustrate the points being discussed.) A menu is a display format that shows a list of alternatives. Selection may be made by clicking on the desired component. Other means of selecting from a menu can be implemented as well, such as using function keys or push buttons. The right side of Figure 4-32 illustrates this approach.

Other forms of selecting items to be controlled are also possible. If the information system provides for task-based displays or computerized procedures, these displays can provide direct selection of appropriate control displays. For example, if a procedure step indicates that pump A should be started, the display could automatically open the needed control display or a link to the display could be provided to open the control display for pump A. Similarly, if alarm response procedures are computerized, access to control from those procedures can be provided. Yet another approach is to provide access to control displays directly from messages that the user receives from the system indicating that control actions are needed.

Users may also be provided a dialog box into which they can type an item identification code to retrieve the control display. However, as is noted in the guidance below, such an approach is not recommended because it relies on recall and it involves typing codes, both of which can be error prone.

Based on how the display system is designed, providing several ways to access control displays can support the user in retrieving the appropriate displays in the most convenient way at the time the control is needed. Thus, it should be considered. As with any aspect of HSI flexibility, its benefits have to be weighed against the increase in complexity of the design, training, and crew decision-making that can negatively impact performance.

⇒ 4.3.4-2 The design of the HSI should clearly distinguish between control actions and interface management actions.

A display, such as a mimic may have areas of the screen that can be used for navigation and areas that can be used to access soft controls. When users look at a display, it should be obvious which is which. This can be accomplished, for example, by using a different symbol to indicate controls from other operations that can be performed using the interface.

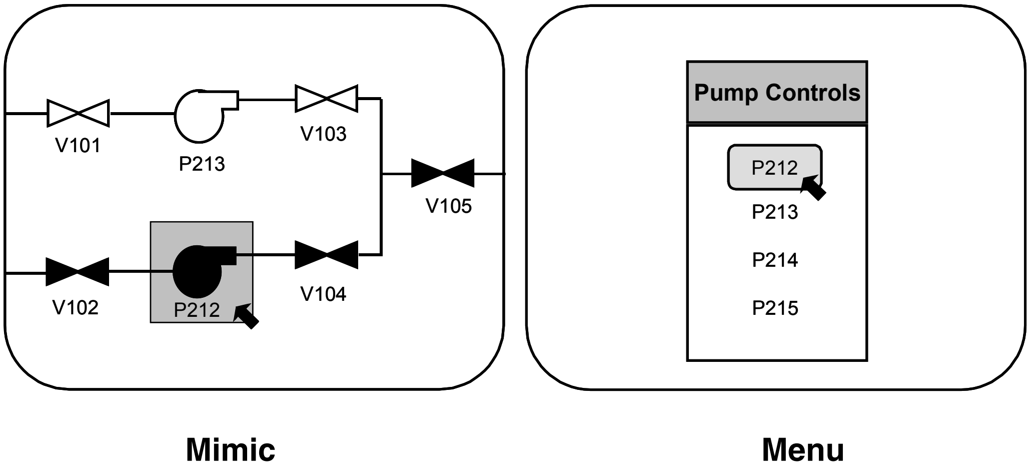


Figure 4-32
Two Displays for Selecting Items to be Controlled (With On-Screen Cursor)

⇒ 4.3.4-3 The selection display should be clearly and prominently labeled to identify the set of items being presented.

⇒ 4.3.4-4 The display should clearly indicate what items can be selected for control and the items themselves should be visually distinct.

The representation of items within the selection display should be visually distinct to support their correct selection. For example, the loops of multiple-loop controls should be clearly identified to prevent the selection or use of the wrong loop.

⇒ 4.3.4-5 The selection display should support the identification of items based on recognition rather than recall.

Menus and mimic displays facilitate recognition because the items are presented. All the user needs to do is know which he wants to control. Command language can also be used for selection, e.g., typing in a code for an item to be controlled. However, typing is slower and more error prone than selection and may require users to remember identification codes.

⇒ 4.3.4-6 Selection of an item from a display should require simple input actions.

Multi-step or complex input operations, such as transcribing identification codes, should be avoided.

⇒ 4.3.4-7 The selection display should provide feedback to the user of the items that have been selected.

For example, the icon or name of the component can be highlighted to indicate that the component has been selected.

4.3.5 Control Displays

Once a selection of an item is made, a control display is provided for making the control action and monitoring its effects. Control displays contain input fields where users enter commands to the control system. Guidelines for Control Displays are provided in this section and organized into the following sections: item identification; display of control logic, modes, and constraints; control input; feedback and monitoring; error detection and correction; and display and input devices.

4.3.5.1 Identification and Management of Control Displays

⇒ 4.3.5.1-1 A clear link should be provided between the selection display and the control display.

The users should be able to readily verify that the control display they are about to use is the one they selected. Highlighting of the item on the mimic display or in the selection menu is one way to accomplish this. This is especially important if the control display is on a separate VDU from the selection display and in cases where there are several control displays open at one time.

⇒ 4.3.5.1-2 The item to be controlled should be clearly and prominently identified in the control display.

The display should include the same identifying information as the selection display, but can include more descriptive information such as the item's system or train. This type of information provides a context for the control and can help minimize accidental operation of the wrong item to be controlled.

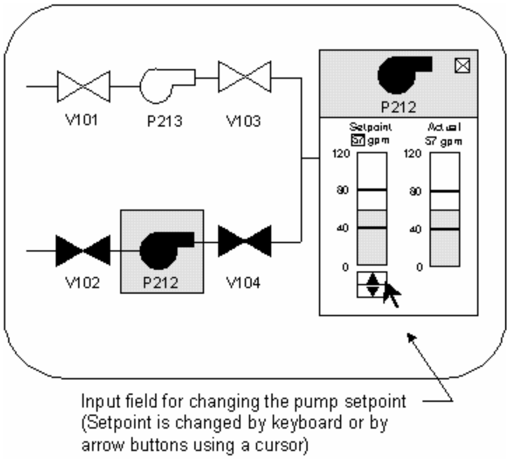
⇒ 4.3.5.1-3 The control display should not obscure associated information. If this is not possible, a means should be provided for viewing information that may be concealed by the control display.

When the selection display is a mimic-type process display, the control display may be presented directly on the mimic (see Figure 4-33.), or it may be presented on a separate display device, such as a second VDU (see Figure 4-34). A similar approach to the latte is to provide a dedicated area of the screen in which to displays controls. The tradeoffs between these different approaches are summarized in Table 4-15 below.

Except for the situation where a soft control is very simple and only one or two will be open at one time, it is probably better to present the control display on a separate VDU or in a dedicated area of a VDU screen and not superimposed on the data display.

Table 4-15
Typical Profile of Hard and Soft Control Features

Control Location	Advantages	Disadvantages
On selection screen (see Figure 4-33)	Close association of item and control. Rapid access to control following selection.	Control display may obscure data. Control display size is limited. Limited number of control displays can be presented at one time.
On separate screen (see Figure 4-34)	No data is obscured. More control related information can be provided. Multiple control displays can be open at one time.	Increased opportunity for operating wrong control. Display management workload may be increased.



Input field for changing the pump setpoint (Setpoint is changed by keyboard or by arrow buttons using a cursor)

Figure 4-33
Soft Control Input Field is a Window within the Selection Display

⇒ 4.3.5.1-4 When multiple control displays are opened at the same location, their unique identification should be visible

Multiple control displays can be offset ("cascaded") to show their identification. It should be noted that there are risks to having many windows open. Window management can become a source of workload and can cause confusion possibly leading to the control of the wrong component.

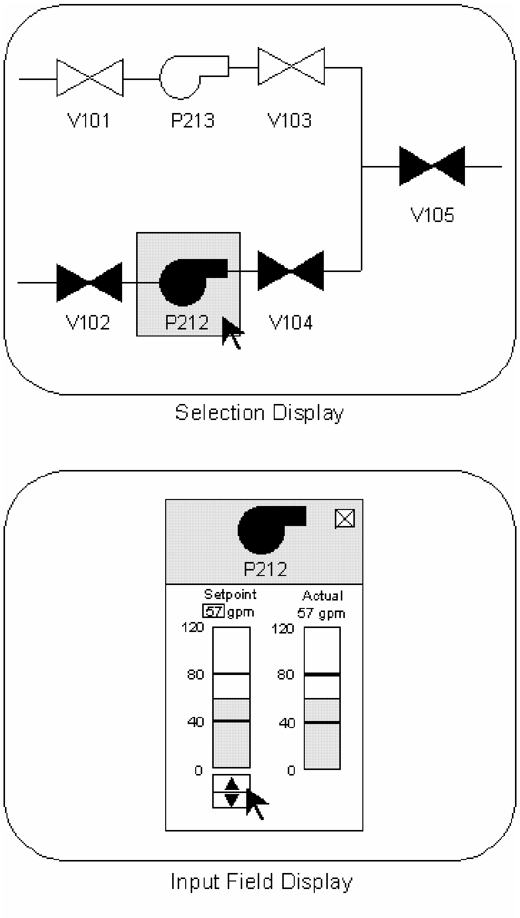


Figure 4-34
Soft Control Input Field and Selection Display are on Separate Display Devices

4.3.5.2 Display of Control Modes, Logic, and Constraints

Soft controls provide an opportunity to provide information that can support the user in making and modifying control actions. This information includes:

- The current and available mode for soft control operations
- The current and available control options
- The control logic, timing, and deadband
- Any constraints (interlocks, lockouts, and lockins) that may affect the control actions, and
- The status of plant systems and components that are affected by the control action.

Modes occur in soft controls when it is designed for more than one function. For example, a soft control that is used for manipulating multiple variables may have a separate mode for each one (e.g., individual modes for variables A, B, and C). In addition, there may be multiple modes for a single variable, each allowing it to be controlled in a different way (e.g., variable A may have separate modes for manual control, automatic control, and testing).

An interlock is a feature that requires user actions to proceed in a specific sequence. A lockout prevents personnel from providing input that may generate a negative effect, e.g., lockouts may restrict inputs to a specific, predefined range or set of values. Context-sensitive lockouts may restrict input values based on the current situation. A lockin keeps an ongoing operation active by preventing personnel from terminating it prematurely.

⇒ 4.3.5.2-1 When the soft control can be operated in more than one mode, the current mode should be clearly and prominently identified and the other mode options should be available.

Good labeling practices can help users avoid mode errors, which occur when the user believes the device is in one mode when it is in another and, as a result, performs an inappropriate input action.

⇒ 4.3.5.2-2 Higher-level controls should be considered for common operational situations.

The I&C upgrade may provide opportunities to implement some control at higher levels that currently exist in a given plant. Higher-level controls can improve performance reliability and lower user workload by allowing user to specify higher-level controls that allow the control system to manage the sequence and timing of lower level actions. Figure 4-35 provides an illustration. In the Figure, the user selects a flow path from the control menu. The selection is highlighted on the data display on the left. Once selected, the computer controls the sequence of valve and pump operations and their timing. As an example, the control system would first ensure the preconditions are satisfied, such as the availability of a suction source. Assume that we are starting with all valves closed and both pumps off. The control system would then open valves V101 and V105, start pump P213, open valve V103, and finally throttle valve V105 to correct the flow rate. At an even higher level, the user may be able to select commands such as “Borate” or “Dilute” with Flow Path A or B and the control system would coordinate the actions of the entire system to borate to an operator specified value.

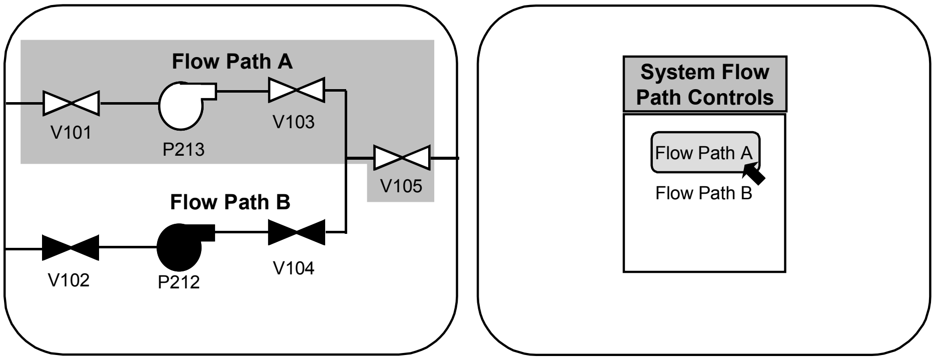


Figure 4-35
High-Level Controls

In more advanced systems, techniques based on artificial intelligence may be used to automate skill and rule based tasks. Some fossil plants, for example, use neural nets in their process control system.

⇒ 4.3.5.2-3 Information defining the control logic should be available to help personnel properly perform control functions.

This can be accomplished in a number of ways and to varying levels of specificity. The design needs and design specifics will vary by control application. At the lowest level of implementation, the design can have a drop-down display that shows the control logic scheme. At a more detailed level of implementation, the design can inform the users where the controller currently is in the control logic sequence and, therefore, what the next control action (that they are expected to take) is. It can also illustrate what interlocks exist and are currently in force.

⇒ 4.3.5.2-4 Timing requirements should be considered in the design of soft controls.

Timing requirements are important for the display of controlled variables. The design should consider the operator's needs for updated information in conjunction with the rate that monitored parameters could physically change. Then they should ensure that the update rate supports these factors.

Also, timing requirements need to be considered for the sample rate of the feedback signal used for process controllers. Oscillations of a poorly performing control systems or oscillations in the process should also be considered in the design of the HSI. Failures of control systems that lead to instabilities should be considered in the specification of I&C requirements.

⇒ 4.3.5.2-5 Deadband should be displayed where appropriate and important for the operators' understanding of the control response.

Deadbands are provided in the design of many control systems to prevent wear out from continuous operation. A deadband can easily be incorporated into a display of the error signal. The deadband for a control system, such as the pressurizer control on a PWR, is important information and should be available to the operator. For example, if a control system does not respond once error is outside its deadband, then it has failed and the operators can then take correct actions, if this information is available to them.

⇒ 4.3.5.2-6 Error signals for control systems should be supplied for selected controls.

The error signal is the difference between the set point and the feedback signal in an automatic control. The human user should not have to subtract demand signal from the feedback signal to determine the error in the control system. By monitoring the error signal of an automatic control system, the performance of the system can be assessed. The rate of change of the error signal may in certain cases also provide useful information to operators. But the designers should not include information that is superfluous, too difficult to understand, or that is prone to misinterpretation.

⇒ 4.3.5.2-7 A soft control display should allow users to quickly assess the status of individual components affected by the control.

⇒ 4.3.5.2-8 Information concerning interlocks, lockouts, and lockins related to the control action should be available to help personnel properly perform control functions. The user should be notified when interlocks, lockouts, and lockins are in effect and which actions are being blocked and what conditions activated the block.

It is a good practice to provide displays that reveal any such constraints that impact the control action. This will enable users to understand when actions cannot be taken as planned and trouble shoot if a problem occurs.

When a lockout blocks inputs that it considers unacceptable or not achievable, the user should be able to determine why the input was blocked and what inputs are acceptable, especially for context-sensitive validation in which complicated rules may be used for assessing the acceptability of an input value. An interlock should inform the user of the condition(s) that activated it and the conditions that must be satisfied to release it. Lockin features should show the user what action is being 'locked in' (i.e., the action that is being caused to operate without interruptions) and how it can be canceled.

⇒ 4.3.5.2-9 An interlock, lockout, or lockin should not initiate an action that was previously blocked merely because the status of the triggering condition has changed.

If a user initiates operation B, but it is blocked because condition A was not satisfied, the system should not automatically start operation B when condition A is met. Instead, a separate action should be required (e.g., the user should be required to take a specific action to allow operation B to resume).

4.3.5.3 Control Input and Commands

A command is an instruction to a computer or system demanding an action. Users provide commands to the soft control system using discrete-adjustment and continuous-adjustment inputs.

A discrete-adjustment input involves selecting the desired option from a set of defined options. Many control actions involve making a selection from a discrete set of states. For example, plant breakers and valves may be changed from the open to the closed state. Automatic controllers often have discrete control modes (e.g., manual, automatic, and cascade). Their operation is similar to physical controls that provide discrete adjustment, such as push buttons and switches.

A continuous-adjustment input involves providing a value from a continuous range, e.g., when changing a control setpoint, the user increases or decreases the setting of a controller within a defined range. Continuous variables are often set using continuous-adjustment controls.

This section also addresses error tolerance and correction.

4.3.5.3.1 General Control Input Guidance

⇒ 4.3.5.3.1-1 The control display should be labeled and contain clear information to identify the item being controlled.

⇒ 4.3.5.3.1-2 The control input field should clearly and predominantly identify the aspect of the item that is being controlled.

The design of a soft control should provide a conspicuous link between the input field and the corresponding variable or component. Starting at the input field, the user should be able to quickly trace the component or variable back to its representation in the display that was used to select it. One example of how this can be accomplished is graphic coding. Graphic codes, such as borders, symbols, and colors, may be applied to both the representation of the component in the display from which it was selected and to the input field, making a strong visual association between them.

⇒ 4.3.5.3.1-3 The control options should be clearly presented and easily distinguished from each other.

⇒ 4.3.5.3.1-4 The user interaction with the control display should minimize the possibility of initiating a control action if the visual display is not working properly.

One potential problem with touch screens, for example, is that sometimes their buttons may remain active even though the video image is not visible. Thus, a user could touch a blank screen and provide a valid input. Such problems may be avoided by requiring multiple actions, such as separate selection and activation steps, for inputs that may have serious consequences (e.g., affect the operation of plant equipment).

⇒ 4.3.5.3.1-5 If an input device controls more than one variable, the user should not have to reset the device to match the value of the new variable before executing a control action.

When switching between variables, the control should automatically display the current value of that variable and position the input device consistent with that value. The user should not be required to adjust the input device to match the current value of a new variable. For example, if variable A is currently set at a value of 100 and variable B at 10, when selecting the latter, the user should not be required to adjust the input device to the 10 position before executing a control action.

⇒ 4.3.5.3.1-6 If multiple soft controls are needed for a particular task, they should be retrievable as a predefined group.

This practice should help minimize the workload and time associated with retrieving multiple soft control displays.

⇒ 4.3.5.3.1-7 If keyboard input is used for a soft control, the input should be displayed in an input field on the control display and the control should not be acted on until a confirming response is made, such as hitting the return or enter key.

Keyboard entry, while often faster than other input techniques, can be error prone. It is very easy, for example, to transpose numbers or to accidentally hit two keys and, therefore, include an extra digit in the control input. Therefore, the input should be clearly displayed and require an "enter" (or similar) command.

4.3.5.3.2 Discrete-Adjustment Controls

The most common discrete-adjustment interfaces used with soft controls are individual buttons and radio buttons (a group of buttons representing a set of related options). However, other formats also are possible, such as rotary selector dials operated via cursor.

⇒ 4.3.5.3.2-1 Discrete-adjustment controls should be used for selecting among a set of individual settings or values.

Discrete-adjustment controls are preferred when the user must select one option from a limited number of choices, or when precision requirements are such that a limited number of settings can represent the entire continuum of values.

⇒ 4.3.5.3.2-2 Discrete-adjustment controls should indicate which setting was selected.

⇒ 4.3.5.3.2-3 If a discrete-adjustment control initiates continuous operation, it should provide continuous indication on the current state.

A continuous-operation control continues to produce an effect until the user provides the next input, or until a predefined action sequence is stopped by a termination criterion. An example is a button that changes to the activated state when pressed and remains in that state until it is pressed again. An example of continuous feedback in a soft control is a checkbox format in which an 'X' appears in the box to indicate that an option has been selected, and disappears only after the option is de-selected.

4.3.5.3.3 Continuous-Adjustment Controls

A common screen element for providing continuous-adjustment control is a soft slider (also called a slider bar or a scroll bar). It is an input format used to directly manipulate a variable over a set range of values. Soft sliders are typically maneuvered via pointing interfaces, such as a touch screen or mouse. They may require careful hand-eye coordination to ensure that the pointing device does not leave the linear path of the slider nor overshoot or undershoot the intended target. If the user's tasks do not permit careful hand-eye coordination, then other interfaces, such as arrow keys, should be used. The slider sometimes is combined with arrow buttons.

⇒ 4.3.5.3.3-1 Continuous-adjustment controls should be used when precise adjustments along a continuum are needed or when many discrete settings are present.

Because these controls often require a gross movement followed by fine adjustments, setting them correctly may require more time and attention than discrete input formats. Therefore, they should not be used in place of a discrete-adjustment interface for selecting from a small set of options.

⇒ 4.3.5.3.3-2 Reference values should be provided to help users judge the appropriateness of values when entering continuous variable inputs.

Reference values commonly used in process control applications include the variable's range, alarm limits, and the current value.

⇒ 4.3.5.3.3-3 When part of the range of values depicted by a continuous-adjustment control represents critical information, such as alarm limits, those values should be coded to facilitate recognition.

For example, on horizontal sliders, the low value should be on the left and the high value on the right. For vertical sliders, the low value should be on the bottom and the high value on the top. Graphical codes may be applied to distinguish the normal operating range, alarm limits, and other abnormal operating ranges.

⇒ 4.3.5.3.3-4 The value to which a continuous-adjustment control is set should be digitally displayed.

⇒ 4.3.5.3.3-5 The physical size of the continuous-adjustment control should allow the user to read the current and target values with the required precision and accuracy.

For example, the length of the slider is determined, in part, by the range of values depicted, the increments between individual values, the degree of precision required for reading the slider's position, and the user's expected viewing distance. The accuracy with which the slider may be positioned may be affected by characteristics of the input device (e.g., mouse devices may allow more accurate positioning than a touch interface due to the size and shape of the finger). A very short slider may be difficult to read or position precisely. A very long slider may produce slow response times due to the long distance that must be traveled and the need to keep the pointing device on its linear path.

⇒ 4.3.5.3.3-6 A means of providing incremental increases or decreases in demanded values should be provided when precise inputs are needed. Each press of an arrow button should change the current value uniformly.

One means of providing such input is arrow buttons. In addition, values may change continuously if a button is held down. Some soft controls have two sets of arrow buttons, one for small and one for large incremental changes. Arrow buttons are sometimes combined with a slider in a soft control. A common practice is to have the input value change by the smallest unit of precision presented by the soft control device for each press of the arrow button. For example, if the soft control presents a variable to one decimal place, then one press of the arrow button will change the value by one tenth (e.g., increase the value from 10.1 to 10.2). If the variable is presented in integer values, then one button press will change the current value to the next integer (e.g., increase the value from 11 to 12). If a variable has a wide range, executing a large change in the value may require pressing the button many times or holding it down for a long time. Some soft controls feature a second set of arrow buttons that can change the input value by a larger amount for each button press. For example, single arrow buttons [>] may be used for making small changes and double arrow [>>] buttons for making large ones. The size of the increment provided by the double arrow buttons may be configured for each soft control. Common values for the double arrow buttons are 2%, 3%, 5%, or 10% of the range of the instrument. Other values may be programmed. Often holding down a button will increase the rate of change.

⇒ 4.3.5.3.3-7 Incremental input devices should provide salient feedback when they are actuated.

Feedback should be sustained when the button is held down. If a button is momentarily pressed, the feedback should be momentary also. However, the continuous feedback should not be a source of irritation to users, such as a loud or piercing sound. In noisy environments the feedback may not be heard at all thus non auditory forms of feedback may be more appropriate such as visual feedback.

4.3.5.3.4 Error Tolerance and Correction

Soft control systems should be as error tolerant as possible. Error tolerance means helping to eliminate user errors where possible, providing means for users to detect errors when they make them, and to minimize to impact of errors when they occur. Section 4.3.8, an appendix to this section discusses some common control errors and design features to minimize them.

Many engineered control system features help guard against errors in control actions. The guidance in this section is intended to provide an added measure of error tolerance.

⇒ 4.3.5.3.4-1 Where possible, a command entry field should show valid value range and the expected number entry format, e.g. 0.XX or XX.XXX as well as a default value.

This type of input format can help minimize error of data entry.

⇒ 4.3.5.3.4-2 Confirmation steps should be considered and, where used, implemented as a separate user input from control actions.

Confirmation steps are steps added to the input action. They should be considered for significant control actions and where system error checking in not sufficient and where response time permits. One approach is to display a message box seeking confirmation of the command. Confirmation steps reduce the likelihood of errors by delaying the control response and drawing users’ attention to the command. However, they can lose their effectiveness if users can perform them unconsciously as part of the input action. When feasible, confirmation steps should draw attention to the goal of the action, not just to the action. The potential benefits of confirmation steps should be weighed by comparing their effects on the user’s response time (e.g., potential delays) to the potential consequences associated with the errors that are being guarded against.

⇒ 4.3.5.3.4-3 User control input verification should be considered.

The soft control system can examine the users input and check it against predefined criteria to help ensure that the input is reasonable. For example, if the user enters a value that is outside of the acceptable range or selects an unacceptable command, the system should alert the user by:

- Visual cues (e.g., changes in symbols to indicate that the user entry is not acceptable or that the selected option is not available),
- Warning messages (e.g., a description of the problem), or
- Auditory tones (e.g., a tone that directs the user’s attention to the problem).

When alerts are given, users should be able to obtain information at lower, more detailed levels, such as describing how the action was performed and why it was inappropriate for the goal. However, user input checking requires that unacceptable values can be defined in advance. It also requires that a time delay for the checking and verification is acceptable.

⇒ 4.3.5.3.4-4 A specific command that produces one action in one mode should not cause a different action in another mode.

⇒ 4.3.5.3.4-5 Unique commands associated with actions that have important consequences should not be easily confused with other commands used in the same or different modes.

Reserving special commands for special actions can prevent mode errors because, if the command is entered while the device is in the wrong mode, it will not be accepted by the system. A unique or reserved command should not be so similar to other commands that a valid entry may result from incorrectly entering another command.

4.3.6 Feedback and Monitoring

The soft control system can provide feedback on the system’s acceptance of the user input, the controls system’s response to the command, and the achievement of the desired goal. These sources of feedback provide the means by which users can monitor the control actions.

⇒ 4.3.6-1 The soft control should display the user’s input in a way that allows the user to review it and determine whether it is correct.

Feedback can aid users in detecting input errors. A variety of text and graphical approaches can be used. For example, when the user enters a control setpoint, the value may be presented in text format by displaying the digits via the user interface. The setpoint may also be represented graphically. One commonly used format is the bar chart. The bar is usually depicted against a reference scale with its length or height corresponding to the magnitude of the input value. Text and graphic feedback may be combined. The input value may be depicted in both digital and bar chart formats.

Further, for control setpoints, reference values can be displayed that convey the implications of a new value and, thus, support the user in identifying a value that is too large or too small. Reference values include the actual value of the process variable, the current setpoint value, the normal operating limits, and the alarm limits. Graphical feedback might include a bar chart depicting the input value (i.e., the bar's length corresponds to the magnitude of the entered value). The reference values and the graphical representation may be combined.

⇒ 4.3.6-2 Immediate feedback should be provided that a command was received. Additional feedback should indicate whether the user's command is being acted upon and the current status of the item being controlled relative to the demanded status.

Feedback will help prevent users from inputting the same command over and over because of a delay in system response. For example, a user may use a soft control to operate a pump by entering a new (higher) control setpoint for pump speed. The soft control should provide feedback indicating whether the pump is responding to the new setpoint and what the current value is in comparison to the demanded value. That is, the user should be able to determine whether the speed of the pump is increasing toward the setpoint value. This type of feedback may be provided by the control display itself, or the soft control may be coordinated with plant displays that indicate system status.

Momentary controls, which operate only during actuation (e.g., while a button is pressed) should provide feedback during operation. Continuous-operation controls, which remain operating after actuation, should provide continuous feedback.

For single actions or sequential actions that involve significant wait times a "Time to Completion" indicator can be provided. This indication shows that the action has commenced and gives the operator and idea of how much longer (down counter) they will be waiting. This indicator can be a preconfigured value or may be based on a calculation (i.e., estimated Download Time).

⇒ 4.3.6-3 Feedback should indicate the status of sequential actions that are in progress.

Errors involving misordering of the steps of an action sequence include skipped, reversed, and repeated steps. Soft controls may be more prone to this type of slip than conventional controls because they introduce additional operations for accessing controls and displays and providing inputs that may also have sequential constraints on their execution. In addition, many control operations must be performed in particular sequences. For example, when configuring a fluid system, it may be necessary to establish the flow path, control mode, and setpoint of a flow controller in a specific sequence of operations (e.g., A, B, C, D, and E). One form of error occurs when a user skips a step thinking that it was completed. For example, a user may perform operations A, B, and C and after some delay or interruption, may perform operation E thinking that D already was finished. The repetitiveness of the task is a factor in this type of error. If a user has performed a set of operations repeatedly on several identical controllers, the memory of performing a particular operation on the other controllers may increase the likelihood of the user incorrectly concluding that the operation was completed on the present controller. Thus, the sequentiality of soft controls can interact with repetitive, sequential tasks to increase the probability of errors involving misordering the components of the action sequence. The display should support users in identifying tasks that are in progress; ideally, they should be designed so that the status of related operations (e.g., A, B, C, D, and E) can be checked at a glance from a single display.

⇒ 4.3.6-4 Systems that can change mode automatically should provide feedback to make the user aware of the current mode.

The soft control system should inform the user of the current operating mode, mode-transition points, limits on actions, and circumstances in which users must assume control. This feedback should help the user assume control without unnecessary actions and without unnecessarily disrupting plant systems and processes.

⇒ 4.3.6-5 Feedback should indicate when the demanded status is achieved.

For plant control actions, such as adjusting the flow rate of a feedwater pump, it is necessary that the user determine that the intended goal (e.g., increased steam generator level) is achieved. This type of feedback may be provided by the control display itself, or the soft control may be coordinated with plant displays that indicate system and plant status. For example, mimic displays may support the user in selecting plant components, monitoring the system's response, and monitoring goal achievement.

Feedback needs interface with I&C requirements, e.g. sample rate of plant parameter must be adequate to insure all significant information is captured and displayed to the operator and for use by control system.

4.3.7 Sources of Additional Information

There are very few standards, guidelines, or other documents that address the design of soft controls. A technically-oriented discussion can be found in the following document. It also provides references to other such documents.

Stubler, W., O'Hara, J., and Kramer, J. (2000). *Soft controls: Technical basis and human factors review guidance* (NUREG/CR-6635). Washington, D.C.: U.S. Nuclear Regulatory Commission.

For design of hard controls, see:

NUREG-0700
IEC 1227
EPRI-NP 3659

4.3.8 Appendix: Error Tolerant Design

Error tolerance means minimizing the occurrence of user errors, providing means for users to detect errors when they are made, and providing means to correct errors. One of the main ways a control system can guard against user errors is through the use of lockouts and interlocks. However, user interface design features can also incorporate error tolerance. The specific errors associated with soft controls mainly reflect "slips," that is, errors of execution where the user intends to do one thing but accomplishes another. Some of the common forms of these types of errors are:

- unintended actuation
- control input errors
- description error
- mode errors
- misordered action-sequence errors
- capture errors
- loss-of-activation errors
- time-induced errors

Each of these types of errors is defined below and some of the design features that support tolerance of them are presented.

Unintended Actuation – Unintended actuation occurs when a user inadvertently makes a control input. Design features to minimize this type of error include:

- require a two-step process: select and actuate
- require confirmation and/or provide an undo command capability
- provide recovery time, e.g., incorporate time delays so command can be terminated
- providing salient feedback that a control has been executed
- provide clear distinction between equipment controls and HSI controls, e.g., click on pump icon sends command to pump and not HSI to call a pump display

Control Input Errors – With many physical input devices, the size of the change in a variable is usually related to the amount of movement that the user applies to the control (i.e., the bigger the movement, the bigger the change). Soft controls do not always have this relationship. For example, when entering numerical values using a keyboard, large errors in the magnitude of input values can result from omitted, transposed, or added digits. This occurs because the magnitude of the input value is not directly related to the actions used to enter data. Design features to minimize this type of error include:

- display formats that provide better feedback about the magnitude of the entered values
- use of interfaces that cause inputs to be entered incrementally, such as arrow buttons

- arranging controls so that a context is provided, e.g., arranging several soft controls on the screen so that they are in the order they will be used
- warnings when a user input does not seem appropriate in the current context and the use of dialog boxes to clarify the users input

Description Error – Description errors occur when the information used to initiate a control action is ambiguous and leads to an incorrect action. For example, an operator wants to start a component, but selects the wrong one by pointing to the right type of icon located in the wrong position on the display. Design features to minimize this type of error include:

- ensure salient differences exist similar icons or formats so the user will discriminate between similar options
- separating similar options within displays
- arranging options to provide a context to support correct identification (e.g., grouping options by a characteristic such as function)
- making VDU displays similar to old physical displays

Mode Errors – Mode errors occur when a user makes an erroneous classification of the mode of a device. This may lead the user to perform operations that are appropriate for one mode when the device is in another mode. Design features to minimize this type of error include:

- eliminating modes (practical only in some cases)
- making modes very distinct to improve mode awareness
- coordinating acceptable inputs across modes such that the same input that produces a benign effect in one mode does not produce negative consequences in another mode

Misordered Action-Sequence Errors – Misordered action-sequence errors occur when steps within a sequence are skipped, reversed, and repeated. Soft controls may be more prone to this type of slip than conventional controls because they introduce additional operations (interface management tasks) for accessing controls and displays and providing inputs. Entering numerical values via a keypad is especially prone to these types of errors. Large errors in the magnitude of input values can result from omitted, transposed, or added digits. Design features to minimize this type of error include:

- provide more forgiving activation logic to give time to undo incorrect commands
- provide confirmation steps
- provide enhanced feedback regarding the status of sequential tasks
  - overview display of sequential operations
  - history display that describes recently performed control actions

Capture Errors – Capture errors occur when an action that is less frequently performed requires a sequence of operations that overlaps with the sequence for an action that is more frequently performed. When performing the less familiar action, the more familiar action is performed instead. This is because soft controls often require sequential interface management tasks, there may be more overlap in operation, e.g., different control actions may require similar navigation paths through display systems, similar dialogs, and manipulations of similar graphical objects. Design features to minimize this type of error include:

- design for discrimination
- clear labeling
- minimize the overlap of sequences to reduce the occurrence of these errors
- consolidate or eliminate unnecessary sequences
- bring these critical points in the action sequence to the user's attention, e.g., important choice points may be designed to be salient or require the user to focus attention on the choice point
- compare operator inputs to stated plans, goals, and intentions

Loss-of-Activation Errors – Loss-of-activation errors are one of the most common types of slips. They occur when events intercede between the preparation of a plan and its execution. One cause of loss-of-activation is the need to access many different displays. The attention shift can disrupt memory of task status. Design features to minimize this type of error include:

- provide task status displays that indicate completed, suspended, and pending tasks
- reminders of suspended tasks

Time-Induced Errors – Time induced errors are those that are caused by the time needed for control actions. Control time is the time it takes to close the control loop from the initiation of a control action to the feedback indicating the desired system change has occurred. There are many factors that contribute to this time: (1) time to execute the control action, (2) time lag between the control action taken at the HSI and when the signal reaches the actuation system, (3) system lag is the time it takes for the system to change in response to the control, and (4) feedback time is the time from the achievement of the goal state to changes in the HSI to indicate that the state has been achieved. While the effects of time lags are task dependent, long control times are usually associated with increased error and system instability. Design features to minimize this type of error include:

- use of time to complete indicators
- displays that provide a historical representation of the change in variables over time and that clearly indicate actual status vs. the control demand
- display of intervening process variables, those coming between control actions and change of the final process parameter of primary interest
- predictive displays and operator aids for "what if" planning. While seldom used in the nuclear industry, predictive displays and simulations have been successfully used in other systems having long time constants, e.g., collision avoidance systems in large ships.

4.4 Alarm Systems

4.4.1 Overview
4.4.2 Display Guidelines Checklist
4.4.3 General Considerations for Alarm Modifications
4.4.4 Alarm Definitions
4.4.5 Alarm Prioritization and Processing
4.4.6 Alarm Display
4.4.6.1 General Alarm Display Considerations
4.4.6.2 Display of Alarm Priority
4.4.6.3 Display of Alarm Status
4.4.6.4 Display of Shared Alarms
4.4.6.5 Coding of Alarms
4.4.6.6 Auditory Characteristics
4.4.6.7 Alarm Location
4.4.7 Alarm Control and Management
4.4.7.1 Alarm Controls
4.4.7.2 Alarm Management
4.4.8 Alarm Response Procedures
4.4.9 Sources of Additional Information

4.4.1 Overview

The operators' task of monitoring the operating condition of nuclear power plants and detecting problems can easily be overwhelming due to the large number of individual parameters and conditions involved. Therefore, operators are supported in these activities by alarms. Digital instrumentation and control (I&C) improvements offer the opportunity to make major improvements in a plant's alarms. Computer-based alarms provide increased capabilities that can make them more effective and provide added features not practical with conventional, hardwired alarm technology. Because the alarms are one of the primary means by which abnormalities and failures come to the attention of plant personnel, there is a major operational incentive to make them as effective as practical.

Alarms provide automated monitoring capability that alerts users via visual and auditory displays when parameters deviate from specified limits. The general functions of alarms are to:

- Alert the user to a system or process deviation
- Inform the user of the nature and priority of the deviation
- Guide the user's initial response to the deviation
- Confirm whether the user's response corrected the deviation.

While monitoring and detection is the primary purpose of alarms, in most plants they are used for other purposes as well, such as

- Providing an overall assessment of plant status (largely by the presence or absence of alarms in key systems)
- Determining the availability of systems and components (again, largely by the absence of alarms
- Diagnosing transients and events
- Supporting testing and maintenance (e.g., surveillance tests).

Alarms in many plants display information by means of arrays of alarm tiles. These panels are often supplemented by dedicated video displays of parameters related to specific systems or functions. In addition, many plants have alarms for other systems in the control room. For example, separate alarms are often provided on auxiliary panels such as radwaste processing, HVAC, switchyard equipment, or a fire alarm panel. Detailed information about alarms is often provided in alarm messages that are typed out on a printer ("alarm typer" or "alarm logger") or shown in lists on video displays. The existence of an incoming (i.e., new, not acknowledged) alarm is typically associated with an audio signal as well as flashing of the visual indication (e.g., alarm tile). Clearing conditions (i.e., parameters re-entering the normal range) are typically indicated by a different audio signal and different flash rate.

While alarms play an important role in plant operation, they have also posed challenges to the users. Common problems include:

- Too many alarms (this creates alarm overload and users cannot process all alarm information)
- Too many spurious or nuisance alarms (this contributes to alarm overload and may cause users to discount alarm information)
- Poor distinction between alarms and normal status indications (this can make it difficult to distinguish normal from abnormal conditions).

Digital I&C improvements offer the opportunity to improve alarms. Computer-based alarms provide increased capabilities designed to improve their effectiveness. They can handle more complex logic than can be implemented in hardwired, and they provide more flexibility in the display of alarm information. Some examples of how the added capabilities can be exploited are as follows:

- Processing logic can be used to eliminate nuisance or irrelevant alarms and reduce the number of alarms that occur in a transient.
- There are increased options for displaying alarm information so that instead of displaying alarms as separate information, alarms can be integrated into process displays to improve their association with related components, systems, and functions.
- Alarms can be integrated into other displays, such as electronic procedures and soft control displays, or presented on common or group view displays to help focus and coordinate the control room staff.

- Alarms can not only be integrated into the displays, but once this is accomplished, alarms can be used as part of these other HSI resources to provide, for example, alarms for entry conditions in emergency operating procedures (EOPs).
- Computer-based alarms can also allow users to add features, e.g., user-defined setpoints to help in monitoring.
- Alarm response procedures can be provided electronically, thereby providing rapid access to detailed information about the alarm without the need to consult books of procedures.
- Alarms can be designed with management facilities to enable personnel to sort alarms by time and by system, and to interrogate the alarms to obtain detailed information about those that are of specific interest.

At the same time, existing alarms have some advantages that should be retained as systems are upgraded to digital technology. For example, the fixed positions and patterns of existing alarm tiles provide an advantage in quickly assessing the state of the plant and in recognizing particular transients. Alarm message lists produced on a computer-driven display have some disadvantages when many alarms are occurring and the messages scroll quickly off the screen. Therefore, it is important that the new alarms be designed and implemented to take advantage of each technology and provide the needed improvement in effectiveness for the alarm users.

Also, it is important to recognize that the introduction of new, digital control and monitoring systems often results in a tendency to create many more alarms. This is due in part to the ease with which alarms can be generated from process information in a digital system. Also, self-diagnostic features of digital systems can provide many detailed alarms on problems or failures detected with the systems themselves. Proliferation of alarms can make the alarm overload problem worse and add to the administrative burden of managing the alarms and alarm response procedures.

This section addresses how the new digital alarm capabilities can be implemented effectively as part of control room modernization. It is recognized that not all modernization projects will require an extensive upgrading of the alarms or provide a practical opportunity for such major changes. However, virtually any new digital system will require some consideration of changes to the alarms, so the information provided in this section will help designers identify the options available to them and the human factors engineering principles that should be applied when making the changes.

From a human factors perspective, alarms have several aspects, illustrated in Figure 4-36. Following a discussion of the general considerations in addressing the alarms in a digital I&C upgrade project, each of the following aspects will be discussed and guidance provided on how they should be considered in the upgrade process.

The general considerations for alarm modifications are discussed within the context of the overall I&C modernization program. These include identifying what additional alarms will be needed and which of the current alarms may need to be modified. They also address the extent to which modifications will be made to the alarms. For significant modifications, the designer will need to consider such fundamental questions as:

- How alarms will be defined
- How alarms will be prioritized
- How the numbers of alarms can be reduced
- How alarms will be displayed to users and how they will be integrated into other displays
- How alarms will be coded for priority, status, and other relevant information
- Where the alarms will be located (overview panel, control panels, workstations, etc.)
- What control and alarm management features will be made available
- How alarm response procedures will be designed, modified, and implemented.

Design guidance for each of these aspects is given in this section.

As one considers the expanded functionality of alarms, it is important to distinguish between them and other user aids. The concept of an alarm can be expanded in time to provide alerts and early warning of equipment failure based on more intelligent condition monitoring for predictive maintenance purposes. Similarly, as plant data analysis becomes more intelligent, it can be applied to fault data in order to analyze the pattern of failures to diagnosis the event. Such predictive maintenance and disturbance analysis functions are not addressed in this section. While both of these are important topics, they are considered beyond basic alarms functionality and are addressed in Section 4.6, Computerized Operator Support Systems.

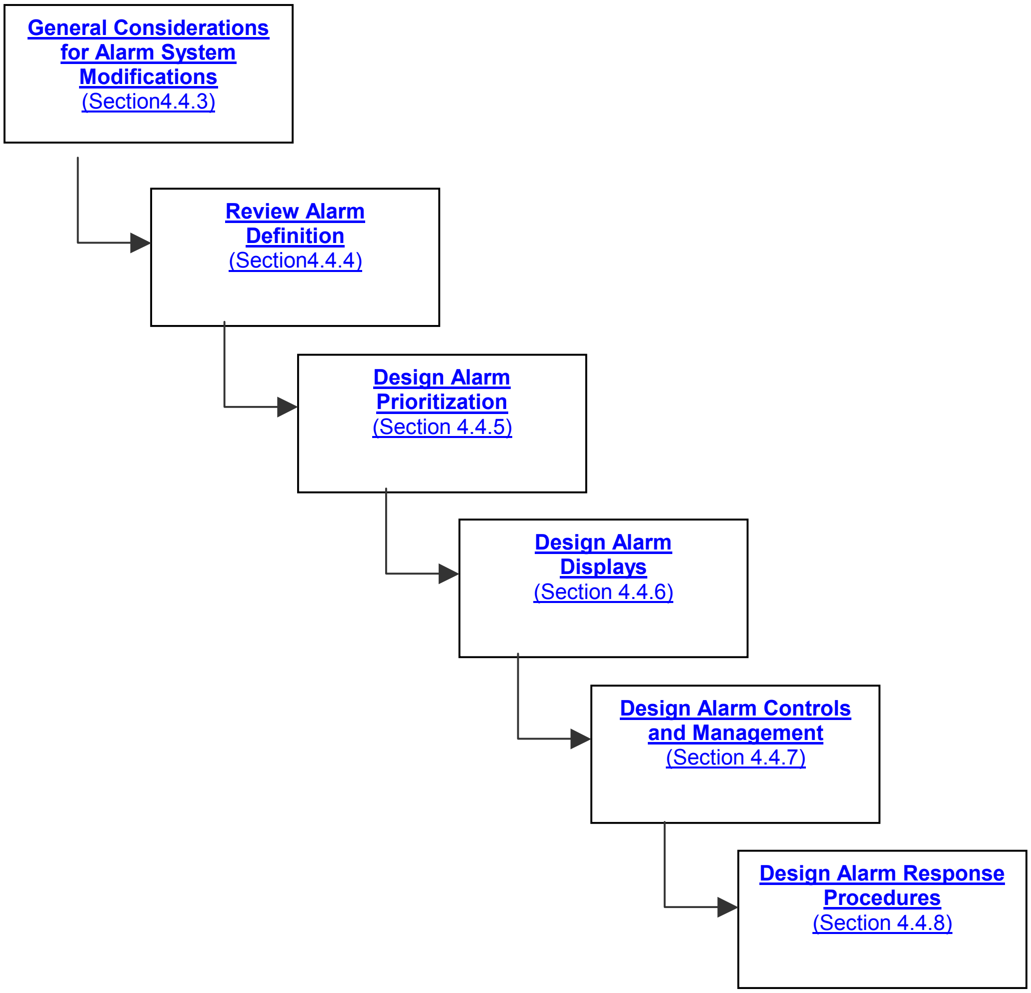

General Considerations for Alarm System Modifications (Section4.4.3)
Review Alarm Definition (Section4.4.4)
Design Alarm Prioritization (Section 4.4.5)
Design Alarm Displays (Section 4.4.6)
Design Alarm Controls and Management (Section 4.4.7)
Design Alarm Response Procedures (Section 4.4.8)

Figure 4-36
Alarm Design Process

4.4.2 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

4.4.3		General Considerations for Alarm Modifications					
	=>	4.4.3-1	The utility should ensure that the characteristics and features of existing alarms are defined, i.e., how the current alarms are used and how the users interact with them. This should include all uses of the alarms, even those that may be beyond the primary detection of abnormal conditions.				
	=>	4.4.3-2	The utility should define the impact of the current I&C modernization program on the plant's alarms. The utility should define: • What existing alarms are no longer needed • What existing alarms now have changed meaning • What additional alarms need to be incorporated, including those alarms associated with the digital system itself • The impact of alarm changes on overall control room changes				
	=>	4.4.3-3	The utility should identify any improvements they would like to make during the modernization program to the way in which alarms are used.				
	=>	4.4.3-4	The utility should consider all sources of alarm information that the users will use, consider the potential to integrate alarm information, and take advantage of the strengths of each approach presenting alarms.				
	=>	4.4.3-5	The utility should consider the effects of failures of portions or all of the equipment that generates or presents alarms, i.e., how failures are handled currently, and how they will be handled after the changes are made and during the process of effecting the changes.				
4.4.4		Alarm Definitions					
	=>	4.4.4-1	Only conditions that require the users' near-term attention or action should be defined as alarms.				

	=>	4.4.4-2	The following criteria should be included in the basis for selecting alarm conditions: • monitoring important plant functions, systems, components, and key parameters • preventing personnel hazards • monitoring the functioning of automatic systems • avoiding significant damage to equipment • assuring that technical specifications are met • monitoring emergency procedure decision points • monitoring plant conditions appropriate to plant modes ranging from full power to shutdown.				
	=>	4.4.4-3	Conditions that result in nuisance alarms should not be defined as alarms.				
	=>	4.4.4-4	Alarm set points should be established so that the operating crew is given timely warnings of accident or abnormal conditions, without establishing thresholds so close to the 'normal' operating values that false alarms are likely.				
	=>	4.4.4-5	The loss of alarm functions (e.g., 'loss of annunciation') should be indicated in the control room.				
4.4.5		Alarm Prioritization and Processing					
	=>	4.4.5-1	Alarms should be prioritized so that users can quickly distinguish which alarms are more important. The criteria used to establish the priority of an alarm condition should include the required immediacy of user action and the threat posed by the condition to safe plant operation.				
	=>	4.4.5-2	If alarms are prioritized into absolute categories, then no more than four alarm priorities should be used.				
	=>	4.4.5-3	Processing should prevent spurious alarms (i.e., alarms that are the result of faulty sensor input).				
	=>	4.4.5-4	Processing should prevent nuisance alarms (i.e., alarm signals for conditions that are not abnormal in the current operating mode or system configuration).				

	=>	4.4.5-5	Processing should identify alarms that are less important because they are redundant with or implied by other alarms (i.e., alarms that necessarily follow from other alarms owing to logical or physical principles or relationships).						
	=>	4.4.5-6	Processing should identify deviations from expected patterns or sequences of events.						
	=>	4.4.5-7	Processing should identify the first-out alarm, the initiating event associated with plant trips.						
	=>	4.4.5-8	Alarm processing should be used to reduce the number of alarms to a manageable level, to support the users' ability to rapidly determine the state of the process.						
	=>	4.4.5-9	Alarm processing should not be so complex that users cannot determine how the current alarms were processed.						
4.4.6	Alarm Display								
	4.4.6.1	General Alarm Display Considerations							
		4.4.6.1.1	SDCV Alarm Displays						
			=>	4.4.6.1.1-1	Spatially dedicated, continuously visible (SDCV) alarm displays should be considered for: • Alarms that require short-term response • The most important alarms used in diagnosing and responding to transients • The most important alarms used to maintain an overview of plant and system status Regulatory Guide 1.97 Type A parameters				
			=>	4.4.6.1.1-2	The format of messages on alarm tiles or tile-like displays should be consistent for all alarms.				
			=>	4.4.6.1.1-3	Detailed alarm information should be immediately available by other means.				
			=>	4.4.6.1.1-4	Alarm elements within a display should be grouped and ordered according to logical principles and/or natural relationships; the same principles and relationships should be used to organize displays throughout the control room.				

			=>	4.4.6.1.1-5	Groups of visual elements in alarm displays should be visually distinctive and arranged to be readily accessible and useable by users.				
		4.4.6.1.2	Alarm Message Lists						
			=>	4.4.6.1.2-1	Alarm messages should contain all the information the users need to respond to them effectively.				
			=>	4.4.6.1.2-2	Lists of alarm messages should typically be segregated by alarm priority with highest priority alarms being listed first, but users should have the capability to group alarm messages according to operationally relevant categories, such as function, chronological order, and status (unacknowledged, acknowledged/active, cleared).				
			=>	4.4.6.1.2-3	The presentation of alarm lists should be designed to enhance the readability of the information.				
			=>	4.4.6.1.2-4	Terminology in alarm message lists should be consistent with that used in other contexts.				
			=>	4.4.6.1.2-5	Printed copies of alarm message lists should convey all the information available in the VDU-displayed lists.				
		4.4.6.1.3	Alarms Integrated into Other Displays						
			=>	4.4.6.1.3-1	Alarms that are important to plant monitoring and user action should be integrated into the associated displays.				
			=>	4.4.6.1.3-2	Alarms should be easily distinguishable, salient features in the display. Alarms should be displayed in a consistent way across all displays of a particular type.				
			=>	4.4.6.1.3-3	Since alarms embedded in displays may not provide messages, this information should be easily retrievable.				
	4.4.6.2	Display of Alarm Priority							
		=>	4.4.6.2-1	The highest-priority alarms should be presented in SDCV displays.					
		=>	4.4.6.2-2	Spurious and nuisance alarms should be filtered.					
		=>	4.4.6.2-3	Redundant and lower-priority alarms should be coded to indicate their lower priority or suppressed. If suppressed, users should be able to access them easily.					

		=>	4.4.6.2-4	When coding priority levels, the highest-priority alarms should have the codes with greatest salience.				
	4.4.6.3		Display of Alarm Status					
		=>	4.4.6.3-1	Visual and auditory signals should be used to convey the status of alarms and these signals should be readily distinguishable.				
		=>	4.4.6.3-2	Visual and auditory signals should direct users' attention so that they are aware of the status of all current alarms.				
	4.4.6.4		Display of Shared Alarms					
		=>	4.4.6.4-1	The use of alarms that are triggered by any one of an aggregate of individual alarms and which require the users to perform additional actions to determine the cause should be limited.				
		=>	4.4.6.4-2	Accessing the individual alarm information represented by a shared alarm should require little effort.				
	4.4.6.5		Coding of Alarms					
		=>	4.4.6.5-1	A systematic approach to coding should be developed across the various alarm displays.				
		=>	4.4.6.5-2	Signals used as codes should be readily detectable in any anticipated control room environment.				
		=>	4.4.6.5-3	Signals used as codes should not startle or annoy users.				
		=>	4.4.6.5-4	Levels of a code should be readily distinguishable from one another.				
		=>	4.4.6.5-5	The coding scheme applied to alarms should be simple and easily understood.				
	4.4.6.6		Auditory Characteristics					
		=>	4.4.6.6-1	The auditory characteristics of an alarm should not startle or annoy users.				
		=>	4.4.6.6-2	Redundant coding should be considered if the source of an audio signal is to be used to indicate where to direct attention.				
		=>	4.4.6.6-3	If audio patterns are used to represent information about alarms (as opposed to just the presence of an alarm), the patterns should be easily recognizable.				

		=>	4.4.6.6-4	When multiple audio signals are used to represent alarm information, interference among them should be avoided.				
	4.4.6.7		Alarm Location					
		=>	4.4.6.7-1	Important SDCV alarms should be located where everyone in the control room can see them.				
		=>	4.4.6.7-2	Lower-priority alarms can be presented at individual workstations or at displays on individual panels.				
4.4.7		Alarm Control and Management						
	4.4.7.1		Alarm Controls					
		=>	4.4.7.1-1	The methods by which alarms are silenced, acknowledged, and reset should be designed to support users' awareness of plant conditions without unnecessarily demanding users' time and attention.				
		=>	4.4.7.1-2	Separate controls should be provided for silence, acknowledgment, reset (acknowledging an alarm that has cleared and returning it to normal), and testing; the controls should be distinctively coded for easy recognition and should have the functions in the same relative locations.				
		=>	4.4.7.1-3	If the alarm presentation includes both alarm tiles and VDU alarm displays, each should have its own set of controls.				
		=>	4.4.7.1-4	Alarm controls should be designed so that they cannot be altered or defeated.				
	4.4.7.2		Alarm Management					
		=>	4.4.7.2-1	Facilities should be provided for selecting, sorting, grouping, searching, and printing the recorded alarm information.				
		=>	4.4.7.2-2	Separate controls should be provided for silence, acknowledgment, reset (acknowledging an alarm that has cleared and returning it to normal), and testing; the controls should be distinctively coded for easy recognition and should have the functions in the same relative locations.				
		=>	4.4.7.2-3	It should be possible to establish temporary, user-defined alarms and user-defined setpoints for specific conditions where such alarms are determined to be of assistance.				

		=>	4.4.7.2-4	When users are able to change the user-defined characteristics of alarms, the existence of such changes should be unambiguously indicated to all users, and should not interfere with normal alarm functioning.				
		=>	4.4.7.2-5	When characteristics of alarms can be modified automatically, the change should be unambiguously signaled to all users; an indication of the current configuration should be prominently displayed.				
		=>	4.4.7.2-6	If a change is automatically made to alarms, users should confirm the change.				
		=>	4.4.7.2-7	An alarm log should be maintained to support analysis of events.				
4.4.8		Alarm Response Procedures						
	=>	4.4.8-1	Alarm response procedures should be available for all alarms requiring users to take an overt action affecting plant process controls or plant equipment.					
	=>	4.4.8-2	Alarm response procedures should be immediately accessible to users.					
	=>	4.4.8-3	Alarm response procedures should contain all the information the users need and should be designed so that users can use them effectively.					
	=>	4.4.8-4	Information and terminology in alarm response procedures should be consistent with that used in other contexts.					

4.4.3 General Considerations for Alarm Modifications

This section discusses the general considerations that should be addressed before applying the more detailed guidance in later sections.

⇒ 4.4.3-1 The utility should ensure that the characteristics and features of existing alarms are defined, i.e., how the current alarms are used and how the users interact with them. This should include all uses of the alarms, even those that may be beyond the primary detection of abnormal conditions.

It is important to establish the basis for all existing alarms, and to understand the ways in which the alarm information is used. This is important because changes to the alarms should consider all these uses to ensure that they are accommodated as necessary following the modification. It is sometimes hard to find this information. Discussions with users can provide valuable information that may not be found in other formal documentation. Another good source of information is training material; however, that information should be checked against the actual design documents. Because there may be alarms associated with several systems, the characteristics of all of these need to be established and considered. It would not be unusual to find significant differences among the practices associated with the various sets of alarms.

How functionality is addressed in a modernized control room will largely depend on the other human-system interface (HSI) resources as well. For example, in current plants alarm tiles are often used for a broad overview of the status of the plant. However, this may be addressed with new information system displays specifically designed for this purpose (see Section 4.1). If improvements in the information displays are not planned, then it will be important to ensure that the alarm presentation maintains this important function.

⇒ 4.4.3-2 The utility should define the impact of the current I&C modernization program on the plant's alarms. The utility should define:

- *What existing alarms are no longer needed*
- *What existing alarms now have changed meaning*
- *What additional alarms need to be incorporated, including those alarms associated with the digital system itself*
- *The impact of alarm changes on overall control room changes*

A relatively limited modification of a few systems to change to programmable logic controllers would not necessarily involve any significant changes to the alarms, except computer alarms associated with the new equipment. A more wholesale change of the HSI to compact work stations with a new information system and soft controls where many controls and displays have been replaced would probably involve major changes in how the users obtain and use alarm information. These impacts should be established early enough in the design process that they can be integrated into the changes without the constraints of an essentially completed design package.

⇒ 4.4.3-3 The utility should identify any improvements they would like to make during the modernization program to the way in which alarms are used.

For smaller scale programs, the approach may be to disrupt existing practices as little as possible. In that case, the utility will want to ensure that the alarms identified in 4.4.3-2 above are introduced using this approach. That is, locating alarm tiles, using terminology, assigning priorities, etc., similar to the other alarms. Where alarms are added, they should usually match the logic of any similar existing alarms or the alarms they are replacing. However, care needs to be taken to be sure that where there are differences in logic or meaning that terminology or presentation does not hide the differences. For example, the same terminology should not be used for an alarm that has a different meaning from an alarm in the original alarm presentation. This may also be an opportunity to better standardize the use of alarms, particularly if users have identified inconsistencies among alarms associated with different system as a problem.

However, if the change in I&C and HSIs is more extensive, then the utility should establish an approach for designing alarms, considering the guidance provided in this and the referenced documents. As part of the definition of this approach a full alarm-by-alarm review should be considered. Some plants performed a complete review of the alarms when the detailed control room design review (DCRDR) was undertaken, and the information developed then might be updated for current use. If large numbers of alarms are going to change, or if significant work is to be done on alarm prioritization, processing, and display, then a full review is probably warranted. Guidance on conducting a full review of alarms can be found in EPRI/NP-3448 (Fink, 1990).

Since there are almost an infinite variety of alarm configurations that can be considered, a clear definition of what problems need to be addressed will help focus the efforts. Information also may be available from the up-front planning effort (Section 2), e.g., from the Concept of Operations, and from the Review of Operating Experience (Section 3). Note, as with all of the modifications considered in this document, the retraining burden associated with new or modified alarm presentations should be considered when defining and planning the changes.

⇒ 4.4.3-4 The utility should consider all sources of alarm information that the users will use, consider the potential to integrate alarm information, and take advantage of the strengths of each approach for presenting alarms.

As upgrades are made, there is the opportunity to integrate the alarms for different systems (e.g., including ancillary alarm panels, fire alarm panels, auxiliary typers, etc.). At a minimum, the user needs to consider effectiveness of the overall alarm information presentation. Consider the strengths and weaknesses of how alarms for the various systems are defined and displayed. For example, dedicated windows or tiles tell the user when an alarm is NOT in, cathode ray tube (CRT) alarm lists give details and timing/chronology, alarms embedded in information displays, control displays, and procedures help users with specific monitoring and control tasks, etc. See Section 4.4.6 below for specific guidelines.

⇒ 4.4.3-5 The utility should consider the effects of failures of portions or all of the equipment that generates or presents alarms, i.e., how failures are handled currently, and how they will be handled after the changes are made and during the process of effecting the changes.

While integration of systems may make sense from a human factors standpoint, the availability of multiple diverse systems provides backup capability that should not be ignored. At each stage of the control room migration, i.e., for each period of time during which the plant has to operate with a different interim configuration, the effectiveness of the resulting alarms should be examined. The need for any additional or different procedures or practices for handling alarm failures should be considered. Some plants have contingency plans or formal procedures for dealing with loss of alarm information. Users must decide whether to hold at power, shut down the plant, declare an event, etc., and use fallback strategies for monitoring critical systems.

4.4.4 Alarm Definitions

Alarm definition is the specification of the types of conditions to be monitored and associated with alarms, and the parameters and setpoints to be used. Important considerations in alarm definition are: alarm categories (the events and states from which alarms are selected) and the criteria for determining the setpoints. The engineering basis for the alarm definition specification should be established to ensure that it is appropriate from the standpoint of operational and economic efficiency and safety.

⇒ 4.4.4-1 Only conditions that require the users' near-term attention or action should be defined as alarms.

Status indications (messages that indicate the status of plant systems but are not intended to alert the user to the need to take action) should not be presented as alarms. While status information is important to users, status indications should be presented to users via a non-alarm display, e.g., on process displays or dedicated status displays. Likewise, indications of conditions that, while abnormal, do not require a near-term response should not be defined as alarms.

⇒ 4.4.4-2 The following criteria should be included in the basis for selecting alarm conditions:

- *monitoring important plant functions, systems, components, and key parameters*
- *preventing personnel hazards*
- *monitoring the functioning of automatic systems*
- *avoiding significant damage to equipment*
- *assuring that technical specifications are met*
- *monitoring emergency procedure decision points*
- *monitoring plant conditions appropriate to plant modes ranging from full power to shutdown.*

Computer-based alarms allow attention to be called to conditions in only those circumstances (e.g., plant mode, system availability, or equipment lineup) in which the resulting alarm would provide users with meaningful information. That is, an alarm definition may include not only the parameter deviation to be alarmed but also the plant circumstances in which the users' attention should be directed toward the deviation. This avoids the need to subsequently process and filter alarms that are not meaningful in the current circumstances (see Section 4.4.5).

⇒ 4.4.4-3 Conditions that result in nuisance alarms should not be defined as alarms.

In many plants alarms are produced regardless of plant mode. Although a condition can be a valid and important alarm in some plant modes, in others it is merely a nuisance. These nuisance alarms can distract users from other tasks. Methods to reduce alarms are addressed in more detail in the next section on prioritization and processing. Nuisance alarms can also result from the inappropriate selection of setpoints as discussed in the next guideline.

⇒ 4.4.4-4 Alarm set points should be established so that the operating crew is given timely warnings of accident or abnormal conditions, without establishing thresholds so close to the 'normal' operating values that false alarms are likely.

Alarm setpoints should be based on plant dynamics, technical specifications requirements, automatic trip points, the likely rate of change of the signal during a transient, and the time it will take the users to respond to the condition causing the alarm. Guidance for determining setpoints is provided in ANSI/IEEE 338-1987 (IEEE, 1988), ISA-RP67.04.01-2000 (ISA, 2000a), and ISA-RP67.04.02-2000 (ISA, 2000b).

There is a trade-off between the timely alerting of a user to off-normal conditions and the creation of nuisance alarms. If setpoints are established such that many false alarms occur, users become less likely to respond to the alarm, especially when their workload is high.

⇒ 4.4.4-5 The loss of alarm functions (e.g., 'loss of annunciation') should be indicated in the control room.

4.4.5 Alarm Prioritization and Processing

A major problem with alarm presentation has been that so many alarms are produced that they become useless during transients. Significant advantages of computer-based alarms are the improved capabilities to prioritize alarms and to use logic to reduce the number of alarms.

Alarm prioritization refers to the determination of the relative importance to users of alarm conditions. The prioritization may be static (as is typical in today's plants) or dynamic (i.e., established by applying alarm processing).

Static prioritization means that the general importance of an alarm is determined in advance of operational use by engineering and operations analysis to decide which alarms are most important. These are color coded red in many existing control rooms.

Dynamic prioritization is the analysis of alarms in real-time to determine which are more important. This information is used to reduce this number to a more manageable level or at least to make it easier for the users to identify the most important in the current situation.

Processing is used to categorize alarms according to the usefulness of the information they can give the users. A given alarm condition may be normal in certain circumstances. For example, there may be low temperature in a system because it is starting up. For startup the condition is normal, however, if it were to occur at full power, it would represent a state of alarm. During the startup, it is a nuisance alarm because it provides no useful information to users.

Alarms may also present redundant information to users. This may occur when the definition of one alarm must logically be satisfied if another alarm condition is present, or when the alarms are all necessary elements of a well-defined condition or sequence of events. For example, once a pump trip alarm is received, an alarm indication that there is low flow is redundant. Note that in some cases the second alarm may provide a valuable confirmation that automatic action related to the first alarm has, in fact, been effected. In such instance it would not be a truly redundant alarm.

Finally, an alarm may provide unique information, however, in the current context (e.g., a significant disturbance), it is not as important as other alarms. For example, an alarm indicating high reactor pressure may be more important than an alarm indicating high bearing temperature of a non-safety related pump in a less critical system.

The purpose of alarm processing is to identify alarms that are irrelevant (nuisance), redundant, or less important. A wide variety of processing techniques has been developed, and combinations of them can be employed. As noted in the previous section, some of the same logic that goes into alarm processing may be built-in to the definition of an alarm.

It is important to consider the impact of alarm processing on users, since each technique changes the resulting information provided to users.

This section provides guidance on alarm prioritization and processing. The design decision as to how to display lower-priority alarms is addressed in the next section.

EPRI (2003) provides additional guidance on improving alarm processing and reducing the number of alarms occurring in plant transients. It provides data on the effectiveness of various alarm reduction techniques and guidance on application of the techniques as part of control room modernization.

⇒ 4.4.5-1 Alarms should be prioritized so that users can quickly distinguish which alarms are more important. The criteria used to establish the priority of an alarm condition should include the required immediacy of user action and the threat posed by the condition to safe plant operation.

Specific considerations used to prioritize alarms include (1) the potential for challenges to safety systems or critical safety functions and the expected time course or pace of different transients, and (2) challenges to plant productivity or equipment protection. The selected prioritization scheme should be logical such that those alarms of the highest safety significance receive the highest priority and that the prioritization appears reasonable to users.

⇒ 4.4.5-2 If alarms are prioritized into absolute categories, then no more than four alarm priorities should be used.

If an unmanageably large number of alarms are designated 'high priority,' the prioritization can lose its ability to effectively direct the user's attention. A rule of thumb is that the number of alarms assigned to the different priorities decreases by roughly a factor of 5 for each increase in priority. For example, about 80% of alarms should be low priority, 15% should be the second lowest priority, 5% high priority, etc. As noted earlier in the context of alarm processing, the effectiveness of the prioritization should be evaluated by simulating the alarm presentation under situations that activate multiple alarm conditions.

⇒ 4.4.5-3 Processing should prevent spurious alarms (i.e., alarms that are the result of faulty sensor input).

When sensors fail, biased or false signals can be generated; these signals may result in the presentation of invalid alarms. Signal validation is a set of alarm processing techniques by which signals from redundant or functionally related sensors are compared and analyzed to determine whether a true alarm condition exists. The purpose of these techniques is to prevent the presentation of false alarms to the user due to malfunctioning plant instrumentation. (This concern for data quality is not limited to the alarms; representation of data quality in the HSI in general is addressed in Section 4.1.5).

Various techniques can be used to prevent drift or noise in plant instrumentation from resulting in signals that momentarily exceed the limit for alarm activation. For example, sensor signals can be low-pass filtered to eliminate momentary 'spikes'. Similarly, delays can be defined to allow inconsequential deviations to re-enter the normal range without generating an alarm. Finally, a band can be established around a parameter's normal value within which deviations are ignored. Any of these techniques will result in some delay in alerting users of an actual deviation, and they should only be used in circumstances where this tradeoff is acceptable.

⇒ 4.4.5-4 Processing should prevent nuisance alarms (i.e., alarm signals for conditions that are not abnormal in the current operating mode or system configuration).

If a component's status or parameter value represents a fault in some plant modes or configurations and not others, it should be alarmed only in the appropriate circumstances. For example, the fact that a particular pump is not running may only have operational significance to the crew when the plant is operating in the power range. Mode dependent alarm processing would allow this alarm to be presented when the plant is in the power range but not when it is in other modes (e.g., hot standby).

Similarly, the fact that a particular pump has a low discharge pressure may indicate that the pump is not running or it might only indicate a fault when the associated fluid system is configured to perform a particular function. Other discharge pressures may be appropriate when the fluid system is configured to perform a different function. In addition, a low pump discharge pressure may not be relevant when the fluid system is taken out of service. System configuration processing would allow the alarm for pump discharge pressure to be presented when the fluid system is in the proper configuration and prevent its presentation when the system is in an alternate configuration. See EPRI (2003) for additional guidance.

⇒ 4.4.5-5 Processing should identify alarms that are less important because they are redundant with or implied by other alarms (i.e., alarms that necessarily follow from other alarms owing to logical or physical principles or relationships).

If a single event invariably leads to subsequent alarmed events that are the direct consequence of this event, only the alarm associated with the main event may be presented and the other alarms suppressed, so long as this does not interfere with the use of alarm information. The same applies to an alarm condition that is logically implied by another alarm (e.g., a 'low level' alarm when conditions for 'low-low level' exist).

⇒ 4.4.5-6 Processing should identify deviations from expected patterns or sequences of events.

Processing will identify (and assign a lower importance to) the occurrence of expected conditions (see above). To the extent possible, instances when expected conditions or sequences of events fail to occur should also be identified. Such analyses may apply, for example, during certain transients (e.g., reactor scram) where the expected alarm pattern is well known.

⇒ 4.4.5-7 Processing should identify the first-out alarm, the initiating event associated with plant trips.

As an aid to diagnostic procedures and root cause analysis, the display identifies the parameter within an interrelated group that first exceeded its setpoint during a series of events leading to a reactor or turbine trip. This type of processing works well where all signals respond equally quickly (e.g. electrical 'sequence of events' monitoring), but are not necessarily as useful to users where response characteristics can be time-variable. This situation arises in process systems because of differential lags in some measurements (e.g. temperature, level) compared to others (e.g. pressure, electrical parameters).

However, it should be noted that discrepancies can occur in chronological data reports. The "First out"' alarm may only mean the first to enter the alarm database. Due to the way some processors scan their database, communications delays or process the logic, the first alarm may not be reported 'first.'

⇒ 4.4.5-8 Alarm processing should be used to reduce the number of alarms to a manageable level, to support the users' ability to rapidly determine the state of the process.

Alarm processing should ensure that the alarms continue to perform their functions under any operational or accident conditions. Some very rough rules of thumb have been proposed regarding the alarm rates that users will find manageable. For example, it is suggested that during major transients a rate of between 2 and 10 alarms per minute will be hard to cope with, and that higher rates would result in users abandoning the use of the alarms.

The alarm presentation rate at which users' performance begins to decline will of course depend on many factors, e.g., the demands imposed by concurrent user tasks such as interface management. Since there is no firm guidance on the degree of alarm reduction required to avoid alarm overload, the designer should evaluate the processing with users to assess the effectiveness of the alarm reduction process. This assessment should include evaluations that simulate the alarm presentation under situations that activate multiple alarm conditions and/or generate increased user workload.

⇒ 4.4.5-9 Alarm processing should not be so complex that users cannot determine how the current alarms were processed.

Processing methods applied to alarm data should not be so complex that they cannot be readily understood and interpreted by the users. If users are unaware of the relationships among displayed alarms and how those relationships might depend on the processing being applied, they may draw incorrect conclusions about the state of the system or the reliability of the alarms. Similarly, users should be able to view the inputs to the processing logic. For example, users may need to view sensor data under certain circumstances, such as if the pattern of alarms appears to be contradictory, or if users suspect that there is a problem with the processing such that the results of alarm processing are incorrect.

4.4.6 Alarm Display

Alarms displays can have both auditory and visual components. The auditory components are typically designed to alert the user to the presence of an alarm (e.g., using horns), while the visual components guide attention to the appropriate alarm (by using techniques such as flashing) and provide detailed alarm information (such as an alarm message).

To support the different functions of alarms, they may be presented in a number of formats. Combinations of different formats (e.g., video display unit (VDU) listing of alarm details combined with alarm tile panels) are often used. Thus, the display format of alarm information and the degree to which that information is presented separately or in an integrated fashion with other process information, are important considerations.

As stated above, current alarm displays often use tiles as the primary means of displaying alarms. As a result of an upgrade or the installation of computer-based systems, additional display techniques may become available. However, it should be noted that the guidance still calls for the most important alarms to be presented on spatially dedicated, continuously visible displays, and not solely in alarm lists.

This section also addresses the coding of key alarm information, such as priority and status, the auditory characteristics of alarms, and the location of alarms.

4.4.6.1 General Alarm Display Considerations

In this section, the general approaches to alarm display are addressed as well as where alarms should be located. There are three basic approaches to displaying alarms:

- spatially dedicated, continuously visible (SDCV) alarm displays (e.g., ‘tiles’ presented in wall-mounted arrays or on VDU screens)
- alarm message lists (e.g., textual alarm information presented on a VDU screen)

- alarms integrated into other displays (e.g., mimic displays or soft control displays that include alarm indicators)

Other types of displays can be developed by combining features of these three basic approaches. This section provides guidance on deciding the type of alarm displays that are best used for specific alarmed conditions.

4.4.6.1.1 SDCV Alarm Displays

⇒ 4.4.6.1.1-1 Spatially dedicated, continuously visible (SDCV) alarm displays should be considered for:

- *Alarms that require short-term response*
- *The most important alarms used in diagnosing and responding to transients*
- *The most important alarms used to maintain an overview of plant and system status*
- *Regulatory Guide 1.97 Type A parameters*

Spatial dedication means that the alarm messages always appear in the same position. Continuously visible means the alarm information is always available to the user, as opposed to presentation methods in which the user must select the information to be seen. These characteristics make it relatively easy for a user to determine that a particular condition is NOT in an alarm state. A SDCV alarm display (such as is provided by conventional tiles) generally has been found during high-density alarm conditions to be superior to other forms of alarm presentation, such as message lists. SDCV displays provide perceptual advantages of rapid detection and enhanced pattern recognition.

The arrays of tile panels typically found in current control rooms are classic examples of spatially dedicated alarm displays. However, spatial dedication can be realized in various ways. For example, a dedicated array of VDUs can be used to create a display whose design and content is similar to that of the tile panels. Alarms integrated into continuously visible mimic displays could also be considered spatially dedicated (although in such displays they are embedded in much more visual noise).

The advantages of information appearing in a predictable and prominent location are generally recognized. Therefore, spatially dedicated, continuously visible (SDCV) displays should be considered for displaying alarms for which certainty and speed of response are critical.

These displays can be very effective in helping users identify conditions or assess the effect of corrective actions. The way in which they are typically implemented (i.e., with spatially dedicated elements organized by system or function) greatly reduces effort required for situation assessment by taking advantage of users' natural abilities to learn and recognize patterns. Accordingly, information that is less critical but nevertheless important to users' situation awareness may also be presented on spatially dedicated displays. However, there are practical limits to the number of spatially dedicated elements that can be provided. Perhaps more important is the issue of visual noise - the potentially decreased salience of more critical indicators as more display elements are added. As noted earlier, the function of providing an overview may be better supported by a display specifically designed for that purpose.

⇒ 4.4.6.1.1-2 The format of messages on alarm tiles or tile-like displays should be consistent for all alarms.

Information on a tile might be organized as follows: top line, name of alarmed parameter; middle line, alarm setpoint value; bottom line, indication of severity. When SDCV alarms are implemented on VDUs there may be more limited space than when on panels. In that case, the designer may consider making a greater use of icons or other strategies to reduce space. The difficulty users will have getting additional information about an alarm is significantly less on VDUs when compared with traditional panels (see the next guideline).

⇒ 4.4.6.1.1-3 Detailed alarm information should be immediately available by other means.

Display elements in traditional alarm tile panels serve both to alert users to the existence of an alarm and to inform them as to its nature. The need for spatially dedicated displays to perform both functions forces a tradeoff between space limitations and the amount of alarm information provided. As a practical matter it is not typically possible to provide all the information users might need. More often, elements of spatially dedicated displays serve to alert and prompt the user to consult a source of detailed information that is presented in alarm message lists and alarm response procedures. In this case, the ease with which users can obtain detailed information upon being alerted is a key consideration.

Computerized alarms may allow users at VDU workstations to access detailed information about an alarm with a single action, without taking their attention from the display they were viewing at the time the alarm came in. Alarm detail may even be presented automatically at a dedicated location on the display. As the ‘cost’ to the user of obtaining alarm information decreases, so does the need to combine alerting and informing functions in the same visual element.

For example, easily accessible alarm response procedures might be keyed to the location of an alarm tile within a wall-mounted matrix. Alternatively, selecting an alarm ‘tile’ presented on a VDU might cause details to be displayed. In either case, the supplementary information would contain those items that could not be incorporated into the alarm display itself (e.g., alarm source, setpoint value, immediate actions, and follow-up actions).

⇒ 4.4.6.1.1-4 Alarm elements within a display should be grouped and ordered according to logical principles and/or natural relationships; the same principles and relationships should be used to organize displays throughout the control room.

Alarm elements should be grouped so that system functional relationships are readily apparent. For example, area radiation alarms should be grouped on one display, not spread throughout the control room. As much as possible, the alarms should be grouped with controls and displays of the same function.

Alarms should be ordered to depict naturally occurring relationships. Naturally occurring relationships (e.g., those derived from the physical process) include the following:

- pressure, flow, level, and temperature alarms in fluid systems;

- alarms for a given thermodynamic parameter at different points within the system that indicate a progression (e.g., within a fluid system, a series of pressure alarms starting with the source tank and ending with the system discharge);
- several alarms for the same variable indicating levels of severity (e.g., tank level low and tank level low-low); and
- alarms related by cause and effect.

For example, pressure, flow, level, and temperature could be arranged left-to-right. Alarm parameters (e.g., pressure, flow, level, and temperature) arranged in one order on one panel should be arranged in the same order on other panels. (Circumstances may dictate different orderings for systems with very different functions. However, once an arrangement has been chosen, the arrangement should be used consistently within similar systems or alarm groups.)

⇒ 4.4.6.1.1-5 Groups of visual elements in alarm displays should be visually distinctive and arranged to be readily accessible and useable by users.

Alarm functional groups should be visually distinct from one another. A label above the display should identify each group of alarm displays. System/functional groups should be clearly delineated and labeled such that users can easily determine which systems have alarms that have not yet cleared and which system is affected by a particular incoming alarm. If alarm displays are organized in matrices, the vertical and horizontal axes of the displays should be labeled with alphanumerics for ready coordinate designation of a particular visual element. An alarm tile display matrix should contain a maximum of 50 alarms. Matrices smaller than 50 alarms are preferred.

4.4.6.1.2 Alarm Message Lists

⇒ 4.4.6.1.2-1 Alarm messages should contain all the information the users need to respond to them effectively.

An alarm message can contain the following information:

- alarm source
- alarm priority
- setpoint values
- parameter values
- required immediate actions
- reference to procedures
- reference to associated displays.

Depending on how the information is displayed, it may not be practical to display all of these quantities at the same time. For similar displays the information needs to be presented in the same order and using the same syntax.

⇒ 4.4.6.1.2-2 Lists of alarm messages should typically be segregated by alarm priority with highest priority alarms being listed first, but users should have the capability to group alarm messages according to operationally relevant categories, such as function, chronological order, and status (unacknowledged, acknowledged/active, cleared).

For example, it should be possible to list alarm messages in chronological order with the most recent messages placed at the top of the alarm list (i.e., alarm messages entered in a pushdown stack mode). Other grouping criteria include system, user responsibility, and priority. Grouping by criteria other than priority should not interfere with the detection of high-priority alarms. The grouping should be easy to implement. The display on which users group, sort, or filter alarm messages should be separate from the screen on which alarms are displayed as they come in.

⇒ 4.4.6.1.2-3 The presentation of alarm lists should be designed to enhance the readability of the information.

One of the greatest obstacles to readability of a message list display is when incoming alarm messages cause the display to scroll rapidly. The alarm display should prevent this from happening. When the display is full, the presence of new alarms that are not displayed should be clearly indicated. One concern may be that such an approach could cause high-priority alarms to be out of the user's view. One approach to resolve this problem is to dedicate a portion of the display or a separate VDU for high-priority alarm messages. However, within the context of the overall display of alarms, the message list should not be the primary display for high-priority alarms. As noted in Guidelines 4.4.6.2-1 and 4.4.6.7-1, high-priority alarms should be spatially dedicated and located where everyone in the control room can see them. Second, when many alarms are coming in, the alarm message list would not be the primary source of alarm information in general. Third, if users are consulting the message list, they should have the option to sort the alarms on priority to display all high-priority alarms (see Guideline 4.4.7.2-1). If users are consulting the message list to examine some other aspect of the alarms, such as the chronology or to group them by system, high-priority alarms may not be displayed.

Another feature to improve the readability of alarm messages is to place a separation (blank row) or line between every four or five alphanumeric messages. The design should not imply that such readability enhancements constitute a logical grouping of alarms.

⇒ 4.4.6.1.2-4 Terminology in alarm message lists should be consistent with that used in other contexts.

Printed and VDU-displayed lists should be consistent and should use the same terminology as in other displays, e.g., SDCV displays, and in procedures and other plant documents. If a plant does not have a standard set of terms, such a lexicon may need to be established.

⇒ 4.4.6.1.2-5 Printed copies of alarm message lists should convey all the information available in the VDU-displayed lists.

If alarm lists may be printed (either for reference during an event, or for later analysis), the text (and any symbols) should remain legible and visual codes used should be equally effective. For example, if a VDU-displayed list may be printed on a black-and-white printer, information related to the messages should not be coded by color alone.

4.4.6.1.3 Alarms Integrated into Other Displays

In addition to SDCV and message list presentations, alarms can also be integrated into other types of displays. For example, alarms can be integrated into mimic (or P&ID) displays to improve their association with related components, systems, and functions. Figure 4-37 illustrates alarms integrated into a mimic display. In the figure, the measurement values with the red and yellow rectangles behind the value are alarms. The two colors indicate two different priorities. Alarms can also be integrated into electronic procedures or soft control displays. This provides improved integration of alarms into user task performance.

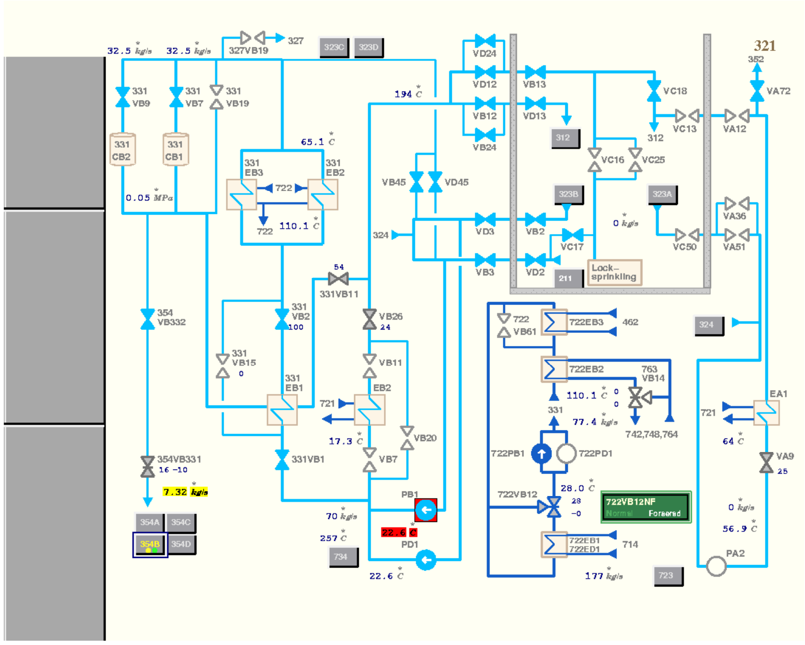


Figure 4-37
Alarms Integrated into a Process Display

⇒ *4.4.6.1.3-1 Alarms that are important to plant monitoring and user action should be integrated into the associated displays.*

A tradeoff that must be considered is the crowding of a display with too much information. Therefore, if space is limited only the most important (highest priority) alarms should be presented. An alternative is to provide a high-level indication that a relevant alarm exists. For example, on a soft control display, a single alarm symbol could be presented; to indicate to the user that an alarm relevant to the control actions exists.

⇒ *4.4.6.1.3-2 Alarms should be easily distinguishable, salient features in the display. Alarms should be displayed in a consistent way across all displays of a particular type.*

Figure 4-37 illustrates the use of color to make alarms salient is a display.

⇒ 4.4.6.1.3-3 Since alarms embedded in displays may not provide messages, this information should be easily retrievable.

For example, if a single alarm indication is presented in a soft control display, easy access to the detailed alarm information should be provided by enabling the user to click on this “master alarm” to reveal a list of the relevant alarms.

4.4.6.2 Display of Alarm Priority

Alarms can be prioritized statically or dynamically. Once the prioritization is done, the designer must determine whether the information is going to be presented at all, and if so, how. In this regard, three techniques can be used: filtering, suppression, and dynamic priority coding. Each is defined below.

- *Filtering* – alarms determined by processing to be less important, irrelevant, or otherwise unnecessary are eliminated and are *not available* to the users.[4]
- *Suppression* – alarms determined by processing to be less important, irrelevant, or otherwise unnecessary are not presented to the users, but can be accessed upon request.
- *Priority coding* – the differences in alarm priority are conveyed by means of coding alarms, such as by color or location (displayed in priority groupings, e.g., low and high priority).

A specific implementation may employ a combination of these approaches. There are trade-offs among these approaches as to which method should be used or in what contexts the various options should be exercised.

Filtering (whether it is done by specific processing or just implied by the alarm definition) completely eliminates the possibility of less important alarms distracting the users. However, the eliminated information may be useful for other purposes. In addition, it is important to be sure that the processing method chosen is adequately validated and will function appropriately in all plant conditions.

Suppression has the potential benefits of filtering by removing distracting alarms. However, since such alarms are still accessible on auxiliary displays, they potentially impose an additional secondary task workload to retrieve them. Priority coding does not conceal any information from users. However, the method requires users to perceptually ‘filter’ alarms, using the priority codes, to identify the ones of higher priority. This creates the potential for distraction because it presents alarms of all levels of importance. The effect of these alternatives on the users’ performance needs to be considered.

Considering these tradeoffs, the following guidance addresses the treatment of alarms at different priority levels.

[4] Note that in the alarm system literature, the terms filtering and suppression are often used interchangeably and inconsistently. The definitions provided here are efforts to standardize the meaning of the terms - at least for this document.

⇒ 4.4.6.2-1 The highest-priority alarms should be presented in SDCV displays.

Alarms that have higher importance should be given greater priority in their presentation than less significant alarms. A dedicated display area or device is often used to do this; color coding is also used. Non-spatially dedicated alarm displays, such as message lists, are generally not used as the primary method of presenting high-priority alarms (although alarm messages may be available to provide additional information). If non-spatially dedicated alarm displays are used, they should have sufficient display space available for simultaneous presentation of all high-priority alarms under the worst credible conditions. Users should never have to page or scroll a display to view high-priority alarms.

⇒ 4.4.6.2-2 Spurious and nuisance alarms should be filtered.

Alarm filtering should only be employed where alarms have no current operational significance. Thus, only alarms that can be demonstrated to have no operational significance to users should be filtered. This includes alarms that are irrelevant within the context of the current plant mode or the configuration of the associated plant system. For example, low temperature alarms can be filtered during startup. As noted in the discussion of processing, computerization may allow alarms to be defined to exclude circumstances having no operational significance.

⇒ 4.4.6.2-3 Redundant and lower-priority alarms should be coded to indicate their lower priority or suppressed. If suppressed, users should be able to access them easily.

When there are not many alarms, it may be better to code all the alarms for priority. Color coding is often used for this purpose. However, during a significant disturbance, suppression may be preferred so the lower-priority alarms do not distract users from attending to primary alarms.

⇒ 4.4.6.2-4 When coding priority levels, the highest-priority alarms should have the codes with greatest salience.

Priority levels should be correlated with coding salience. When the higher-priority alarms are coded with high salience, the user’s attention will be directed toward them. For example, if using color to code priority, red is usually used for the high-priority alarms.

4.4.6.3 Display of Alarm Status

Alarms can be in a number of status conditions: unacknowledged, acknowledged, cleared, reset. Alarm status is typically conveyed by visual and/or auditory coding.

⇒ 4.4.6.3-1 Visual and auditory signals should be used to convey the status of alarms and these signals should be readily distinguishable.

After the user has acknowledged an alarm (e.g., pressed the acknowledge button), the alarm display should change to a visually distinct acknowledged state, e.g., from blinking to steady. When an alarm clears (i.e., the parameter returns to the normal range from an abnormal range), the return to normal conditions should be indicated by visual and audible means. If an alarm was cleared but was not reset and the variable re-enters the abnormal range, then the condition should be presented as a new, unacknowledged alarm.

⇒ 4.4.6.3-2 Visual and auditory signals should direct users' attention so that they are aware of the status of all current alarms.

If the user is not currently viewing a VDU display where an unacknowledged alarm appears, the user should be made aware that an alarm message is available, the priority of the alarm, and the location where the alarm message can be found.

4.4.6.4 Display of Shared Alarms

A shared (or 'multiple-input') alarm is one that represents a set of two or more related process deviation conditions. An example of a shared alarm is a 'reactor coolant system trouble' message, which may be displayed when any one of the reactor coolant pumps malfunctions. An individual alarm message associated with the particular malfunctioning reactor coolant pump may also be displayed in addition to the reactor coolant system trouble message.

⇒ 4.4.6.4-1 The use of alarms that are triggered by any one of an aggregate of individual alarms and which require the users to perform additional actions to determine the cause should be limited.

This guideline does not apply to the use of alarm processing through which individual alarms are logically processed to provide more operationally meaningful, higher-level alarms. By contrast, shared alarms are defined by the activation of one or more of a set of different process deviations. For example, a 'trouble' message may combine several potential problems associated with a single plant system or component, or it may address the same problem for a group of similar components (e.g., a bearing temperature alarm may address bearings from more than one component). This approach should not be used if it might result in minor alarms 'hiding' a major one that shares the same indicator. Shared alarms should also be avoided if they interrupt users' activities by forcing them to seek specific information about which of the ganged parameters exceeded its setpoint. If the disruption or added effort is minimal, shared alarms may be acceptable. For example, information might automatically be presented related to the deviant parameter when the shared alarm is initiated. This reduces the user workload associated with retrieving alarm information and minimizes the negative effects of the shared alarm. Criteria for the use/avoidance of shared alarms are given in Table 4-16.

Table 4-16
Considerations for Sharing Alarms

Types of Alarms that may be Considered for Combination
• Alarms for the same condition on redundant components, or logic trains, when each has a separate indicator and the indicators are placed in close proximity on the console (e.g., pump A or B trip, logic train A or B actuation)
• Alarms for several conditions relating to one component or several redundant components, which require the user to obtain further diagnostic information (e.g., pump A or B trouble)
• Alarms for several conditions that call for the same corrective action
• Alarms that summarize single-input alarms elsewhere in the control room
Conditions Under which Alarms should not be Combined
• Different actions are to be taken depending on which alarm condition exists and information is not readily available to the user to identify which constituent is alarming
• Information or protection for other alarm constituents is not available to the user after any one alarm constituent has activated the combined alarm (reflash can provide such protection)
• The constituent conditions are not of the same importance

⇒ 4.4.6.4-2 Accessing the individual alarm information represented by a shared alarm should require little effort.

The information could be provided by means of alarm messages on a VDU, an alarm list on an alarm printer, or by other means. This information may be obtained by a simple action or automatically (e.g., upon acknowledgement of the shared alarm, the triggering alarm or alarms are automatically presented on a VDU). Similarly, a shared alarm should ‘reflash’ (i.e., reactivate the visual and audible alert indications for an unacknowledged alarm) if another of the constituent conditions occurs before the preceding acknowledged alarm has cleared. Users’ should not be required to continually check the status of individual alarms.

4.4.6.5 Coding of Alarms

⇒ 4.4.6.5-1 A systematic approach to coding should be developed across the various alarm displays.

Numerous coding schemes may be employed, e.g., for prioritizing, indicating status, and other relevant information. Developing a systematic approach will help to ensure a consistent use of coding within and across the alarm presentation. It should be determined that visually coded information is equally detectable and distinguishable on all displays.

⇒ 4.4.6.5-2 Signals used as codes should be readily detectable in any anticipated control room environment.

For example, a light used to signal an alarm condition should be easily detectable under all anticipated levels of ambient control room illumination, under emergency lighting conditions, and in the presence of other nearby light sources (e.g., other alarm indicators, status indicators, lighting fixture, or windows). Likewise, a sound used in association an alarm condition should be clearly audible over other sound sources in the control room (e.g., other alarm sounds, spoken communication or equipment noise).

⇒ 4.4.6.5-3 Signals used as codes should not startle or annoy users.

For example, users will find a very rapidly flashing light in their peripheral vision to be distracting. Indicators that are too bright can cause visual fatigue and make nearby indicators difficult to see. In either case, the unpleasantness of the signal can lead users to seek to terminate it before fully investigating the condition it represents. Well-designed signals can be detectable without being disruptive to users' activities.

⇒ 4.4.6.5-4 Levels of a code should be readily distinguishable from one another.

For example, if color is used, the different colors should be easily discriminated. Each color should have a single, precise meaning that is consistent with applicable population stereotypes. A formal coding scheme that encompasses all coding methods (e.g., color, brightness, or repetition rate) and specifies a hierarchical order should be established and formally documented.

⇒ 4.4.6.5-5 The coding scheme applied to alarms should be simple and easily understood.

The number of different coding techniques should be kept to a minimum, so that the coding system does not become too difficult to use or understand. Each technique used to code alarms should represent only one dimension of the alarm classification. For example, if flash rate is being used to indicate alarm state (e.g., unacknowledged, acknowledged, or cleared), it should not also be used to indicate need for user action (e.g., immediate action required, action required within 15 minutes, or no near-term action needed).

4.4.6.6 Auditory Characteristics

The audio characteristics of alarms are often seen as contributing to the effects of alarm overload. The signals are usually presented at high levels (to ensure that they are heard) and have abrupt onsets. These characteristics make them potentially startling and aversive. Signals associated with incoming alarms also tend to sound continuously or repeat rapidly. This can be disruptive to communication or thought, and users can find it necessary to immediately silence them. This forced redirection of attention (which is desirable in circumstances where immediate action is needed to avert serious consequences) can add to the users' workload at critical times.

Computer-related alarm upgrades offer an opportunity to address recognized problems with the audio aspects of alarms, and perhaps to expand the use of audio codes to represent alarm information.

⇒ 4.4.6.6-1 The auditory characteristics of an alarm should not startle or annoy users.

An intense sound with a sudden onset can be aversive and can interrupt spoken communication. Well-designed signals can be detectable without being disruptive to users' activities. Research on the audio characteristics of alarms has shown that by taking into account the frequency characteristics of the noise environment in which they must be heard, alarms can be made less intense while remaining reliably audible. In addition, sounds will be less startling and aversive if their onset envelope incorporates even a brief 'ramp' or if they are low-pass filtered.

Disruption of ongoing user tasks and spoken communication can also be reduced by reducing the rate at which alarm signals associated with unacknowledged alarms repeat. That is, designers might consider having the audio signals for incoming alarms (especially those that are not of the highest priority) repeat at longer intervals.

⇒ 4.4.6.6-2 Redundant coding should be considered if the source of an audio signal is to be used to indicate where to direct attention.

By placing the source of an audio alarm signal at or near the location where corresponding alarm information can be found, designers can take advantage of users' natural abilities to rapidly localize and orient toward a sound. However, certain types of sounds (e.g., continuous pure tones) are not easily localized, and reflections and sound shadows may make localization unreliable in some areas of the control room. Therefore, direction of attention should not depend solely on users localizing the sound source.

⇒ 4.4.6.6-3 If audio patterns are used to represent information about alarms (as opposed to just the presence of an alarm), the patterns should be easily recognizable.

Warning sounds consisting of "bursts" composed of five or more brief pulses (about 0.1 second in duration) with inter-pulse intervals of .15 to .3 seconds have been recommended. The pulses may be designed to be distinctive with respect to their onset and offset shaping, fundamental frequency, and harmonic structure. The bursts may vary as to the number of pulses, the tempo at which they are presented, and the rhythmic and pitch contours.

Audio signals used in control rooms are typically not as varied as they might be. Typically, audio signals either draw attention to incoming (i.e., new) alarms or alarms that remain unacknowledged, or draw attention to clearing conditions. Each of these functions is typically associated with a different, distinctive sound. In computer-based systems, they may also be used to draw attention to the existence of conditions defined by users (i.e., user-defined alarms); these too would be associated with a distinctive sound.

However, there are control rooms in which the characteristics of the sound associated with an incoming alarm indicate which user is to respond. This can lower users' workload by decreasing number of times each user's attention is diverted. Similarly, audio signals can code the system in which an alarm condition has occurred (or, in multi-unit control rooms, the unit to which the alarm applies), making users aware of this information immediately without requiring them to turn their attention to a visual alarm display.

Less common is the use of audio characteristics to code the urgency or importance of an alarm condition. Approaches have also been suggested for using audio signals to represent parameter trends (e.g., monitoring the return of a parameter to normal after responding to an alarm). Both techniques make users aware of information that has become available without forcing them to redirect their attention. Because they are audible to everyone in the control room, audio alarm signals that carry information about the nature of alarms may play a part in maintaining team situation awareness in setting where users are located at individual workstations. For example, a user interacting with a specialized set of displays would remain aware of the types of alarms coming in without having to glance at or call up a different display.

⇒ 4.4.6.6-4 When multiple audio signals are used to represent alarm information, interference among them should be avoided.

Even if audio alarm signals are individually designed so that they are not masked by or confusable with other sounds in the control room, they may still interfere with each other if they are sounded simultaneously.

4.4.6.7 Alarm Location

Designers have options as to where alarms are located or where they can be accessed. These options depend on other aspects of the control room design. For example, alarms can be located on existing panels, on a new large screen display, or on displays accessed at individual workstations. Some of the considerations involved in making these decisions are provided below. The way in which alarms are displayed most effectively will be influenced by the crewmembers' roles and operating practices.

⇒ 4.4.6.7-1 Important SDCV alarms should be located where everyone in the control room can see them.

Included in this category are the highest-priority alarms. Also included are the next priority categories, as space permits. This will depend on the unique aspects of the design. These alarms should be located on group-view displays or on panels positioned in the control room where they will be visible from the users normal working area. While these alarms can be presented at individual workstations, this should not be the only location.

⇒ 4.4.6.7-2 Lower-priority alarms can be presented at individual workstations or at displays on individual panels.

On way to make important alarms more conspicuous is to reduce the noise associated with lower priority alarms. One way to do this is to have these alarms presented at individual workstations or presented on VDUs on the panels to which they are associated. For example, if the responsibility to respond to alarms of various types is formally divided among crewmembers, then presenting alarms only at the corresponding workstation may be effective in that it reduces the number of alarms each user must manage. However, if users' roles are not that specialized, then it must be recognized that presenting alarms in this way forces a change in the functioning of the crew. When information is made available to users at individual workstations, the contribution of that information to other users' general awareness of the state of the plant must be considered. It may be advisable, for example, to make the alerting signals (and some indication of the general nature of the alarm) available to the entire crew while presenting details at individual workstations.

4.4.7 Alarm Control and Management

Alarm controls are the means by which alarms are silenced, acknowledged, reset, and tested. Alarm management functions allow users to customize or automate aspects of their interaction with alarms in order to reduce workload.

4.4.7.1 Alarm Controls

The typical controls include silence, acknowledge, reset, and test (SART). A variety of control devices can be used, such as pushbuttons, function keys, and on-screen controls. These should conform to general human factors guidance for these types of controls. In addition there are specific considerations for controls related to alarms, as discussed below.

⇒ 4.4.7.1-1 The methods by which alarms are silenced, acknowledged, and reset should be designed to support users' awareness of plant conditions without unnecessarily demanding users' time and attention.

For example, users may be allowed to *silence* alarms from any set of alarm controls in the main operating area, while requiring them to *acknowledge* these alarms at their respective panels or at a workstation dedicated to the function to which the alarm pertains. The rationale for this is that the primary purpose of the auditory signal is to alert the user to a new alarm. It is not necessary that silence capability be provided only where the specific alarm can be read, so long as the user is made aware of all alarms that are being silenced. (The user should not be able to silence alarms that cannot be visually detected from the global silence control.) However, in order to support users' situation awareness, acknowledgement should be possible only at locations from which the alarms can be read. By the same logic, a manual reset sequence should be used where it is important to explicitly inform users of a cleared condition, but an automatic reset sequence should be available where users have to respond to numerous alarms or where it is essential to quickly reset the alarm. As with acknowledgement, the reset function should be effective only from locations at which users know which alarm they are resetting.

⇒ 4.4.7.1-2 Separate controls should be provided for silence, acknowledgment, reset (acknowledging an alarm that has cleared and returning it to normal), and testing; the controls should be distinctively coded for easy recognition and should have the functions in the same relative locations.

The controls should be distinguishable from each other, by touch and sight, to prevent accidental operation of the wrong control. Such techniques as color coding, color shading the group of alarm controls, demarcating the group of alarm controls, or shape coding should be used.

⇒ 4.4.7.1-3 If the alarm presentation includes both alarm tiles and VDU alarm displays, each should have its own set of controls.

If alarm information is presented redundantly on tile and VDU displays, then alarm acknowledgment via one device (i.e., either the VDU or tile panel control station) should cause the redundant alarm to be automatically acknowledged on the other device. All other control actions (acknowledge, reset and test) should be specific to the workstation associated with the alarm. The aim, as described above, is to have alarms acknowledged or reset only from locations at which they can be read. However, there is a potential for confusion if different sets of alarms are presented at multiple separate workstations; redundant or group-view presentation may be preferable.

⇒ 4.4.7.1-4 Alarm controls should be designed so that they cannot be altered or defeated.

Instances have been noted where silence buttons, in particular, have been secured with pins or clips in the depressed position.

4.4.7.2 Alarm Management

In addition to the basic SART controls, there may be many and varied alarm management functions. For example, the user may be able to define temporary alarms, adjust setpoints, control filtering options, and sort alarms according to many separate dimensions, such as time, priority, and system. When designing these management features, it is important to minimize the effort required for users to perform these activities. Note that in some cases, particularly setpoints, there may be strict administrative limitations and changes must be strictly controlled.

In certain situations, such as during major process disturbances, it may be desirable to reduce workload by automating some alarm-related functions, such as by silencing lower priority alarms. Similarly, automated controls may be implemented to trigger appropriate displays, such as alarm graphics, data windows, or display pages.

⇒ 4.4.7.2-1 Facilities should be provided for selecting, sorting, grouping, searching, and printing the recorded alarm information.

Users should be able to arrange alarms in different ways to support trouble shooting and situation assessment. For example, sorting alarms based on priority, system, and chronology can assist users in evaluating the current situation.

⇒ 4.4.7.2-2 When alarm alerts are displayed separately from other alarm information, the design should support rapid transitions between alerts, alarm priority and status information, and detailed information.

In presentations based on alarm tiles, a tile typically performs both the alerting function (i.e., providing a salient indication of the presence of an alarm condition) and the informing function (i.e., providing information that describes the nature of the alarm condition). In other designs, the alerting and informing functions may be separated. For example, a spatially dedicated display might alert the user to the presence of an alarm condition while an alarm message list provides detailed information such as the alarm parameter name and setpoint value. The presentation of the alerting and informing information should be coordinated so the user can rapidly access detailed alarm information associated with the alarm condition alerts.

⇒ 4.4.7.2-3 It should be possible to establish temporary, user-defined alarms and user-defined setpoints for specific conditions where such alarms are determined to be of assistance.

For example, users might define temporary alarms to support increased monitoring of a problem component, or at other times when they want to know of a parameter trend that is approaching a limit.

⇒ 4.4.7.2-4 When users are able to change the user-defined characteristics of alarms, the existence of such changes should be unambiguously indicated to all users, and should not interfere with normal alarm functioning

The definition and removal of user-defined alarm characteristics should be under administrative controls. It should be clearly spelled out what changes are permitted to be made by users and what changes are to be only made through the plant’s modifications process.

⇒ 4.4.7.2-5 When characteristics of alarms can be modified automatically, the change should be unambiguously signaled to all users; an indication of the current configuration should be prominently displayed.

If the operational configuration automatically changes under some alarm situations, then these configuration changes should be coupled with an alert to the users and an indication that the configuration has changed.

⇒ 4.4.7.2-6 If a change is automatically made to alarms, users should confirm the change.

While such changes may be associated with well-understood, easily recognizable plant conditions, others may be less familiar and not readily understood by plant personnel. In the latter situation, plant personnel may misunderstand the alarm information because they do not realize that alarm behavior has changed.

⇒ 4.4.7.2-7 An alarm log should be maintained to support analysis of events.

The record should include the time and sequence of alarm appearance and disappearance together with the sequence of other binary signals and analogue trends. Recorded alarm and event information can also be used for monitoring and improving the performance of the alarms.

When alarm processing and display are mediated by a comprehensive control room (or plant) information system, it may not be necessary to have a dedicated record specifically for alarms and associated events. However, to the extent that alarm information is handled by a stand-alone system, that system should be able to preserve the information.

Analysis of events may be enhanced by providing alarm displays that highlight unusual alarms, or suppress alarms that normally occur during a major plant transient, through use of processing based on stored alarm sequences for anticipated transients (EPRI, 2003).

4.4.8 Alarm Response Procedures

Alarm response procedures (ARPs) provide more detailed information concerning the nature of the alarm condition than is typically provided in the alarm message. This information is especially important to users when an unfamiliar alarm is activated or when an alarm seems inconsistent with the user's understanding of the status of the plant. ARPs may be hardcopy or computer-based display. The benefit of the latter is that the user gains instant access to detailed information about the alarm without the need to consult a hardcopy.

Important aspects of ARPs include the means by which they are accessed, their information content, and their format.

⇒ 4.4.8-1 Alarm response procedures should be available for all alarms requiring users to take an overt action affecting plant process controls or plant equipment.

Alarms that require only the user's attention (rather than action) may not require alarm response procedures. Minor alarms associated with data input errors or computer space navigation errors may also not require ARPs. In addition, other alarms such as those in systems that are separate from the main process alarms and require simple responses, may not need ARPs. In this latter case, the lack of ARPs should be specifically considered and justified.

⇒ 4.4.8-2 Alarm response procedures should be immediately accessible to users.

A user should not be required to leave the location at which the alarm is displayed in order to access ARP information. In a tile presentation, the identification and indexing of ARPs should be consistent with the method of identifying the alarm. The means used for identifying row and column locations of alarms should be distinct so that possible confusion of these identifiers is avoided. A computerized system may display the appropriate procedure for a given alarm on a VDU when the user 'selects' the alarm.

⇒ 4.4.8-3 Alarm response procedures should contain all the information the users need and should be designed so that users can use them effectively.

ARPs should contain the following information:

- The system/functional group to which the alarm belongs
- The exact alarm text or legend
- The alarm source (i.e., the sensor(s) sending the signal, processors and signal validation logic, and the actuating device(s) for the alarm with a reference to a schematic diagram on which such devices can be found)
- Alarm setpoints
- Priority
- Potential underlying causes for the alarm (e.g., low water level - inadequate feed flow)
- Required immediate actions, including actions that can be taken to confirm the existence of the alarm condition
- Actions which occur automatically when the alarm occurs (and which should be verified as having taken place)
- Follow-up actions
- Explanations of relevant alarm processing (e.g., comparisons and combinations of plant parameters; alarm filtering and suppression; alarm setpoints that are conditional, such as setpoint values and time delays used to prevent the occurrence of nuisance alarms when a parameter oscillates in an out of the alarm range)
- Pertinent references

The ARP format should highlight the ARP identifier on each page of the procedure, highlight important items, locate information categories in the same position on each page, consistently present information throughout the ARP, and minimize the need for paging back and forth to obtain the information.

⇒ 4.4.8-4 Information and terminology in alarm response procedures should be consistent with that used in other contexts.

The ARPs should use the same conventions, such as terminology for plant systems and equipment, identification codes for plant components and parameters, and measurement units, that are used in the main HSI displays and procedures. Defined values, such as alarm setpoints, should be consistent. In addition, information-coding schemes used in the ARPs should be consistent with the rest of the HSI.

4.4.9 Sources of Additional Information

Brown, W.S., O'Hara, J.M., and Higgins, J.C. (2000). *Advanced alarm systems: Revision of guidance and its technical basis* (NUREG/CR-6684). Washington, DC: U.S. Nuclear Regulatory Commission.

IEEE (1988). *IEEE standard criteria for the periodic surveillance testing of nuclear power plant generation station safety systems* (ANSI/IEEE 338-1987). New York: The Institute for Electrical and Electronics Engineers, Inc.

EEMUA (1999). Alarm systems - A guide to design, management and procurement (EEMUA Publication No. 191. London, UK: The Engineering Equipment and Materials Users Association. (http://www.eemua.co.uk/publications/cat-cont.htm).

Alarm Processing Methods – Improving Alarm Management in Nuclear Power Plant Control Rooms, EPRI, Palo Alto, CA: 2003. EPRI 1003662.

Fink, R. *A procedure for reviewing and improving power plant alarm systems, EPRI*. Palo Alto, CA: 1990. EPRI NP-3448-L-R1.

Fujii, M. (Draft, 2001). Project IEC 62241: Alarm system of the control room - Supplement to IEC 60964. International Electrotechnical Commission.

ISA (2000a). *Setpoints for safety-related instrumentation* (ISA-RP67.04.01-2000). North Carolina: Instrument Society of America.

ISA (2000b). Methodologies for determination of *setpoints for nuclear- related instrumentation.* (ISA-RP67.04.02-2000). North Carolina: Instrument Society of America.

NRC (2002) *Human-system interface design review guidelin*e (NUREG-0700, Rev 2). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Brown, W., Higgins, J., and Stubler, W. (1994). *Human factors engineering guidance for the review of advanced alarm systems* (NUREG/CR-6105). Washington, DC: U.S. Nuclear Regulatory Commission.

Sørenssen, A., Veland, Ø., Farbrot, J., Kaarstad, M., Seim, L., Fordestrømmen, M. and Bye, A. (HPR-354, 2001). *Recommendations to alarm systems and lessons learned on alarm system implementation*. Halden: OECD Halden Reactor Project.

4.5 Computer-Based Procedure Systems

4.5.1 Overview

4.5.2 Computer-Based Procedures Guidelines Checklist

4.5.3 Scope and Functionality of the CBP System

4.5.4 Display of Procedures

4.5.4.1 General

4.5.4.2 Format and Screen Layout

4.5.4.3 Procedure Steps

4.5.4.4 Warnings, Cautions, Notes, and Supplementary Information

4.5.4.5 Lists

4.5.5 Interaction with CBPs

4.5.5.1 Users' Control of Procedure Execution

4.5.5.2 Indicating the Status of Procedure Execution

4.5.5.3 Navigation

4.5.5.4 Explanation and Help

4.5.6 CBP Functions

4.5.6.1 Sensing of Plant Conditions

4.5.6.2 Providing Relevant Parameter Values and Equipment Status

4.5.6.3 Resolving Step Logic

4.5.6.4 Monitoring User Actions

4.5.7 Degraded Conditions and CBP Failure

4.5.8 Sources of Additional Information

4.5.9 Appendix: Initial Implementation and Maintenance of CBP

4.5.1 Overview

This section provides guidance on computer-based procedures. An overview of the considerations involved in designing and implementing such systems is illustrated in Figure 4-38. The detailed guidance begins with Section 4.5.3.

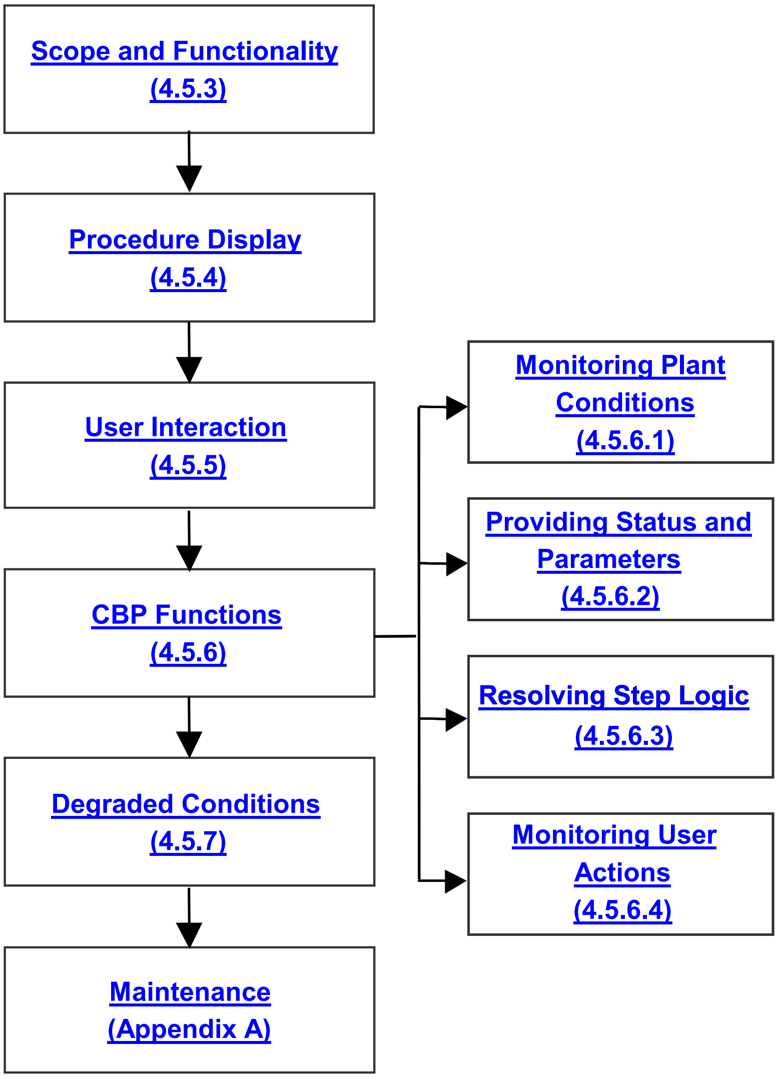


Figure 4-38
CBP Design and Implementation Considerations

Procedures are typically written documents (including both text and graphic formats) that present a series of decision and action steps to be performed by plant personnel (e.g., operators and technicians) in order to accomplish a wide variety of tasks from administration to testing and plant operation. Computer-based procedure (CBP) systems were developed to assist personnel by computerizing paper-based procedures (PBPs) with the aim of increasing the likelihood that the goals of the procedures would be achieved more efficiently.

Computerization can be applied to any procedures, e.g.,

- emergency operating procedures (EOPs)
- abnormal procedures
- normal operating procedures

- test and surveillance procedures
- maintenance procedures
- administrative procedures.

CBP systems may provide different levels of functionality, ranging from translations of traditional procedures for use via a VDU, to systems that integrate process and equipment information and alarms with procedure steps, and provide control and automation features to aid the execution of tasks. The treatment of computer-based procedures presented here was informed by examinations of current mature CBP systems (e.g., the Westinghouse COMPRO, the EdF Computerized Control Room, and the EPRI BWR EOPTS). Therefore, the guidance will allow the features and functions likely to be found in commercially available systems to be evaluated. Discussions of the HFE aspects of specific systems can be found in O'Hara, Higgins, Stubler, and Kramer (2000) and O'Hara, Pirus, Nilsen, Bisio, Hulsund, and Zhang (2001).

Computer-based procedures have the potential to greatly support crew performance. Computerizing tasks such as data gathering, monitoring of steps of continuous applicability, and keeping track of procedure navigation paths allows the crew to devote more attention to achieving the goals of the procedure. Since these tasks also demand a lot of communication and are sources of error, computerization also can improve performance (Roth and O'Hara, 2002). Computerization can also allow users to access varying levels of detail, tailor information display based on context, support simultaneous use of multiple procedures, and facilitate the administrative aspects of maintaining the technical accuracy of procedures (O'Hara et al., 2001).

Since CBPs alter the level of task-automation, they have a direct impact on crewmember roles and responsibilities (see Roth and O'Hara, 2002 for a discussion of this issue). When the procedures involve significant operations, such as emergency response, the concept of operations will be altered and the new roles and responsibilities should be addressed and evaluated as part of CBP design and implementation. Changes to the mode of interaction and degree of automation of users' tasks may require existing function allocations or task analyses to be updated or reconsidered.

Like any new technology, there are potential drawbacks to CBP implementation as well. If poorly designed, users can lose the bigger picture of objectives because the computer only shows them a small portion of the procedure at a time, automation can reduce crew independence and increase complacency, and design errors can lead to computer-based procedure errors.[5]

[5] While is may not seen like a drawback, computerized procedures can make it difficult for operators to question what the procedure is doing, or perhaps it is more accurate to say that they may be reluctant to challenge them. This may stem from two factors. First, operator may become confident in the procedures thus question it less. Second, the CBP has been developed by experts and validated; thus even if the operator detects something wrong, it may be difficult to override in real time. These issues can be addressed, in part, by (1) making the procedure "open" to inquiry so that questioning the procedure is a built-in part of its functionality, and (2) emphasize the need for operator independence as part of training.

These tradeoffs are discussed in more detail in the detailed guidance section.

The first step toward implementing computer-based procedures is to determine which procedures are to be computerized (the scope of the system) and what level of functionality the system will provide. Considerations for making these determinations are given in Section 4.5.3.

The design of CBP systems requires three types of guidance. The first type addresses the presentation of procedures per se. While some guidance of this type is given here (in Section 4.5.4), there are more detailed treatments of procedure design available, e.g., U.S. Nuclear Regulatory Commission (1982). In addition, HFE considerations related to the development of procedures are addressed by NUREG-0711, Rev.1 (Element 8, Procedures).

The second type of guidance covers the human-system interaction aspects of their design. CBPs use other HSI resources, e.g., information is presented on VDUs, and users interact with the CBP information using dialogue and navigation capabilities provided by the computer system. Many of the aspects of CBP design are addressed by human factors guidelines in other sections of this document. (For example, since the display devices and input devices for computer-based procedures are the same as for interacting with the computer-system in general, these topics are not addressed in this section.) The guidelines provided in Section 4.5.5 emphasize HSI characteristics specific to implementing procedures in computerized form, such as features that help users manage concurrent procedures or monitor continuously applicable steps in an ongoing operation. Guidance may also be needed on the human factors aspects of specific functions that a CBP system may have (e.g., providing parameter values or monitoring user actions); this guidance is given in Section 4.5.6.

Third, there are provisions for degraded conditions or CBP failure (Section 4.5.7).

Design considerations for the initial implementation of CBPs from paper procedures and CBP maintenance are addressed in the Appendix. There are also training issues associated with computerization of procedures. Guidance related to training is given in Section 3.4.

4.5.2 Computer-Based Procedures Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.5.3	Scope and Functionality of the CBP System							
	=>	4.5.3-1	Determine the scope of the computer-based procedure system; i.e., identify the procedures or types of procedures that will be computerized.					
	=>	4.5.3-2	Determine the functionality of the computer-based procedure system.					
4.5.4	Display of Procedures							
	4.5.4.1	General Alarm Display Considerations						
		=>	4.5.4.1-1	The detailed CBP design should be fully consistent with the rest of the HSI.				
		=>	4.5.4.1-2	CBP material should be legible and easy to read on any device at which it might be displayed.				
		=>	4.5.4.1-3	The display area dedicated to procedure-related information should be sufficient to show all the material that the user must view in parallel to execute a procedure step, including cautions and reference material.				
	4.5.4.2	Format and Screen Layout						
		=>	4.5.4.2-1	The procedure’s title and identification should be continuously presented.				
		=>	4.5.4.2-2	The status of high-level procedure goals should be continuously presented.				
		=>	4.5.4.2-3	The procedure’s format should reflect its organization.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.5.4.2-4	A consistent format should be used to display procedures.				
		=>	4.5.4.2-5	A consistent approach to partitioning procedures should be used.				
		=>	4.5.4.2-6	Each display screen should locate information and HSI features consistently.				
	4.5.4.3		Procedure Steps					
		=>	4.5.4.3-1	Procedure steps should be clear and unambiguous.				
		=>	4.5.4.3-2	Numerical information in procedure steps should be immediately understandable and useable.				
		=>	4.5.4.3-3	Procedure steps should be coded to indicate importance.				
		=>	4.5.4.3-4	Procedure steps should be coded to indicate when communication between the procedure user and other crew members in necessary or desirable.				
	4.5.4.4		Warnings, Cautions, Notes, and Supplementary Information					
		=>	4.5.4.4-1	The warnings and cautions applicable to a single step (or to a series of steps) should be displayed when the step(s) is on the screen.				
		=>	4.5.4.4-2	Warnings, cautions, and notes should be presented so that they will be read before the applicable action steps.				
		=>	4.5.4.4-3	Warnings, cautions, and notes should not include implied or actual action steps.				
		=>	4.5.4.4-4	Warnings, cautions, and notes should be uniquely presented, so that they are easily distinguished from each other and from other display elements.				
		=>	4.5.4.4-5	All supplementary information (such as tables and figures) associated with a procedure step and available to the CBP should be available on the screen concurrently with the step, or on another easily viewed display.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	4.5.4.5	Lists						
		=>	4.5.4.5-1	Groups of related items (e.g., actions, conditions, components, criteria, systems) should be presented as a list.				
		=>	4.5.4.5-2	Formatting should be used to differentiate items in a list from other procedure elements.				
		=>	4.5.4.5-3	The presence or absence of precedence among items in lists should be indicated.				
		=>	4.5.4.5-4	Overviews should introduce each list.				
		=>	4.5.4.5-5	The method for assuring that each item in a list has received the users' attention should be consistent.				
4.5.5	Interaction with CBPs							
	4.5.5.1	Users' Control of Procedure Execution						
		=>	4.5.5.1-1	Users should control the execution of computer-based procedures.				
		=>	4.5.5.1-2	Users should be able to evaluate the acceptability of the CBP's assessments, calculations, or recommendations and, if needed, override them.				
	4.5.5.2	Indicating the Status of Procedure Execution						
		=>	4.5.5.2-1	There should be an indication of whether or not a step was completed.				
		=>	4.5.5.2-2	Users should be alerted to incomplete procedure steps.				
		=>	4.5.5.2-3	The current procedure step(s) should be indicated.				
		=>	4.5.5.2-4	The pathway taken through procedures should be stored and made available to users.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.5.5.2-5	The user should be informed when multiple procedures or multiple procedure steps are to be followed concurrently. A list of all currently active procedures should be available.				
	4.5.5.3		Navigation					
		=>	4.5.5.3-1	Navigation support should allow users to freely and easily move between procedure steps, to other parts of the same procedure, and to other procedures.				
		=>	4.5.5.3-2	Users should be able to easily access cross-referenced information, notes, cautions, warnings, and reference material.				
		=>	4.5.5.3-3	Users should be able to easily access appropriate contingency actions.				
	4.5.5.4		Explanation and Help					
		=>	4.5.5.4-1	CBPs should have facilities to enable the user to determine how CBP functions are performed.				
		=>	4.5.5.4-2	Help for performing procedure specified activities should be provided.				
		=>	4.5.5.4-3	There should be a way for users to record their notes and comments in the CBP.				
4.5.6		CBP Functions						
	4.5.6.1		Sensing of Plant Conditions					
		=>	4.5.6.1-1	The CBP should automatically identify when the entry conditions for a procedure exist.				
		=>	4.5.6.1-2	The CBP should monitor conditions for transitioning or exiting from a procedure (or for jumping to different non-sequential steps within the procedure) and indicate when those conditions exist.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.5.6.1-3	The link from an existing procedure and the related entry to another procedure should be clearly displayed and saved.				
	=>	4.5.6.1-4	The CBP should continuously assess and present the status of higher-level safety goals, such as critical safety functions, and alert the user to any challenges.				
4.5.6.2		Providing Relevant Parameter Values and Equipment Status					
	=>	4.5.6.2-1	The CBP should automatically provide accurate and valid information on the values of parameters and status of equipment, when they are available to the system.				
	=>	4.5.6.2-2	Parameters that are displayed or used by the CBP system should be updated with a frequency that is appropriate given the purpose for which they are used, but no more frequently than the response of the underlying sensor will support.				
	=>	4.5.6.2-3	If values required when using procedures (e.g., subcooling margin) are not available from the general plant information system, the CBP system should perform those calculations.				
	=>	4.5.6.2-4	Procedure guidance should be context sensitive where possible.				
	=>	4.5.6.2-5	The CBP should provide users with clear, timely prompts when users need to input information not available to the CBP.				
	=>	4.5.6.2-6	This CBP should clearly indicate the required immediate operator actions after a reactor trip.				
4.5.6.3		Resolving Step Logic					
	=>	4.5.6.3-1	The CBP should evaluate the logic of each procedure step and provide the result to the user. The CBP should make available the inputs, logic, and results, along with any associated limitations or assumptions.				
	=>	4.5.6.3-2	The results of the step analysis should be coded to make it salient to users.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.5.6.3-3	Steps of continuous applicability, time-dependent steps, and process-dependent steps should be monitored by the CBP and the user should be alerted when conditions in those steps become effective.				
	4.5.6.4		Monitoring User Actions					
		=>	4.5.6.4-1	Users should be alerted when their inputs and actions are not consistent with CBP evaluations.				
4.5.7		Degraded Conditions and CBP Failure						
	=>	4.5.7-1	The CBP system should clearly indicate when data are degraded or unavailable.					
	=>	4.5.7-2	An alarm should be presented for loss of the CBP.					
	=>	4.5.7-3	A procedure should be available for managing operations with a degraded CBP.					
	=>	4.5.7-4	PBPs should be available for selected procedures in the event of complete CBP failure.					
	=>	4.5.7-5	Upon transfer to PBPs, a means should be provided to support the user's determination of currently open procedures, location in the procedures, completed and not completed steps, and currently monitored steps.					

4.5.3 Scope and Functionality of the CBP System

This section discusses the general considerations that should be addressed before applying the more detailed guidance in later sections.

- *Procedure design goals* – the overall vision of where the utility would like to see their procedures finally end up when all modifications are completed, e.g., fully computerized and highly automated operating and maintenance procedures vs. computerization of selected procedures with limited functionality.
- *Operating experience* – choices about scope and/or functionality may be driven by a need to address identified issues associated with existing procedures.
- *I&C considerations* – the scope of I&C modernization impacts the possible scope and functionality of the CBP system, especially in the case of higher-level functionality which requires information about plant systems to be made accessible; i.e., the implementation of higher degrees of CBP functionality require that the information that is used in the procedure be available through the I&C system.

Training considerations – the training that will be needed as computerized procedures are introduced needs to be considered. Training will be affected by a variety of factors, such as whether computerized procedures are phased in incrementally as each additional feature is added or introduced all at one time, and the nature of the backup capability if part or all of the computerized procedures should malfunction.

As with any upgrade, designers considering CBPs will need a complete and accurate understanding of the contents and use of the existing procedures. It will include assessing the types and number of procedures, the style and formats used for the procedures, how the procedures are used (individually, in groups, etc.), how procedures are revised, the practices for signoff and record keeping, etc. Without such knowledge it will be hard to determine, e.g., what has to be included in the CBP system, or whether a commercial product provides all the needed functions. Designers will also need substantial input from the plant operating staff, especially the procedure writers, experienced senior operators, training staff and the maintenance staff. Any decisions related to CBPs must have their involvement from the earliest stages.

⇒ 4.5.3-1 Determine the scope of the computer-based procedure system; i.e., identify the procedures or types of procedures that will be computerized.

One of the first considerations in designing a CBP system is the scope. As computer technology is integrated into various operations and maintenance functions, plants will typically have identified opportunities for computerizing procedures. Even if the endpoint vision calls for the computerization of all procedures, this may not be accomplished all at once (owing, for example, to limited availability of resources needed to create, verify, and test the procedures). Various approaches might be taken to the incremental computerization of a plant's procedures. In order to realize the most 'value' early in the process, utilities might choose to begin with test and maintenance procedures in order to gain experience in their use. On the other hand, utilities might give priority to procedures that, based on operating experience, are associated with operational issues. In addition, the relationships among procedures (i.e., the degree to which they reference each other) should be considered to avoid creating a situation in which it is necessary for procedure users to switch repeatedly from one medium to the other while performing a task.

Several factors (and the tradeoffs among them) should be considered in determining the scope of computerized procedures:

- Consequences of human error
- User familiarity
- Numbers of parameters and conditions to be monitored
- Numbers of parameters and conditions that are monitored
- Complexity of decision logic of procedure steps
- Numbers of deferred decisions or continuous steps
- Need for navigation (to go to other parts of a procedure or to other procedures in a non-linear way)
- Frequency of procedures changes

Factors favoring and not favoring the computerization of various types of procedures are summarized in Table 4-17.

Table 4-17
Factors Influencing the Decision to Computerize Procedures

Consideration	Computerized	Paper
Consequences of human error	Significant in terms of loss of production, equipment damage, or safety compromise.	If the consequences of deviating from procedures is not significant.
User familiarity	When users may not be very familiar with procedure use.	When users are familiar with the procedure
No. of parameters/conditions to be monitored	Large	Small
No. of parameters/conditions that are monitored	When many parameters/conditions are available to the CBP	When only a few of the parameters/conditions are available to the CBP
Complexity of decision logic of procedure steps	Complex logic is used (e.g., conditional and Boolean)	No or simple logical analysis is needed
Deferred decisions or continuous steps	Procedure includes such steps	None or very few
Need for navigation (within and between procedures)	High	Low
Frequency of procedures changes	Frequent	Seldom

⇒ 4.5.3-2 Determine the functionality of the computer-based procedure system.

Once the desired scope has been identified, the next consideration is the level of functionality to be provided by the CBP system, since systems differ in terms of their levels of functionality they provide (i.e., the extent to which they provide features beyond the basic procedure elements). For example, to allow manual control of components, the CBP must include a control, e.g., a soft control, for that equipment.

On the low end of the functionality spectrum, procedures might simply be presented on a VDU nothing done automatically. We do not recommend this option because it has all of the disadvantages of VDU-based information displays without most of the benefits associated with computerization.

In the middle of the functionality spectrum is a system that would monitor procedure-referenced parameter and equipment status, resolve step logic, and provide support for navigation and place keeping. Based on the research and experience to date, this is the minimal functionality recommended. It provides great support to procedure use by handling much of the busy work involved in procedure use. Crews can then attend to the higher goals of monitoring the procedures success at achieving goals.

At the other end of the continuum are systems that execute procedure steps by obtaining information from and sending control inputs directly to the systems that are the subject of the procedure, with only supervisory involvement of the user. Again, in the extreme, these might better be thought of as automated functions rather than computerized procedure systems. When a high degree of automation is included in a procedure system to assist users in executing steps, the system's HSI must include features that allow users to supervise and evaluate the automation's performance. Such an interface would provide tool for the operator to see the systems analysis of any step or decision.

In some cases, highly automated functioning may not necessarily be advisable. (The human performance issues associated with automation have been well documented; see O'Hara, Stubler, and Higgins, 1996). For example, when the procedures or steps are selected automatically, users involvement in the activity can be reduced. In such a case, it is better for the responsibility for selecting steps or procedures to be shared between the user and the system, rather than being fully automated; i.e., the system might identify the next appropriate step or procedure, but the act of invoking it would be performed by the user.

Another aspect of procedure automation that should be considered is the analysis of procedure step logic; that is, comparing actual parameter values to the reference value in procedures using the logical relationships described in the step. To support computerization of procedures, some of the steps may have to be specified more precisely to eliminate any ambiguity that might exist. For example, if an apparently straightforward statement such as "If pressure is decreasing..." is implemented in the CBP as a simple check of the sign of the change in pressure at a particular time (when what is implied by the condition is a consistent decrease of an operationally significant size), the CBP may interpret a small, momentary downward fluctuation as satisfying the condition, potentially misleading the user Thus, computerizing procedures may require that non-specific or subjectively worded steps be clarified.

4.5.4 Display of Procedures

Computerization of procedures involves display of procedures via a computer-driven medium (typically a VDU) rather than on paper. In addition to some general principles, this section contains specific guidance on procedure steps, the display of warnings and cautions, the presentation of information in lists, and the organization and layout of computerized procedures.

4.5.4.1 General

⇒ 4.5.4.1-1 The detailed CBP design should be fully consistent with the rest of the HSI.

HSI features for format and functionality (such as labeling, acronyms, dialog conventions, use of colors, and input devices) should be consistent between the CBP and other HSI components. Consistency may be a special consideration when reviewing ‘off-the-shelf’ systems.

⇒ 4.5.4.1-2 CBP material should be legible and easy to read on any device at which it might be displayed.

CBPs should conform to guidance given in this document (see Section 4.1) and elsewhere regarding presentation of information on computer-driven displays, e.g., selection of fonts, use of color, and presentation of text, tables, and figures.

⇒ 4.5.4.1-3 The display area dedicated to procedure-related information should be sufficient to show all the material that the user must view in parallel to execute a procedure step, including cautions and reference material.

Windowing allows supplementary or reference information to be presented with procedures on the same VDU; this is an effective technique for displaying material that is typically consulted for a short time and then no longer needed. However, when information must be used simultaneously (e.g., comparing displayed measurements to tabled values) in executing a step, it may be necessary to provide more display area (i.e., multiple displays) for procedure information to avoid having important information obscured or requiring users to repeatedly manipulate windows.

4.5.4.2 Format and Screen Layout

PBPs generally present the basic steps in a step-by-step format (e.g., operating or test procedures), in a two-column format (e.g., Westinghouse PWR EOPs), or in a flowchart format (e.g., BWR EOP). Figures 4-39 and 4-40 show the presentation of EOPs in computerized format using Westinghouse’s Computerized Procedure (COMPRO) system.

The Westinghouse system uses two VDUs to display procedure information. (Figure 4-39). The main procedure step display is shown in Figure 4-40. Note that the display shows the current step in detail and the previous and next steps in brief to provide the procedure context. The status of critical safety functions is shown in the upper left panel. Color coding is used to show status. COMPRO is used in several NPPs, including the Beznau plant in Switzerland, where it was included as part of a plant modernization program.

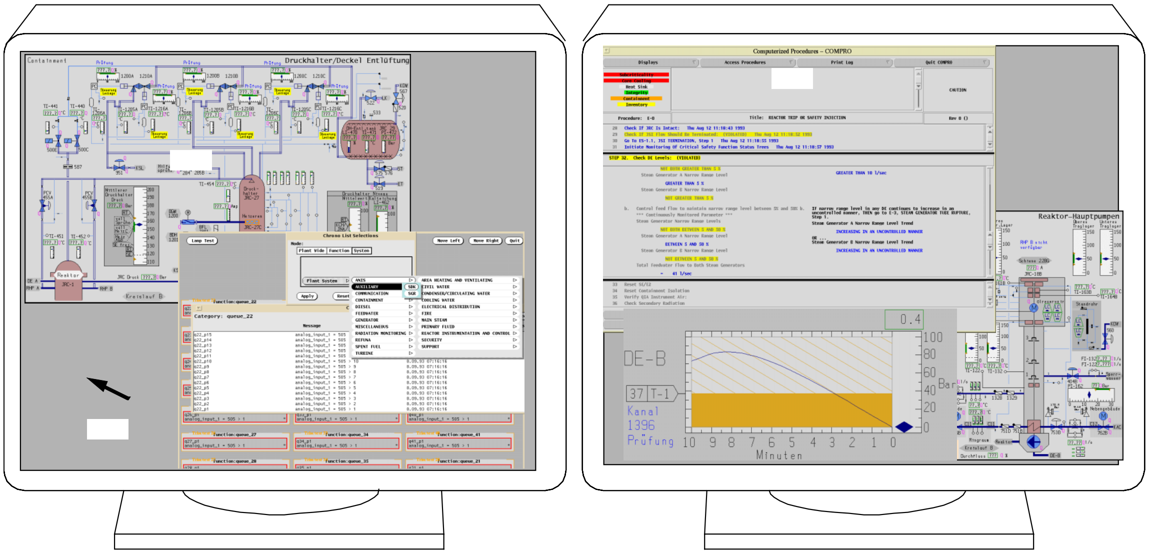
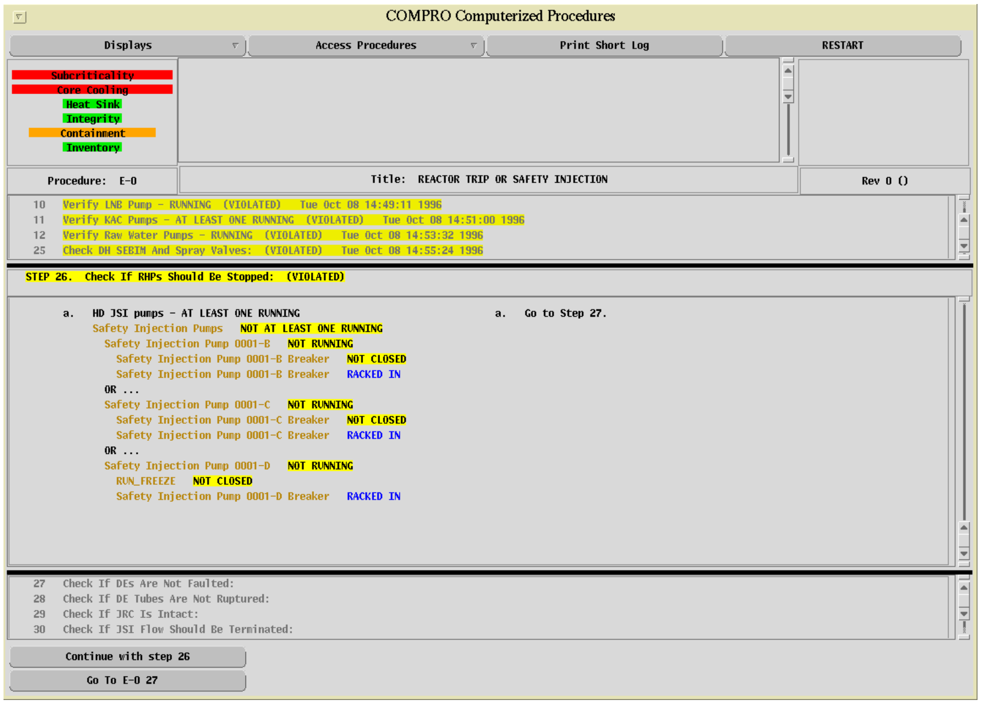


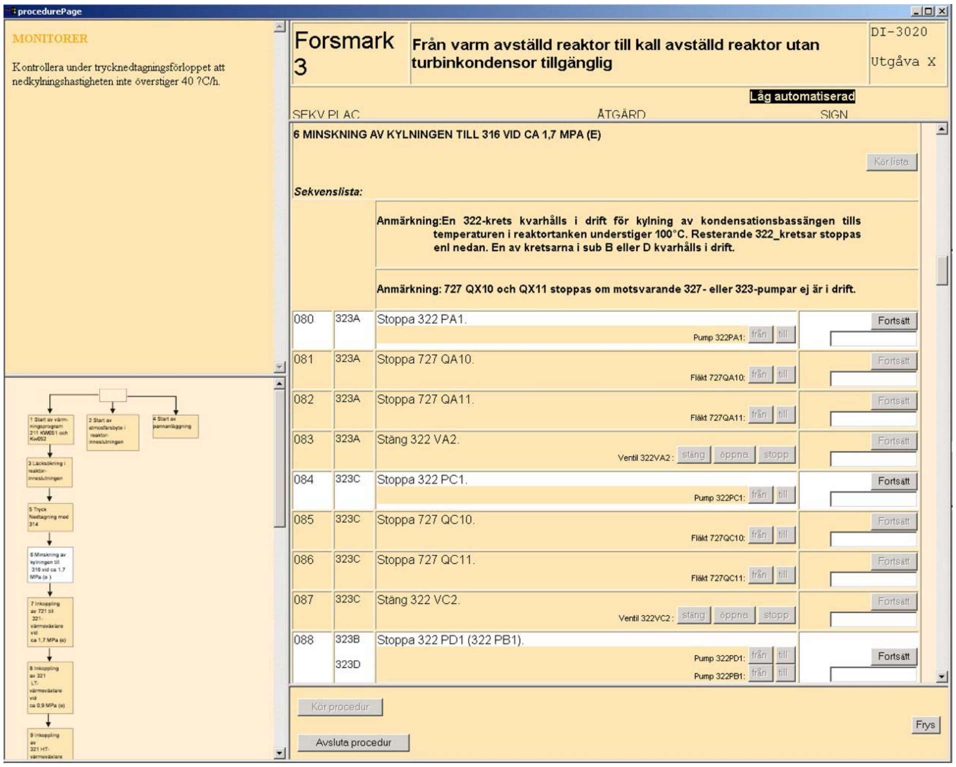
Figure 4-39
CBP Workstation for the Westinghouse COMPRO System



```
Procedure:   E-0          Title:   REACTOR TRIP OR SAFETY INJECTION          Rev 0 ()

  10   Verify LNB Pump - RUNNING  (VIOLATED)   Tue Oct 08 14:49:11 1996
  11   Verify KAC Pumps - AT LEAST ONE RUNNING  (VIOLATED)   Tue Oct 08 14:51:00 1996
  12   Verify Raw Water Pumps - RUNNING  (VIOLATED)   Tue Oct 08 14:53:32 1996
  25   Check DH SEBIM And Spray Valves:  (VIOLATED)   Tue Oct 08 14:55:24 1996

STEP 26.  Check If RHPs Should Be Stopped:  (VIOLATED)

     a.   HD JSI pumps - AT LEAST ONE RUNNING                   a.   Go to Step 27.
          Safety Injection Pumps   NOT AT LEAST ONE RUNNING
            Safety Injection Pump 0001-B   NOT RUNNING
              Safety Injection Pump 0001-B Breaker   NOT CLOSED
              Safety Injection Pump 0001-B Breaker   RACKED IN
            OR ...
            Safety Injection Pump 0001-C   NOT RUNNING
              Safety Injection Pump 0001-C Breaker   NOT CLOSED
              Safety Injection Pump 0001-C Breaker   RACKED IN
            OR ...
            Safety Injection Pump 0001-D   NOT RUNNING
              RUN_FREEZE   NOT CLOSED
              Safety Injection Pump 0001-D Breaker   RACKED IN

  27   Check If DEs Are Not Faulted:
  28   Check If DE Tubes Are Not Ruptured:
  29   Check If JRC Is Intact:
  30   Check If JSI Flow Should Be Terminated:
```

Figure 4-40
Main Procedure Display for the Westinghouse COMPRO System

Of course, other formats may also be used for CBPs. Figure 4-41 shows a screen from the CBP system at the Forsmark plant in Sweden (another plant that has modernized). This was developed using the Halden Reactor Project's Computerized Operation Manual (COPMA) software. The right panel shows the current steps and the lower left provides and overview of all steps.



procedurePage

MONITORER

Kontrollera under trycknedtagningsförloppet att nedkylningshastigheten inte överstiger 40 ?C/h.

Forsmark 3

Från varm avställd reaktor till kall avställd reaktor utan turbinkondensor tillgänglig

DI-3020

Utgåva X

Låg automatiserad

SEKV PLAC ÅTGÄRD SIGN

6 MINSKNING AV KYLNINGEN TILL 316 VID CA 1,7 MPA (E)

Sekvenslista:

Anmärkning:En 322-krets kvarhålls i drift för kylning av kondensationsbassängen tills temperaturen i reaktortanken understiger 100°C. Resterande 322_kretsar stoppas enl nedan. En av kretsarna i sub B eller D kvarhålls i drift.

Anmärkning: 727 QX10 och QX11 stoppas om motsvarande 327- eller 323-pumpar ej är i drift.

SEKV	PLAC	ÅTGÄRD	SIGN
080	323A	Stoppa 322 PA1. Pump 322PA1: från till	Fortsätt
081	323A	Stoppa 727 QA10. Fläkt 727QA10: från till	Fortsätt
082	323A	Stoppa 727 QA11. Fläkt 727QA11: från till	Fortsätt
083	323A	Stäng 322 VA2. Ventil 322VA2 : stäng öppna stopp	Fortsätt
084	323C	Stoppa 322 PC1. Pump 322PC1: från till	Fortsätt
085	323C	Stoppa 727 QC10. Fläkt 727QC10: från till	Fortsätt
086	323C	Stoppa 727 QC11. Fläkt 727QC11: från till	Fortsätt
087	323C	Stäng 322 VC2. Ventil 322VC2 : stäng öppna stopp	Fortsätt
088	323B 323D	Stoppa 322 PD1 (322 PB1). Pump 322PD1: från till Pump 322PB1: från till	Fortsätt

Kör lista
Kör procedur
Avsluta procedur
Frys
1 Start av värm-ningsprogram 211 KW051 och Kw052
2 Start av atmosfärsbyte i reaktor-inneslutningen
4 Start av pannanläggning
3 Läcksökning i reaktor-inneslutningen
5 Tryck Nedtagning med 314
6 Minskning av kylningen till 316 vid ca 1,7 MPa (e)
7 Inkoppling av 721 till 321-värmeväxlare vid ca 1,7 MPa (e)
8 Inkoppling av 321 LT-värmeväxlare vid ca 0,9 MPa (e)
9 Inkoppling av 321 HT-värmeväxlare

Figure 4-41
Main Procedure Display for the Forsmark CBP using COPMA

Regardless of the format used to present the procedures, the designer must decide whether they will be presented to the user in a continuous, scrollable display or divided into discrete display pages. General human-computer interaction guidance is equivocal on the question, except to point out that paging is preferable for novice users (perhaps because page boundaries provide 'landmarks'). However, in the case of a CBP, training will ensure that users are familiar with both its content and its user interface. Furthermore, it may not be possible to partition procedures into coherent pages that can be presented entirely within the available display space. In addition, if the displayed procedure information is changeable (e.g., if different levels of detail can be shown), the lengths of pages will vary. Under such circumstance it may be preferable to consistently use scrolling.

The overall screen layout for presentation of the procedure elements refers to the

- determination as to what information should be continuously presented
- manner in which individual procedure elements are presented.

For example, the procedure title and identification information should be continuously presented at the top of the CBP screen, while the steps may be shown in a scrollable window.

Supplementary information may be represented in a separate window or VDU. The CBP may also display such supporting features as bookmarks, checklists, and user comments.

Presentation formats, such as columns and flowcharts, can be enhanced by the coding capabilities of computer-based displays, e.g., color, flashing, animation, and auditory cueing. Coding is generally used to increase the salience of important information. CBPs use coding for conditions such as:

- whether procedure step logic is satisfied or not
- whether information is static or dynamic with plant state
- when a caution is in effect
- when a change in the status of a continuously monitored step has occurred

CBPs can be designed to allow users to choose the level of detail in which procedures are presented. For example, users may select to have less detail displayed when a procedure step is satisfied. Alternatively, a user may choose to show all of the individual evaluations that led to the conclusion that the step is satisfied.

Similarities in format between CBPs and the existing PBPs can help users adapt to CBPs when they are first introduced. Furthermore, since PBPs provide backup if the CBP system fails, consistency between the two must be maintained. However, changes will be necessary to take advantage of computer functionality and tradeoffs should be considered. It has been suggested that adding functionality (e.g., hyperlinks) will be less disruptive than reorganizing the information presentation (O'Hara et al., 2001).

⇒ 4.5.4.2-1 The procedure's title and identification should be continuously presented.

This information helps set the context for the overall procedure within which its steps are interpreted. It is especially important when more than one procedure can be open at one time.

⇒ 4.5.4.2-2 The status of high-level procedure goals should be continuously presented.

This information helps set the overall context in which procedure steps are interpreted. Continuous presentation of high-level goal status, such as status of critical safety functions, will facilitate users' awareness of them, particularly when more than one procedure is open simultaneously.

⇒ 4.5.4.2-3 The procedure's format should reflect its organization.

Formatting methods to indicate the organization of a procedure may include the use of headings or colors to distinguish parts of the procedure.

⇒ 4.5.4.2-4 A consistent format should be used to display procedures.

Whether procedures are presented in text, flowchart, or otherwise, a consistent approach across procedures will facilitate using and moving between multiple procedures.

⇒ 4.5.4.2-5 A consistent approach to partitioning procedures should be used.

Partitioning refers to how a procedure is organized to be displayed on the VDU screen. For example, it may be divided into distinct pages, and users would navigate from one to the next. Alternatively, it may be presented as one continuous display that the user scrolls.

⇒ 4.5.4.2-6 Each display screen should locate information and HSI features consistently.

When the information and features, such as procedure steps, controls, and navigation aids are consistently located, users' performance improves because expectations can guide the search for information, and reduce the time and workload associated with finding it.

4.5.4.3 Procedure Steps

Steps are the basic unit of the procedure. Each step is composed of a verb and a direct object. In general, the rules of English grammar are followed and the syntax reflects concise language that is simply stated, explicit, and consistent. Decision steps provide instructions to evaluate conditions and then to choose appropriate action(s) from a predefined set. The decisions may involve conditional logic, i.e., where actions are to be performed only if a specified set of conditions exists. Action steps identify actions to be taken; i.e., instructions to perform physical (e.g., "Depress") and mental (e.g., "Verify") actions as well as describing the objective of those actions. Some procedure steps (e.g., in EOPs) have a dual nature, with an action to be accomplished in one column and a second action if the first is not successful. Some procedure steps may also require calculations.

Implementation of procedures has a temporal flow, i.e., some steps are taken when encountered, others are performed continuously (i.e., steps of continuous applicability), while others are done based on time or process criteria. Performance of a procedure step may be supported by information, such as cautions and notes, that qualifies the actions and decisions required.

⇒ 4.5.4.3-1 Procedure steps should be clear and unambiguous.

Steps should be worded so that they are easily understood and interpreted without error. The presentation should conform to principles for text display given elsewhere in this document (e.g., Section 4.1.3.1, Continuous Text Displays). There is considerable guidance on procedure design (e.g., U.S. Nuclear Regulatory Commission, 1982; Weiringa, Moore, and Barnes, 1993; NUREG-0700, Rev.2). The following are some key principles:

- Procedure steps should be written as short sentences.
- Procedure steps should be written in active voice.
- Procedure steps should be written as positive commands.
- Short, simple words from standard American English should be used.

- Punctuation should conform to standard American English usage.
- Words, phrases, and equipment names and numbers should be used consistently within and among procedures, drawings, other HSIs, and equipment labels.
- Abbreviations and acronyms should be used consistently and limited to those well known to the users.

⇒ 4.5.4.3-2 Numerical information in procedure steps should be immediately understandable and useable.

Guidance on the presentation of numerical information in procedures is given in the same sources cited above. The following are some principles regarding the use of numbers in procedures:

- Numerical information should include units of measure.
- Numbers should be specified at the appropriate precision.
- Ranges of numbers should be specified, rather than error bands.
- Arabic numerals should be used.
- Numbers that are spelled out should be consistently spelled under the same conditions.

⇒ 4.5.4.3-3 Procedure steps should be coded to indicate importance.

Steps with important consequences to equipment and safety should be clearly indicated in the procedure step presentation.

⇒ 4.5.4.3-4 Procedure steps should be coded to indicate when communication between the procedure user and other crew members in necessary or desirable.

Some procedure steps may require users to obtain information from other crew members, such as a valve position not sensed by the I&C. This should be clearly indicated in the presentation of the step. In addition, since CBPs can be often used by one crewmember, it is a good practice to build in places where crew communication and coordination should occur to support teamwork.

4.5.4.4 Warnings, Cautions, Notes, and Supplementary Information

Warnings alert users of procedures to potential hazards of their actions that may result in death or injury. Cautions alert operators to potential hazards of their actions that may damage machinery or equipment. Notes call attention to important supplemental information that may enhance an operator’s understanding and performance of the procedure. Procedure steps may reference supplementary material that helps the operator implement the step; it can be in the form of tables, figures, lists, text, or numeric information.

⇒ 4.5.4.4-1 The warnings and cautions applicable to a single step (or to a series of steps) should be displayed when the step(s) is on the screen.

Displaying warnings and cautions at the same time as their associated procedure steps will help ensure that users read the information when they evaluate the step. Information provided elsewhere may be overlooked, or may require retrieval by distracting and time-consuming actions.

⇒ 4.5.4.4-2 Warnings, cautions, and notes should be presented so that they will be read before the applicable action steps.

Displaying warnings, cautions, and notes before action steps will help ensure that users will read the information before taking action. Information provided in other places may be overlooked or may be distracting and time consuming to retrieve.

⇒ 4.5.4.4-3 Warnings, cautions, and notes should not include implied or actual action steps.

Actions should be specified in procedure steps only.

⇒ 4.5.4.4-4 Warnings, cautions, and notes should be uniquely presented, so that they are easily distinguished from each other and from other display elements.

Techniques used to highlight warnings, cautions, or notes (e.g., displaying text in a different font or color, or adding a colored background or border) should be used only for that purpose, so that this material will be immediately recognized.

⇒ 4.5.4.4-5 All supplementary information (such as tables and figures) associated with a procedure step and available to the CBP should be available on the screen concurrently with the step, or on another easily viewed display.

Results (such as calculations or table lookups) that are needed to complete a step should be presented directly in the context of the step; see 4.5.6.2-3. Additional information (e.g., tables or figures) should be easily called up if needed.

4.5.4.5 Lists

Procedures frequently use lists to present groups of items such as actions, conditions, components, criteria, and systems. When lists are used in CBPs, additional consideration must be given to the grouping of items, provision of check-off capability, and alerts to items that may be overlooked.

⇒ 4.5.4.5-1 Groups of related items (e.g., actions, conditions, components, criteria, systems) should be presented as a list.

A series of items given in continuous text is not as easy to read as a list.

⇒ 4.5.4.5-2 Formatting should be used to differentiate items in a list from other procedure elements.

Items in a list can be set off other text (and from each other) by using white space, bullet symbols, or a distinctive font, for example.

⇒ 4.5.4.5-3 The presence or absence of precedence among items in lists should be indicated.

It should be clear to users whether some items take precedence over others.

⇒ 4.5.4.5-4 Overviews should introduce each list.

An example of an overview is “Ensure that all of the following tests were completed”.

⇒ 4.5.4.5-5 The method for assuring that each item in a list has received the users’ attention should be consistent.

For example, an electronic checklist may be provided so that users can check off items they have attended to. The means for indicating completed items and the ways in which completed items are presented should be the same throughout the CBP system. If users proceed before all items are checked off, the CBP may alert them to the unchecked items.

4.5.5 Interaction with CBPs

4.5.5.1 Users’ Control of Procedure Execution

⇒ 4.5.5.1-1 Users should control the execution of computer-based procedures.

The CBP should not constrain the ways in which user perform tasks. For example, users should have the flexibility to move around within the procedure, so that they can check and make verifications. Furthermore, to maintain situation awareness, user should also control the pace at which steps are followed.

⇒ 4.5.5.1-2 Users should be able to evaluate the acceptability of the CBP’s assessments, calculations, or recommendations and, if needed, override them.

The users should be able to verify the CBP system’s assessment of plant status. This verification includes process parameters, equipment status, analysis of procedure step logic, and evaluation of cautions. Any analysis done by the CBP should be accessible to users for review. The methods by which CBPs analyze procedure steps should be consistent with the methods by which users analyze steps in procedure logic steps, so that the results are understandable.

4.5.5.2 Indicating the Status of Procedure Execution

⇒ 4.5.5.2-1 There should be an indication of whether or not a step was completed.

The indication can be manual or automatic, depending on whether the CBP has the specific criteria and information to determine this. If a plant's existing procedures require individual steps or groups of steps to be "signed off" by procedure users (as in maintenance procedures, for example), the means by which the equivalent capability will be implemented in the CBP system should be considered.

⇒ 4.5.5.2-2 Users should be alerted to incomplete procedure steps.

The alert should be advisory and not discourage the crew's actions.

⇒ 4.5.5.2-3 The current procedure step(s) should be indicated.

⇒ 4.5.5.2-4 The pathway taken through procedures should be stored and made available to users.

A history should be maintained and available for display on request. Time-stamping of step completion can facilitate not only post-hoc incident analysis, but also real-time operations. The ability to reconstruct the past pathway through the procedures can help users orient themselves.

⇒ 4.5.5.2-5 The user should be informed when multiple procedures or multiple procedure steps are to be followed concurrently. A list of all currently active procedures should be available.

It may be helpful for the list of active procedures to include start and stop times for the procedures in use.

4.5.5.3 Navigation

⇒ 4.5.5.3-1 Navigation support should allow users to freely and easily move between procedure steps, to other parts of the same procedure, and to other procedures.

Users should not be forced to access procedures in a fixed sequence of the procedure nor should their access to supporting information be limited. The CBP system should support parallel access to information, i.e., users should be free to navigate as needed to consult multiple sources of information.

⇒ 4.5.5.3-2 Users should be able to easily access cross-referenced information, notes, cautions, warnings, and reference material.

Techniques such as hyperlinks can expedite navigation to information material cross-referenced in a procedure or its supporting material. Links to communication and help facilities should also be provided.

⇒ 4.5.5.3-3 Users should be able to easily access appropriate contingency actions.

4.5.5.4 Explanation and Help

⇒ 4.5.5.4-1 CBPs should have facilities to enable the user to determine how CBP functions are performed.

When CBPs support users' decision making, such as offering advice on how to select procedures, analyze step logic or follow procedure paths, users should be able to examine the basis for the advice. That is, user should be able to inspect the parameter values, system conditions, and procedure logic that the CBP used in making a selection or recommendation.

⇒ 4.5.5.4-2 Help for performing procedure specified activities should be provided.

The CBP should make available information to help operators carry out procedure steps. For example, a help facility could provide information on how a control action should be carried out.

⇒ 4.5.5.4-3 There should be a way for users to record their notes and comments in the CBP.

CBP systems should support improvements in procedures. One way to do this is to allow users of procedures to note instances in which the procedure doesn't cover specific situations or actions. These annotations could be consulted to identify aspects of the procedure that need improvement.

4.5.6 CBP Functions

CBP systems may provide assistance for or automate certain functions that would otherwise be performed manually by the users of conventional procedures. Guidance for implementing such functions is given below, grouped by the general types of support provided by the CBP system. Which, if any, of the guidance applies to a given design will depend on the level of assistance or automation the CBP system includes.

4.5.6.1 Sensing of Plant Conditions

⇒ 4.5.6.1-1 The CBP should automatically identify when the entry conditions for a procedure exist.

This capability will help users determine the appropriate procedures for the existing plant situation.

⇒ 4.5.6.1-2 The CBP should monitor conditions for transitioning or exiting from a procedure (or for jumping to different non-sequential steps within the procedure) and indicate when those conditions exist.

This capability will help users determine when procedures they are using are no longer appropriate for the existing situation.

⇒ 4.5.6.1-3 The link from an existing procedure and the related entry to another procedure should be clearly displayed and saved.

⇒ 4.5.6.1-4 The CBP should continuously assess and present the status of higher-level safety goals, such as critical safety functions, and alert the user to any challenges.

4.5.6.2 Providing Relevant Parameter Values and Equipment Status

⇒ 4.5.6.2-1 The CBP should automatically provide accurate and valid information on the values of parameters and status of equipment, when they are available to the system.

It should be clear to users what specific information is used as the source of these actual values and states. If the quality of the information provided is degraded, this should be indicated to the user (see Section 4.5.7); if users repeatedly encounter invalid information, they may lose confidence in the system.

⇒ 4.5.6.2-2 Parameters that are displayed or used by the CBP system should be updated with a frequency that is appropriate given the purpose for which they are used, but no more frequently than the response of the underlying sensor will support.

Information requirements should be analyzed to determine the rate at which the CBP system updates the parameters it accesses. This will depend on the rapidity with which particular parameters can change, and the urgency with which a particular change must be indicated to the user. The aim is to prevent users from being unaware of important changes in status owing to unreported changes and, on the other hand, to avoid placing unrealistic burdens on data sensing and processing resources by requiring unnecessarily high refresh rates.

⇒ 4.5.6.2-3 If values required when using procedures (e.g., subcooling margin) are not available from the general plant information system, the CBP system should perform those calculations.

For example, the computer system can perform computations or projections and display them for use in procedures. A potential use is in post reactor trip state for time to boiling calculations when conditions warrant computation.

Calculation of a single variable should not be done at multiple locations owing to the difficulty of assuring that any changes to the algorithm are properly accounted for in all systems.

Sensor accuracy may be a factor (e.g., for Small Subcooling Margins); see 4.5.7-4.

⇒ 4.5.6.2-4 Procedure guidance should be context sensitive where possible.

For example, the CBP system should not require an action to be taken to start a pump when it can determine that the pump is already running or is "out of service." However, the desired or expected action or state should be presented to the operator, along with the actual process conditions.

⇒ 4.5.6.2-5 The CBP should provide users with clear, timely prompts when users need to input information not available to the CBP.

CBPs may rely on users to evaluate parameter values, equipment status (such as whether a valve is open or closed), analyses of logic steps where users' judgment is involved, or to assess any conditions not within the capability of the CBP.

⇒ 4.5.6.2-6 This CBP should clearly indicate the required immediate operator actions after a reactor trip.

Such information could be provided in a table listing:

- all of the parameters required to be checked
- the procedure required value
- the actual value as sensed by the I&C system
- an indication of whether the current situation is acceptable or not (e.g., with a green/ red color).

There are typically about 20 parameters that address the critical safety functions. This allows the operator a quick check that all required parameters are acceptable. It also allows a more specific check of actual values for each parameter if/when desired. The information could possibly be presented in two levels/screens.

4.5.6.3 Resolving Step Logic

⇒ 4.5.6.3-1 The CBP should evaluate the logic of each procedure step and provide the result to the user. The CBP should make available the inputs, logic, and results, along with any associated limitations or assumptions.

Procedure steps often contain logical relationships; for example, actions are to be performed if an identified set of conditions exists. As noted earlier, the computerization of the procedure may require that some steps be more precisely defined so that all of the considerations that users do when evaluating the step is included.

There are options for how to present results to the users. One approach is to make the results immediately known and displayed. The alternative is to have the user analyze the step first, and then the user's input is compared to the computer analysis. The latter approach ensures the user stays in the loop be doing the analysis independently from the system. However, it requires increased workload and time when compared with the former. Both approaches are use in current commercial systems.

⇒ 4.5.6.3-2 The results of the step analysis should be coded to make it salient to users.

⇒ 4.5.6.3-3 Steps of continuous applicability, time-dependent steps, and process-dependent steps should be monitored by the CBP and the user should be alerted when conditions in those steps become effective.

The analysis must be carefully verified to avoid oversimplifying its logic. The alert should not automatically remove the user's current display. Instead, it should be presented as a supplemental display or as an alert.

4.5.6.4 Monitoring User Actions

⇒ 4.5.6.4-1 Users should be alerted when their inputs and actions are not consistent with CBP evaluations.

The alert should be advisory and informative only; the CBP system should not prevent the user from taking an action. This helps make the system more error-tolerant by support users in detecting their errors. However, users may have valid reasons for their actions, so their actions should not be discouraged. This interaction must be supported with training, so users recognize the role of such messages and functions.

4.5.7 Degraded Conditions and CBP Failure

CBP conditions can degrade along a continuum from loss of a single data point to complete loss of the system.

⇒ 4.5.7-1 The CBP system should clearly indicate when data are degraded or unavailable.

To the extent the CBPs display or perform functions (e.g., resolving step logic) based on data from other systems or equipment, it is important to make users of the procedures aware of any degradation in the quality of that data. Procedures used in important operations that cannot be suspended or put off while the system is repaired should be able to continue to be used, albeit with manual input of data that is normally made available automatically.

⇒ 4.5.7-2 An alarm should be presented for loss of the CBP

⇒ 4.5.7-3 A procedure should be available for managing operations with a degraded CBP.

The transition from computer to paper procedures is supported by the availability of a procedures that describes the actions to be taken in case abnormalities are detected. The procedure should address when the user should leave the CBP (what criteria) and how to manage the transition.

⇒ 4.5.7-4 PBPs should be available for selected procedures in the event of complete CBP failure.

Backup is necessary for procedures used in important operations that cannot be suspended or put off while the system is repaired. For example, in the case of EOPs a delay in operations in the event of a failure may not be acceptable, and some form of procedure backup is warranted.

⇒ 4.5.7-5 Upon transfer to PBPs, a means should be provided to support the user's determination of currently open procedures, location in the procedures, completed and not completed steps, and currently monitored steps.

When the CBP is lost, it may be difficult for users to reconstruct this information from memory. Therefore, the user should be supported in making a safe, easy transition. For example, a CBP system might automatically print out a status sheet with this information once every minute so that if it fails, the user can retrieve the latest sheet and use it to establish the crew's tasks for using PBPs.

4.5.8 Sources of Additional Information

There are very few standards, guidelines, or other documents that address the design of computer-based procedures. Technically oriented discussions can be found in the following documents. These also provide references to other such documents.

O'Hara, J., Higgins, J., Stubler, W., and Kramer, J. (2000). *Computer-based procedure systems: Technical basis and human factors review guidance* (NUREG/CR-6634). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Pirus, D., Nilsen, S., Bisio, R., Hulsund, J-E., and Zhang, W. (2001). *Computerisation of procedures – Lessons learned and future perspectives* (HPR-355).

Halden, Norway: OECD Halden Reactor Project.

O'Hara, J. Stubler, W., and Higgins, J. (1996). Hybrid human-system interfaces: Human factors considerations (BNL Report J6012-T1-4/96). Upton, NY: Brookhaven National Laboratory.

Roth, E. and O'Hara, J. (2002). Integrating digital and conventional human system interface technology: Lessons learned from a control room modernization program. (NUREG/CR-6749). Washington, D.C.: U.S. Nuclear Regulatory Commission.

U.S. Nuclear Regulatory Commission (1982). *Guidelines for the preparation of emergency operating procedures* (NUREG-0899). Washington, DC: U.S. Nuclear Regulation Commission.

Wieringa, D., Moore, C., and Barnes, V. (1993) *Procedure writing: Principles and practices*. Piscataway, NJ: IEEE Press.

4.5.9 Appendix: Initial Implementation and Maintenance of CBP

This Appendix addresses the transition from PBPs to CBPs and CBP maintenance issues. The topics addressed are:

- transforming the existing procedures into computer amenable formats
- identification of the procedural structure and its elements
- linking the procedure system to the process database
- configuring/implementing the user interfaces
- inserting and deleting procedures in the set of procedures
- modifying procedures
- updating plant instrumentation
- changing or replacing adjoining systems
- replacing the computerized procedure system software

Transforming the Existing Procedures Into Computer Amenable Formats

The contents of paper-based procedures will have to be transformed into electronic (i.e., computer-readable) form before they can be developed into a computer-based system. If the (paper) procedure documents are produced using word processing software, this step is trivial. For purely paper systems, however, it can be labor intensive. Optical character recognition systems may assist in the transformation (depending on the quality of the printed documents), but careful checking will be needed to ensure that errors are not introduce during the process.

Identification of the Procedural Structure and Its Elements

The content of this task may be highly diverse depending on the particular procedure system being used. As a general rule, the more sophisticated the procedure system, the more complicated the task. To illustrate the type of activities within this task, consider the example of a structural component that is part of almost all kinds of procedure systems. A procedure is typically made up of a set of instructions. This means that parts of the transformed (i.e., electronically formatted) procedures must be grouped into chunks, with each chunk representing an individual instruction. Such a chunking process is useful to help the operator keep a record of what instructions have been completed and what instructions are under execution. In a very rudimentary procedure system, this can be used to allow different coloring of the displayed text, depending on the status of the instruction. A small elaboration of the structure, associating a small descriptive text to each instruction, could be used to generate a list of instructions. In this list of instructions, each item could be colored according to the status of the instruction, and clicking on a given instruction labeling could result in a navigation to the complete instruction. Without this extra structuring of the original text, the operator would be obliged to manually mark the text while executing the procedure, and there would be no help for navigating in the procedure (other than general text search).

Most procedure systems will have a more sophisticated procedure structure than the one in this example, e.g., steps, sub-steps, individual instructions at an arbitrary depth, branching points etc. The means for accomplishing the structuring is an important consideration. Early computerized procedure systems (some of which are still on the market) provided a special purpose editor to do this. The editor would use a format proprietary to the system to maintain the structuring of the procedure. The internal format of the procedure was not intended to be used directly by the utility's system personnel; this was even considered potentially harmful since it might introduce inconsistencies, especially in situations where more than one file was used to store the set of procedures). In some cases this made the migration process exceptionally laborious, since it required a person to re-type the procedures text into various slots in a frame-based editor. The availability of cut-and-paste functionality would facilitate the process a little, since the various parts of the text could be copied from the original word processor file and into the editor. Still, even with a cut and paste functionality, the migration becomes cumbersome, because it can in no respect be automated. Returning to our example above, it may be much more convenient to mark the text directly in a word processing program, e.g. by brackets (given such brackets are not used for any other purpose); i.e., {{short description 1}original text instruction 1}{{short description 2} original text instruction 2}.....{{short description n} original text instruction n}. The structuring could then be automated using a script that would transform this format into the format required by the computerized procedure system. This is only possible if the computerized tool is based on an open procedure representation format; the following recommendation should be considered.

It is recommended that system providers store the procedure (with all structuring) in a format that is well documented (i.e., no undocumented constructs in the procedure files), preferably with a simple file structure that does not require the use of the special purpose editor for its access and interpretation. Standard document encoding solutions (like XML) should be preferred. The fulfillment of this requirement should make the procedure files accessible from other system solutions than the one provided by the current system supplier.

Even though a script needs to be developed to automate procedure input, this may pay off in situations where large amount of procedure text need to be transferred. As we will se later, the fulfillment of this requirement also makes the maintenance of the procedures more straightforward.

In some cases, when the original (paper based) procedure is well structured, some of the extra tagging may be avoided. For instance if the instructions are organized as rows in a word processor table, the tagging of the table may be used similarly to the extra brackets used in the example above. Another example of such automatic translations is given in the next section.

Linking the Procedure System to the Process Database

This task is relevant for most types of procedure systems. Without connection to the process database it is impossible to display current values within the procedure and it will neither be possible for the procedure system to monitor process conditions. In order to establish the connection to the process database the following tasks must be accomplished:

- Insertion of process variable reference points in the procedure (most often inline in the procedure text).
- Translation of reference points into equivalent process database variable tags.

Implementing a software bridge between the procedure system and the process database to transfer information in either direction (at least from the process database to the procedure system).

One might think that there would be no need for an extra translation process between process and procedure system, however process database systems often use quite different variable identifiers than those used within the procedures. Thus a translation process becomes necessary. The solution to this might be as simple as a cross-reference listing.

When it comes to identifying the process variables within the procedure text, automation opportunities are usually present. The process variable references are often a finite set of possible strings, and the identification of process variables thus reduces to a simple string matching problem. In spite of this, certain computerized procedure systems require the systems personnel to explicitly identify the process variable references wherever they are used. This is absolutely unnecessary, and should be avoided to decrease implementations costs. However, having an open system as recommended above should make automation possible.

Configuring/Implementing the User Interfaces

Computerized procedure systems often come with a predefined end user interface to the procedures. Even though there will be no extra costs to configure the end user interface, there might be some serious complications connected to this. The most important circumstances are:

1. The predefined computerized procedure layout and structure differs greatly from that of the original, so that the procedures need to be restructured (which can be quite costly, depending on how far the existing procedures are from the required format). Another potential problem is that extensive retraining of the operators could be needed. However, in certain cases, if the original set of procedures are poorly organized and laid out, so a restructuring of the procedures may also have some positive effects (even though they are costly).
2. Consistency between the procedure system and remaining operator displays cannot be established. A typical example is the organization of component manipulation buttons, let's say a 'pump'. In the process mimic diagrams the pumps might be consistently operated with the *close* button to the left and the *open* button to the right. However, in the procedure display, this is opposite, the *close* button to the right and the *open* button to the left. Obviously, this may create dangerous situations.

So, even though configurable procedure systems may introduce extra costs for the configuration, they might be preferred in certain situation if no system is available that adequately matches existing procedures or remaining I&C interface.

Inserting and Deleting Procedures in the Set of Procedures

There are typically links among the individual procedures within a procedure set. One procedure might be implemented as part of one procedure or a procedure may be specified as a subsidiary action to a given instruction in the procedure. Inconsistencies (e.g. references to non-existing procedures) may be introduced in representing these links in the computer-based system, and there is a need to assert absolute consistency at the when this is done. The specialized procedure editor may have features for checking this, or, if the procedure representation format is accessible using general purpose tools, simple scripts may be written to check for this.

When a *new* procedure is inserted, it needs to be properly integrated with the rest of the procedures. New links need to be created wherever relevant. Process conditions may also be associated with the procedure, and the procedure may or may not have features for automatically suggesting the procedure when the conditions are met.

In more sophisticated systems, both procedures and single instructions may be represented by presumed effects (process conditions established after the completion of the instruction or procedure), and a matching of desired effects (and preconditions) may be used to suggest relevant reference points during the inclusion of the procedures in the procedure set. As a simple example, suppose there is an instruction within a procedure with the objective to increase the level of the feedwater tank above a certain level, and it is left to the discretion of the operator to find out how this could be done. This information may be useful when a new procedure is included. Suppose the new procedure is described by a post condition increasing the feedwater level. The editor could use this information to propose a link from the old to the new procedure, just by matching the two conditions.

Obviously, such functionality would require the procedure to be meticulously ‘instrumented’ with respect to objectives of procedures and instructions. Such ‘instrumentation’ might be costly and should be subject to a comparison with needs/benefits.

In any case, this type of update and consistency problem needs to be solved, irrespective of whether the procedure is computerized or not, and this is one example of how introduction of computerized procedures may lead to important cost cuts.

Modifying Procedures

Changes in the characteristics of users, systems, regulatory requirements, and operational and management practices require procedures to be revised; such revisions may lead to technical inaccuracies. For example, a CBP system may depend upon a database to maintain a list of required setpoints for different conditions and automatically generate setpoint information included in procedure steps. To maintain the integrity of the CBPs if the database is revised, it is critical that the implications of changing any value can be traced and controlled whenever that value appears in procedure steps. Changes to procedures may also lead to the kinds of inconsistencies described in the previous discussion of between- and within-procedure references. As an example, if one procedure instructs the operator to perform instruction 2 through 4 in another procedure, and if instruction 2 in the second procedure is modified (e.g. deleted), an update of the first procedure may be needed. If the references are made explicit (recognizable to the procedure system), the editor may be able to propose a review of the second procedure. Again, if the procedure representation is available to external software modules, a script may accomplish the same functionality.

Certain circumstances (e.g., equipment upgrades in progress) may also require procedures to be modified temporarily; such changes must be clearly identified so that it is clear to personnel what temporary changes were made and whether an aspect of the procedure being used is a temporary one. As with permanent changes, maintaining that the technical content of the procedures as a structured file makes it possible to easily produce multiple instances of the procedure (e.g., temporary CBP pages, corresponding change pages for paper backup documents) without introducing inconsistencies, since the modifications are made by transforming a single source.

These types of problems occur irrespective of the procedure format (computerized or not), and computerization may lead to cost reductions by making it easier to identify and remedy them.

Updating Plant Instrumentation

Instrumentation is commonly replaced or enhanced during the life-time of the plant. In the case of replacements, there are number of process references that may be changed within the set of procedures. Identification of the needed changes should be easy (provided a cross-reference list of the kind mentioned earlier is available).

Inclusion of completely new instrumentation creates a more challenging update problem. Completely new signals may be relevant in many places in the existing set of procedure, even in places where no prior instrumentation was available (e.g. where a phenomenon was only observable indirectly by means of some other measurement). This type of problem is similar to the problem occurring when completely new procedures are being included. Extensive tagging (costly) may be needed to offer computerized assistance.

Changing or Replacing Interfacing Systems

Sometimes individual I&C modules are replaced. This might cause problems when it comes to connecting to old modules of the I&C system. Clearly identified interfacing protocols between the modules will alleviate this problem. In spite of this, it is conceivable that protocols needs to be changed e.g. due to altered input information needs of the new modules (the new modules require information that was not needed in the old modules). In such cases, extra software adaptation modules may be piggybacked on the old procedure system. Access to the existing set of procedure may facilitate this piggybacking process.

Replacing the Computerized Procedure System Software

The need for changing procedure system software should be considered. The cause might be obsolescence (i.e., the system provider unable to provide maintenance and support), the need to include functionality that cannot be provided within the current implementation, or an inability to link the CBP with adjoining systems that have been replaced (e.g. replacement of process database). For such situations, it is an absolute advantage to be able to use the old procedures in the new system. The same considerations are relevant as for the original migration. If the format of the old and the new computerized solution is an open and accessible representation, the chances for making scripts to do the transformation automatically are quite good (thus avoiding substantial additional costs).

4.6 Computerized Operator Support Systems (COSS)

4.6.1 Overview

4.6.2 COSS Guidelines Checklist

4.6.3 Deciding if COSS is Needed

4.6.4 COSS Design and Integration

4.6.5 Modes of Operation

4.6.6 User Control of Interaction

4.6.7 Appendix – Examples of COSS Applications

4.6.7.1 Condition Monitoring, Fault Detection and Diagnosis (CMFDD)
4.6.7.2 COSS for Core Surveillance

4.6.1 Overview

Section 3.3, Function Analysis and Allocation, discusses the expansion of automation to cognitive functions, such as monitoring, detection, and situation assessment. Computerized Operator Support Systems (COSSs) are one class of HSIs that provide support for these activities. COSSs are defined as systems that use computer technology to support operators or maintenance personnel to perform a wide variety of tasks. For example, COSSs may provide personnel with the following capabilities:

- Monitor the plant processes and other parameters, and present current, past, and possibly predicted future plant data and information. Future process data may be computed using a model of the process. The data and information may be presented in forms that facilitate user situation awareness, understanding, and decision-making.
- Calculate signals and values that cannot be measured. Calculations may be based on existing measurements and a model of the process. Results may be presented independently or integrated with measured data.
- Perform diagnosis based on measurements, stored data and information, logic of some sort, and a process model.
- Predict future states based on the user entering possible future actions. Then the COSS computes the reaction of the plant process, and the predicted results are shown to the user. By doing this the user can evaluate effects of different actions as part of deciding which actions to take.
- COSS computes and presents the user with recommended actions to change the process based on measurements, stored data and information, logic of some sort, and a process model. The user can accept the recommendations or can take other actions. COSS may be authorized by the user to implement some or all of the recommended actions.

COSSs are made up of basic HSI resources, such as displays, interface management facilities, alarms. The design of these features should follow the appropriate guidance is those sections. What is unique about COSSs is that they provide personnel support that is beyond that provided be typical computer-based HSI resources. For example, an alarm system supports personnel to monitor the plant. A COSS providing condition monitoring support also monitors the plant but does so be applying sophisticated analysis capabilities. Thus, as we are discussing them here a COSS is distinguished by its capability to process information in ways that extend beyond those typically provided by typical HSIs. An appendix to this section provides two examples of this extended capability: (1) condition monitoring, fault detection and diagnosis, and (2) core surveillance. The increase in sophistication is associated unique requirements for their design, such as user control of operational modes and need for facilities for users to interrogate the COSS to reveal the bases for their results. This section addresses these aspects of COSS design. As for basic information presentation, alarm presentation, and user interaction features, COSS designers should use the guidance provided in the other sections of Section 4. What this section addresses is design guidance to address the unique aspects of a COSS. The design of COSSs is discussed further in Section 3.7.3.4.4, Design for Differing Levels of Automation.

An overview of the considerations in designing and implementing COSS is illustrated in Figure 4-42. The detailed guidance begins with Section 4.6.3. In addition, 4.6.7.1 and 4.6.7.2 Appendices contain information about two possible COSS: Condition Monitoring and Fault Detection and Diagnosis (CMFDD), and Core Surveillance.

Figure 4-43 illustrates the relationship of COSS to the available provisions for plant control, management, and maintenance. The role of the operators is to understand what is happening in the process, make decisions, and take the required actions. In order to do this, operators must rely on appropriate plant instrumentation and an information system to provide pertinent operating parameters and plant status indicators.

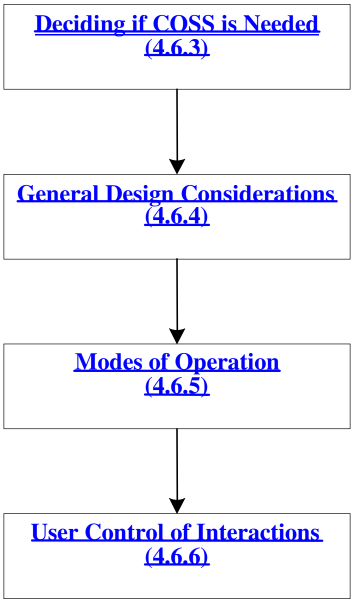

Deciding if COSS is Needed (4.6.3)
General Design Considerations (4.6.4)
Modes of Operation (4.6.5)
User Control of Interactions (4.6.6)

Figure 4-42
COSS Design and Implementation Considerations

As the figure shows, an operator relies on automatic control to take care of many routine tasks; this is represented in the figure by the path from the information system to the actuators. The operator's involvement is not needed for the loop to function. For tasks or circumstances where automatic control is not needed or not sufficient, the operator, assisted by various support systems, makes manual control inputs.

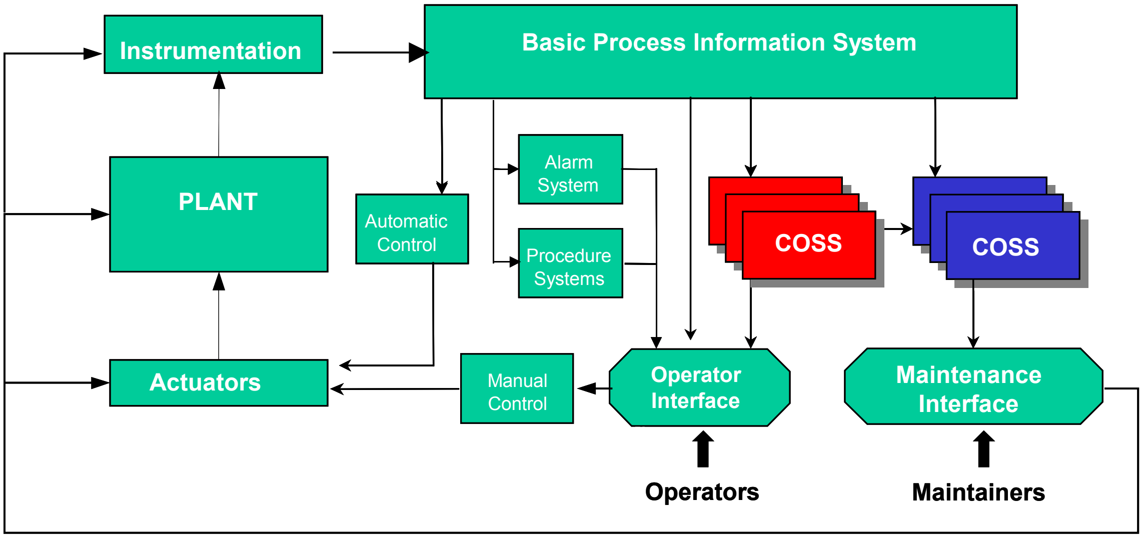


Figure 4-43
COSS for Operations and Maintenance

The maintenance of plant equipment represents an important part of the plant operation costs. Making maintenance more cost-effective may lead to substantial savings. The introduction of COSS may contribute to such cost savings.

There are several types of maintenance activities to be performed at a plant. These include:

- Maintenance of the plant and plant components
- Upgrades of the procedures and operating strategy
- Changes in the plant administration (procurement, handling of outages, etc.)
- Upgrades of operator support systems

In many plants, maintenance is coordinated through the use of computerized maintenance forms. These forms are filled in on the computer by maintenance personnel and are saved in a database for use as needed. A COSS might be able to capture equipment data automatically, check the data with action points, e.g., need for corrective or preventive maintenance, and advise of the needed actions.

4.6.2 COSS Guidelines Checklist

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.6.3		Deciding if COSS is Needed					
4.6.4		General Design Considerations					
	=>	4.6.4-1	Where practical, the COSS should be fully integrated with and consistent with the rest of the HSIs. The operator should be able to use the COSS as a natural element of the tasks being performed.				
	=>	4.6.4-2	The appearance and functionality of the COSS should follow the same design conventions as other HSI resources, e.g., use the same nomenclature, abbreviations, acronyms, symbology, iconic representations, and coding techniques as the general information display system.				
	=>	4.6.4-3	The COSS should be able to access needed plant information already available in other information and other HSI systems, thus minimizing the need for the operator to manually input information.				
	=>	4.6.4-4	If necessary, different user groups should have different access levels to COSS functions.				
4.6.5		Modes of Operation					
	=>	4.6.5-1	For COSSs capable of different modes of operations, the current mode should be clearly indicated.				
	=>	4.6.5-2	Mode switching should require an explicit command.				
	=>	4.6.5-3	The COSS should provide an overview of which data are included in each analysis mode.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.6.5-4	If the COSS performs any sort of filtering or selective use of data, the current filter that is active should be identified. It should also be possible for the operator to access the unfiltered data.				
4.6.6		User Control of Interaction					
	=>	4.6.6-1	If the COSS is designed to support problem solving, it should provide the capability to plan a strategy for addressing problems.				
	=>	4.6.6-2	When the COSS is capable of a range of problem solving strategies, it should be capable of accepting direction from the user regarding which strategy to employ.				
	=>	4.6.6-3	The COSS should automatically record all rules invoked during an analysis.				
	=>	4.6.6-4	Query and explanation facilities should be provided so that users can determine the basis of COSS analyses and recommendations. User should be able to recall each invoked rule and relate it with a specific event (i.e., question or conclusion) to explain the rationale for the event.				
	=>	4.6.6-5	The system should permit rapid retrieval of previous exchanges between the user and the COSS.				
	=>	4.6.6-6	The user should be capable of requesting a hardcopy of data including screen displays (text and graphics), data employed during a consultation, summaries of consultations, lists of rules/facts invoked during a consultation, and summaries of hypotheses tested.				

4.6.3 Deciding if COSS is Needed

There are two basic reasons for incorporating a COSS in plant design:

- Design analyses have indicated that task support is needed
- Performance improvements are sought

In Section 3.3, Function Analysis and Allocation, functions and task are analyzed to determine whether they should be performed using automation, manually by personnel, or some combination of the two (see Figure 3-12). The analysis considers factors such as task complexity, workload, and precision needed, to identify tasks for which task support is needed. COSSs may provide the needed support for these tasks.

The focus of the function analysis is on task characteristics where support is needed to achieve adequate performance. However, there are also circumstances where performance is already adequate, but improvements are sought. Providing a COSS to improve core performance monitoring is an example (see Section 4.6.7.2 in the Appendix).

Another important consideration is the development and maintenance costs of a COSS. Cost is influenced by the complexity of the COSS, the necessary maintenance foreseen for the COSS lifecycle, and possibly the availability of an acceptable off-the-shelf system. The design process may be complex and costly if it is necessary to design a new COSS. Thus, certain key technical and cost issues must be considered, including:

- What are the technical requirements and administrative routines for designing, developing, implementing, and maintaining and updating a COSS? A COSS may have different requirements than the traditional control room HSIs reflecting the fact that it may be dependent on and require interfacing to other control room I&C systems, plant data, and plant databases.
- What are the technical issues to be solved in installing and integrating a COSS into the control room? Some COSS may require access to sensor data, and calculated data from several sources. For example, an Artificial Neural Network incorporated in a COSS may need to be acquired, provided appropriate data and information, and occasionally recalibrated to reflect changing conditions (i.e., changes for reasons other than component replacement, general age, or wear of the components).
- Will the COSS be considered a safety-related system? If the answer is yes, then the factors related to planning for regulatory and licensing activities presented in Sections 2.5, and licensing presented in Section 5 must be considered. The COSS examples presented in the Appendix of this Section probably do not fall into this category.
- Will the expected benefits justify the cost of design, development, installation, and maintenance, or acquisition of an off-the-shelf system? If the COSS is not safety-related, does the expected increase in plant availability and/or the prevention of equipment damage justify the cost?

4.6.4 COSS Design and Integration

⇒ 4.6.4-1 Where practical, the COSS should be fully integrated with and consistent with the rest of the HSIs. The operator should be able to use the COSS as a natural element of the tasks being performed.

There may be situations where a COSS is a stand-alone system, however, in general a COSS should be integrated to the maximum extent possible with other I&C upgrades and the parts of the control room that are not changed during the upgrade. Integration is a key issue, both with respect to usability and cost savings. Some of the reasons that integration is important are listed below.

- In the past, specialized systems have been introduced into control rooms to supplement existing support resources without sufficient consideration having been given to whether the use of the system is compatible with routine tasks, working procedures, or other support systems that the operators normally use. Various deficiencies arise when the fit is poor. For example, the system may be inconveniently located (e.g., removed from associated controls and displays on the control board). It may require extra input from the operator (due to lack of COSS access to needed data).
- The design of the user interface may not be compatible with the tasks of the operator or be compatible with other interfaces, e.g., requiring excessive navigation to find the needed information. Even though the system itself generates correct and helpful information, the lack of integration (with respect to physical layout, other information resources, or the operator task requirements) may result in its being underutilized or even ignored.

⇒ 4.6.4-2 The appearance and functionality of the COSS should follow the same design conventions as other HSI resources, e.g., use the same nomenclature, abbreviations, acronyms, symbology, iconic representations, and coding techniques as the general information display system.

Use of the plant's style guide (see Section 3.1.3) will help ensure a consistent look and feel across all HSI resources.

⇒ 4.6.4-3 The COSS should be able to access needed plant information already available in other information and other HSI systems, thus minimizing the need for the operator to manually input information.

Users should not have to input information already in the HSIs. It is recognized that this principle may be difficult to follow when partial upgrades of the control room are implemented.

⇒ 4.6.4-4 If necessary, different user groups should have different access levels to COSS functions.

As an example, a core surveillance system may contain extensive data and system functions to serve plant personnel with different responsibilities. There should be different access levels to match the different user needs and to protect against inadvertent misuse of the system. In this example, there may be several users. *The Reactor Operator* needs access to the functions for on-line operation and short-term prediction of core behavior. *The Reactor Engineer* needs access to all the functions supporting core history analysis, and long term planning and optimization, e.g., core loading optimization and fuel management. *The System Administrator* needs access to software maintenance functions and configuration management.

4.6.5 Modes of Operation

A COSS has certain operating modes and characteristics that are different than found with more conventional HSIs. Guidance regarding some of these characteristics is provided below.

⇒ 4.6.5-1 For COSSs capable of different modes of operations, the current mode should be clearly indicated.

There should be no ambiguity for the new operators as to which mode the COSS is in. For example, a “Simulation Mode” symbol can be used to clearly distinguish simulation from other operational modes.

⇒ 4.6.5-2 Mode switching should require an explicit command.

⇒ 4.6.5-3 The COSS should provide an overview of which data are included in each analysis mode.

⇒ 4.6.5-4 If the COSS performs any sort of filtering or selective use of data, the current filter that is active should be identified. It should also be possible for the operator to access the unfiltered data.

4.6.6 User Control of Interaction

⇒ 4.6.6-1 If the COSS is designed to support problem solving, it should provide the capability to plan a strategy for addressing problems.

The capability provided by the COSS will vary depending on its intended functions. Possible capabilities include planning aids (such as time lines and worksheets); an evaluation function that assesses the adequacy of the user’s plan and recommends revisions where necessary; the ability to form, state, and test hypotheses in a manner consistent with the user’s plan; and the capacity to store and recall plans.

⇒ 4.6.6-2 When the COSS is capable of a range of problem solving strategies, it should be capable of accepting direction from the user regarding which strategy to employ.

⇒ 4.6.6-3 The COSS should automatically record all rules invoked during an analysis.

⇒ 4.6.6-4 Query and explanation facilities should be provided so that users can determine the basis of COSS analyses and recommendations. User should be able to recall each invoked rule and relate it with a specific event (i.e., question or conclusion) to explain the rationale for the event.

⇒ 4.6.6-5 The system should permit rapid retrieval of previous exchanges between the user and the COSS.

⇒ 4.6.6-6 The user should be capable of requesting a hardcopy of data including screen displays (text and graphics), data employed during a consultation, summaries of consultations, lists of rules/facts invoked during a consultation, and summaries of hypotheses tested.

This guideline is applicable to COSS for which a hardcopy is needed. Functions performed by some COSS will not require that a hardcopy be available.

4.6.7 Appendix – Examples of COSS Applications

This Appendix provides two examples of COSS applications. There are many other COSSs that could be considered. The driving force for COSS should be the need identified during the upgrade planning and design process activities.

4.6.7.1 Condition Monitoring, Fault Detection and Diagnosis (CMFDD)

The goal of condition monitoring, fault detection, and diagnosis is to ensure success of planned operations by recognizing anomalies of a system (plant). This is achieved by monitoring the condition of equipment and instrumentation, and by detection, identification, diagnosis, and removal of faults. These are the primary tasks to be supported by the type of COSS applications that are described in this Appendix.

The main benefit provided by a CMFDD COSS is an enhanced awareness of existing, incipient, and potential problems related to both safety and efficiency. This, in turn, leads to improved operations and maintenance.

The operator through unsupported supervision of systems and signals commonly performs condition monitoring and situation assessment (fault detection and diagnosis). By providing a COSS to support these activities it is possible to reduce the workload on the operator while performing these primary tasks. This should lead to economic benefits, such as improved plant productivity, protection of investments (i.e., prevent damage to components), and labor savings. At the same time, safety may be maintained or even improved. These advantages are possible because of the following benefits provided by a COSS:

- COSS may perform large-scale quantitative and qualitative calculations that may reveal structure in the data not perceivable by the operator without such support.
- The operator may experiment with a model to predict process behavior ("what-if" analysis). This can be useful for process recovery.
- A condition-based maintenance strategy may be employed instead of a more traditional preventive maintenance strategy. That is, only instruments in need of calibration are calibrated, only feedwater heaters in need of service are serviced, etc. The results may be reduction in costs, sometimes substantially (Davis, *et al.*, 2000).
- When timing is critical, the early warnings often provided by COSS could be a decisive factor in avoiding the evolution towards undesirable situations, such as plant scrams or damage to components. COSS are able to provide these early warnings because they continuously monitor plant parameters, as contrasted with the periodic checking done by an operator.
- The COSS may enhance the operator's situation awareness by revealing faults and anomalies, and through the presentation of performance indicators.

As used in this section, a **condition** is defined as the collective of characteristic properties of the monitored system. Examples of characteristic properties include pump characteristics, heat exchanger efficiencies, expansion lines for turbines, etc. Characteristic properties exclude variables such as temperatures, flows and pressures, which are referred to as process variables.

A **fault** is an "unpermitted deviation" in at least one characteristic property or variable of the monitored system. Thus, a fault is an unpermitted deviation in the condition of at least one piece of equipment or at least one process variable. An unpermitted deviation in a process variable is not necessarily the result of an unpermitted condition deviation, e.g., if combinations of minor condition deviations are involved.

The principal tasks to be dealt with include:

- **Condition monitoring**: To continuously or at least periodically assess the condition of the monitored system to quantify its characteristic properties. Typically, condition monitoring relies on calculated values for the characteristic properties.
- **Fault detection**: **Situation assessment to** determine whether there are any faults present in the system. Faults may be uncovered by condition monitoring, or they may be detected by noting that process variables, such as temperatures and flows, are out of limits. Thus, a fault may be detected by noting an efficiency reduction of a pump, or it may be detected by discovering that the power production is less than what the thermal power of the boiler and the cooling water temperature dictate that it should be.
- **Fault identification**: To identify the observation variables most relevant to diagnosing the fault. In complex plants with large process variations, this may not be straightforward since the operator would have to assess a large number of combinations of process variables.
- **Fault diagnosis**: To determine which fault occurred. Fault diagnosis implies determining the location, type, magnitude, and time of the fault. Fault diagnosis may be aided by evaluating the condition of equipment in the vicinity of the variables identified in the fault identification step.

- **Process recovery**: Response planning to develop a strategy for removing the effects of the fault. Intervention may be required in the short term, e.g., to avoid accidents or shutdowns, or in the longer term, e.g., by scheduling a feedwater heater for maintenance during the annual shutdown.

Although there appears to be no standard terminology in this field, the four latter tasks are frequently referred to as **process monitoring** (Chiang, *et al.*, 2001).

Another class of tasks involves **fault isolation**, which is to locate the faulty component. Fault isolation differs from fault identification in that it not only identifies the variables associated with the detected fault, but also specifies its exact location. Fault isolation differs from fault diagnosis in that fault diagnosis also determines the type of fault, not only its location. Fault isolation may therefore somewhat loosely be defined as being at a level in between fault identification and fault diagnosis.

An example of the process-monitoring loop is as follows. An operator notices that the electric output of the plant is less than expected. Thus, a fault has been detected. All process variables in the high-pressure part of the turbine cycle appear normal, whereas the extraction pressures of the low-pressure turbines and the associated temperatures in the feedwater heater train (fault identification) lead to the inference that something is wrong with the state of the condenser (fault isolation). The operator notices that the temperature of the condenser shell is lower than what the shell pressure measurement and the saturation properties of water would dictate. The operator therefore infers that there is a problem with the ejectors, or that there are larger amounts of non-condensables in the condenser than the ejectors can handle. Further investigation might result in determination of the exact location of the problem; in this case, the operator has succeeded in diagnosing the fault.

Techniques that allow for COSS implementation exist that support all of these primary tasks, although it may not always be desirable to do so. In some situations, however, their integration in one system may seem natural. One example is systems that contain both the fault detection and isolation stages, and which are frequently referred to as **FDI systems**.

To be useful in reducing the cognitive load of the users, process-monitoring systems typically contain one or a few **performance indices** or **process measures** derived from the on-line data. These indices (measures) represent a transformation of the full set of on-line data into a few meaningful numbers representing the state of the process. For fault detection, limits may be placed on some of the measures, and a fault detected whenever a measure moves outside its limits. Faults can also be identified and diagnosed using these measures. A goal of process monitoring techniques is to develop indices/measures that are sensitive and robust to all faults. A high sensitivity implies a small number of missed alarms, i.e., faults occurring but not resulting in an alarm. Robustness implies a small number of false alarms, that is, alarms that are activated when there is no fault in the system.

Examples of process indices include produced power relative to nominal power, relative efficiencies of equipment, and probabilities that the process contains faults. Other indices or measures proposed in the literature may have a more abstract meaning and their significance is something the operator will have to learn by experience or training.

Process monitoring measures may be classified according to the approaches employed to generate them. There are three such approaches: **data-driven**, **analytical,** and **knowledge-based**.

Data-driven techniques, as the name implies, derive models directly from process data. Previously stored data that are available off-line are projected into lower-dimensional spaces, e.g., for some processes down to even two or three dimensions. Variability in the data under normal operating conditions is captured, while taking into account spatial correlations. The latter distinguishes the data-driven techniques from traditional monitoring methods, such as simple limit sensing (univariate statistical monitoring) where fault-detection thresholds are defined for each monitored variable separately. Data-driven techniques are therefore more robust than univariate methods. They may also be extended to include serial (temporal) correlations.

A major advantage of data-driven techniques is that they are able to handle large complex systems, and development costs are moderate. They easily provide fault detection and fault identification. However, in practice fault diagnosis requires that data are available for pre-diagnosed faults. The latter fact alludes to the main drawback of data-driven techniques, i.e., that their proficiency depends crucially on the quantity and quality of the available data. Some data-driven techniques are as follows:

- Principal Component Analysis (PCA)
- Fisher Discriminant Analysis (FDA)
- Partial Least Squares (PLS) (Chiang, *et al.,* 2001)
- Artificial Neural Networks (ANN)

Analytical techniques are based on consistency checks between plant (on-line) data and mathematical models. Frequently residuals are defined such that these will be large when faults are present and small when absent. Analytical methods may be based on parameter estimation, observers, parity relations and data reconciliation (Chiang, *et al.,* 2001).

Efficient process monitoring systems based on analytical techniques require accurate quantitative models, typically based on first-principles. This may render them unsuitable for large complex systems, for which their development may be too costly and time-consuming. In such cases, knowledge-based methods may offer an alternative. These are based on models obtained through, for example, causal modeling, qualitative modeling, expert knowledge acquisition, and pattern recognition techniques.

The three classes of process monitoring are summarized in Table 4-18. Hybrid techniques also exist, but are not represented independently in the Table.

Table 4-18
Classes of Techniques for Condition Monitoring, Fault Detection, and Diagnosis

Technique	Principal Features	Applications*	References**
Data-driven methods (multivariate statistics, principal component analysis, neural networks, system identification)	Models derived from existing data. Dimensional reduction. Well suited for large complex processes.	Feedwater flow measurements, thermal power estimation, steam generators, signal validation, thermal-performance optimization, fault detection and diagnosis	Heo, *et al.*, 2003 Rasmussen, *et al.*, 2003 Upadhyaya, *et al.*, 2003 Gou and Uhrig, 1992
Analytical methods (parameter estimation, observer-based methods, parity relations, data reconciliation)	Models based on first principles or system identification. Less suited for large complex processes.	Thermal performance monitoring, monitoring the condition of equipment, signal validation, feedwater and condenser analysis, vibration analysis	Sunde, *et al.*, 2003 Dorr, *et al.*, 1997
Knowledge based methods (causal analysis, expert systems, pattern recognition techniques)	Qualitative models stemming from expert knowledge and/or first principles.	Vibration analysis, thermal performance monitoring, transient analysis, loose part detection	Chou, *et al.*, 1994 Por, *et al.*, 2003 Nabeshima, *et al.*, 2003

* This column describes applications whose descriptions are openly available at present. The table should **not** be interpreted as claiming that these are the only possible applications for the class of techniques given.

** The list is by no means exhaustive, but rather meant to give some examples.

4.6.7.2 COSS for Core Surveillance

The main purpose of core surveillance systems is to provide ***on-line*** support to control room operators for:

- Core performance monitoring
- Core performance prediction and optimization

In addition, Core Surveillance COSSs provide support to reactor engineers who are responsible for following the long-term trend of core/fuel behavior, as well as ***off-line*** functions for fuel management, core loading optimization, and calculation of core performance parameters.

While *on-line* and *off-line* functions were separate systems in the past, the trend now is to integrate these functions into one system, sharing common functions/methods where possible, e.g., using the same core simulator for fuel management, safety analysis, on-line monitoring, and prediction. This makes the system consistent and easier to maintain.

The systems have different access levels depending on the user categories. This means that a limited set of functions are available for reactor operators in the control room, while the reactor engineers also have access to all the off-line support tools.

The systems are similar in functionality for PWRs and BWRs, but may vary when it comes to the detailed system design due to the inherent differences of the two reactor types. Typical features offered by on-line systems for PWR reactor designs are listed below.

- Core Follow Mode support functions:
  - Display present values and history of main core measurements.
  - Preprocess measured data.
  - Perform 3D core simulation calculations.
  - Combine measurements and simulation to minimize the deviation between calculated and measured power distribution.
  - Limit calculations of F_Q (LOCA) and $F_{\Delta H}$ (DNBR) based on pin-wise power distributions.
- Predictive Mode support functions:
  - Determination of start-up critical boron concentrations/control rod banks positions (after reactor scram, etc.).
  - Generate various operational strategies. For instance, one objective might be to keep the axial offset as close as possible to the target value in transient situations; another objective might be to minimize boron consumption.
  - Specify and run predictive 3D-analysis of Xenon transients from the present state and at different burn up states including end of cycle.
  - Limit check and display of margins to F_Q and $F_{\Delta H}$ limits.
- Logging of data important for core monitoring:
  - Measured data, calculated data, limits, and margins (These data can be provided to a central data base system for long term archiving.)
- Maintenance utilities to keep track of data from the end of one operational cycle through off-line design of fuel reload patterns to new cycle start-up.
- Tailored HSIs for each type of user (e.g., reactor operator, shift supervisor, engineer, and maintainer)

Monitoring the core is a challenging task, especially in situation where there is a combination of more sophisticated fuel/core design (e.g., burnable poisoning Gd fuel, MOX), longer fuel cycles, and higher burn up, , and power uprate demands. In addition, failures and unforeseen events are increasingly common. Examples include:

- Crud deposition and axial offset anomalies (AOA)
- Failure of control rods to insert completely following a scram due to “S” shaped bowing of fuel assemblies.
- Partially blocked coolant channel flow
- Various types of sensor failures (in-core/ex-core)

These demands call for introduction of improved core surveillance tools and methods with the ability to detect and diagnose potential operational problems. Traditional techniques for core monitoring are based on readings from in-core/ex-core detectors combined with core physics code calculations, where the codes are based on first principles; these may vary with respect to level of detail and accuracy often compromised with computational power of the plant computers available. More advanced fuel designs and methods of operating the core are being developed. Consequently, there is a need to reconsider how the core is monitored. Some general trends include (Lefvert, *et al.*, 1999):

- The introduction of more detailed physics models in on-line calculations for both BWRs and PWRs.
- More widespread discussion of the possible advantages of back fitting some PWR types with fixed in-core detectors
- Enhanced methods for combining information from on-line measurements and on-line calculations

The most important techniques and methods for core surveillance are related to reactor core physics modeling and codes to provide operators with detailed and accurate core follow mode calculations and fast predictive calculations.

Use of advanced computerized core surveillance systems has the potential to substantially increase the quality and quantity of the information on core status and dynamic behavior available to the operating staff. The benefits from this improved information are twofold. First, the safety of the plant is improved since undesired core conditions can more easily be prevented. Second, more flexible and efficient operation of the plant is made possible.

The degree to which safety and economy can be improved through use of computerized core surveillance systems depends strongly on factors such as which functions are included, the accuracy of the various modules (e.g., core simulators), and how user-oriented the design of the system is made. It is important that the system is designed for simplicity in operation, and for clear and comprehensible presentation of the relevant information to the operator. It is, therefore, essential to consider carefully these factors and develop the system following the guidance in other parts of this document to meet user requirements.

Advanced core surveillance systems for **PWRs** can provide operational support in many situations, e.g.:

- **Criticality calculations**. If the power history is complex, it is difficult to calculate and predict critical boron concentration as a function of time. An on-line core simulator can track the power history in detail and make faster-than-real-time predictions several hours into the future.
- **Optimization of planned power changes**. Power reductions, load following and start-up after shutdown are transients more efficiently performed if planned ahead with a predictive system. Critical passages can be detected and anticipated.

- **Axial power distribution control**. Operation outside the delta-flux operating band is only permitted for a limited period. Various control strategies to deal with axial xenon redistribution are efficiently and rapidly evaluated with modern systems.
- **Coast-down operation support**. Operation at low boron concentration is difficult for a number of reasons. Return to power after a trip might create problems with the delta-flux operating band. With a predictive system, the consequences of power maneuvers at coast-down or low boron concentration can be fully investigated.
- **Trend analysis**. Reactivity related parameters both measured and calculated are available for trend analysis. The relationship, for example, between temperature variations and impact on the power distribution might be investigated in detail with monitoring functions.
- **Xenon transients**. The general behavior of transients might also be investigated, e.g., xenon transient during load follow operation.
- **Power distribution (local, global)**. The 3D power distribution functions make it possible to see how the power distribution varies radially and axially, and locally as well as globally, during transients.
- **Thermal margin limit**. The impact of control rods and the power level on the thermal margins can be illustrated, e.g., how F_{Δ_H} increases with rod insertion.
- **Training**. Many core related parameters are difficult to simulate on full-scale simulators. Predictive functions can demonstrate the impact of various strategies and the consequences of inappropriate actions.

The following are examples of benefits expected when providing a COSS for core surveillance:

- Improved limit checking and thermal margin calculation.
- On-line 3D power distribution calculation
- Improved validation of plant measurement and identification of sensor failures by utilizing the core simulator as an independent means for calculating 3D power distribution
- Optimum combination of measurements and calculations to obtain more precise critical parameter values
- Predictive capabilities and strategy planning off-line and on-line, offering the possibility to check the consequences of operational maneuvers in advance, prediction of critical parameters, etc.
- Interfaces to off-line analysis codes for core loading pattern design, etc.
- Integration of modules for monitoring fuel performance and coolant activity as a means for detection and identification of fuel failures
- Improved software framework that is flexible, adaptable and user-friendly
- Improved interfaces for operators and reactor engineers.

4.7 Communication Systems

4.7.1 Overview
4.7.2 Display Guidelines Checklist
4.7.3 Main Aspects of Communication System Design
4.7.4 Communication System Design
4.7.4.1 General Considerations
4.7.4.2 Speech-Based Communications
4.7.4.3 Computer-Based Communications
4.7.5 Control Room Design and Communication System

4.7.1 Overview

Typically, plant operators and maintenance personnel obtain plant status information from two main sources:

- Interfaces with plant systems and equipment (e.g., displays on control panels and workstations, overview displays, and alarm panels) and
- Communications with other personnel.

Communication between personnel is an essential part of the Human-System Interface. Communicating with other humans is a task in the same manner as any other monitoring and control action and should be included in the human factors task analyses. Upgrading to advanced digital or hybrid systems may change the way operators interact with each other or may change the type and content of the information and instructions that are exchanged between personnel. Existing communication systems may or may not be compatible with the demands of the modified systems. An essential part of evaluating the human factors of any potential change to the HSI is evaluation of its effects on communications.

Introduction of new system interfaces (e.g., screen-based systems) into the workplace may lead to establishing means of communication among personnel that will be based on the use of the digital system display screens for direct communication between personnel. In addition, modifications that bring more information into the control room and make it directly available to the operators may reduce the need for communications with remote or roving operators for the purpose of obtaining information.

The primary objective of the communication system is to transfer information between personnel. There is also information transfer to and from the system; however, this subject is not directly addressed in this section of the guidelines. It must be recognized that these two types of communication are closely related and that the HSI does not operate independently of the communication system. The communication system plays an important role in helping the operators maintain situation awareness and respond to situations during all plant operational conditions.

This section addresses the communication system used by plant personnel and the importance of communication for teamwork in the control room. Methods used for peer checking between operators in the control room, i.e., one operator checking another operator’s planned actions against mutually understood planned actions certainly involve communication and information exchange. Personnel located within short distance from each other usually communicate via direct unaided voice communications. However, when distance separates operators, communication devices (e.g., telephones, radios, display screens, etc.) will be used to aid operators.

This section contains guidance for both modifications to existing communication systems necessitated by digital upgrades and modifications made specifically to communication systems. Figure 4-44 provides a map of the various communication system design aspects addressed by this section, along with the corresponding subsection numbers. Planning for the overall I&C and Main Control Room modernization effort, the endpoint vision for the control room, and the migration strategy for achieving the endpoint will be the major factors in determining the effect that the modifications will have on communications and communication systems. See Section 2 for guidance on planning of the modernization program.

Changes to the existing communication systems are derived from and guided by the endpoint vision for the control room and the overall concept of operations (Section 2.2). These changes should be consistent with the plant technical and safety requirements and the timing of their implementation should be coordinated with other related system changes. Of special concern are the effects of control system modifications on communication tasks in workplaces and how the design of new control interfaces may affect the ability of and the need for the operators to communicate with other personnel. Other modifications can significantly affect the communication among the operators and other plant staff. Section 4.7.3 addresses the main considerations for communication system design. The following are examples of modification aspects that can have significant impact on communications:

- Distribution of workstations and their layout (Section 4.8),
- Handling and presentation of alarms (Section 4.4),
- Use of computer-based procedures (Section 4.5),
- Changes to the I&C system maintenance practices, such as equipment tagging logs, (Section 6.1), and
- Use of computerized operator support systems (Section 4.6).

The design phase for a modification that involves the I&C systems and/or HSI should consider the impact that it will have on plant personnel communications. In many cases, the analyses of the changes to the operators' tasks resulting from the modification should identify those areas where the communication systems are being relied upon. The uses of communication systems should then be evaluated to establish if the existing communication systems are adequate to support personnel tasks; if not, modifications to the communication systems may be required. If modifications to communication systems are being made to address existing problems and shortcomings, then Function Analysis and Allocation (Section 3.3) and Task Analysis (Section 3.4) should address all tasks that involve the modified communications system.

Changes to personnel communication techniques may affect workload. For example, overview displays can provide information to several crewmembers simultaneously, thus enhancing communication and coordination. On the other hand, communication among the crewmembers may become more challenging with I&C upgrades as the placement of display screens and workstations and their visibility may result in an increase in workload (e.g., operators may have difficulties observing other operators execute their tasks, the necessity to use more time for verbal communication because the workstations are too far apart, etc.).

As discussed in Section 4.8, workstations and workplaces are locations where the HSI resources (e.g., displays) are situated and where personnel perform their functions and tasks. The workplace layout may have a major impact on communications. General guidance on workplace design, including that related to communications, is provided in Section 4.8. Some specific communication-related workplace layout guidance is also offered in Section 4.7.5.

A lot of detailed HFE guidance on communications and communication system design can be found in Section 10 of NUREG-0700. It also provides references to useful sources of information that can be helpful in applying the guidance. The approach taken in this section is to cite and discuss only those guidelines that are particularly relevant to I&C modernization projects using digital control systems for hybrid control rooms. This section contains guidance related to communication systems that has not been addressed in Section 10 of NUREG-0700; such is the case with guidance on communication at local control stations and for general guidance on communication systems. If a major change to the communication system is being planned, essentially all the communication-related guidance provided in NUREG-0700 will have to be considered and referenced documents may need to be consulted. References are provided given in Section 4.7.6.

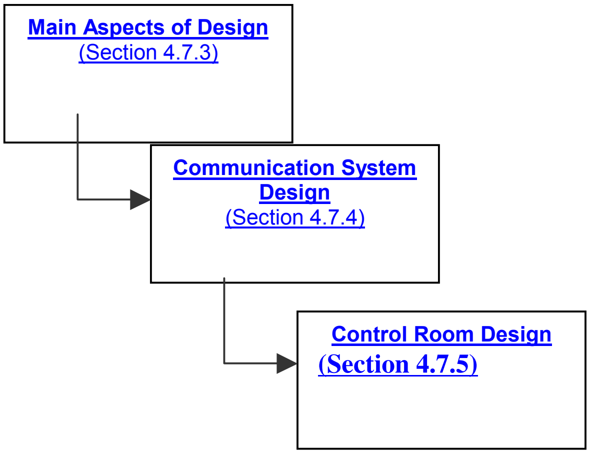


Figure 4-44
Communication System Design

4.7.2 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining communication system sections. For additional information, consult the sections and guidelines referenced.

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.7.3	Main Aspects of Communication System Design							
	=>	4.7.3-1	Identify the implications to communications and communication systems as part of defining the endpoint vision and developing the migration strategy.					
	=>	4.7.3-2	Identify the changes that need to be made to the communication system due to modification impacts.					
	=>	4.7.3-3	Identify the changes to the communication system required by the new I&C and HSI systems. The functions and features of any aspects of the existing communication system that will be affected by the plant modifications should be identified.					
	=>	4.7.3-4	Identify the changes desired to correct existing communication problems.					
4.7.4	Communication System Design							
	4.7.4.1	General Considerations						
		=>	4.7.4.1-1	Location of workstations should facilitate communication and interaction among operators.				
		=>	4.7.4.1-2	HSIs should provide information quickly and comprehensively to facilitate communication among operators without creating additional workload burden.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.7.4.1-3	Communication among personnel should remain effective under any foreseeable operational conditions and at any stage of the upgrade.				
		=>	4.7.4.1-4	Changes in task allocation and workload should not adversely affect the way people communicate.				
		=>	4.7.4.1-5	Training on communication system should be performed to ensure adequate use.				
		=>	4.7.4.1-6	Evaluation of communications and identification of any problem areas should be part of in-service monitoring.				
	4.7.4.2		Speech-Based Communication					
		=>	4.7.4.2-1	Communication devices (e.g. telephones, radios, etc.) should be reliable and reasonably located within the workplace for ease of operators use.				
		=>	4.7.4.2-2	Visual aids (e.g. overview displays) may be used to reinforce communication among operators or to call attention to various operational conditions, such as abnormal conditions.				
		=>	4.7.4.2-3	Auxiliary, backup and/or emergency communication devices should be available at local control stations, especially where communications are critical.				
		=>	4.7.4.2-4	If the communication system requires entry of device addresses or numbers, these should be posted in open view close to the communication devices (e.g., telephones).				
		=>	4.7.4.2-5	When telephone systems are used as part of the announcing system (e.g. loudspeakers), the systems should be provided with multiple channels.				
		=>	4.7.4.2-6	Communication devices (e.g. intercoms) should be easily accessible to personnel at local control stations.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.7.4.2-7	Communication devices should have special administrative controls that regulate their use.				
		=>	4.7.4.2-8	The communication media should remain effective under any foreseeable conditions.				
		=>	4.7.4.2-9	In areas with high noise levels, visual annunciation (e.g. indicators) may be installed to emphasize alert conditions and/or receiving information through the communication device.				
		=>	4.7.4.2-10	The communication system in local control stations should be subjected to periodic surveillance.				
	4.7.4.3		Computer-Based Communication					
		=>	4.7.4.3-1	Procedures for preparing, sending, and receiving messages should be designed and incorporated as part of the operating philosophy so consistency is promoted when handling information and critical tasks requiring communication between personnel.				
		=>	4.7.4.3-2	Both sending and receiving messages should be accomplished by an unambiguous user action.				
		=>	4.7.4.3-3	Personnel should have full control of what, when, and where the data are transmitted.				
		=>	4.7.4.3-4	Personnel should be able to interrupt message preparation, review, or disposition. Resumption should be from the point of interruption.				
		=>	4.7.4.3-5	When important or critical data is transmitted, the message should be annotated with any alarm or alert conditions, priority indicators, and other significant information that exists.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.7.4.3-6	The computer-based communication system should be independent and part of a secure network and therefore, should have filter capabilities to block messages, such as commercial advertising, deceptive, quasi-legal services, and partly or entirely fraudulent messages.				
		=>	4.7.4.3-7	Notification of new messages can be enhanced by sound annunciation.				
		=>	4.7.4.3-8	The arrival of a message in a format incompatible with that of the system receiving the message should not result in the loss of the message or of any ongoing operation.				
		=>	4.7.4.3-9	Computer-based communication systems in local control stations should be capable of exchanging the information with other locations including the Main Control Room.				
		=>	4.7.4.3-10	The throughput time of communication data should be adequate for the message being sent or received.				
		=>	4.7.4.3-11	If possible, adequate indications should be provided at the local control station to show the communication network status.				
4.7.5	Control Room Design and Communication System							
	=>	4.7.5-1	Enhance communication in the control room by identifying the different ways that the operators interact with each other and by incorporating the solutions that meet the operator needs at the design level.					
	=>	4.7.5-2	The types and locations of communication devices, such as telephones and radios, should not interfere or disturb other operators.					

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.7.5-3	Communication between the members of operational teams should be considered when modifying the control room so that communication among the team members and other personnel is enhanced.				
	=>	4.7.5-4	The location of the supervisor's workstation should be chosen considering the communication and observation needs between him/her and other personnel.				
	=>	4.7.5-5	Provide means to improve inter-shift communication without disrupting operations.				
	=>	4.7.5-6	The communication capabilities should be usable in the expected acoustical environment.				
	=>	4.7.5-7	Non-operating personnel in the control room should not be a source of distraction for control operators.				

4.7.3 Main Aspects of Communication System Design

This section discusses the general considerations that should be addressed before applying the more detailed guidance provided in the following sections.

⇒ 4.7.3-1 Identify the implications to communications and communication systems as part of defining the endpoint vision and developing the migration strategy.

Modification to the communication system should consider both the design basis as well as the use of the system within the plant. Specifically, the workplace layout, workstation location, the size and visibility of display screens, and tasks to be performed in the upgraded control room are among the factors that may affect communication patterns and practices.

⇒ 4.7.3-2 Identify the changes that need to be made to the communication system due to modification impacts.

During the planning stage, decide, in broad terms, how communication among personnel will be affected by the changes. The endpoint vision for the workstation and workplace design will define how personnel interact with each other. For example:

- Organization of the control room (e.g., functions allocated to plant personnel and their organization in the control room),
- Use of advanced process control and instrumentation,
- Workstation design (See Section 4.8),
- Location and layout of workstations and workplaces,
- Resources used to communicate process data to personnel (e.g. overview display, radios, etc.),
- Location of supervisor's workstation, and
- Tasks that are involved - the upgrade effort may eliminate or add tasks involving verbal communication.

⇒ 4.7.3-3 Identify the changes to the communication system required by the new I&C and HSI systems. The functions and features of any aspects of the existing communication system that will be affected by the plant modifications should be identified.

The use of advanced process control, instrumentation, and new equipment will alter the way that operations personnel interact with each other. Effective communication does not always require the latest technology. Sometimes the implementation of advanced systems can affect or restrict the ability of personnel to communicate effectively. For example, if workstations are too far apart, operators can have trouble observing other operators execute their tasks, resulting in potential difficulties and necessitate more time for verbal communication among the crewmembers.

The modification design process should establish whether the new system will improve communications among the control room crew or may have the potential to add to their communication burdens. Communication in the control room can be enhanced by simply recognizing the various ways personnel need to communicate with each other and, at the design level, by incorporating solutions that meet those needs. For example, the following items should be considered during the modification design:

- Effectiveness of the existing communication system,
- Control room design (e.g. workplace layout, workstation design, etc.),
- Concept of operations including crew coordination and supervision,
- Corporate culture, such as organization's beliefs, attitudes, and priorities, and how these items affect communication between personnel, and
- Procedures, such as operating and maintenance procedures

For example, the design team members should determine how the communication between team members would be affected by the modification if the locations of operators change with respect to each other.

⇒ 4.7.3-4 Identify the changes desired to correct existing communication problems.

Task analysis and personnel input can serve as effective sources of information for identifying existing communication problems. For example, some of the inputs that should be considered while determining whether the modification effort can be used to improve the existing communication problems may include information about:

- How existing communication systems support situation awareness,
- How communication affects work procedures and methods, and
- How operators work around existing communication problems.

In addition, based on operating experience, the design team can identify potential communication system improvements. Instrumentation and control modifications may provide opportunities to improve communication and solve the existing problems. The communication system(s) includes all interaction between the control room operators and these operators with others, such as the Technical Support Center (TSC) and plant personnel (e.g., maintainers, field operators, etc.). Communications should be addressed in the overall task analyses (Section 3.2). When analyzing communication tasks, designers should include input from appropriate personnel potentially involved in the modification being undertaken so that opportunities for improvement can be identified and evaluated.

4.7.4 Communication System Design

The subject of communication covers all interactions among personnel, including communication inside the control room, between the Main Control Room and local control stations, and between the Main Control Room or local control stations and other locations within the plant.

NUREG-0700 contains detailed guidelines for communication systems, as identified in Table 4-19 below.

Table 4-19
Available Guidance for Communciation

Topic	Source
General Considerations	NUREG-0700, Section 10.1
Speech-Based Communication	NUREG-0700, Section 10.2
Computer-Based Communication	NUREG-0700, Section 10.3

In addition to the guidance provided in NUREG-0700, the following supplementary guidance should be considered for hybrid control rooms.

4.7.4.1 General Considerations

As mentioned previously, it is important to establish the techniques that personnel use to interact and communicate during various modes of plant operation. The introduction of a new communication system can affect the communication burden and the time required to assess plant conditions. A new communication system will likely have different benefits and/or consequences to plant operation. Similarly, modifications may affect personnel roles or tasks, with consequent effects on communication.

This section provides guidance on general considerations for designing a communication system or making modifications to the HSI that may affect communications.

⇒ 4.7.4.1-1 Location of workstations should facilitate communication and interaction among operators.

The location of workstations plays an important role in communication and crew interaction (Section 4.8). For example, if operators are placed far away from each other, it will be difficult for them to support each other's tasks if displays and/or workstations are placed between them. Therefore, workstations within the control room should be arranged such that they do not obstruct interaction among personnel.

⇒ 4.7.4.1-2 HSIs should provide information quickly and comprehensively to facilitate communication among operators without creating additional workload burden.

In general, control room upgrades will improve crew communications because of the increase in the information quality and speed. For example, an overview display (wall size) can provide information simultaneously to multiple crew members, thus enhancing communication and coordination.

⇒ 4.7.4.1-3 Communication among personnel should remain effective under any foreseeable operational conditions and at any stage of the upgrade.

It is important to understand existing traffic patterns and means of communication so that changes to the control room support task performance and do not adversely affect communication.

⇒ 4.7.4.1-4 Changes in task allocation and workload should not adversely affect the way people communicate.

Changes in task allocation can affect personnel communication by changing who's doing what, and thus who has to communicate what to whom. The tasks performed in the control room or at local stations will define the interaction of the operators.

⇒ 4.7.4.1-5 Training on communication system should be performed to ensure adequate use.

Regardless what methods or systems are used for communication in the plant, personnel should be frequently trained to ensure effective communication and use of communication devices.

Modern HSI will provide advanced capabilities for presenting and processing information. However, operators may not receive enough training on how to communicate this information nor the effective way to do it. Designers should ensure that changes made to the communication system are addressed by training programs and work procedures.

⇒ 4.7.4.1-6 Evaluation of communications and identification of any problem areas should be part of in-service monitoring (Section 3.5).

Inspection and evaluation of the communication system should be performed periodically.

4.7.4.2 Speech-Based Communications

Personnel in the control room communicate directly via unaided speech. However, when personnel are separated by a large distance, communication devices may be used. This section provides guidelines for speech-based communication systems.

⇒ 4.7.4.2-1 Communication devices (e.g., telephones, radios, etc.) should be reliable and reasonably located within the workplace for ease of operator use.

Communication devices should be located within the workplace so they can be easily accessed by personnel. During migration, equipment will be removed or installed; however designers should ensure that the quantity of communication devices (e.g., telephones, radios, etc.) is sufficient to meet the communication task needs.

⇒ 4.7.4.2-2 Visual aids (e.g. overview displays) may be used to reinforce communication among operators or to call attention to various operational conditions, such as abnormal conditions.

The Main Control Room design may need to incorporate an overview display so that all control room personnel can obtain the same plant status information at the same time (i.e., to help maintain the crew situation awareness).

⇒ 4.7.4.2-3 Auxiliary, backup and/or emergency communication devices should be available at local control stations, especially where communications are critical.

The loss or failure of a communication device should not prevent operators from communicating with plant personnel.

Portable systems (e.g. radio communications) should be available at local control stations to support communication between different plant areas and the Main Control Room. The increased use of digital systems may prevent the use of radios in a greater portion of the plant. Areas where the use of portable systems is restricted or not available should be identified and different communication approaches should be adopted.

⇒ 4.7.4.2-4 If the communication system requires entry of device addresses or numbers, these should be posted in the open view close to the communication devices (e.g., telephones).

⇒ 4.7.4.2-5 When telephone systems are used as part of the announcing system (e.g. loudspeakers), the systems should be provided with multiple channels.

Multiple channels or lines should be provided to relieve traffic of incoming calls. When multi-channel phones are used, means should be provided to identify the incoming source. Also, the phone system should have the ability to place the calls on hold. A visual signal should be provided to show which channels are in use.

⇒ 4.7.4.2-6 Communication devices (e.g. intercoms) should be easily accessible to personnel at local control stations.

⇒ 4.7.4.2-7 Communication devices should have special administrative controls that regulate their use.

Communication devices should be accessible and available to sustain operation. Administrative controls should limit unauthorized or excessive use of communication devices. For example, workstations and phones should not be for personal use (e.g. surfing the internet).

⇒ 4.7.4.2-8 The communication media should remain effective under any foreseeable conditions.

Personnel at local control stations must be able to understand the information transmitted through the communication device. One of the principal concerns for the communication system in local control stations is that the environment where they are located may be more severe than in the control room (e.g. higher levels of background noise).

For example, if loudspeakers are used in local control stations, the operators should be able to listen to and understand the information transmitted via the speakers. Therefore, the design and location of the speakers should be chosen to limit the impact of background noise in the area, or if the noise is so high that it restricts hearing the messages, some device other than a loudspeaker (e.g. headphones, noise-attenuating enclosures, noise canceling microphones) should be provided such that it permits the message to be heard.

⇒ 4.7.4.2-9 In areas with high noise levels, visual annunciation (e.g. indicators) may be installed to emphasize alert conditions and/or receiving information through the communication device.

In cases where local stations are located in a high noise area, attempts should be made to install an announcing system to alert personnel. For example, a visual indicator (e.g. light) can be installed in a visible area to announce an incoming call.

⇒ 4.7.4.2-10 The communication system in local control stations should be subjected to periodic surveillance.

Since many local control stations are not used frequently, maintenance personnel should periodically check the functionality of the communication system to ensure proper operation.

4.7.4.3 Computer-Based Communications

This section addresses communication among personnel using computer systems. It provides guidelines for communication among personnel using different interconnected computer systems. It also addresses transmission of different types of data (e.g. text files) between users and focuses on the exchange of messages. Special considerations and restrictions that apply to data that must be protected against unauthorized change or interference or interception should be considered.

4.7.4.3-1 Procedures for preparing, sending, and receiving messages should be designed and incorporated as part of the operating philosophy so consistency is promoted when handling information and critical tasks requiring communication between personnel.

Procedures should be established for preparation of messages, including determining the priority levels for the message, destinations, and the information required as part of the message text. These procedures should also address message handling, such that high priority messages can receive special attention and if actions are required, these would be properly addressed.

⇒ 4.7.4.3-2 Both sending and receiving messages should be accomplished by an unambiguous user action.

Data transmission should be easy to implement and should not require special instructions.

⇒ 4.7.4.3-3 Personnel should have full control of what, when, and where the data are transmitted.

⇒ 4.7.4.3-4 Personnel should be able to interrupt message preparation, review, or disposition. Resumption should be from the point of interruption.

Operators should be able to halt message preparation to perform other tasks in the system, such as monitoring, without loosing the information. The systems should be capable of automatically saving the data or prompting the operator to save data.

⇒ 4.7.4.3-5 When important or critical data is transmitted, the message should be annotated with any alarm or alert conditions, priority indicators, and other significant information that exists.

Operators should be able to highlight messages to emphasize priority. In addition, operators should have the capability to flag messages that are still pending, need a follow-up, or require other action. Features can be added to the system to allow the operators create notes as a part of the message.

⇒ 4.7.4.3-6 The computer-based communication system should be independent and part of a secure network and therefore, should have filter capabilities to block messages, such as commercial advertising, deceptive, quasi-legal services, and partly or entirely fraudulent messages.

With the increase of electronic mail has come an increase in “junk mail” which winds up in the email Inbox. These messages are called “Spam”. Communication systems should be designed with “anti-spam” capabilities that prevent such messages from reaching the recipient’s Inbox.

⇒ 4.7.4.3-7 Notification of new messages can be enhanced by sound annunciation.

A sound (e.g. beep) automatically generated when a new message is received can help the user identify incoming mail. However, the announcing system should not interfere with other communication systems. The tone of the beep should be easily distinguishable from process indications signals or signals associated with alarms, and the user should be able to disable the sound annunciation.

⇒ 4.7.4.3-8 The arrival of a message in a format incompatible with that of the system receiving the message should not result in the loss of the message or of any ongoing operation.

If the format of the transmitted data is incompatible with the system receiving it, the recipient should be notified. For example, if a text-based message is faxed to the Main Control Room and the fax cannot receive the information because the format is incompatible, the fax should announce the error (e.g., sound a beep) and/or print a report.

⇒ 4.7.4.3-9 Computer-based communication systems in local control stations should be capable of exchanging information with other locations, including the Main Control Room.

Portable computers (e.g., laptops) should be easily connected to the network and able to retrieve messages and other information. Therefore, communication networks should be installed to support geographic distribution.

⇒ 4.7.4.3-10 The throughput time of communication data should be adequate for the message being sent or received.

The rate at which a computer-based communication system receives or transmits data should be adequate so that plant operation is not interrupted and critical messages are received in a timely manner. Regardless of the communication system used, all communication data transmission throughput time should be examined carefully.

⇒ 4.7.4.3-11 If possible, adequate indications should be provided at the local control station to show the communication network status.

4.7.5 Control Room Design and Communication System

This section provides guidance on how the design of the control room layout affects the design of the communication system.

Design considerations and guidelines should be used to ensure that the workplace provides a work environment that maximizes personnel attention (Section 4.8) and allows proper communication among personnel.

⇒ 4.7.5-1 Enhance communication in the control room by identifying the different ways that the operators interact with each other and by incorporating the solutions that meet the operator needs at the design level.

Advanced process control has altered the way operators communicate with each other. Changes in the workplace layout can result in changes to the location of operators with respect to each other. For example, if there is strong need for certain personnel under some circumstances to engage in critical unaided voice communications, their work areas might need to be placed together to eliminate the need to talk across the room and disrupt other personnel.

⇒ 4.7.5-2 The types and locations of communication devices, such as telephones and radios, should not interfere or disturb other operators.

⇒ 4.7.5-3 Communication between the members of operational teams should be considered when modifying the control room so that communication among the team members and other personnel is enhanced.

The introduction of digital systems will improve communication among operators because of the increase in information quality and the use of display screens for control and monitoring.

⇒ 4.7.5-4 The location of the supervisor's workstation should be chosen considering the communication and observation needs between him/her and other personnel.

⇒ 4.7.5-5 Provide means to improve inter-shift communication without disrupting operations.

Communication issues can arise during shift turnovers. Information about equipment failure, out-of-service devices, and changes in process status need to be communicated to the following shift, and as a larger number of people occupies the Main Control Room, the noise level increases.

⇒ 4.7.5-6 The communication capabilities should be usable in the expected acoustical environment.

Interim control room configurations that occur during modernization migration have the potential to increase the number of workstations or work areas resulting in an adverse impact on communication. Therefore, the workplace design should be such that it minimizes the uncontrolled noise (e.g., conversational noise that creates distractions) and provides an acoustical environment that promotes communication (Section 4.8).

⇒ 4.7.5-7 Non-operating personnel in the control room should not be a source of distraction for control operators.

During control room upgrade, contractors and visitors will often have to be present in the control room to discuss possible upgrades of systems or services, creating a potential source of distraction and stress to the control room operators. Therefore, workplace designers should provide means (e.g. conference room, traffic barriers, etc.) to facilitate work and conversations without disturbing operators.

4.8 Workstations and Workplaces

4.8.1 Overview

4.8.2 Workstations and Workplaces Guidelines Checklist

4.8.3 General Considerations

4.8.4 Workstation Design

4.8.4.1 Configuration

    4.8.4.2 Control and Display Device Layout

    4.8.4.3 Labeling and Demarcations

4.8.5 Workplace Design

    4.8.5.1 Control Room Layout and Configuration

    4.8.5.2 Control Room Environment

    4.8.5.3 Local Control Stations

4.8.6 Managing the Impact of Modifications

4.8.7 Sources of Additional Information

4.8.1 Overview

This section contains guidance for addressing changes to workstations and workplaces (W&W) associated with digital upgrades. Figure 4-45 provides an overview of the design aspects addressed and their corresponding section numbers.

The first aspect of W&W design is the general considerations that provide input to the process. These include:

- the endpoint vision
- changes necessitated by the new plant systems
- desired improvements based on operating experience[6]

Workstations, including consoles and panels, are locations where individual HSI resources (i.e., alarms, displays, and controls) are situated to provide the means for personnel to perform their tasks. Even if the basic layout of the workplace is not changed, individual workstations and panels will be affected by the incorporation of digital technology. The main design considerations for workstations include their configuration, arrangement of HSI devices, such as displays and controls, and labeling and demarcations. The guidance in this section can also be applied to modifications to interfaces outside the control room.

A workplace is defined to be the location where the personnel perform their functions and tasks. This typically includes the main control room, remote shutdown stations, the Technical Support Center (TSC), and the Emergency Operations Facility (EOF). Workplaces often include operator workstations, overview displays, vertical panels, wraparound benchboards, laydown space, procedure storage, a supervisor area, etc. One of the main considerations for the workplace design is the layout, location, and orientation of this equipment. Design of the control room environment is another important workspace consideration. Control room modernizations, even those that are limited in scope, can affect the workplace environment, such as lighting and noise. As not all workplaces involve a control room, consideration is give to local workplaces as well.

The final section addresses the management of modifications. This includes considerations of supporting crew performance during modifications that take place while the control room is still in use and across successive outages.

Detailed guidance already exists on many aspects of W&W design. Our approach in this section is to discuss the important considerations for each topic above and provide cross-references to the appropriate documents containing the relevant guidance. New guidance is present only when existing guidance did not address an important topic. Full references to identified sources are given in Section 4.8.7.

[6] Even modifications to workstations and workplaces of more limited scope can provide opportunities to improve the overall design by fixing existing problems or accomplishing improvements not specifically related to those required by the modification.

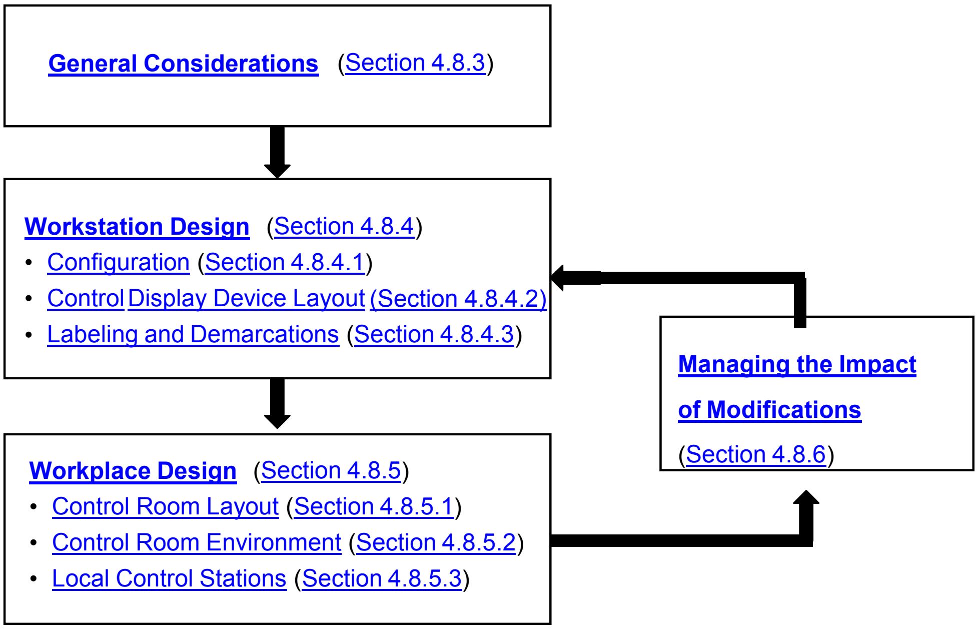

General Considerations (Section 4.8.3)
Workstation Design (Section 4.8.4)
• Configuration (Section 4.8.4.1)
• Control Display Device Layout (Section 4.8.4.2)
• Labeling and Demarcations (Section 4.8.4.3)
Managing the Impact of Modifications (Section 4.8.6)
Workplace Design (Section 4.8.5)
• Control Room Layout (Section 4.8.5.1)
• Control Room Environment (Section 4.8.5.2)
• Local Control Stations (Section 4.8.5.3)

Figure 4-45
Overview of Workstation and Workplace Design

4.8.2 Workstations and Workplaces Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining sections. For additional information, please consult the sections and guidelines referenced.

Guidelines					Complies	Does not comply, but with Justification	Does not comply, but without Justification	Not Applicable
4.8.3	Overview							
	=>	4.8.3-1	W&W implications of the endpoint vision should be identified.					
	=>	4.8.3-2	W&W changes necessitated by any new systems or equipment that will be added to the plant should be identified.					
	=>	4.8.3-3	Control room improvements based on operating experience should be identified.					
	=>	4.8.3-4	The functions and features of any aspects of the existing workplaces that will be affected by the plant modifications should be identified.					
4.8.4	Workstation Design							
	4.8.4.1	Configuration						
		=>	4.8.4.1-1	In choosing the workstation modifications or additional workstations to be introduced into the control room, consider the tasks to be carried out and the users' needs to access other control room resources or interfaces while performing the tasks.				
		=>	4.8.4.1-2	The number and kind of display devices (i.e., amount of display area) provided at a workstation should reflect a comprehensive consideration of what information is needed, where it is available, how it is organized, and what must be done to obtain it.				

Guidelines					Complies	Does not comply, but with Justification	Does not comply, but without Justification	Not Applicable
		=>	4.8.4.1-3	The number and location of display devices should take into account the need for coordination of activities across crewmembers.				
		=>	4.8.4.1-4	For seated workstations, rolling chairs should be considered for flexibility and comfort.				
		=>	4.8.4.1-5	Workstation designs should be flexible, so that they can accommodate infrequent or unusual user activity, or simply provide an opportunity for users to alleviate fatigue.				
		=>	4.8.4.1-6	When conventional instrumentation is physically replaced in an existing console or panel by computer-driven equipment, it should be verified that the new equipment is visible and readable from the work positions.				
		=>	4.8.4.1-7	Changes to workstations or interfaces should not force users to have to unlearn existing skills.				
		=>	4.8.4.1-8	Changes to the workstations or interfaces should be conspicuous.				
		=>	4.8.4.1-9	Non-functional interfaces in the control room should be eliminated or minimized.				
	4.8.4.2		Control and Display Device Layout					
	4.8.4.3		Labeling and Demarcations					
4.8.5		Workplace Design						
	4.8.5.1		Control Room Layout and Configuration					
		=>	4.8.5.1-1	Workplace elements, such as panels, workstations, large displays, etc., should be laid out to support smooth movement of people to and from their work areas and allow easy access to needed interfaces and support equipment with minimal disruption of others.				

			Guidelines	Complies	Does not comply, but with Justification	Does not comply, but without Justification	Not Applicable
	=>	4.8.5.1-2	Workplace components that must be viewed from a primary work location should be located to provide the required visibility.				
	=>	4.8.5.1-3	Workstations should be located so that crewmembers can easily communicate and observe each other's actions.				
	=>	4.8.5.1-4	The workplace should be large enough to allow the operating crew to interact with others (auxiliary personnel, crews coming on shift) comfortably without crowding or interference.				
	=>	4.8.5.1-5	When workstations are added to the workplace, they should be located so that personnel at those stations (and at other stations) remain able to see displays elsewhere in the room, and their presence doesn't interfere with operations (e.g., operator movements from one station to another).				
4.8.5.2			Control Room Environment				
4.8.5.2.1			Illumination				
	=>	4.8.5.2.1-1	Illumination should be suitable for the tasks performed at all work locations.				
	=>	4.8.5.2.1-2	To meet varying lighting requirements, adjustable task lighting should be considered.				
	=>	4.8.5.2.1-3	Workstation VDUs should be positioned to minimize variations in brightness in the user's field of view.				
	=>	4.8.5.2.1-4	Workstation VDUs should be positioned to minimize glare on the display surfaces.				
	=>	4.8.5.2.1-5	VDUs, workstation surfaces, and lighting fixtures should be designed to minimize reflections and glare.				

Guidelines						Complies	Does not comply, but with Justification	Does not comply, but without Justification	Not Applicable
		4.8.5.2.2		Sound					
			=>	4.8.5.2.2-1	Equipment or cabinets that make noise (e.g., those containing ventilating fans) should be located away from operators whenever possible.				
			=>	4.8.5.2.2-2	Sounds produced by computerized interfaces introduced into the control room should not interfere with existing control room audio codes, especially those that signal important information.				
			=>	4.8.5.2.2-3	Audio signals associated with different computer-driven HSIs in the control room should not interfere with each other.				
			=>	4.8.5.2.2-4	If operators use similar interfaces in proximity to one another (e.g., operators at a bench consisting of a row of displays and pointing devices), measures should be taken to prevent an operator at one workstation from mistakenly attending to auditory feedback from neighboring workstations.				
			=>	4.8.5.2.2-5	Sound levels at the workstation should be such that the workstation operators may still hear any workplace alarms or announcements and so that general conversation and communication between operators or between any personnel in the workroom is convenient.				
			=>	4.8.5.2.2-6	After modifications are implemented, the workplace should still conform to human factors guidance on the effectiveness of auditory signals (alarms in particular) and the intelligibility of speech.				
		4.8.5.2.3		Temperature					
			=>	4.8.5.2.3-1	Verify either by analyses or testing or both that the control room HVAC system can keep the area within the established comfort limits.				
			=>	4.8.5.2.3-2	Ensure that the airflow produced by the equipment itself or that is required to keep it within temperature limits does not result in areas in the control room where air velocity is too high.				

Guidelines				Complies	Does not comply, but with Justification	Does not comply, but without Justification	Not Applicable
	4.8.5.3	Local Control Stations					
4.8.6		Managing the Impact of Modifications					
	=>	4.8.6-1	For each stage of the migration, possible changes to the workplaces and workstations should be considered that are ancillary to the planned modifications of the interface per se.				
	=>	4.8.6-2	Activities associated with the implementation of modifications should not result in obstruction of users' view of or physical access to controls and displays.				
	=>	4.8.6-3	Implementation activities should be planned so that the ability of operating personnel to access needed HSIs and support material in the control room is not restricted.				
	=>	4.8.6-4	Errors or misinterpretations as a result of a phased introduction of digital upgrades should be minimized.				
	=>	4.8.6-5	Measures should be taken to minimize the distraction or interference associated with the activities of personnel involved in implementing modifications.				
	=>	4.8.6-6	Provisions should be made so that workplace hazards are not created during any work in the control room.				

4.8.3 General Considerations

⇒ 4.8.3-1 W&W implications of the endpoint vision should be identified.

The endpoint vision includes the overall design concept for what the workplaces will be like after all the planned modifications are completed. Section 2.2 provides guidance on establishing an endpoint vision as part of HSI modernization planning. If the endpoint vision calls for operations to be conducted primarily at compact workstations with a great deal of flexibility, then this suggests a seated workstation with a computer console as the major focal point of the design. Such a choice may eliminate part of the existing sit-stand benchboard panel consoles. During the planning stage, decisions will have been made that will establish, in broad terms, how the control room is expected to change. Some considerations are given below:

- Will the roles of individual crewmembers be changed in any way, e.g., whether there will be dedicated operators for given functions or systems (this impacts the overall organization of the control room)
- Will crewmembers work at existing panels with upgraded instrumentation
- Will crewmembers use computerized workstations
- Will crewmembers use some combination of workstations and a reduced number of panels
- How will operations be conducted when HSI failures occur (e.g., failure of computerized workstations)
- What other display resources will be available (e.g., group-view or walk-up displays)
- Will there be separate individual workstations or an overall working area used by multiple crewmembers
- Will the workstations be redundant (each having similar functionality) or specialized for particular purposes or to cover specific areas of responsibility
- Will there be a dedicated supervisor's workstation

The plan for implementing upgrades is arrived at by translating high-level aims for the control room into specific modifications that provide an orderly transition or "migration" to the final endpoint. Guidance on planning the migration strategy is given in Section 2.3.

⇒ 4.8.3-2 W&W changes necessitated by any new systems or equipment that will be added to the plant should be identified.

The planned modifications may include addition of new systems or equipment to the plant; see Section 2.2, Endpoint Definition. The new HSIs associated with these additions will have to be accommodated in the workplace; guidance for planning the migration is given in Section 2.3, Migration Strategy.

⇒ 4.8.3-3 Control room improvements based on operating experience should be identified.

Control room modification may afford opportunities to remedy problems not directly related to the planned modifications. For example, this may include relocation of some controls and displays unrelated to the systems being upgraded in order to make an operator’s task performance easier. As another example, operating experience may suggest moving some controls and displays from local control stations into the control room (or vice versa) to improve operations.

⇒ 4.8.3-4 The functions and features of any aspects of the existing workplaces that will be affected by the plant modifications should be identified.

The following are some topics that should be considered:

- The current operating methods
- The functions and tasks performed in the workplace
- The existing layout of HSI resources, e.g., displays, controls, and communication equipment, and how they are distributed across the control room or other workplace
- Any “secondary” uses of the workstation. (e.g., writing surface, communication devices, or reference storage)

The last item is an important consideration. Workstations may support uses other than those connected with the components affected by the modification (e.g., they may provide writing surfaces or document storage). Furthermore the components themselves may have multiple functions. For example, conventional strip chart recorders may have functions in addition to indicating current trends in plant parameters; e.g., by their nature, they produce permanent records (short term histories for analysis for an ongoing event and longer term archives for engineering analysis), and they can be annotated contemporaneously or post hoc. If digital displays are to replace such devices, the interface must support all of the functions present previously.

4.8.4 Workstation Design

4.8.4.1 Configuration

HSI elements are organized into workstations, where the operators perform their functions and tasks. Workstations can be broadly characterized according to whether users are expected to be standing or sitting (or a combination of both) while working. Interfaces designed to be used while standing are found in situations where users have to move about to carry out their tasks, as is the case in traditional control rooms with spatially dispersed displays and controls. Workstations designed for seated users are typical when most or all of the users’ tasks can be accomplished from a single location, as is possible when displays and control functions are consolidated at computer workstations. A third type, the sit-stand workstation, is usually designed to be operable while standing or while seated on a high stool (although current height-adjustable workstations can accommodate users in standard chairs).

Designers should identify the characteristics of the existing workstations, including type of workstation, spatial arrangement of controls and displays, special tasks performed, physical dimensions, workspace, etc. This information will be used to verify that the modified design will have features supporting the current functions, as well as any needs that task analyses or operating experience suggest are not being met.

Designers should identify how characteristics such as reach, vision, and comfort may affect the operators' performance. Unique considerations for these types of workstations include the following:

- Workstation height (i.e., for workstations that the operator must see over)
- Benchboard slope, angle, and depth for consoles and sit-stand workstations (i.e., accommodations for reach; provision of writing space)
- Control device location (i.e., placement of highest and lowest controls; distance from front edge of workstation)
- Display device location (i.e., placement of highest and lowest display devices, orientation relative to line of sight, viewing distance, position of frequently and infrequently monitored display devices)
- Lateral spread of control and display devices at a console or workstation
- Laydown space (e.g., for paper procedures)
- Clearances for legs and feet.

When workstations include seating, there are additional important considerations, including mobility; rests for back, arms, and feet; seat adjustability, and cushioning.

Available guidance on workstation configurations is identified in Table 4-20.

Table 4-20
Available Guidance for Workstation Configuration

Topic	Source
Anthropometric data	NUREG-0700, Section 11.1
Stand-up consoles	NUREG-0700, Section 11.1.1 ISO 11064, Section x
Sit-down consoles	NUREG-0700, Section 11.1.2
Sit-stand workstations	NUREG-0700, Section 11.1.3
Vertical panels	NUREG-0700, Section 11.1.4
Desks	NUREG-0700, Section 11.1.5
Chairs	NUREG-0700, Section 11.1.6

In addition to the guidance provided in these sources, the following additional guidance should be considered.

⇒ 4.8.4.1-1 In choosing the workstation modifications or additional workstations to be introduced into the control room, consider the tasks to be carried out and the users' needs to access other control room resources or interfaces while performing the tasks.

Introducing computer-mediated monitoring and control interfaces typically involves the addition of one or more computer workstations (typically consisting of VDUs and means for input). The types of workstation at which the equipment is placed should be appropriate at each point in a phased introduction of digital interfaces and in all operating contexts.

In the final stages of a comprehensive digital upgrade, the functions may be consolidated to such an extent that, under normal operating conditions, users seldom have to leave their principal workstations. In this case a workstation designed to be usable from a seated position would be appropriate. On the other hand, in hybrid control rooms (or at interim stages of a migration), users might frequently be required to leave the workstations to monitor parameters or take action at control boards; in this case, a workstation designed for standing (or one that is adaptable for either sitting or standing) might be preferable. Such a workstation might include VDUs mounted on telescoping arms that allow them to be rotated and positioned for viewing by standing or seated users.

⇒ 4.8.4.1-2 The number and kind of display devices (i.e., amount of display area) provided at a workstation should reflect a comprehensive consideration of what information is needed, where it is available, how it is organized, and what must be done to obtain it.

The appropriate amount of display area will be determined primarily by:

- the information that will be needed at one time by the operators
- the information available via other sources (such as group-view displays)

Additional considerations may include:

- the arrangement of information within display pages
- the arrangement of pages within the display network
- the means used to access the information

The above serves to underscore the fact that determining the number and types of display devices to be provided at workstations (and at other locations in the control room) requires detailed knowledge of the information users require to carry out each of their tasks, including the sequence in which it is needed and the actions users must take to display it.

It may seem desirable to limit the number of computer-driven display units in a control room from a design perspective. Fewer devices means greater simplicity in that there are fewer user interfaces to integrate, less cost for equipment, and a lower maintenance burden. However, the advantages of fewer screens may not be justified when considering the potential cost to operating crew performance. Users might be expected to take advantage of the flexibility of the computer-based interfaces to configure the interface in such a way that it is ideally tailored to the unique demands of the current situation. However, research and operating experience show that they are often reluctant to perform such tasks, especially under high-workload conditions, opting instead to configure their display as a spatially dedicated one. Thus, while the number of display devices may seem reasonable to the designer when considering the flexible access to displays, it may not to the user who is attempting to minimize the effort associated with retrieving them. Users prefer to have more display devices available so that their initial "set-up" can provide most, if not all, the information they will need.

⇒ 4.8.4.1-3 The number and location of display devices should take into account the need for coordination of activities across crewmembers.

Additional display devices may be provided to support communication and coordination among personnel. For example, some displays, such as plant overviews, may be shared by multiple users at a workstation; this may reduce the total number needed (see Figure 4-46).

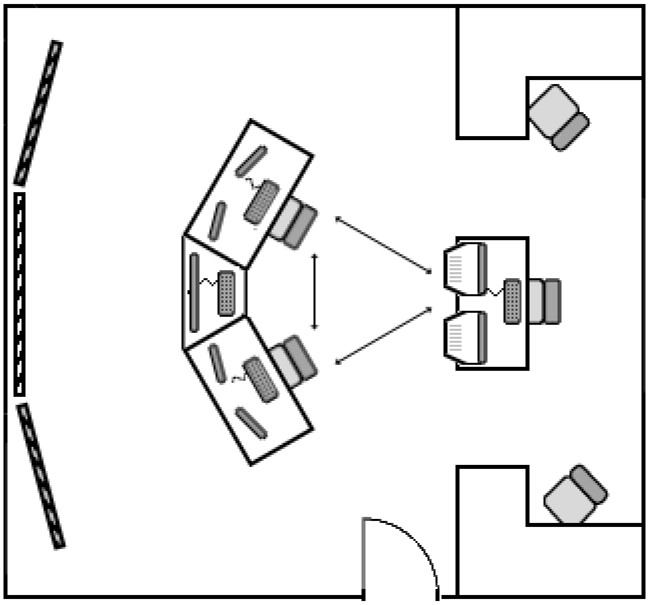


Figure 4-46
The Overall Layout of Workstations should Reflect the Ways in which Users are Expected to Work
For example, if coordinated activity is expected, workstations can be placed close together and oriented so that operators can easily communicate and observe each other's actions. if cooperative activity will be needed, the workstation should be designed to accommodate operators working together (e.g., the workstation with the large display screen at the center of the console in the above example).

⇒ 4.8.4.1-4 For seated workstations, rolling chairs should be considered for flexibility and comfort.

By using chairs that are on casters, components can be placed at locations that are separate from the principal workstations, but still easily reached. For example, secondary displays (and their associated controls) or controls for functions that are shared might be located between the workstations that are normally used (as in Figure 4-46). Components remain easily reached, but the movement required to reach them can help keep users aware of each other's actions and prevent unintended conflicting inputs.

The composition of the caster wheels should be appropriate for the floor surface (soft wheels for hard surfaces, hard wheels for soft, i.e., carpeted, surfaces), and chairs should require little effort to move. Ample floor space should be provided to allow easy repositioning of the chairs. If rolling chairs are used in this way, consider providing a rail or similar feature at the forward edge of the workstation surface to assist users in moving from one position to another. This will reduce the chances of users' hands inadvertently striking input devices while changing positions.

⇒ 4.8.4.1-5 Workstation designs should be flexible, so that they can accommodate infrequent or unusual user activity, or simply provide an opportunity for users to alleviate fatigue.

Even when it can be anticipated that, through consolidation of functions and provision of group view displays, users will typically (i.e., under normal operating conditions) be able to remain seated at a single workstation much of the time, workstations that can be adjusted to accommodate both seated and standing postures should be considered. The degree of flexibility has to consider visibility of panels and overviews and impact on supervision.

⇒ 4.8.4.1-6 When conventional instrumentation is physically replaced in an existing console or panel by computer-driven equipment, it should be verified that the new equipment is visible and readable from the work positions.

A VDU may be assumed to perform identically to the original equipment, since it displays the same data at the same location, but characteristics specific to computer displays (e.g., susceptibility to glare; see Section 4.8.5.2) may constrain the use of the display. For example, some computer-driven displays can be difficult to read at an angle or may not be readable at as great a distance (see Figure 4-47); this might result in users in certain parts of the control room being unable to 'check-read' the display the way they were accustomed to before the modification. It is important for the new design to provide (to the extent possible) the same functionality as the old instrument.

⇒ 4.8.4.1-7 Changes to workstations or interfaces should not force users to have to unlearn existing skills.

It is better for an upgrade to require the user to learn additional skills rather than expect the user to change existing ones. For example, changes limited to physical appearance typically do not seriously disrupt users' performance, whereas changes in the operation of the system almost certainly will. However, sometimes the appearance of a system is strongly linked to user skills. For example, when a conventional display is computerized, the layout (i.e., relative positions) of controls associated with it should change as little as possible. Significant changes will force users to devote attention to overcoming habits, and may lead to errors.

⇒ 4.8.4.1-8 Changes to the workstations or interfaces should be conspicuous.

Drawing the user's attention to characteristics that have changed can help them to adapt their skills. If changes are unavoidable, they should not be subtle. Instead, the interactions surrounding the changed item should be made quite different from the way they were previously, so that users' habitual responses are not evoked.

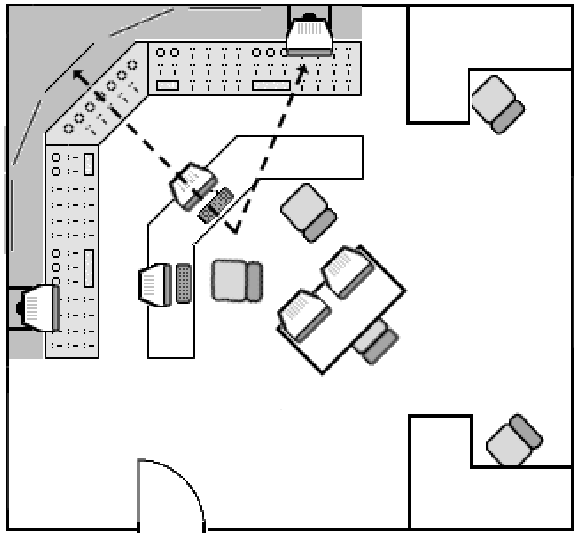


Figure 4-47
In Hybrid or Interim Control Room Configurations, Operators may be Positioned at Computer Equipment Placed Atop Former Laydown Space Located Opposite the Control Boards
As a Result their Typical Working Position is Further from Existing Displays; Designers should Verify that the Displays will Still be easily Readable

⇒ 4.8.4.1-9 Non-functional interfaces in the control room should be eliminated or minimized.

Non-functional HSIs, such as a meter that is no longer operational, can cause confusion in the workstation area. In many cases, it will be sufficient for non-functional HSIs to be clearly identified as such (e.g., with tags). However, an indicator that might in its unactivated state mislead an operator glancing at it (out of longstanding habit) should probably be removed or covered. For example, non-functional meters that ‘fail’ to an operationally plausible value should be eliminated whenever possible.

4.8.4.2 Control and Display Device Layout

Typically, control and display devices are not used in isolation. Groups of devices are used together to perform a task. Therefore, the following relationships among devices should be addressed:

- Grouping of related controls or displays (i.e., by sequence of use, frequency of use, and importance)
- Control devices (i.e., spacing; interference with access; inadvertent actuation of adjacent controls; simultaneous actuation of controls; sequence of use)
- Display devices (i.e., how multiple devices are arrayed at a work station, e.g., in rows or one above another)

- Control-display layout integration (e.g., orientation, proximity, obscuration, and indication of association) for
  - a single control and display pair
  - multiple controls and a single display
  - a single control and multiple displays
- Dynamic control-display relationships (i.e., response compatibility between controls, including rotary and linear devices, and displays, such as linear scales, digital displays, indicator light strings, and circular meter points)
- Between-group and within-group relationships (i.e., control and display modules; repeated groups and functions; mirror-image layouts)

Available guidance on control and display device layout is identified in Table 4-21.

Table 4-21
Available Guidance for Control and Display Device Layout

Topic	Source
Control and Display Device Layout	NUREG-0700, Section 11.2 ISO 11064, Section x

4.8.4.3 Labeling and Demarcations

Labels and demarcations can help operators find and identify controls, displays, and other equipment.

Labels

Permanent labels may be used for panels, groups of controls and displays, individual items, instructions, control direction, and access openings. In addition, temporary labels may be used for such purposes as tagging-out equipment. The following characteristics of labels are important to operator performance:

- Location (i.e., proximity of adjacent labels; orientation; surface mounting considerations)
- Content (i.e., information content, distinguishability, consistency, and agreement with procedures)
- Lettering (i.e., character height, width, font, spacing, stroke width, and contrast with background)

Demarcation

Demarcation lines are used to identify workstation sections and groups of controls and displays. Important characteristics include contrast, consistency, and permanence. Another important consideration is the rationale that was used in applying them (e.g., the types of controls and displays they enclose). Note that modifications that create hybrid interfaces (e.g., introducing a computer-driven VDU display for some controls and indications while retaining some conventional controls and indicators) have the potential to degrade the effectiveness of demarcations, or make it difficult to maintain the benefits intended with the original demarcation design. This should be considered in the design of the upgrades.

Available guidance on labels and demarcations is identified in Table 4-22.

Table 4-22
Available Guidance for Labels and Demarcations

Topic	Source
Labels and demarcations	NUREG-0700, Section 11.3 ISO 11064, Section x

4.8.5 Workplace Design

It is possible (e.g., in the case of direct one-for-one replacement of conventional with digital interface elements in panels) that no changes will be made to the overall ‘footprint’ of the control room. However, when equipment is added (e.g., adding computerized workstation) or eliminated (as a result of consolidating the functions of two or more panels), some aspects of the workplace may change (e.g., the physical layout of equipment and how it affects traffic flow and crew coordination).

4.8.5.1 Control Room Layout and Configuration

Two important aspects of a control room are its configuration (i.e., the arrangement of workstations and other equipment within it) and its environment. The important characteristics of each are described below. Many of these characteristics are also applicable to other workplaces, such as the remote shutdown station, technical support center, and emergency operations facility.

Control room configuration refers to the overall layout and arrangement of the control room; it comprises the following factors:

Accessibility of instrumentation/equipment – Accessibility refers to the ease with which control room personnel can gain access to needed instrumentation and equipment. Any instrumentation and equipment needed by control room personnel for detecting abnormal conditions and shutting down the plant, but which are not located inside the control room, should be identified. Similarly, the controls and displays required for continuous monitoring and the timing of control actions that are not located in the primary operating area of the control room should be identified.

Consistency of staffing with equipment layout – This refers to factors that may affect the adequacy of personnel staffing levels, including: the ability of control room personnel to monitor and operate all necessary controls, displays, and other equipment during all modes of plant operation (e.g., consistency of the control room layout with staffing levels and task assignments); the ability of additional onsite or offsite personnel to augment the normal crew complement under certain unusual conditions, such as refueling (e.g., consistency of control room layout with anticipated activities and task assignments); the ability to operate effectively under conditions of degraded HSIs (e.g., workstation failures); the ability to limit access and movement of nonessential but authorized personnel to prescribed areas within the control room (e.g., adequate designations of prescribed areas; doors, gates, and other physical barriers).

Furniture, instrumentation and equipment layout – The arrangement of furniture, instrumentation, and equipment in the control room that might affect the operators' requirements for viewing, communication, accessibility, and movement.

Document organization and storage – The availability, storage, and accessibility of procedures and other documents needed for ready reference.

Spare parts, operating expendables, and tools – The availability, storage, and accessibility of spare parts, operating expendables, and tools needed by personnel.

Supervisor access – The accessibility of the shift supervisor's office by walking and communication links.

Multiunit control rooms – The characteristics of multi-unit control rooms that may affect personnel performance include whether or not the control room has a mirror-image design, design factors that distinguish the operating units, equipment layout that might affect personnel movement and communication.

Emergency equipment and protective clothing – If personnel are required to wear protective clothing in the workplace, then this clothing should be considered, along with warning systems that signal the need for its use, and storage for protective clothing.

Personal storage – Provisions for storing personal items (e.g., coats and other belongings) can help maintain a clutter-free work environment. Storage places, including those located outside on the control room such as lockers, should be addressed.

Ambience and comfort – Eating, restroom, and lounge facilities contribute to the operators' comfort, health, and performance.

Available guidance on control room layout and configuration is identified in Table 4-23.

Table 4-23
Available Guidance for Control Room Layout and Configuration

Topic	Source
Accessibility of instrumentation/equipment	NUREG-0700, Section 12.1.1.1. ISO 11064, Section x
Consistency of staffing with equipment layout	NUREG-0700, Section 12.1.1.2
Furniture, instrumentation and equipment layout	NUREG-0700, Section 12.1.1.3
Document organization and storage	NUREG-0700, Section 12.1.1.4
Spare parts, operating expendables, and tools	NUREG-0700, Section 12.1.1.5
Supervisor access	NUREG-0700, Section 12.1.1.6
Multiunit control rooms	NUREG-0700, Section 12.1.1.7
Emergency equipment and protective clothing	NUREG-0700, Section 12.1.1.8
Personal storage	NUREG-0700, Section 12.1.1.9
Ambience and comfort	NUREG-0700, Section 12.1.1.10

In addition to the guidance provided in these sources, the following additional guidance should be considered.

⇒ 4.8.5.1-1 Workplace elements, such as panels, workstations, large displays, etc., should be laid out to support smooth movement of people to and from their work areas and allow easy access to needed interfaces and support equipment with minimal disruption of others.

Designers should consider how modifications might affect traffic patterns in the control room. Simple, one-for-one replacement of console or panel components will likely not affect traffic patterns. However, adding computer-based workstations will also typically add desk- or table-like workstations and chairs to the workplace. Furthermore, when functions are consolidated (as they may be with the introduction of computer-driven interfaces), operators' movements may shift to different, more limited areas of the control room. Finally, in a hybrid control room, or during migration, both old and new HSI components are present in the workplace, which can increase and change operators' movements, with operators working in different places alternating the use of workstations (old and new). The design should lead to favorable traffic patterns; for example,

- crewmembers should have easy access to interfaces used in their primary tasks
- personnel entering the control room should not interfere with crewmembers' monitoring or control activities
- traffic should not interfere with the supervisor's monitoring of crewmembers

The other locations that users may need to go to frequently or quickly should be identified, and workstations should be located so that they can be reached with minimal disruption of the ongoing task (see Figure 4-48).

⇒ 4.8.5.1-2 Workplace components that must be viewed from a primary work location should be located to provide the required visibility.

Workplace components such as group-view displays or alarm panels, have to be situated such that they can be viewed from the work areas where they will be used, such as operator workstations (see Figure 4-46). Of course this is not only a function of location, but also of the size of the information in the display. The two considerations have to be addressed together; design of displayed information is addressed in Section 4.1.

⇒ 4.8.5.1-3 Workstations should be located so that crewmembers can easily communicate and observe each other's actions.

While the need to accommodate multiple personnel may favor widely spaced workstations, the advantages of having users located close to each other should not be overlooked. (Compare Figure 4-49 to Figure 4-46). While being able to see other users at workstations may not reveal as much about their actions as watching users at conventional boards, proximity will nevertheless make verbal communication easier.

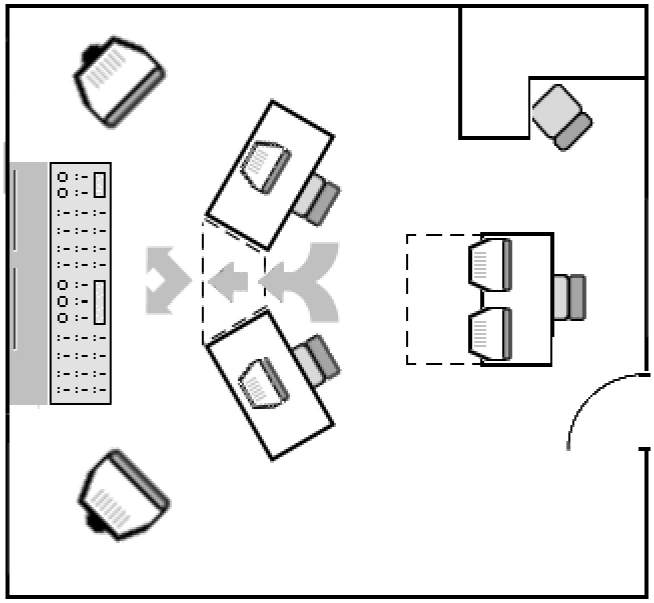


Figure 4-48
The Arrangement of Workstations in Hybrid or Interim Control Rooms should take into Account the Operators' Continuing need to Access the Boards as well as the Computer-Mediated Controls and Displays
In the illustration above, it would be preferable to locate document storage and laydown space directly behind the operators rather than between the desks so as to allow easier access to the panel.

With multiple, redundant digital workstations, some input interfaces for controlling plant variables may be accessed from multiple locations in the control room. If a control function is shared among users but only one user can operate it at a time, or if an override capability is provided (allowing one user to take the control capability of a shared control from another user), user must be aware of each other's actions in order to work effectively. Because computerization can make crewmembers' actions less observable to others, steps should be taken to prevent interference (programmed into the control interfaces) and promote coordinated action (arrangement of workstations to increase visibility and communication); see also Section 4.1.3.3, Display Design for Teamwork, Crew Coordination, and Collaborative Work. In cases where the ability to share responsibilities for control is not essential, or if error or delay might have serious consequences, the problem might be addressed by assigning control capabilities for a plant variable to a particular control console; i.e., users at other consoles can observe the control setting but cannot initiate changes.

Computer-mediated interaction with the plant can have the effect of reducing the crew's awareness of each other's actions. At the same time, the consolidation possible with computerization also makes it possible to perform functions from multiple locations. When more than one user can control equipment, the design should support coordinated activity. The design should also maximize the ability of users who share the responsibilities for monitoring and control to share the required interface resources. The guidance below addressed these issues primarily in the context of the arrangement of interfaces in the control room. Guidance for display system features specifically designed to support crewmembers' awareness of others' actions are provided in Section 4.1.3.3, Display Design for Teamwork, Crew Coordination, and Collaborative Work).

Digital upgrades may have the effect of removing some constraints on the physical location of the supervisor's station. Digital information systems will allow supervisors to monitor important parameters without necessarily having to view the same physical displays the operators are using. However, because computer-mediated monitoring and control makes operators' activities less 'visible' to an observer, designers must ensure that the changes in interaction don't leave 'blind spots' that might lessen supervisors' awareness. Specifically, the design should include features that increase supervisors' awareness of operators' actions (see Section 4.1.3.3, Display Design for Teamwork, Crew Coordination, and Collaborative Work).

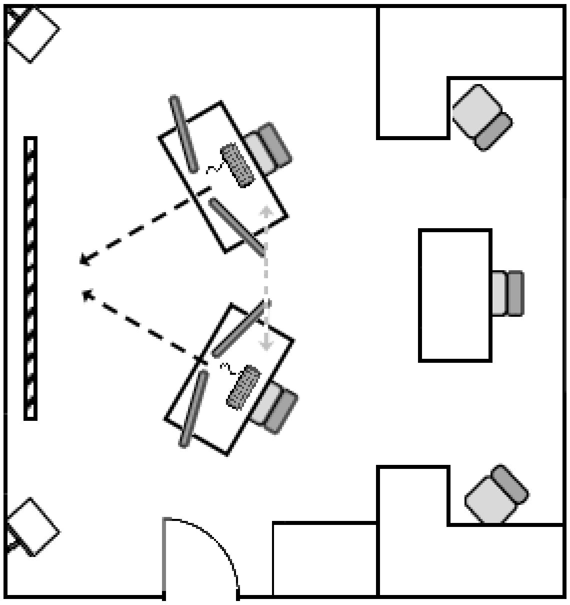


Figure 4-49
The Overall Layout of Workstations should Reflect the ways in which Users are Expected to Work
For example, if operators roles are specialized, involving little cooperative or coordinated action, their workstations might be separated as shown above. Workstations might also be separated if interference (e.g., from audio feedback/displays, voice input/output, or verbal communication with personnel outside the control room) were considered a potential problem. The effects of diminished direct visual contact can be compensated for by displays that echo the operators' actions.

⇒ 4.8.5.1-4 The workplace should be large enough to allow the operating crew to interact with others (auxiliary personnel, crews coming on shift) comfortably without crowding or interference.

With the elimination of physical HSIs in favor of soft controls and displays, the workstations may require considerably less space. Nevertheless, working areas must remain large enough to comfortably accommodate additional personnel when needed (e.g., during shift turnover or technical specialists during unusual conditions).

⇒ 4.8.5.1-5 When workstations are added to the workplace, they should be located so that personnel at those stations (and at other stations) remain able to see displays elsewhere in the room, and their presence doesn't interfere with operations (e.g., operator movements from one station to another).

Users of computer workstations are typically seated. In locating such workstations, the need for the user to see displays from a seated position should be considered; see Figure 4-50. For example, displays on the lower parts of wall panels (easily seen by personnel performing tasks standing at the boards) may not be visible to users doing the same tasks at the workstation. In addition it should be verified that the added workstations do not themselves block the users' view of other displays of frequently monitored information; see Figure 4-50. Workstations designed to adjust for both seated and standing use should not be placed so that a standing user blocks another user's view.

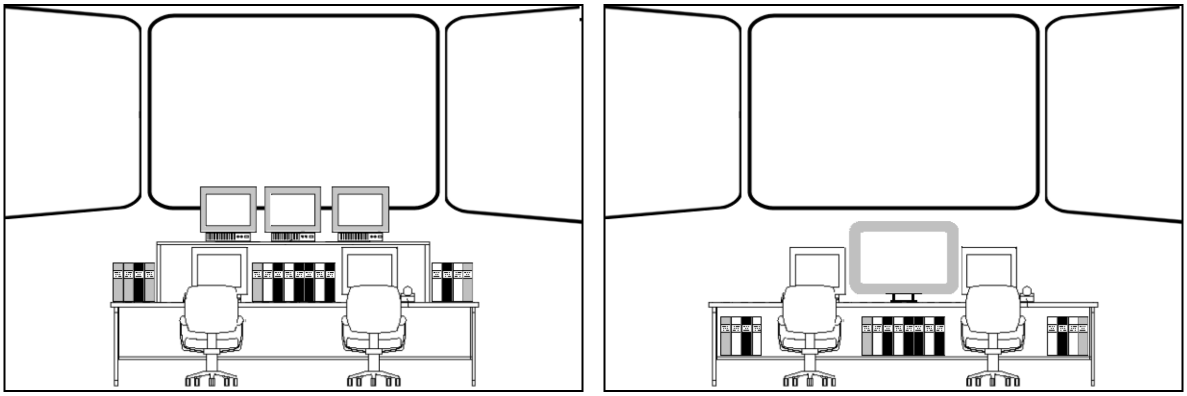


Figure 4-50
The Operators' Workstations should be Designed to Allow an Unobstructed View of Wall-Mounted Displays
In the example above, monitors on a high shelf over the workstation (left) are replaced by a larger, shared display on a wider work surface (right).

4.8.5.2 Control Room Environment

Environmental factors that can have important effects on operators' performance include thermal comfort, illumination, the auditory environment, and facility layout.

Illumination – Illumination encompasses general illumination levels (i.e., for the main operating area and auxiliary areas) and specific levels for particular areas, such as workstations, individual control and display devices, and areas used for reading and writing; emergency lighting systems intended for special operating conditions are also included. VDUs, traditional control/display HSIs, and paper documentation usually require different lighting environments within the same control room area. The light level needed to read P&IDs comfortably may be twice that recommended for instrument panels. The level recommended for panels corresponds roughly to the upper bound of that recommended for emissive computer displays (such as CRTs); reflective displays (e.g., LCDs) require more light. Furthermore, with respect to computer-driven displays, glare may be a greater concern than the level of illumination per se – so that it is necessary to consider the arrangement of lighting sources and surfaces as well as their intensities or luminances.

Sound – The auditory environment includes the background noise level and the reverberation and sound absorption characteristics of the workplace. Changes in the control room associated with digital upgrades may affect the auditory characteristics of the workplace. For example, computer equipment may incorporate cooling fans, the sound of which may change the level or masking (frequency) characteristics of ambient control room noise. In addition, computerized HSIs often incorporate sounds that provide feedback for user actions. These sounds may also add to the noise level, but more importantly they may interfere with other signals in the control room. The guidance below deals with specific sound-related aspects of control room upgrades.

Temperature – Thermal comfort includes temperature, humidity, and ventilation. Because computer equipment typically produces heat, larger scale modifications to include such technology may affect the HVAC requirements for the control room.

Available guidance on control room environment is identified in Table 4-24. The sources given in the table include specific design criteria for illumination, sound, and temperature.

Table 4-24
Available Guidance for Control Room Environment

Topic	Source
Illumination	NUREG-0700, Sections 12.1.2.3 and 12.1.2.4 ISO 11064, Section x BSR/HFES100
Sound	NUREG-0700, Section 12.1.2.5
Temperature	NUREG-0700, Sections 12.1.2.1 and 12.1.2.2

In addition to the guidance provided in these sources, the following additional guidance should be considered.

4.8.5.2.1 Illumination

⇒ 4.8.5.2.1-1 Illumination should be suitable for the tasks performed at all work locations.

⇒ 4.8.5.2.1-2 To meet varying lighting requirements, adjustable task lighting should be considered.

Additional lighting should be provided at workstations where demanding visual tasks may be performed. Wherever possible, light level as well as positioning should be adjustable. Local lighting controls should be placed within reach of the user at the workstation. The overall lighting should be designed to minimize the following

- lights oriented toward other workstations, potentially resulting in glare
- lights oriented toward illuminated indicators, potentially reducing their contrast
- thermal hazards (e.g., hot surfaces on task lighting)

⇒ 4.8.5.2.1-3 Workstation VDUs should be positioned to minimize variations in brightness in the user's field of view.

Luminance balance should be considered in placing, e.g., VDU-based workstations relative to more brightly lit, light-colored control boards. Bright surfaces behind the display device may result in distraction or fatigue. BSR/HFES100 provides guidance on computer workstations; it recommends the luminance of surfaces within a 5 degrees field of view

- not exceed 10 times the average screen luminance for positive-polarity displays (bright characters on a dark background)
- not exceed 3 times average screen luminance for negative-polarity displays (dark characters on a bright background)

⇒ 4.8.5.2.1-4 Workstation VDUs should be positioned to minimize glare on the display surfaces.

Bright surfaces behind operators may be reflected on VDUs causing glare and lowered contrast. Location of overhead lighting fixtures should also be considered. If they are directly above (or above and slightly behind) the operator's viewing position, and the display screen is tilted up (as is typical), the lights may be reflected in the screen; overhead lights located to the left or right will pose less of a problem. These considerations may be less important for an adjustable workstation, since the user will be able to rotate or tilt the display to reduce reflections.

⇒ 4.8.5.2.1-5 VDUs, workstation surfaces, and lighting fixtures should be designed to minimize reflections and glare.

VDUs can be equipped with shields to reduce reflections, or the display faces themselves treated to diffuse reflections. Matte finishes should be used on workstation surfaces, and care should be taken to avoid reflections that might impair the readability of screens, panels, and displays. In addition to positioning lighting and workstations to minimize reflections (see above), designers might consider lighting fixture treatments (e.g., egg-crate diffusers) that reduce bright spots that may be reflected in display faces.

4.8.5.2.2 Sound

⇒ 4.8.5.2.2-1 Equipment or cabinets that make noise (e.g., those containing ventilating fans) should be located away from operators whenever possible.

Some interfaces may require local ventilation, but it may be possible to reduce noise in areas occupied by operators by having other equipment (e.g., mass storage devices or switch cabinets) moved further away, located behind sound attenuating barriers, or removed from the control room entirely (i.e., located in adjacent rooms).

⇒ 4.8.5.2.2-2 Sounds produced by computerized interfaces introduced into the control room should not interfere with existing control room audio codes, especially those that signal important information.

Sounds with similar temporal or frequency characteristics can be confused with one another or, when sounded together, can mask one another (i.e., one sound can make another less audible). For example, a signal consisting of a brief tone sounded once per second may be confused with an existing periodic tone differing only in rate or pitch; in this case using different temporal patterns would make the signals more distinctive.

⇒ 4.8.5.2.2-3 Audio signals associated with different computer-driven HSIs in the control room should not interfere with each other.

An upgrade effort may result in multiple computer-driven interfaces being introducing into the control room, each one of which might employ a number of different sounds to provide feedback to the user. Unless all of the interfaces (and their audio signals) were specifically designed to be used together, the sounds may well interfere with one another, or have conflicting meaning from one device to another.

⇒ 4.8.5.2.2-4 If operators use similar interfaces in proximity to one another (e.g., operators at a bench consisting of a row of displays and pointing devices), measures should be taken to prevent an operator at one workstation from mistakenly attending to auditory feedback from neighboring workstations.

At a minimum, it would seem imperative for there to be separate sound sources for each workstation, and sound levels would have to be kept to the minimum effective level at each station. (Note that this recommendation applies to interface feedback, not to process-related signals, i.e., alarm sounds).

⇒ 4.8.5.2.2-5 Sound levels at the workstation should be such that the workstation operators may still hear any workplace alarms or announcements and so that general conversation and communication between operators or between any personnel in the workroom is convenient.

⇒ 4.8.5.2.2-6 After modifications are implemented, the workplace should still conform to human factors guidance on the effectiveness of auditory signals (alarms in particular) and the intelligibility of speech.

If the sound environment has changed substantially, it may be necessary to take steps to reduce noise.

4.8.5.2.3 Temperature

⇒ 4.8.5.2.3-1 Verify either by analyses or testing or both that the control room HVAC system can keep the area within the established comfort limits.

Even if temperatures in the control room as a whole are not noticeably affected, it should be verified that workstation equipment doesn’t locally raise temperatures where crewmembers are positioned.

⇒ 4.8.5.2.3-2 Ensure that the airflow produced by the equipment itself or that is required to keep it within temperature limits does not result in areas in the control room where air velocity is too high.

Air conditioning vents and cooling fans in equipment should not produce noticeable drafts in areas occupied by operators.

4.8.5.3 Local Control Stations

A local control station is a place outside of the main control room where operators interact with the plant. Local control stations may include multifunction workstations and panels, as well as operator interfaces, such as controls (e.g., valves, switches, and breakers) and displays (e.g., meters and VDUs). They have many characteristics in common with the main control room. However, they may also have unique characteristics when located in environments that are not as controlled as the main control room. For example, local control stations may have higher levels of background noise and more demanding conditions for use than the main control room. Accordingly, they may have a diverse range of communication media, such as loudspeakers, public address/pager stations, and two-way communication systems (e.g., telephones and walkie-talkies). In addition, these media may have special administrative controls that regulate their use.

Available guidance on local control stations is identified in Table 4-25.[7]

Table 4-25
Available Guidance for Local Control Stations

Topic	Source
Local control stations	NUREG-0700, Sections 12.2 ISO 11064, Section x

4.8.6 Managing the Impact of Modifications

This section includes guidance that minimizes the impact of implementing modifications on operators’ performance. This is especially important since operators will typically be present in the workplace during the modification, and still will be required to carry out their tasks. An installation plan should address such concerns as the effects of staged equipment and additional personnel on the operators’ ability to move around, the possible need for temporary instrumentation, and the provision of a safe work environment.

[7] Additional guidance on local stations is being developed in another project.

⇒ 4.8.6-1 For each stage of the migration, possible changes to the workplaces and workstations should be considered that are ancillary to the planned modifications of the interface per se.

As described in Section 2.3, Migration, intermediate control room configurations must adequately support performance. For example, during migration, both old and new HSI components are present in the workplace. The new HSI components (as well as temporary computers, telephones, radios, and drawings) might be placed on desks or provisional areas, possibly reducing laydown space for procedures and prints. At the same time, personnel may continue operation from the benchboard, and the designer should ensure that the interim arrangements accommodate this (e.g., by considering traffic patterns and lines of sight at each stage).

It is important to systematically analyze the functioning and physical configuration of interfaces and workstations at each step in the process to ensure that interim configurations are feasible and workable. If performance cannot be adequately supported throughout the process, then the migration strategy may have to be altered. This is an inherent tradeoff that will be part of the design process. Some of the major discrepancies may become obvious during the initial conceptual designs for the migration steps. Others may not emerge until further into the process.

⇒ 4.8.6-2 Activities associated with the implementation of modifications should not result in obstruction of users' view of or physical access to controls and displays.

Planning should ensure that operators remain able to carry out their tasks even if workstations, displays, or panels are moved from their original (or eventual planned) positions. Care should be taken not to allow staged supplies or non-functional equipment to block user interfaces; see Figure 4-51.

⇒ 4.8.6-3 Implementation activities should be planned so that the ability of operating personnel to access needed HSIs and support material in the control room is not restricted.

Interim configurations may require operators to move around more than they did previously to carry out their tasks. The paths they will take should be anticipated and measures taken to keep them clear.

⇒ 4.8.6-4 Errors or misinterpretations as a result of a phased introduction of digital upgrades should be minimized.

As described in Section 2.3, Migration, the migration strategy may call for changing the I&C equipment 'behind the boards' while leaving the HSI largely the same for a time. On the other hand, the plant may choose to change to computer driven displays before the associated I&C systems have been converted to digital. While such circumstances may typically not cause problems, designers should be alert to the possibility that incorrect assumptions about the displayed data (e.g., its reliability, timeliness, or precision) might have important consequences.

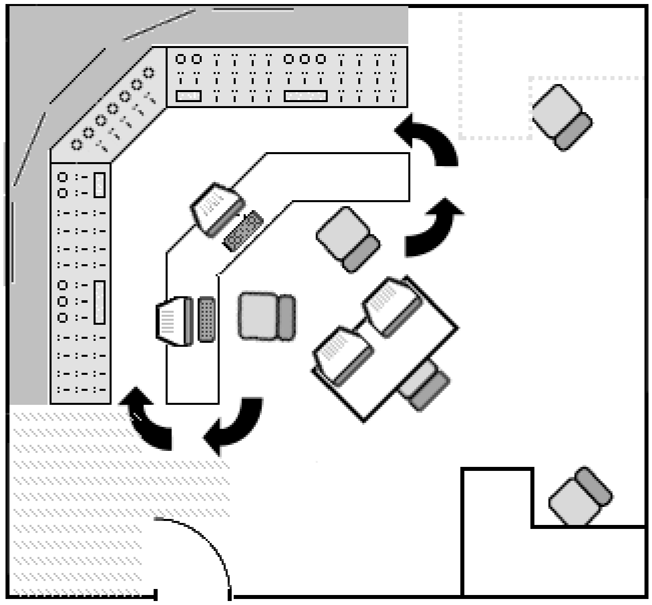


Figure 4-51
Operators may be Positioned at Computer Equipment Placed Atop Former Laydown Space Opposite the Control Boards
Operators should be able to move freely from the computer workstation to the boards. In the example above, material being readied for installation (shading at lower left) should be kept out of the expected traffic pattern. It may be necessary to relocate other equipment or furnishings (e.g., the auxiliary workstation at the upper right) to accommodate changes in the traffic patterns.

Similarly, potential effects of having both old controls and new controls available to users should be evaluated. Standardization and consistency should still exist and remain between old and new equipment and across the new systems that are implemented.

⇒ 4.8.6-5 Measures should be taken to minimize the distraction or interference associated with the activities of personnel involved in implementing modifications.

Provisions should be made for workers carrying out modifications to move around as needed without interfering with the operators. This is important both to minimize distraction and to prevent controls from being inadvertently actuated. Similarly, it is necessary to minimize the amount of noise associated with activity in the control room. It may be necessary to temporarily locate principal workstations away from areas where extensive work is being done. In hybrid control rooms it may be necessary to perform upgrade work affecting critical workstations during a shutdown.

⇒ 4.8.6-6 Provisions should be made so that workplace hazards are not created during any work in the control room.

A well-designed workplace decreases the factors that contribute to accidents or injuries, and minimize stress. For example, trip hazards should be prevented and it should be possible to connect electric cords such that they are kept clear of walkways and critical access areas. In addition, poor organization and housekeeping; for example, supplies piled near workstations or panels, or in doorways, or equipment left on the floor can cause accidents and impede performance.

4.8.7 Sources of Additional Information

O’Hara, J., Brown, W., Lewis, P., and Persensky, J.J. (2002). Human-system interface design review guidelines [NUREG-0700, Rev.2]. Washington, DC: U.S. Nuclear Regulatory Commission.

Human Factors and Ergonomics Society (2002). Human factors engineering of computer workstations [BSR/HFES 100]. Santa Monica, CA: Human Factors and Ergonomics Society.

International Standards Organization (2000). Ergonomic design of control centres – Part 1: Principles for the design of control centres [ISO 11064-1]. Geneva, Switzerland: International Standards Organization.

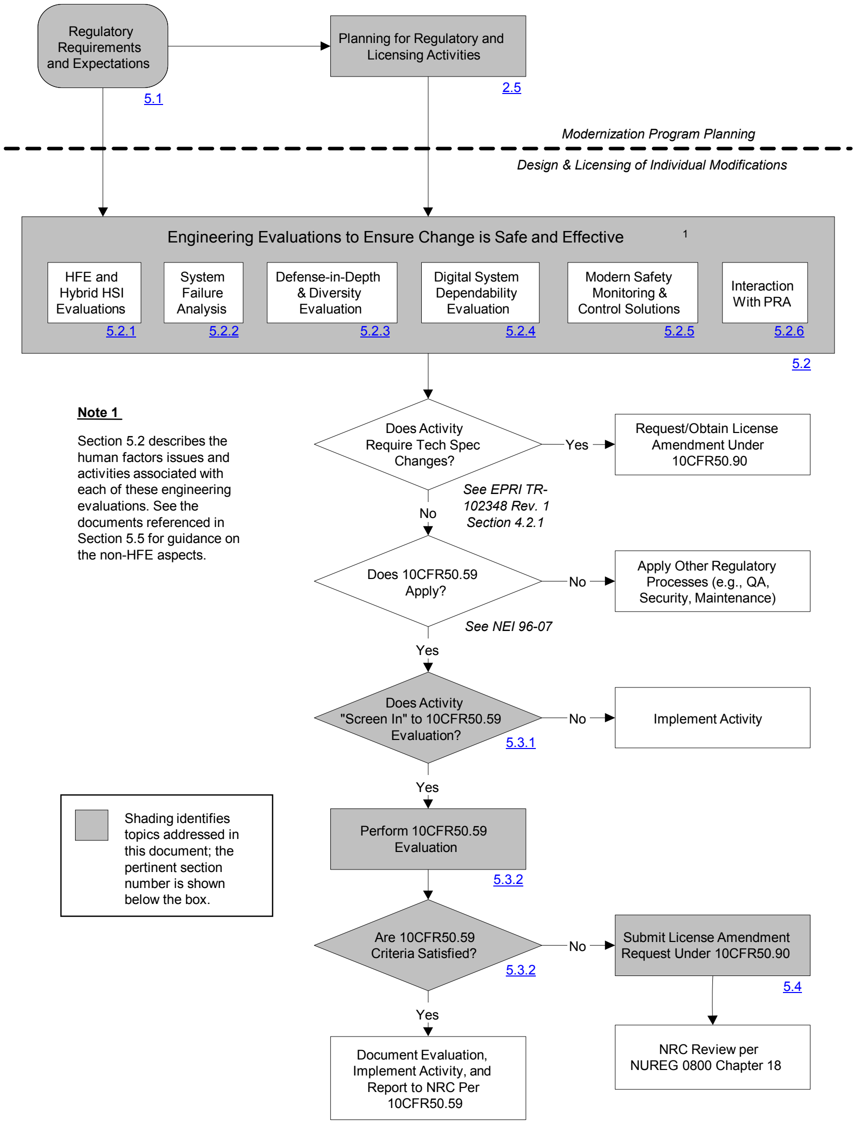
5
REGULATORY AND LICENSING ACTIVITIES

This section provides guidance on regulatory and licensing activities related to control room modifications and other human factors engineering (HFE) aspects of digital instrumentation and control (I&C) upgrades. The section includes guidance on:

- Determining when a change to the control room or other human-system interface (HSI) requires prior Nuclear Regulatory Commission (NRC) review and approval per 10 CFR 50.59
- Demonstrating regulatory compliance regarding appropriate use of human factors engineering when making changes
- Addressing hybrid HSI issues in licensing
- The role of human factors and human performance considerations in failure analysis and dependability evaluations for digital systems, which are key elements in licensing of digital I&C upgrades
- Human factors aspects of the defense-in-depth and diversity (D3) evaluation and its potential impact on the HSI
- Demonstrating compliance with regulatory requirements and guidelines for specific HSI design features, such as post-TMI requirements and requirements on what portions of the HSI should be qualified, while employing more modern solutions for these HSI features (Section 6.4 provides more detailed guidance in this area)
- Interaction with the plant's probabilistic risk assessment (PRA) including use of risk insights when evaluating changes
- Addressing HFE and human performance considerations in licensing submittals and other interactions with the NRC.

Regulatory and licensing activities should be addressed first in the planning stage of a modernization program, as discussed in Section 2.5. It is recommended that users of this document read through the Frequently Asked Questions in Section 2.5 before reading this section, as they provide an overview of the licensing topics that are addressed in more detail here.

Figure 5-1 shows an overview of the licensing process. There is no special or separate licensing process that applies to control room modifications or other changes that impact human performance – they are like any other modification in that they are governed by the 10 CFR 50.59 regulation. The 50.59 regulation allows licensees to determine whether a change requires a license amendment and thus needs prior NRC review and approval, or the change can be implemented within the current licensing basis (no license amendment and no prior review required). It provides a set of criteria to be used for making this determination for each change evaluated under 10 CFR 50.59.


Regulatory Requirements and Expectations
5.1
Planning for Regulatory and Licensing Activities
2.5
Modernization Program Planning
Design & Licensing of Individual Modifications
Engineering Evaluations to Ensure Change is Safe and Effective 1
HFE and Hybrid HSI Evaluations
5.2.1
System Failure Analysis
5.2.2
Defense-in-Depth & Diversity Evaluation
5.2.3
Digital System Dependability Evaluation
5.2.4
Modern Safety Monitoring & Control Solutions
5.2.5
Interaction With PRA
5.2.6
5.2
Does Activity Require Tech Spec Changes?
Yes
Request/Obtain License Amendment Under 10CFR50.90
See EPRI TR-102348 Rev. 1 Section 4.2.1
No
Does 10CFR50.59 Apply?
No
Apply Other Regulatory Processes (e.g., QA, Security, Maintenance)
See NEI 96-07
Yes
Does Activity "Screen In" to 10CFR50.59 Evaluation?
5.3.1
No
Implement Activity
Yes
Perform 10CFR50.59 Evaluation
5.3.2
Are 10CFR50.59 Criteria Satisfied?
5.3.2
No
Submit License Amendment Request Under 10CFR50.90
5.4
NRC Review per NUREG 0800 Chapter 18
Yes
Document Evaluation, Implement Activity, and Report to NRC Per 10CFR50.59

Note 1

Section 5.2 describes the human factors issues and activities associated with each of these engineering evaluations. See the documents referenced in Section 5.5 for guidance on the non-HFE aspects.

▨ Shading identifies topics addressed in this document; the pertinent section number is shown below the box.

Figure 5-1
Overview of the Licensing Process

It is important to note that the 10 CFR 50.59 evaluation is performed for the overall modification, including all aspects such as mechanical, electrical, I&C, and HFE. The HFE aspects of the modification are addressed at appropriate points in design and in the 10 CFR 50.59 evaluation.

For licensing of digital I&C upgrades, the primary industry guidance document is EPRI TR 102348 Rev. 1, also designated as NEI 01-01 (this document is referred to hereafter as TR 102348). It was endorsed by the NRC in Regulatory Issue Summary 2002-22. The guidance given in this section is consistent with and supplements the guidance given in TR 102348.

Figure 5-1 shows the basic steps involved in the licensing process for a digital I&C upgrade, adapted from a similar illustration in TR-102348. The figure also indicates where each topic is addressed either in this document or in the other reference documents. Note that although the figure shows the various activities as being performed in a particular sequence, in an actual project many of these are accomplished in parallel with significant interaction among the various activities.

The basic steps in the licensing process include:

- Planning for regulatory and licensing activities, which should be done as part of planning the overall modernization program – this is discussed in Section 2.5.
- Understanding the applicable regulatory requirements and NRC expectations – Section 5.1 addresses this and provides a roadmap to the various regulatory requirements and guidance documents that apply to HSI changes.
- Engineering evaluations performed as part of the design effort – as discussed in TR 102348, the information needed to support licensing activities, including the 10 CFR 50.59 evaluation, comes from the engineering evaluations performed as part of design. Section 5.2 describes the HFE aspects of engineering evaluations performed for digital I&C upgrades that support licensing.
- Determining whether the modification requires any changes to the Technical Specifications – this is discussed in TR-102348. Note that even if a modification does not require a change to the Tech Specs, it may be desirable to change the Tech Specs in order to take full advantage of the digital I&C technology being installed – for example, to reduce surveillance testing burden by extending surveillance intervals.
- Screening the change to determine whether 10 CFR 50.59 applies – if it does not apply, then no 10 CFR 50.59 evaluation is required. This is addressed in Section 5.3.1, drawing on the guidance in TR-102348.
- Performing the 10 CFR 50.59 evaluation – guidance is provided in Section 5.3.2.
- Licensing submittals and other NRC interaction – this is addressed in Section 5.4.

Sources of Additional Information

1. 10 CFR 50 Appendix A. *General Design Criteria for Nuclear Power Plants*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.
2. 10 CFR 50 Appendix E. E*mergency Planning and Preparedness for Production and Utilization Facilities*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.
3. 10 CFR 50 Appendix R. *Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.
4. 10 CFR 50.34(f). *Contents of applications; technical information; Additional TMI-related requirements*, Code of Federal Regulations Title 10, Part 50.34, U.S. Nuclear Regulatory Commission, Washington, DC.

5. 10 CFR 50.36. *Technical Specifications*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

6. 10 CFR 50.47. *Emergency plans*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

7. 10 CFR 50.54. *Conditions of licenses*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

8. 10 CFR 50.55a(h). *Protection and safety systems*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

9. 10 CFR 50.59. *Changes, Tests and Experiments*, Code of Federal Regulations Title 10, Part 50.59, U.S. Nuclear Regulatory Commission, Washington, DC: 2000.

10. 10 CFR 55. *Operators' Licenses*, Code of Federal Regulations Title 10, Part 55, U.S. Nuclear Regulatory Commission, Washington, DC.

11. 10 CFR 50.72. *Immediate notification requirements for operating nuclear power reactors*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

12. ANSI/ANS-3.5-1998. *Requirements for Simulators Used for Operator Training, Testing and Requalification*, American National Standards Institute, La Grange Park, IL: 1998.

13. EPRI TR-102348 Revision 1 – NEI 01-01. *Guideline on Licensing Digital Upgrades: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule*, EPRI, Palo Alto, CA: 2002. 1002833.

14. *Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades*, EPRI, Palo Alto, CA: 2004. 1002835.

15. IEEE 497-2002. *IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations*, Institute of Electrical and Electronics Engineers, New York, NY: September 2002.

16. IEEE 603-1991. *Criteria for Protection Systems for Nuclear Power Generating Stations*, Institute of Electrical and Electronics Engineers, New York, NY: 1991.

17. Information Notice (IN) 97-78. *Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times*, U.S. Nuclear Regulatory Commission, Washington, DC: October 1997.

18. NEI 96-07 Revision 1. *Guidelines for 10 CFR 50.59 Implementation*, Nuclear Energy Institute, Washington, DC: November 2000.

19. NEI 99-01 Revision 4. *Methodology for Development of Emergency Action Levels*, Nuclear Energy Institute, Washington, DC: January 2003.

20. NEI 00-02. *10 CFR 50.69 Option 2 Categorization*, Nuclear Energy Institute, Washington, DC: ____.

21. NUMARC 93-01. *Maintenance Rule Implementation*, Nuclear Energy Institute (formerly NUMARC), Washington, DC: ____.

22. NUREG-0654 (FEMA-REP-1) Rev. 1. *Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, Appendix 1, Emergency Action Level Guidelines for Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, Washington, DC.

23. NUREG-0700 Revision 2. *Human-System Interface Design Review Guidelines*, U.S. Nuclear Regulatory Commission, Washington, DC: 2002.

24. NUREG-0711 Revision 2. *Human Factors Engineering Program Review Model*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

25. NUREG-0737 Supplement 1. *Clarification of TMI Action Plan Requirements – Requirements for Emergency Response Capability*, U.S. Nuclear Regulatory Commission, Washington, DC: January 1983.

26. NUREG-0800. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

27. NUREG-1220 Revision 1. *Training Review Criteria and Procedures*, U.S. Nuclear Regulatory Commission, Washington, DC: 1993.

28. NUREG-1430. *Standard Technical Specifications, B&W Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

29. NUREG-1431 Revision 2. *Standard Technical Specifications, Westinghouse Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: 2001.

30. NUREG-1432. *Standard Technical Specifications, CE Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

31. NUREG-1433 and NUREG-1434. *Standard Technical Specifications, GE Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

32. NUREG-1764. *Guidance for the Review of Changes to Human Actions*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

33. NUREG/CR-6303. *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, U.S. Nuclear Regulatory Commission, Washington, DC: December 1994.

34. Regulatory Guide 1.8 Revision 3. *Qualification and Training of Personnel for Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: May 2000.

35. Regulatory Guide 1.47. *Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems*, U.S. Nuclear Regulatory Commission, Washington, DC: 1973.

36. Regulatory Guide 1.62. *Manual Initiation of Protective Actions*, U.S. Nuclear Regulatory Commission, Washington, DC: 1973.

37. Regulatory Guide 1.97 Revision 3. *Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident*, U.S. Nuclear Regulatory Commission, Washington, DC: 1983.

38. Regulatory Guide 1.101 Revision 4. *Emergency Planning and Preparedness for Nuclear Power Reactors*, U.S. Nuclear Regulatory Commission, Washington, DC: July 2003.

39. Regulatory Guide 1.114 Revision 2. *Guidance to Operators at the Controls and to Senior Operators in the Control Room of a Nuclear Power Unit*, U.S. Nuclear Regulatory Commission, Washington, DC: May 1989.

40. Regulatory Guide 1.149 Revision 3. *Nuclear Power Plant Simulation Facilities for Use in Operator Training and License Examinations*, U.S. Nuclear Regulatory Commission, Washington, DC: October 2001.

41. Regulatory Guide 1.153 Revision 1. *Criteria for Safety Systems*, U.S. Nuclear Regulatory Commission, Washington, DC: June 1996.

42. Regulatory Guide 1.174 Revision 1. *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, U.S. Nuclear Regulatory Commission, Washington, DC: April 2002.

43. Regulatory Guide 1.187. *Guidance for Implementation of 10 CFR 50.59 Changes, Tests, Experiments*, U.S. Nuclear Regulatory Commission, Washington, DC: November 2000.

44. RIS 2002-22. NRC Regulatory Issue Summary 2002-22, *Use of EPRI/NEI Joint Task Force Report, 'Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,'* U.S. Nuclear Regulatory Commission, Washington, DC: November 2002.

45. SECY 93-087. *Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs*, U.S. Nuclear Regulatory Commission, Washington, DC: July 1993.

5.1 Regulatory Requirements and Expectations

5.1.1 Roadmap to the Relevant Documents

5.1.2 NRC HFE Reviews

5.1.2.1 Standard Review Plan – NUREG-0800

5.1.2.2 HFE Program Review – NUREG-0711

5.1.2.3 HFE Review Guidelines – NUREG-0700

The purpose of this section is to provide an overview and roadmap to regulatory requirements, expectations, and guidance that may be applicable when making digital I&C changes that affect the control room or otherwise impact human functions and tasks. These are contained in many documents, including federal regulations, regulatory guides, regulatory review guidance, standards, and industry guidance documents. It is important to distinguish the three types of information provided in these documents (the roadmap addresses all three of these):

- *Regulatory requirements* – These are mandated by law, and thus must be complied with. As discussed above, the primary regulation that governs changes to a nuclear facility is 10 CFR 50.59. However, the 50.59 regulation only addresses determining when a change requires NRC review before it is implemented, not how the change should be designed or what design features are required. There are additional regulatory requirements that must be complied with when making changes to the control room or other HSIs – for example, requirements on application of human factors engineering in the design, requirements on specific HSI design features such as post-accident monitoring capabilities, requirements for qualified HSIs, operator licensing requirements, and others. Most of these are contained in the Code of Federal Regulations. In some instances, the regulations invoke the requirements of a standard (e.g., some IEEE standards are invoked) and thus those requirements become mandatory as well.

- *NRC expectations* – The regulations typically are written at a relatively high level. However, the NRC has issued a number of NUREG reports and Regulatory Guides that describe in more detail what the NRC Staff considers as acceptable methods for meeting the regulations. The provisions outlined in these documents do not represent hard requirements unless the licensee commits to them formally. However, they do characterize the NRC Staff's expectations, so it is important to be aware of them. Also, any deviations from the approaches described in these documents are likely to receive extra scrutiny during an NRC review.
- *Guidance* – In many cases there are also industry guidelines available which, when followed, can help the licensee ensure that regulatory requirements and NRC expectations are met for a given topic area. One example is the digital I&C licensing guideline, EPRI TR-102348, which was mentioned earlier. The guidelines contained in the various sections of this report also fall into this category.

This section provides a roadmap through the various documents containing this information, focusing only on HFE or HSI-related aspects. It also provides a graphical overview of the key documents for several topic areas. These are discussed in Section 5.1.1. Finally, Section 5.1.2 provides a brief description of the NRC's regulatory review guidance on human factors engineering. This is a key part of NRC's expectations for any changes to the control room or other changes affecting human functions and tasks.

5.1.1 Roadmap to the Relevant Documents

The Appendix to this section provides a roadmap to the documents relevant to HFE or HSI regulatory requirements, expectations, and guidance. The documents are grouped according to the topics listed below. Within a topic, the documents are organized by regulatory requirements, expectations, and guidance:

1. Determining when an HSI change needs prior NRC review and approval per 10 CFR 50.59 – Figure 5-2 below provides an overview of the key documents in this area
2. Human factors engineering – Figure 5-3 provides an overview of these documents
3. HSI design – Figure 5-4 provides an overview of these documents
4. Operator licensing
5. Failure analysis and dependability evaluations for digital I&C systems
6. Defense-in-depth and diversity (D3) evaluations
7. Remote shutdown
8. Emergency plans and notifications

9. Changes to risk-important human actions – Figure 5-3 provides an overview of these documents
10. Risk-informed licensing submittals
11. Technical specifications and LCOs

Graphical overviews for the first three topical areas are provided in Figures 5-2 through 5-4.

The references to regulatory documents given here were based on the current revisions at the time of this writing. Users of this guidance should consult the latest versions of the regulatory documents, which may have been updated since this was published.

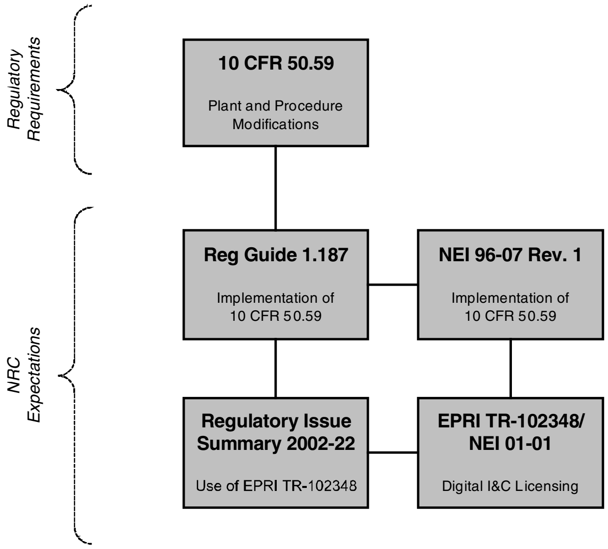

Regulatory Requirements
NRC Expectations
10 CFR 50.59
Plant and Procedure Modifications
Reg Guide 1.187
Implementation of 10 CFR 50.59
NEI 96-07 Rev. 1
Implementation of 10 CFR 50.59
Regulatory Issue Summary 2002-22
Use of EPRI TR-102348
EPRI TR-102348/ NEI 01-01
Digital I&C Licensing

Figure 5-2
Regulatory Requirements and Expectations Related to Determining when a Digital I&C Change Requires Prior NRC Approval

5.1.2 NRC HFE Reviews

NRC review of changes to the control room or other HSIs will be focused primarily on the HFE program or process used in developing and implementing the modification. The HFE review addresses the design process, the final design, implementation, and ongoing performance monitoring.

Guidance used by the NRC reviewers in conducting the HFE review is contained in three main documents (see Figure 5-3). The first document is Chapter 18, Human Factors Engineering, of the Standard Review Plan (NUREG-0800). It provides a high-level review framework for the conduct of HFE reviews. NUREG-0800 refers to a second document, the Human Factors Engineering Program Review Model (NUREG-0711), for detailed review criteria. The third document, referenced in both of the other two is the Human-System Interface Design Review Guidelines (NUREG-0700). It contains detailed guidelines used as part of the NUREG-0711 review process. A brief description of each document is given in the three sub-sections below.

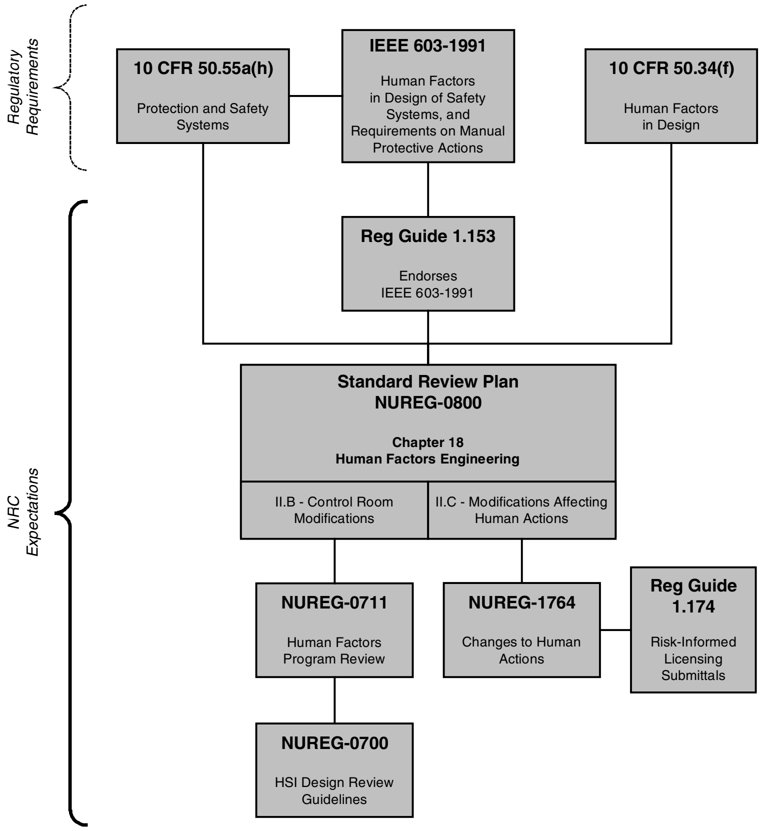

Regulatory Requirements
10 CFR 50.55a(h)
Protection and Safety Systems
IEEE 603-1991
Human Factors in Design of Safety Systems, and Requirements on Manual Protective Actions
10 CFR 50.34(f)
Human Factors in Design
Reg Guide 1.153
Endorses IEEE 603-1991
NRC Expectations
Standard Review Plan NUREG-0800
Chapter 18 Human Factors Engineering
II.B - Control Room Modifications
II.C - Modifications Affecting Human Actions
NUREG-0711
Human Factors Program Review
NUREG-1764
Changes to Human Actions
Reg Guide 1.174
Risk-Informed Licensing Submittals
NUREG-0700
HSI Design Review Guidelines

Figure 5-3
Regulatory Requirements and Expectations Related to Human Factors Engineering and Changes Affecting Human Actions

It should be noted that while NUREGs- 0800, 0711, and 0700 are the principal sources of design review guidance, where necessary the NRC will use additional NUREGs and NUREG/CRs in support of the review process.

Also, it is important to note that the NRC uses a graded approach in their HFE reviews. This is discussed in Chapter 18 of NUREG-0800. As stated in Section I.B of Chapter 18, “The level of staff review of an applicant’s HFE design should reflect the unique circumstances of the review.” It also states that “risk importance is taken into account when deciding which particular items to review and the depth of review necessary.” The areas of review that are given attention for a particular submittal, per Chapter 18, are based on:

- An evaluation of the information provided by the applicant.
- The similarity of the associated HFE issues to those recently reviewed for other plants.
- The determination of whether items of special or unique safety significance are involved.
- Because the criteria for grading the review and the regulatory requirements and criteria for HSI design and for human factors engineering are relatively high level and not very prescriptive, the review necessarily involves a fair amount of subjectivity. This is one of the reasons that early interaction with the NRC, at the beginning of a modernization program before significant design work is started, can be very beneficial. This is discussed further in Section 2.5 and Section 5.4.

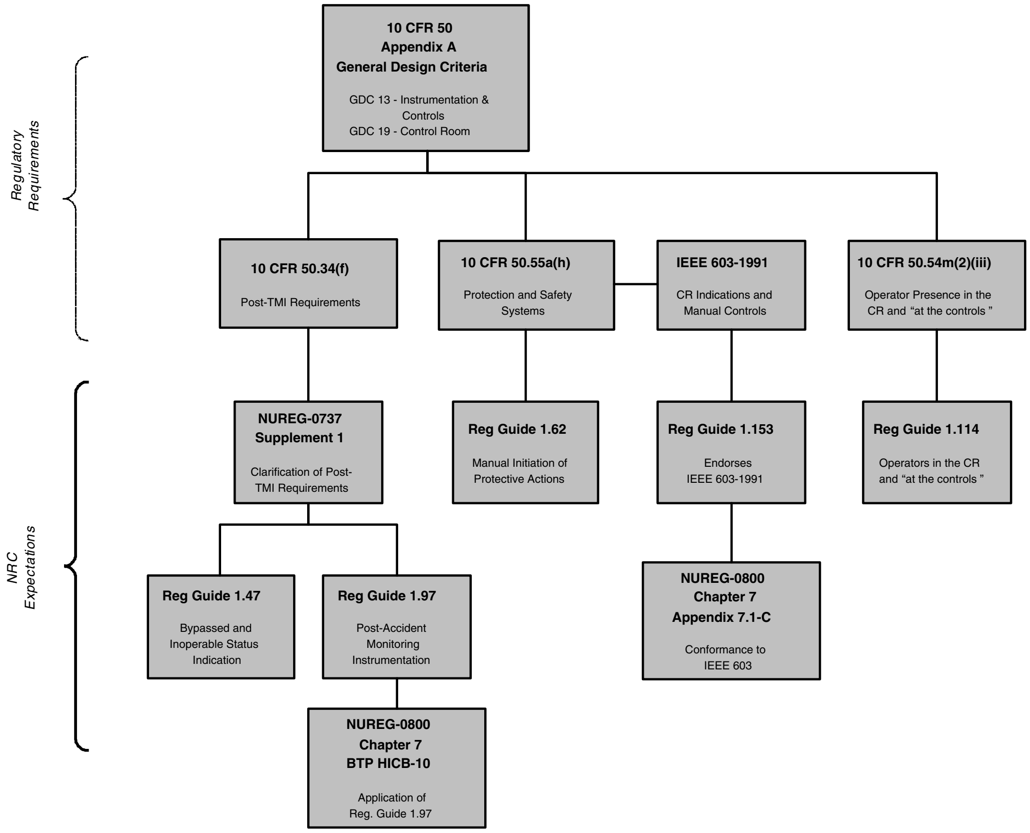

Regulatory Requirements
NRC Expectations
10 CFR 50 Appendix A General Design Criteria
GDC 13 - Instrumentation & Controls
GDC 19 - Control Room
10 CFR 50.34(f)
Post-TMI Requirements
10 CFR 50.55a(h)
Protection and Safety Systems
IEEE 603-1991
CR Indications and Manual Controls
10 CFR 50.54m(2)(iii)
Operator Presence in the CR and "at the controls"
NUREG-0737 Supplement 1
Clarification of Post-TMI Requirements
Reg Guide 1.62
Manual Initiation of Protective Actions
Reg Guide 1.153
Endorses IEEE 603-1991
Reg Guide 1.114
Operators in the CR and "at the controls"
Reg Guide 1.47
Bypassed and Inoperable Status Indication
Reg Guide 1.97
Post-Accident Monitoring Instrumentation
NUREG-0800 Chapter 7 Appendix 7.1-C
Conformance to IEEE 603
NUREG-0800 Chapter 7 BTP HICB-10
Application of Reg. Guide 1.97

Figure 5-4
Regulatory Requirements and Expectations Related to HSI Design

5.1.2.1 Standard Review Plan – NUREG-0800

Chapter 18 of NUREG-0800 is used for three main applications:

1. Review of the HFE Aspects of a New Plant – review criteria are contained in Section II.A of Chapter 18.
2. Review of the HFE Aspects of Control Room Modifications – this review addresses the new plant criteria of Section II.A, but tailors these to match the circumstances of the particular modification being reviewed according to the graded approach discussed above. Additional criteria for review of modifications are contained in Section II.B.
3. Review of the HFE Aspects of Modifications Affecting Human Actions – criteria for this review are contained in Section II.C. Note that digital I&C upgrades can affect human actions even when the HSI is not changed (e.g., through a change in automation or an I&C modification that affects the required operator response time for an action). Such changes would be reviewed according to the Section II.C criteria for changes to human actions, which apply a risk-informed approach to the review. Section 5.2.6.3 discusses this further.

5.1.2.2 HFE Program Review – NUREG-0711

The areas of review identified in NUREG-0800 correspond to the detailed review elements of NUREG-0711:

- HFE Program Management
- Operating Experience Review
- Functional Requirements Analysis and Function Allocation
- Task Analysis
- Staffing and Qualifications
- Human Reliability Analysis
- Procedure Development
- Training Program Development
- Human-System Interface Design
- Human Factors Verification and Validation
- Design Implementation
- Human Performance Monitoring

While the process defines 12 areas of review, not all may be applicable to the review of a particular modernization project. The elements that are relevant to each review are selected to reflect the unique circumstances of the project under review, using a graded approach to the review as discussed above.

NUREG-0711 identifies the types of HFE documentation that NRC expects to review. In general, for each review element that is applicable NRC would expect to see:

1. An implementation plan describing the proposed methodology for meeting the acceptance criteria of the element. Review of the implementation plan provides the opportunity to resolve methodological issues and to receive NRC input early in the process when staff concerns can more easily be addressed than when the effort is completed.
2. A summary of the results from activities related to each element. NRC may also want to review samples of the HFE work products.

This information need not necessarily be provided in two separate reports – it could be combined into one. Also, as discussed above, not all elements will apply to a given submittal, and the level of NRC review will be based on the circumstances of the particular project being reviewed. Finally, the documentation that is produced should be consistent with the plant's own graded approach for applying HFE to plant modifications. Obtaining early review and approval of the plant's HFE program and graded approach can help ensure that the level of documentation produced for each change will be consistent with NRC expectations.

An overview of the objectives for each review element in NUREG-0711 follows.

5.1.2.2.1 HFE Program Management

The overall purpose of the HFE program review is to verify that

- HFE is integrated into the modification's development, design, and evaluation
- HSIs, procedures, and training support the performance of operation, maintenance, test, inspection, and surveillance tasks in a safe, efficient, and reliable manner
- The HFE program and its products reflect "state-of-the-art human factors principles" and satisfy all specific regulatory requirements (for example, the specific HSI design requirements shown in the overview of Figure 5-4).

As part of its review, the NRC considers the HFE expertise of the design team and its processes and procedures. The plan defining the overall scope and technical aspects of the HFE activities is also reviewed.

5.1.2.2.2 Operating Experience Review

The issues and lessons learned from operating experience provide a basis for improving the plant design in a timely way, i.e., at the beginning of the design process. This applies both to new plant designs and to plant modifications where it may be the design of a system that is being changed. The NRC review objective is to verify that HFE-related problems and issues have been identified and analyzed. In this way, negative features associated with predecessor designs may be avoided in the current one while retaining positive features.

5.1.2.2.3 Functional Requirements Analysis and Function Allocation

Plant modernization projects provide opportunities to change the level of automation in the plant and the NRC reviews address the associated implications for human performance. Functional requirements analysis is the identification of those functions that must be performed to satisfy the plant's safety objectives, i.e., to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. This analysis determines the objectives, performance requirements, and constraints of the design, and sets a framework for understanding the role of controllers (whether personnel or system) in controlling plant processes. In the context of plant modifications, the focus is on changes to these functions or their performance characteristics that may involve personnel monitoring and control. Function allocation is the analysis of the requirements for plant control and the assignment of control functions to (1) personnel (e.g., manual control), (2) system elements (e.g., automatic control and passive, self-controlling phenomena), and (3) combinations of the two (e.g., shared control and automatic systems with manual backup).

5.1.2.2.4 Task Analysis

The objective of a task analysis review is to verify that the requirements for task performance have been analyzed. The task analysis should (1) provide one of the bases for making decisions on design, (2) assure that human-performance requirements do not exceed human capabilities, (3) be used as basic input for developing procedures, (4) be used as basic information for developing the staffing, training, and communication requirements of the plant, and (5) form the basis for specifying the requirements for the displays, data processing, and controls needed to carry out tasks.

5.1.2.2.5 Staffing and Qualifications

The objective of the staffing review is to verify that the number and qualifications of personnel have been systematically analyzed based on task and regulatory requirements.

5.1.2.2.6 Human Reliability Analysis

The objective of this review element is to verify that (1) human-error mechanisms are addressed in the design to minimize the likelihood of personnel error, and provide the opportunity for errors to be detected and recovered from; and (2) the HRA activity effectively integrates the HFE program with the PRA and risk analysis.

5.1.2.2.7 Human-System Interface Design

The objective of this review element is to evaluate the process by which HSI design requirements are developed and HSI designs are identified and refined. The review verifies that functional and task requirements are appropriately translated to the detailed design of alarms, displays, controls, and other aspects of the HSI.

5.1.2.2.8 Procedure Development

The objective of the review is to verify that HFE principles and guidance have been applied, along with all other design requirements, to develop procedures that are technically accurate, comprehensive, explicit, easy to use, and validated.

5.1.2.2.9 Training Program Development

The NRC review verifies that a systems approach to training is used that is based on the systematic analysis of job and task requirements. The objective of the training review is to verify that such an approach is used and that the program:

- Evaluates the knowledge and skill requirements of personnel
- Coordinates the development of the training program with the other elements of the HFE design process
- Implements the training effectively in a manner consistent with human factors principles and practices.

5.1.2.2.10 Human Factors Verification and Validation

The objective of verification and validation (V&V) is to confirm that the final design conforms to HFE design principles, and personnel can successfully and safely perform their tasks to achieve operational goals. The NRC review of this element evaluates three aspects of the V&V activities to assure that this objective is met:

- HSI Task Support Verification, which should verify that the HSI supports personnel task requirements as defined by task analyses.
- HFE Design Verification, which should verify that the HSI is designed to accommodate human capabilities and limitations as reflected in HFE guidelines such as those provided in NUREG-0700.
- Integrated System Validation, which should use performance-based tests to determine whether the integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and acceptably supports safe operation of the plant.

Another aspect of V&V activities is the identification and resolution of human engineering discrepancies (HEDs). NRC review of HED resolution evaluates how the importance of HEDs has been assessed and important HEDs are corrected.

5.1.2.2.11 Design Implementation

This element addresses HFE aspects of the implementation of plant modifications. The objective of the review is to verify that the implementation of the modifications in the plant takes into account the effects on personnel performance and provides the necessary support for safe operations as the changes are made. The review also verifies that the as-built design conforms to the verified and validated design.

5.1.2.2.12 Human Performance Monitoring

The objective of this review is to provide assurance that the licensee has prepared a post-implementation monitoring strategy for ensuring that no safety degradation occurs because of any changes that are made to the HSIs and to provide assurance that the conclusions that have been drawn from the HFE evaluation remain valid over time. NOTE: In this document we use the term “in-service monitoring” as opposed to “human performance monitoring” as used in NUREG-0711 – see Section 3.9 for further discussion.

5.1.2.3 HFE Review Guidelines – NUREG-0700

NUREG-0700 provides detailed guidelines for the review of the physical and functional characteristics of plant HSIs, such as alarms, displays, and controls. In NUREG-0711, these guidelines are used for two applications. The first is part of the Human-System Interface Design element where a design-specific HFE guidelines document or style guide can be reviewed. The second application is for conduct of HFE Design Verification as part of the V&V element review.

While previous versions of NUREG-0700 contained design review procedures, these have all been moved to NUREG-0711. Thus, NUREG-0700 only contains HFE guidelines.

5.2 Engineering Evaluations Related to Licensing

5.2.1 HFE Evaluations and Hybrid HSI Issues

5.2.1.1 Overall HFE Evaluations

5.2.1.2 Evaluation of Hybrid HSI Issues

5.2.2 System Failure Analysis

5.2.3 Defense-in-Depth and Diversity (D3) Evaluation

5.2.3.3 What is a D3 Evaluation?

5.2.3.4 Impact on the Plant Design Basis

5.2.3.5 Determining When a D3 Evaluation is Needed

5.2.3.6 Use of Risk-Informed versus Deterministic Methods

5.2.3.7 Impact of D3 on HSI and Associated HFE Activities

5.2.4 Digital System Dependability Evaluations

5.2.5 Modern Safety Monitoring and Control Solutions

5.2.6 Interaction with PRA

5.2.6.1 Impact of I&C and HSI Changes on the PRA/HRA

5.2.6.2 Use of PRA/HRA to Support HSI Design and Evaluation

5.2.6.3 Use of PRA/HRA to Support Licensing

As discussed in the digital I&C licensing guideline, TR-102348, the issues that may arise in regulatory and licensing activities are most appropriately addressed first in design, and then in licensing. Most of the information that will be needed for licensing submittals or to support an NRC inspection comes from the engineering evaluations performed as part of the design effort. This is illustrated in the licensing process overview of Figure 5-1. Engineering evaluations that may have HFE related elements include, but may not be limited to, the following (the subsection that addresses each of these is indicated in parentheses):

- HFE evaluations including evaluation of hybrid HSI issues (5.2.1)
- System failure analysis (5.2.2)
- Defense-in-depth and diversity evaluation (5.2.3)
- Digital system dependability evaluation (5.2.4)
- Evaluation of modern solutions for safety monitoring and control (5.2.5)
- Evaluation of risk and other interactions with the PRA (5.2.6).

This section discusses the human performance and HFE aspects of these evaluations. TR 102348 gives more general guidance and addresses I&C aspects of these evaluations. The information given here is intended to supplement the guidance contained in TR 102348.

5.2.1 HFE Evaluations and Hybrid HSI Issues

5.2.1.1 Overall HFE Evaluations

Application of human factors engineering principles and use of an appropriate HFE design process are fundamental to ensuring that changes to the control room and other HSIs are safe and effective. As discussed in Section 5.1.2, NRC review of such changes will focus on the HFE process used. Section 2.4 provides guidance on establishing an HFE program that is in compliance with the NRC's expectations. It also describes how a graded approach can be used such that the scope and depth of HFE activities are tailored as appropriate based on a number of criteria, including potential impact of the change on plant safety or risk. Thus the number and types of HFE evaluations that will be performed will depend on the nature of the change and its impact on plant risk, as well as other factors. Section 3.1 describes how HFE activities can be integrated into the overall modification process. Other sub-sections of Section 3 provide details on the various HFE activities, including how they can be tailored as appropriate based on the grade determined for the modification.

As discussed in Section 2.4, the HFE program and its use in grading the level of HFE activity should be consistent, to the extent possible, with NRC expectations for use of graded approaches. One way to help ensure this is to obtain NRC review of the plant's HFE program as early as possible in the modernization process. Any issues that arise from that review can be addressed, and the program can then be applied with confidence and referenced in any licensing activities for subsequent modifications. See Section 2.5 and Section 5.4 for further discussion of planning for NRC interactions.

5.2.1.2 Evaluation of Hybrid HSI Issues

Section 2.3.4.1, Hybrid HSI Issues, identified a number of potential issues or concerns related to hybrid HSIs. As discussed in that section, hybrid HSI issues should be considered when designing each interim configuration of the control room that will result from incremental migration toward the final control room endpoint. In addition, these issues should be considered in regulatory and licensing activities to ensure that they have been adequately addressed prior to making any licensing submittals or undergoing regulatory reviews. The hybrid HSI issues are repeated here for the reader's convenience.

Note that many of these issues are not new, as existing plants have dealt with a mix of analog and digital technologies for some time. For example, in many plants the operators currently work with a combination of analog and digital or computer-driven displays for monitoring plant variables, including Safety Parameter Display Systems (SPDS) and Post-Accident Monitoring Systems (PAMS). Plant computers provide graphical displays that are used under normal and emergency conditions along with conventional meters and indicators. However, as plants further modernize their control rooms over time there will be a significant increase in the number of digital HSIs that will be used and thus hybrid issues will be more pronounced, particularly as digital controls (e.g., soft controls at workstations) are introduced alongside conventional controls.

A good HFE design process and use of the guidelines given in Sections 3 and 4 of this document can adequately address these hybrid issues and concerns and deal with them appropriately in design, validation, and training. From the standpoint of licensing and regulatory compliance, the potential impact of hybrid issues on plant safety should be examined, and the licensee should be prepared to describe how they have been addressed when making submittals to the NRC or in any regulatory reviews that are required.

High-level issues related to overall plant operation are described first, followed by specific issues related to individual hybrid HSI elements.

Note that in addition to these issues, which relate to potential differences between older analog and newer digital HSIs, there are other aspects of HSI design that also can introduce differences in the interfaces the operators use – for example, use of both qualified and non-qualified HSIs (see Section 6.4.3.4). These should be considered along with the hybrid analog-digital issues discussed here.

5.2.1.2.1 Hybrid Issues Related to Overall Plant Operation

HFE evaluations should address the potential impact of hybrid HSIs on operator tasks, and how this might affect plant safety. For example, the following hybrid issues or concerns should be addressed:

- Inconsistencies in design or operation between different systems (e.g., one still analog, the other converted to digital) or between different sections of the interface, when these must be used together or alternately to perform operator tasks, such as:
  - Carrying out abnormal and emergency operating procedures – where in these procedures must the operators transition across the technology interface (i.e., move from analog to digital or vice-versa), what confusion or errors or delays might occur at these transitions, and what would be the impact on plant safety? How is this addressed in the HFE evaluations?
  - Assessing the state of the plant, its systems, and the status of the critical safety functions – is there a mix of technologies that must be used here? Does this impact operator performance, and has this been addressed in the HFE evaluations?
  - Operator actions credited in the licensing basis – are there transitions across technologies that must be made to carry out these tasks? If so, what errors or delays might be imposed by this, and how has this been addressed in the HFE evaluations?
  - Other risk-important operator actions or tasks, such as those identified as risk significant in the PRA – what transitions between interface technologies are involved in these tasks, and has this been addressed in the HFE evaluations? See Section 5.2.6 for guidance on use of the PRA to identify risk-important human actions, and assessing impact on the PRA of the control room changes being made.

- Increased training burden to allow operators to remain proficient with old interfaces that are retained, while gaining proficiency on the newer ones being installed – sufficient resources and time must be available to ensure that this training is accomplished effectively. If it is not, there is risk that operators may lose their proficiency with older interfaces they use infrequently, or there may be insufficient time or attention paid to training and familiarization on the new interfaces, either of which could lead to errors. See Section 6.3 for a more detailed discussion of training issues associated with digital I&C and HSI upgrades.
- Compromises in design to accommodate old and new technologies – for example, attempts to set lighting levels high enough to make remaining analog gauges readable but not too high for recently installed CRT or flat panel displays.

5.2.1.2.2 Specific Issues Associated with Hybrid HSI Elements

At a more detailed level, there are a number of specific issues or concerns related to different aspects of hybrid HSI designs. For example, hybrid issues need to be examined for the following types of hybrid HSI elements:

- Duplicated indications – both analog and digital indications of the same variable
- Duplicated controls – both analog and digital controls provided for the same function
- Control tasks that require use of analog and digital controls at different steps in the same task
- Deactivated controls and/or indications (those left in place but non-functional)
- System/functional groupings of controls and indications in hybrid designs
- Differences in level of automation between analog and digital implementations
- Hybrid alarm systems, or different implementations of alarms between analog and digital systems
- Hybrid procedure implementations – some procedures converted to computer-based format but others not
- Differences in failure modes between analog and digital HSIs

Table 5-1 lists examples of hybrid issues or concerns for each of these HSI elements. These are examples only – it is important for the design team to identify hybrid issues applicable to the plant-specific design at each step in the modernization program and to ensure that they are adequately addressed. This is discussed as part of Migration Planning in Section 2.3.4, Ensuring Adequacy of Interim Hybrid HSIs.

Table 5-1
Specific Hybrid Issues for Individual HSI Elements

Hybrid Issues for Individual HSI Elements
Duplicated (analog and digital) indications ● Are the same values shown on each? How will potential differences in displayed values be handled by the operators? Which one will they trust to be correct? ● Will there be differences in accuracy of the two indications, or perceived accuracy and potential confusion (e.g., a digital indication with several significant digits appearing to be more accurate than an analog meter reading, but in fact based on a wider-range or less accurate instrument) ● Are both types of indication referenced in the procedures?
Duplicated (analog and digital) controls ● Differences in how the controls operate, including potentially subtle differences such as range of control, rate of change, etc. ● Differences in how auto/manual controls are used, how bumpless transfer is accomplished, indications used when operating the controls (e.g., demand, actual) ● Are both types of control referenced in the procedures?
Control tasks that require use of analog and digital controls at different steps ● How smooth are the transitions between use of one type of control at one step, and another type at the following step? ● Are there subtle differences in how the controls operate (e.g., analog and digital controllers with auto/manual stations that on the surface appear to perform similar functions, but the details of their operation reveal differences in behavior between the analog and digital devices)? ● Will there be extra mental workload during transitions due to the need to focus on the differences between the controls? ● If an operator were to become confused as to which type of control is being used at any given step, what types of errors would be most likely to occur and what would the consequences be? How would such errors be detected and corrected?
Deactivated (left in place but non-functional) controls and/or indications ● How might these interfere with task performance? ● What is the potential for an operator to mistake one of these for an active control or indication, particularly in stressful or high-workload situations? What errors might be made, and what would the potential consequences be?
System/functional grouping of controls and indications ● Will the benefits obtained from system/functional groupings of controls and indications that were implemented post-TMI be lost or degraded with a hybrid arrangement? ● Are the groupings of controls and indications on new digital HSIs compatible with the groupings of the remaining analog controls and indicators? ● If controls related to a single system or function are split between two different locations (e.g., some control actions can be taken at a workstation while others must still be performed at the control boards), is there potential for operator confusion as to where an action can be taken? Could this lead to delays that impact task performance?

Table 5-1
Specific Hybrid Issues for Individual HSI Elements (Continued)

Hybrid Issues for Individual HSI Elements
Differences in information presentation ● Are there differences in how information is arranged on new computer-driven displays as compared to the way similar information is presented on control boards that are retained? ● Are there differences in coding used for digital versus analog information presentations (e.g., different use of symbols or colors)?
Differences in level of automation ● If some systems/functions have been upgraded but others have not, could differences in the level of automation of the systems/functions lead to confusion or errors (e.g., if some steps in a sequence of control actions are automated with the new digital implementation for a given component or function, but these steps must be performed manually for a very similar component or function that has not been upgraded to digital)? ● What types of errors might occur, how would they be detected and corrected, and what would be the consequences of such errors?
Hybrid alarm systems ● Are there differences in how alarms are defined and generated for new digital systems as compared to alarms for existing systems? ● Are there alarms generated by new digital systems that are not presented on the main alarm system (e.g., overhead annunciators)? Are any of these at the same level of importance as the main alarms? How will the operators integrate these alarms when responding to plant events or upsets? ● Are the prioritization of alarms and the methods for indicating alarm priority consistent among the various alarm implementations? ● Are the annunciation sequences different between analog and digital alarm implementations (e.g., different behavior of incoming versus clearing alarms, momentary alarms, flash rates, etc.)? ● Are the alarm controls (e.g., for silence, acknowledge, reset, and test) consistent among the various alarm implementations? ● Will the addition of new digital systems result in additional alarms requiring separate acknowledgment? Will the operators be burdened by having to take multiple actions to acknowledge all the alarms and silence audible indications during plant upsets?
Hybrid procedure implementations ● If some procedures have been converted to computer-based procedures, but others have not, how smooth will the transitions be between the two types of procedures? ● How might this affect task performance?
Differences in failure modes ● Are there differences in the behavior of digital versus analog devices when power is lost to the device? When the input signal is lost or off-scale? ● Have functions been combined as part of the digital upgrade? If so, will the consequences of failure of the new equipment (e.g., failure of a card, module, or communication link) be more severe or otherwise different as compared to failures of the remaining analog equipment? ● Will the indications the operators receive when these types of failures occur be different for the digital implementation than for the analog? Is there potential for operator confusion or errors to result from these differences?

5.2.2 System Failure Analysis

Failure analysis is very important to the design of digital systems and is a significant input to licensing, particularly 10 CFR 50.59 evaluations. See TR-102348 for general guidance on failure analysis.

For changes that impact the control room or other HSIs, the failure analysis should include consideration of HSI failures and potential human errors in using the HSI (including both operator and maintainer errors). Any identified failures with new results, not previously analyzed, will be important inputs to the 10 CFR 50.59 evaluation.

Failure analysis should address:

- Impact of I&C failures on operations – are the failure modes different? Are the indications to the operators different? Is there potential for confusion? How is this handled in training? Have these scenarios been tested/validated?
- Impact of HSI failures or degraded functionality, including loss of data to update displays, loss of alarms, display failure, loss of entire workstations including control capability, etc.
- How the operators will handle I&C and/or HSI "pre-failure" situations, where problems have been detected (e.g., through self-diagnostics) but the system is still functional.
- Consideration of human errors in using the new HSIs – are there new types of errors possible? Are the results new? Have these been evaluated to show how they would be detected and corrected, and has adequate response capability been demonstrated?

When considering the potential loss or degradation of HSIs resulting in significant loss of control, monitoring and/or alarming capability, the following issues should be addressed:

- What failures or modes of degradation are credible and should be considered in the design? How frequently would these be expected to occur? Plausible common cause failures should be considered as well as single failures in determining what situations need to be evaluated.
- What controls, alarms, indications should be provided as a backup for each situation? What criteria should these be designed to meet? Should they be sufficient to monitor steady-state conditions and detect any need to trip? Should they be designed to allow maneuvering the power level? Should they be sufficient to meet the Technical Specification (Tech Spec) surveillance requirements within the time required to restore HSI capability? There are several approaches to consider when there is a significant loss of HSI capability:
  - Shut the plant down using the remote shutdown panel – adequacy of this approach has already been addressed in the plant's licensing basis. Although it is probably acceptable from a regulatory standpoint, this is not likely to be the safest approach.
  - Provide enough backup HSI to allow the operators to hold the plant at power for a fixed timeframe – after that time, the plant would be tripped.
  - Hold at power indefinitely (no predetermined timeframe) – as long as there is no transient, simply hold present power level until repairs are made. Shut down if a transient or a situation requiring trip occurs.

Other options having greater functionality such as ability to maneuver power level also may be considered.

- What is the impact of the HSI failure situation on ability to meet Tech Specs and LCOs?
- What is the impact on the Emergency Plan and declaration of Emergency Action Levels (EALs)? At a minimum, be aware of the potential to have to make notifications of unusual events when failures occur.

See Section 6.4 for discussion of modernized designs for safety monitoring and control, including consideration of potential HSI failure modes.

5.2.3 Defense-in-Depth and Diversity (D3) Evaluation

This section discusses the HFE aspects of defense-in-depth and diversity (D3) evaluations. Because this is a relatively complicated and sometimes misunderstood topic, the section begins with some background on what a D3 evaluation is, when it is required, and new methods recently developed for performing the evaluation. Then the impact of D3 on the HSI and associated HFE activities is discussed.

5.2.3.1 What is a D3 Evaluation?

A defense-in-depth and diversity (D3) evaluation is an assessment of the vulnerability of the plant's instrumentation and control systems to common mode failures due to software design errors. As described in the Standard Review Plan, NUREG-0800, Branch Technical Position HICB-19 (referred to hereafter as BTP-19), the NRC Staff has identified four echelons of defense against common mode failures that are present in current plant designs:

- The control systems, which prevent reactor excursions toward unsafe regimes of operation
- The Reactor Trip System (RTS), which reduces reactivity rapidly in response to an uncontrolled excursion
- The Engineered Safety Features Actuation System (ESFAS), which actuates safety equipment when needed to maintain the integrity of the three physical barriers to radioactive release (fuel cladding, reactor coolant system pressure boundary, and containment pressure boundary), and
- Monitoring and indications, which consist of the sensors, displays, data communication systems, and manual controls required for the operators to respond to plant events (this can be thought of as the human echelon).

The NRC has expressed the concern that software design errors are a credible source of common mode failures and, as plants upgrade the I&C systems to incorporate digital equipment containing software, the plant's defense-in-depth might be compromised. To address this concern, the NRC Staff established the following four-point position on defense-in-depth and diversity. Points 1, 2 and 3 of this position apply to digital system modifications to operating plants, while all four points apply to advanced reactors. Quoting from BTP-19, the NRC's position is:

1. *The applicant/licensee should assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.*
2. *In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.*
3. *If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.*
4. *A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.*

The NRC expects that a D3 evaluation will be performed according to Points 1, 2 and 3 above any time a plant replaces its existing (typically analog or relay-based) RTS or ESFAS with a digital system. BTP-19 describes a method for performing the D3 evaluation that has been determined acceptable by the NRC. NUREG/CR-6303 provides more detailed guidance on how to perform the evaluation, which involves identifying portions of the system containing the same software, assuming a common mode (or common cause) failure of that part of the system, and examining each of the events currently analyzed in the SAR for each assumed common cause failure.

BTP-19 provides acceptance criteria for judging the results of the evaluation. The acceptance criteria are based on ensuring that, in the unlikely event such a common cause failure were to occur, there would be no violation of the primary coolant system pressure boundary or containment integrity, and any radiation releases that result would be within the limits of 10 CFR 100. It is important to note that these acceptance criteria are less restrictive than those applied to the accident analyses described in the SAR. The evaluation can be performed on a “best estimate” basis. This means that realistic assumptions can be used, as opposed to the conservative assumptions applied in the plant licensing basis safety analysis. The evaluation should attempt to evaluate, on a “best estimate” engineering basis, how the plant would actually respond to an initiating event.

Non-safety systems can be assumed to function as designed if they are of sufficient quality and are not susceptible to the same common cause failure. Also, manual operator actions can be relied upon if adequate time and information are available so that it is reasonable to expect the operators to take such actions.

5.2.3.2 Impact on the Plant Design Basis

It is important to note that evaluations of defense-in-depth and diversity to address digital common cause failures (CCFs) are “beyond design basis.” This concept is discussed in the digital I&C licensing guideline TR-102348, and in the new D3 guideline EPRI 1002835. For equipment that has been evaluated and accepted for safety applications, the likelihood of digital CCF should be well below the likelihood of random single failures assumed in the licensing basis. Therefore, although the potential for digital CCFs should be considered in the evaluation, it typically would not by itself lead to the need for a license amendment per 10 CFR 50.59. However, digital CCFs and their potential D3 issues should be addressed in the design process for the modification (independent of the 10 CFR 50.59 evaluation).

Any manual backup manual actions and associated controls that are identified in the D3 evaluation for mitigation of common cause failures do not become part of the plant's licensing basis – they are not credited in the accident analyses in the SAR. The D3 evaluation is an engineering design activity that provides some assurance that very low-probability events involving digital common cause failures could be satisfactorily mitigated if they were to occur.

5.2.3.3 Determining when a D3 Evaluation is Needed

D3 evaluations are not required for all digital I&C upgrades. According to the Standard Review Plan (SRP), NUREG-0800 Chapter 7, Section 7.0A, NRC expects a D3 evaluation to be performed for digital upgrades "*…that involve a reactor trip system (RTS) or an engineered safety features actuation system (ESFAS)…*" The SRP further states that D3 evaluations should be performed specifically for "*I&C safety systems incorporating digital computer technology…*" within RTS or ESFAS. This was reiterated in TR-102348, which was endorsed by the NRC in RIS 2002-22. More detailed guidance on determining whether a change requires a D3 evaluation is provided in EPRI 1002835. The guidance addresses whether a D3 evaluation is needed from a regulatory standpoint, as discussed here, and also from a risk-informed viewpoint.

5.2.3.4 Use of Risk-Informed versus Deterministic Methods

Industry experience has shown that the deterministic method of BTP-19 has a number of shortcomings. It addresses only the events included in the SAR accident analyses and not all of the events evaluated in the plant PRA. Consequently, it may not address significant contributors to risk. Also, all of the SAR events are treated as though they are equally safety-significant, and diverse backups are considered equally valuable for all events/systems. Meeting the acceptance criteria for some events may require additional diverse mitigating functions even though the events may have been shown to be insignificant contributors to risk in the plant PRA. In addition, the BTP-19 method also does not allow the analyst to factor into the evaluation the potential positive impacts of digital I&C on reliability of the mitigating systems.

EPRI 1002835 suggests several additional methods that can be used to perform D3 evaluations, which are considered to be acceptable alternatives to the BTP-19 method. The methods make use of both deterministic and risk-informed insights to focus the D3 effort on areas of greatest potential benefit in terms of plant safety. They also allow credit to be taken for the positive impact of modern digital systems on system reliability and safety, and can avoid addition of unnecessary backups that do not provide benefit in controlling plant risk.

5.2.3.5 Impact of D3 on HSI and Associated HFE Activities

Figure 5-5 illustrates the HSI-related aspects of the D3 evaluation process. The relevant impacts of D3 on the HSI and associated HFE activities are discussed below.

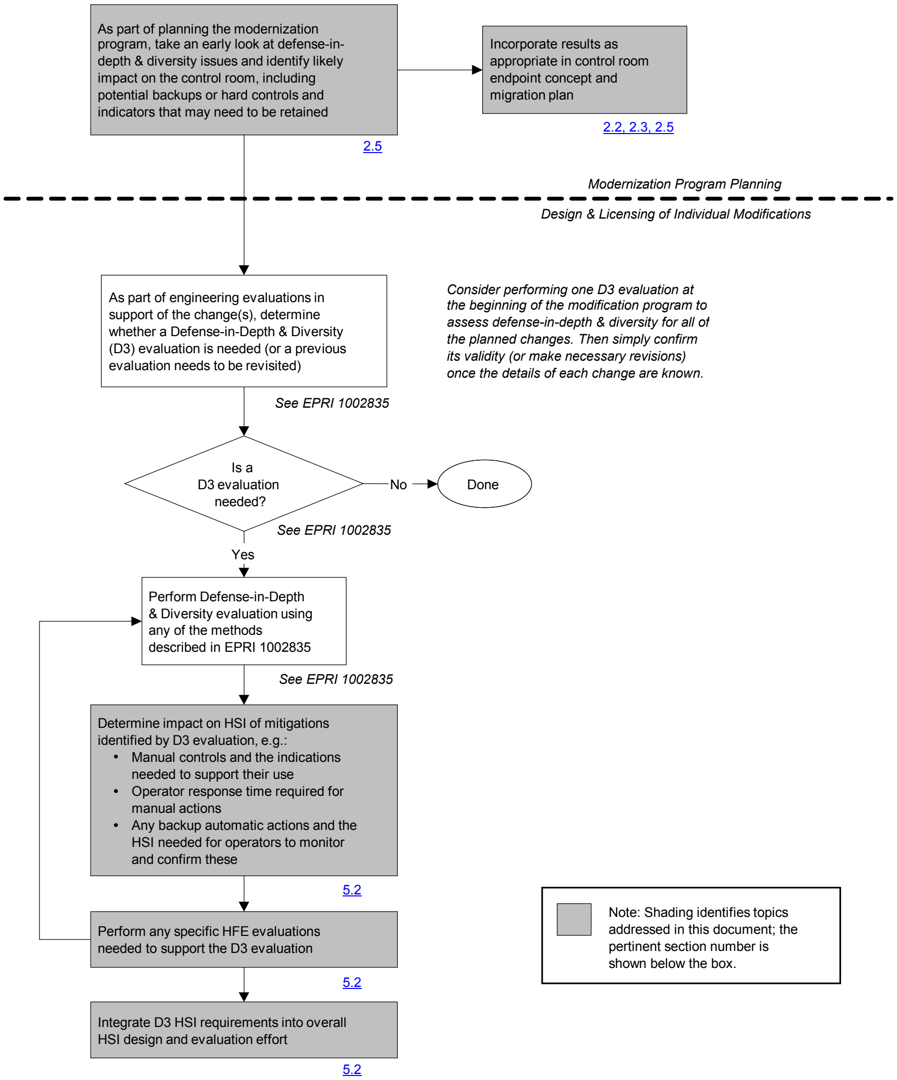

As part of planning the modernization program, take an early look at defense-in-depth & diversity issues and identify likely impact on the control room, including potential backups or hard controls and indicators that may need to be retained
2.5
Incorporate results as appropriate in control room endpoint concept and migration plan
2.2, 2.3, 2.5
Modernization Program Planning
Design & Licensing of Individual Modifications
As part of engineering evaluations in support of the change(s), determine whether a Defense-in-Depth & Diversity (D3) evaluation is needed (or a previous evaluation needs to be revisited)
See EPRI 1002835
Consider performing one D3 evaluation at the beginning of the modification program to assess defense-in-depth & diversity for all of the planned changes. Then simply confirm its validity (or make necessary revisions) once the details of each change are known.
Is a D3 evaluation needed?
No
Done
See EPRI 1002835
Yes
Perform Defense-in-Depth & Diversity evaluation using any of the methods described in EPRI 1002835
See EPRI 1002835
Determine impact on HSI of mitigations identified by D3 evaluation, e.g.:
• Manual controls and the indications needed to support their use
• Operator response time required for manual actions
• Any backup automatic actions and the HSI needed for operators to monitor and confirm these
5.2
Perform any specific HFE evaluations needed to support the D3 evaluation
5.2
Integrate D3 HSI requirements into overall HSI design and evaluation effort
5.2
Note: Shading identifies topics addressed in this document; the pertinent section number is shown below the box.

Figure 5-5
Defense-in-Depth and Diversity Evaluation

Section 2.5 discusses the importance of considering defense-in-depth and diversity issues early in the modernization process so that the potential impact on the control room can be identified and included in the modernization planning. Results of an early look at D3 should be factored into the control room endpoint concept and migration plan – see Sections 2.2 and 2.3. Also, D3 issues should be addressed as part of the overall design of modern HSIs for safety monitoring and control, as discussed in Section 5.2.5 below.

As indicated in Figure 5-5, performing the full D3 evaluation at the beginning of the modernization program can help streamline the licensing process and reduce the cost and time associated with downstream regulatory reviews. If a D3 evaluation is performed once at the beginning that addresses D3 for the entire series of planned modifications, and this is reviewed and approved by NRC, then its validity can simply be re-confirmed as the details become known for each individual modification, and it can be referenced in any licensing submittals or reviews.

The D3 evaluation (regardless of which method is used) typically identifies some manual actions that would be taken to mitigate the accident sequences evaluated in the analysis. These actions may use either dedicated, hard-wired controls and indicators, or digital equipment if it is shown to be diverse (not subject to the common cause failure for which it is to provide backup). Non-safety HSIs can be used to support these manual actions if they are of sufficient quality to perform the needed functions. The plant's HFE program and appropriate HFE principles should be applied in evaluating these potential mitigating actions, as part of determining whether they can be relied upon as backups for these situations. Information and control requirements should be identified, applying the process guidance in Section 3 and design guidelines of Section 4 of this document, and the required operator response time should be determined and evaluated.

Note that the response times for these backup manual actions can be shorter than the conservative response times used previously in the licensing basis analyses – the D3 evaluation is intended to be a "best estimate" assessment of how the events actually would be mitigated. Operator response times much shorter than the times assumed in licensing basis analyses have been defended successfully in licensing submittals and NRC reviews, for specific situations identified in the D3 evaluation. However, NRC will expect that any operator response times assumed in the D3 evaluation will have adequate justification.

If the response times cannot be validated directly using the plant simulator, there are other approaches that can be used. For example, expert judgment by persons who have experience in plant operations and training of operators may be used to develop and justify assumed response times. This might be based on comparison to other scenarios for which response times have been validated using the simulator (e.g., as part of EOP validation), as long as it can be shown that extrapolation from the previously validated events to the D3 events is reasonable. The D3 evaluation is a best-estimate assessment, so the estimates of response times should not be overly conservative. However, the validation of the assumed response times should show sufficient margin in the estimates that there is a reasonable level of confidence in the assumed values. Again, this can be based on qualitative judgments/extrapolations if direct validation exercises are not practical for the specific scenarios being evaluated. See Section 3.6 for discussion of other approaches that also can be used.

Backup controls, displays and alarms identified for mitigation, and the HSI needed to support any automated backups added for mitigation (e.g., indications required to verify that the backup automatic actions have taken place) should be integrated into the overall control room and HSI design, included in the HFE evaluations performed to validate the design, and properly reflected in procedures and operator training.

5.2.4 Digital System Dependability Evaluations

Use of a human factors engineering process to achieve high quality and effectiveness of the human-system interface is an important part of demonstrating adequate overall dependability of digital systems. This is very similar to the role that software engineering and software quality assurance play in ensuring dependability. This is discussed in Section 5.3.4.2 of TR-102348.

The principal concerns regarding the HSI relate to the possibility of system failure due to human error (by operators or maintenance technicians) or due to unauthorized entries or alterations of the system through a maintenance, test, or configuration interface. Adherence to an appropriate HFE program as described in Section 2.4 and use of the guidance given in Sections 3 and 4 of this document will help ensure dependability of the new or modified systems. These HFE activities can be cited as part of the basis for dependability claims made in 10 CFR 50.59 evaluations or in licensing submittals. Also, failure analyses performed for the digital systems should include consideration of potential human errors as discussed in Section 5.2.2.

Digital technology provides a number of features that can enhance dependability. These positive aspects of the technology should be considered along with the potential for negative impact due to the types of errors discussed above. Design efforts should attempt to exploit the advantages offered with digital systems, employing HSI features that can help operators or maintenance personnel to detect and correct human errors, and also to manage faults or failures that may occur in the digital I&C systems. Such features should be credited as appropriate in dependability assessments and related licensing submittals.

5.2.5 Modern Safety Monitoring and Control Solutions

Following the accident at Three-Mile Island plant, the NRC and the nuclear industry established requirements aimed at providing better support to plant personnel for accident monitoring and control. This led to the identification of many different safety-related systems that have HSI aspects, e.g., SPDS, PAMS (PAMI), and BISI. In present plants there is not a uniform and consistent approach to how these HSIs are designed. As a result, they tend to be separate and isolated systems that are rarely used and that may not follow the conventions of the other control room HSIs. Also, the regulatory guidance for these features was written long ago and was based primarily on the analog instrumentation installed in the plants at that time. With I&C and HSI modernization, better and more integrated approaches are possible in these areas. However, some interpretation of the regulatory guides is needed in certain areas to show how more modern solutions meet the intent of the original requirements.

Also, as the control room is modernized and conventional instruments and controls are replaced with newer digital implementations, design decisions must be made regarding which HSIs or HSI components must be qualified as safety-related equipment, and which ones can be implemented using non-safety equipment such as a non-safety DCS. Plants currently have qualified HSIs (typically qualified meters and switches) that can be used to control safety equipment, but in many cases this was done more as a matter of expediency than because of any specific regulatory requirements or guidance. The regulations are clear on the need for qualified HSIs to perform actions credited in the SAR safety analyses. However, they are not so clear on the level of qualification needed for HSIs used to support other emergency operations called out in the plant's EOPs. (An exception is post-accident monitoring instrumentation for which there is relatively detailed guidance on qualification requirements.) If some HSIs that are presently qualified as safety-related equipment are to be moved to non-safety interfaces or HSIs that have a lower level of qualification, this may require regulatory justification.

In addition to deciding which HSIs must be qualified, decisions also must be made on other HSI design requirements, including identifying which HSIs should be located in fixed positions, which ones should be continuously displayed, and those that can be selected by the operator on demand. The regulatory requirements and guidelines in these areas are not always clear and thus require some interpretation. A related topic is the concept of a "minimum inventory." It relates to decisions on what should be fixed position, and also what backup capabilities should be provided for when HSIs that are normally used by the operators have failed (see the next issue listed below). The concept of a minimum inventory arose as part of the NRC's reviews of advanced reactors. While the inventory pertains to advanced plants and not existing plants, it is useful to consider the issues involved and their operational consequences.

Another consideration is the implementation of HSIs to support manual actions credited in the defense-in-depth and diversity (D3) evaluation discussed in Section 5.2.3. These should be considered when developing the overall safety monitoring and control solution.

Section 6.4 discusses these challenging design issues in more detail. It discusses the intent of the relevant regulatory requirements and guidelines and identifies other design and operational considerations that should be addressed, along with the regulatory requirements, when designing modernized HSIs for safety monitoring and control. Design activities are identified that should be carried out using the guidance in Sections 3 and 4 to examine the tradeoffs and develop HSIs that meet the overall design objectives and associated regulatory requirements.

5.2.6 Interaction with PRA

The plant-specific Probabilistic Risk Assessment (PRA) is used as a tool to support a number of different activities in design, maintenance, licensing, and other areas. The PRA includes consideration of human actions and the associated probability of failure (human error probabilities), particularly where these are considered important to the frequency of accident sequences analyzed in the PRA (e.g., those sequences leading to core damage or large releases). Human Reliability Analysis (HRA) techniques can be used to evaluate the potential for human error and the "performance shaping factors" contributing to such errors.

In a new plant design, HRA is used to support both the HFE program and the PRA, and NRC expects that these activities will be integrated throughout the process. See NUREG-0711, Figure 7.1, for an illustration of the various interactions among these activities.

For most operating plants, there was no PRA or HRA activity used at the design stage. In fact, PRAs for the current generation of plants were developed subsequent to initial operation to meet the IPE requirement, and they have been refined to meet various needs including the Reactor Oversight Process (ROP), the Maintenance Rule, and risk-informed licensing activities. Human actions are considered in the plant PRA, even if the activity is not called HRA. The overall activity, including the PRA and its human action component, is referred to here as "PRA/HRA."

Section 3.6 discusses human error analysis in the context of the overall design process. This section addresses the interactions between PRA/HRA and the design and licensing of I&C and HSI modifications that may impact human actions. Figure 5-6 illustrates these interactions.

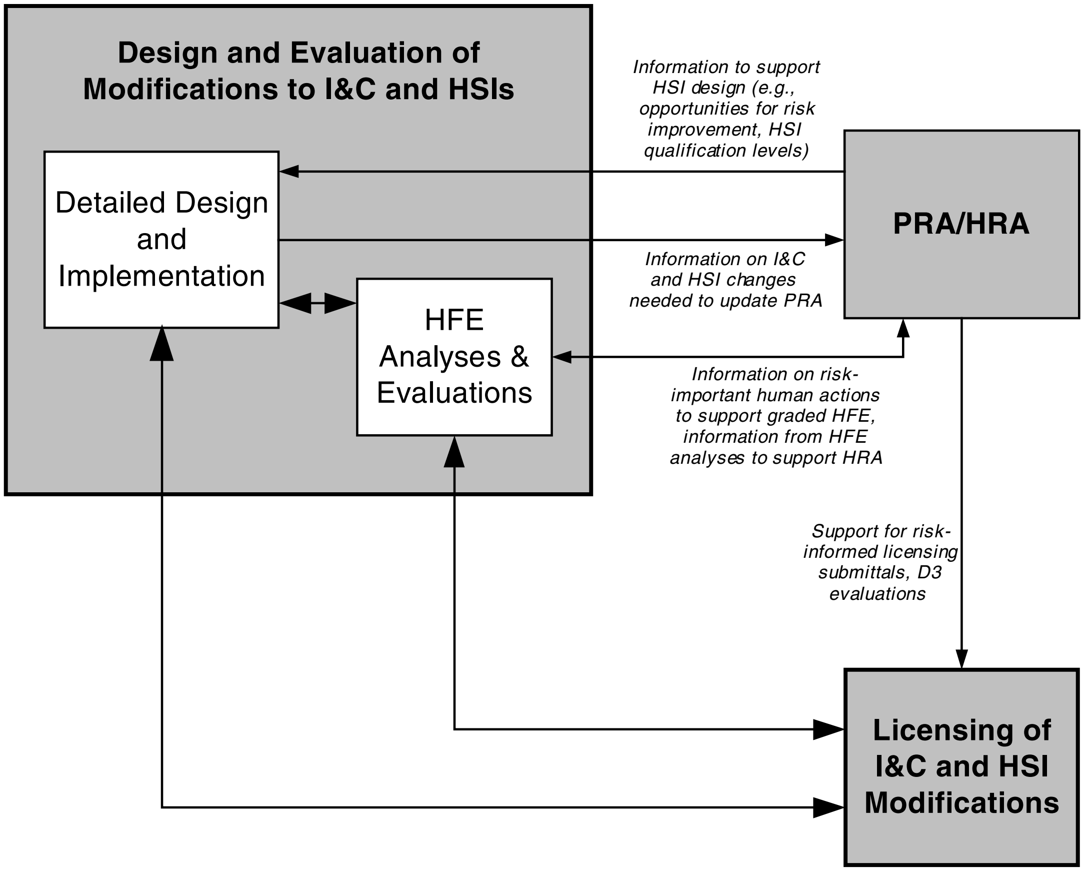

Design and Evaluation of Modifications to I&C and HSIs
Detailed Design and Implementation
HFE Analyses & Evaluations
PRA/HRA
Licensing of I&C and HSI Modifications
Information to support HSI design (e.g., opportunities for risk improvement, HSI qualification levels)
Information on I&C and HSI changes needed to update PRA
Information on risk-important human actions to support graded HFE, information from HFE analyses to support HRA
Support for risk-informed licensing submittals, D3 evaluations

Figure 5-6
Interactions with PRA/HRA

5.2.6.1 Impact of I&C and HSI Changes on the PRA/HRA

The I&C and HSI changes made as part of modernization may affect risk-important human actions that have been analyzed in the PRA. This impact may result from:

- Changes in automation, reducing the need for some actions or placing the operators as backup to actions for which they were once principally responsible
- Introduction of new HSI technologies that introduce new human actions that did not exist before
- New types of errors associated with existing actions that were not considered previously, or
- Other changes that affect assumptions used to derive human error probabilities included in the PRA (e.g., better or reduced access to compelling signals needed by the operators to diagnose the need to take action).

If the PRA is to be used to support risk-informed licensing submittals, the Reactor Oversight Process (ROP), compliance with the Maintenance Rule, or other design or licensing activities, it must be kept up to date as the plant is changed. The I&C/HSI designers will need to provide information to the PRA group to assess the impact of the changes on the human actions considered in the PRA and the associated human error probabilities. Information that is typically used when addressing human actions in the PRA includes:

- What is/are the compelling signal(s) that would prompt the human action?
- What information or instrumentation is available to provide the compelling signal(s) during specific accident sequences?
- How much time is available for the action to be taken?
- How long is it likely to take the operator to perform the action?
- What is the level of stress and workload on the operator at the time the action is taking place?

There may be other performance shaping factors that influence the successful performance of the human action, and these would also be considered in the PRA/HRA. See Section 3.6 for further discussion and guidance regarding human error analysis and performance shaping factors.

5.2.6.2 Use of PRA/HRA to Support HSI Design and Evaluation

The PRA/HRA can provide insights that are helpful in design of the I&C and HSI changes. For example, Section 2.4.2 describes how a graded approach can be taken in determining the scope of HFE activities to be undertaken for a given modification. This would be based in part on the risk significance of the tasks affected by the change. The PRA/HRA can assess the risk significance of each action and thus help focus resources on the areas of highest risk when designing, verifying and validating the HSI changes. Also, information from the PRA/HRA can be used to identify opportunities for HSI upgrades to improve human performance in areas that will have the greatest impact on plant safety.

The plant's PRA group can provide a list of the human actions that are considered in the PRA, along with risk-importance measures for each of these actions. Tables 5-2 and 5-3 give examples of the type of information that may be readily available from the PRA/HRA for a PWR and BWR, respectively. Although the data were adapted from actual plant PRAs, the tables are only examples and should not be used to represent the actual set of human actions or probabilities for any specific plant. Each plant-specific PRA determines what operator actions should be considered and assigns probabilities of failure based on plant-specific design features, procedures and training associated with each action. Sensitivity studies using the resulting PRA are used to determine the risk importance of each human action and allow ranking of the actions to identify those that dominate from a risk standpoint.

Two types of risk-importance measures are often used, as shown in the tables:

- *Risk Achievement Worth (RAW)* – The RAW score gives an indication of potential impact on risk if the human action were to be made less reliable. Events with high RAW scores might be examined to ensure that the HSI changes will not have a significant negative impact on risk.

- *Fussell-Vesely* – The Fussell-Vesely measure provides an indication of how much each human action currently contributes to plant risk. Events with a high Fussell-Vesely score may represent opportunities to improve safety, for example, by providing HSI features that reduce the probability an operator will fail to perform the needed action, or by eliminating the need for the operator action, thus improving overall plant risk.

The results of the PRA also can be used to support determining the level of qualification for various HSIs. As discussed in Section 6.4, the regulatory requirements are not clear in some areas regarding the level of qualification needed for various HSIs used for safety monitoring and control. Graded approaches can be used to define appropriate levels of qualification (equipment qualification, redundancy and single failure protection, separation, etc.) along with other design requirements (e.g., fixed position, continuously displayed) depending on importance of the HSIs and associated tasks to plant safety. The PRA can be used to help determine risk significance.

5.2.6.3 Use of PRA/HRA to Support Licensing

The PRA can be used to support risk-informed licensing submittals in accordance with the approach outlined in Reg. Guide 1.174. Use of the PRA to support defense-in-depth and diversity evaluations and identification of needed manual backups is discussed in Section 5.2.3. The NRC guidance for review of changes to risk-important human actions, contained in Chapter 18 of NUREG-0800, has been updated to apply risk insights in the review similar to the approach in Reg. Guide 1.174, regardless of whether the licensee's submittal is risk-informed or not.

Risk insights derived from the PRA can be used even in licensing submittals that are not risk-informed. For example, as discussed above and in Section 2.4, PRA insights used in determining the level of HFE activities to be performed for an HSI change, in accordance with the plant's graded HFE program, can be cited in licensing submittals in demonstrating adequacy of the HFE activities performed.

Note that in the absence of any risk information provided by the licensee, an NRC reviewer may make his or her own assessment of risk associated with a change as part of grading the NRC review and assessing the adequacy of the proposed change. For example, NUREG-1764 provides generic lists of risk-important human actions, derived from review of multiple plants' PRAs, for use by NRC reviewers in assessing the risk associated with changes to human actions.

Table 5-2
Sample List of Operator Actions and Importance Measures for a Pressurized Water Reactor (PWR)

PWR Operator Actions[1-5]	Failure Probability	Current Contribution to CDF (F-V)[3]	Potential Contribution to CDF (RAW)[4]
Failure to align SI for recirc from the containment sump for Small LOCA or Feed & Bleed	0.005	1.8E-01	37.8
Failure to initiate pressurizer spray to reduce reactor pressure (SGTR)	0.001	1.8E-02	13.2
Failure to makeup to the suction of AFW from any source following CST depletion	0.003	8.4E-03	4.1
Failure to repair a diesel generator in 4h	0.170	4.0E-01	2.9
Failure to manually initiate equipment following load shed	0.003	4.7E-03	2.8
Failure to align SI for recirc from the containment sump for intermediate LOCA	0.005	5.2E-03	2.1
Failure to initiate Feed & Bleed	0.003	2.5E-03	2.0
Failure to isolate SG dump valves on spurious operation	0.040	3.9E-02	1.9
Failure to recover offsite power in 30m	0.350	4.0E-01	1.7
Failure to initiate charging flow (ATWS)	0.056	3.6E-02	1.6
Failure to increase AFW flow given failure of one or more headers to SG	0.001	5.8E-04	1.4
Failure to recover offsite power in 4h (conditional on failure to recover power in 30m)	0.600	4.0E-01	1.3
Failure to recover offsite power in 24h (conditional on failure to recover power in 30m)	0.100	3.0E-02	1.3
Failure to initiate shutdown cooling	0.016	3.6E-03	1.2
Failure to align backup cooling water source to ECCS pumps on loss of CCW	0.043	2.4E-03	1.1
Failure to align SI for recirc from the containment sump for large LOCA	0.008	1.0E-03	1.1
Failure to manually restore non-safety buses after load shed	0.100	4.6E-03	1.0
Failure to manually initiate AFW	0.100	1.2E-03	1.0
Failure to recover a diesel generator in 2h	0.170	9.6E-04	1.0
Failure to recover offsite power in 2h (conditional on failure to recover power in 30m)	0.740	9.6E-04	1.0
Failure to locally control turbine driven AFW pump	0.108	1.3E-04	1.0
Failure to makeup to the CST from alternate supplies	0.003	9.6E-05	1.0

Notes:

1. This listing is an example only. Each plant determines what operator actions to consider and assigns probabilities of failure based on plant-specific design features and criteria.
2. CDF is Core Damage Frequency as calculated by the PRA.
3. Fussell-Vesely value (F-V) represents the current contribution to risk from the operator action in question, i.e., risk would go down by this fraction if the probability of failure of the operator action were to be reduced to 0 (e.g., if F-V=0.1, CDF would drop by 10% to 0.9 times the current value).
4. Risk Achievement Worth (RAW) represents the potential contribution to risk from the operator action in question if it were to degrade in reliability significantly, i.e., risk would go up by this factor if the operator action were to fail with a probability of 1 (e.g., if RAW=2.0, CDF would double).
5. The shaded areas represent those events that would be considered to be high in risk significance based on traditional thresholds used in risk ranking (i.e., F-V >0.005 or RAW >2.0 – for reference, see NUMARC 93-01, Maintenance Rule Implementation, and NEI 00-02, 10CFR50.69 Option 2 Categorization).

Table 5-3
Sample List of Operator Actions and Importance Measures for a Boiling Water Reactor (BWR)

BWR Operator Actions[1-5]	Failure Probability	Current Contribution to CDF (F-V)[3]	Potential Contribution to CDF (RAW)[4]
Failure to initiate emergency depressurization	0.001	3.8E-01	378
Failure to restore feedwater after a high reactor water level trip	0.003	1.1E-02	5.1
Failure to initiate SLC (ATWS)	0.040	9.3E-02	3.3
Failure of level control following successful SLC	0.010	1.6E-02	2.6
Failure to initiate containment venting	0.001	1.2E-03	2.2
Failure to recover offsite power in 6h (conditional on failure to recover in 30m)	0.160	1.4E-01	1.7
Failure to repair RHR in 48h	0.080	3.9E-02	1.5
Failure to repair a diesel generator in 6h	0.350	1.4E-01	1.3
Failure to restore feedwater after a loss of feedwater initiating event	0.110	3.5E-02	1.3
Failure to recover offsite power in 30m	0.640	2.9E-01	1.2
Failure to align blackout diesel	0.500	1.1E-01	1.1
Failure to recover offsite power in 2h (conditional on failure to recover at 30m)	0.450	6.0E-02	1.1
Failure to repair diesel generator in 2h	0.660	6.0E-02	1.0
Failure to align fire water for makeup to reactor	0.750	5.8E-02	1.0
Failure to manually close breakers locally	0.120	4.9E-03	1.0
Failure to align service water makeup to hotwell	0.750	4.9E-03	1.0
Failure to restore a CRD pump after load shed	0.100	2.7E-04	1.0
Failure to recover condenser vacuum after a loss of main condenser	0.330	3.4E-05	1.0
Failure to recover condenser vacuum after an MSIV closure	0.080	3.1E-05	1.0
Failure to restore offsite power in 4h (conditional on failure to restore power in 30m)	0.530	2.9E-05	1.0
Failure to restore offsite power in 24h (conditional on failure to restore power in 4h)	0.110	2.0E-05	1.0

Notes:

1. This listing is an example only. Each plant determines what operator actions to consider and assigns probabilities of failure based on plant-specific design features and criteria.
2. CDF is Core Damage Frequency, as calculated by the PRA.
3. Fussell-Vesely value (F-V) represents the current contribution to risk from the operator action in question, i.e., risk would go down by this fraction if the probability of failure of the operator action were to be reduced to 0 (e.g., if F-V=0.1, CDF would drop by 10% to 0.9 times the current value).
4. Risk Achievement Worth (RAW) represents the potential contribution to risk from the operator action in question if it were to degrade in reliability significantly, i.e., risk would go up by this factor if the operator action were to fail with a probability of 1 (e.g., if RAW=2.0, CDF would double).
5. The shaded areas represent those events that would be considered to be high in risk significance based on traditional thresholds used in risk ranking (i.e., F-V >0.005 or RAW >2.0 – for reference, see NUMARC 93-01, Maintenance Rule Implementation, and NEI 00-02, 10CFR50.69 Option 2 Categorization).

5.3 10 CFR 50.59 Evaluations

5.3.1 Screening

5.3.2 CFR 50.59 Evaluation

5.3.2.1 10 CFR 50.59 Evaluation Criteria

5.3.2.2 HFE-Related Considerations in Performing and Documenting the Evaluation

The 10 CFR 50.59 regulation allows the licensee to determine when a planned change to the nuclear facility requires that a license amendment be submitted for NRC review and approval prior to implementation. Figure 5-2 shows the pertinent regulatory and industry guidance documents that can be used to support the application of 10 CFR 50.59. These include:

- Regulatory Guide 1.187, which endorses the industry guideline NEI 96-07
- NEI 96-07 Revision 1, the primary industry guideline for application of the 10 CFR 50.59 rule – this guidance document covers all changes to the plant, including procedure changes as well as physical modifications
- Regulatory Issue Summary 2002-22, which endorses the use of EPRI TR-102348 for design and licensing of digital I&C systems, including application of 10 CFR 50.59 to digital I&C upgrades
- EPRI TR-102348 Revision 1 (NEI 01-01), the primary industry guideline for licensing of digital I&C upgrades – this document includes guidance on application of 10 CFR 50.59 to HSI changes and provides some relevant examples.

The information provided in this section supplements the guidance in TR-102348 specifically for changes to the control room and other changes that may affect human functions and tasks.

As shown in Figure 5-1, there are two major steps involved in applying the 10 CFR 50.59 regulation to a planned modification. The first step, referred to as “screening,” determines whether the 10 CFR 50.59 regulation applies to the change – some changes do not fall under the regulation and thus do not require a 10 CFR 50.59 evaluation.

The second step, if the change “screens in,” is to perform the 10 CFR 50.59 evaluation. This evaluation determines whether the change will require a license amendment and associated NRC review and approval, or whether the change can be implemented without NRC review.

The 10 CFR 50.59 evaluation is typically performed for the modification as a whole, including all aspects such as mechanical, electrical, I&C, and HFE. The human factors and HSI aspects of the change are evaluated along with all other aspects to determine whether the change requires NRC review prior to implementation. Most of the information needed to support the 10 CFR 50.59 evaluation can be obtained from the evaluations performed as part of the design effort, as shown in Figure 5-1 and discussed in Section 5.2.

Note that plant changes may affect operator performance even when they do not physically change the HSI. For example, an I&C change that significantly alters the time response or sensitivity of a control system can affect operator performance when manually operating the system. Changes to plant equipment can do the same thing (e.g., replacing a valve with one that opens significantly faster or slower than the previous one). If such a change has a significant adverse effect on an operator action credited in the SAR, a 10 CFR 50.59 evaluation may be required to determine whether NRC review must be obtained prior to implementing the change.

TR-102348 makes some important points about evaluation of digital I&C systems that also apply to HSI changes:

- Failure analysis is an important source of information for 10 CFR 50.59 screening and evaluation. Section 5.2.2 discusses the importance of considering potential human errors and potential failures or degraded modes of the HSI as part of the failure analysis.
- Using a design process that follows accepted industry and regulatory standards and guidelines for implementation of digital I&C systems helps demonstrate that a change will not significantly increase the consequences of accidents or malfunctions, or create new malfunctions with different results – key aspects of the 10 CFR 50.59 evaluation. This is true for the HSI as well – following an appropriate HFE design process in accordance with accepted standards and guidelines, including those contained in this document, can help demonstrate that HSI modifications will not have a significant adverse impact on human performance in the context of 10 CFR 50.59.

5.3.1 Screening

In the context of 10 CFR 50.59, screening is a review of the planned modification to determine whether 10 CFR 50.59 applies and thus the change must be evaluated according to the criteria given in 10 CFR 50.59. In general, a change "screens in" (requires an evaluation) if it has an adverse effect on a design function described in the SAR.

Section 4.3.4 of TR-102348 provides guidance on screening of digital I&C upgrades, including changes to the HSI. Figure 5-7 below, adapted from TR-102348, illustrates the screening process. The shaded boxes indicate where HSI changes are addressed in screening.

As pointed out in NEI 96-07, the industry guideline on implementation of 10 CFR 50.59, changes to the HSI may fundamentally alter the means of performing or controlling a design function described in the SAR. NEI 96-07 recommends that such changes be conservatively treated as adverse and screened in. Digital I&C changes that significantly impact operator actions credited in the SAR (even if they do not modify the HSI) also may fall into this category.

It is important to note that not all changes to the HSI fundamentally alter the means of performing or controlling design functions. Section 4.3.4 of TR-102348 lists characteristics of HSI changes that could lead to potential adverse effects. Quoting from that section, *'Characteristics of HSI changes that could lead to potential adverse effects may include, but are not limited to:*

- *Changes to parameters monitored, decisions made, and actions taken in the control of plant equipment and systems during transients,*
- *Changes that could affect the overall response time of the human/machine system (e.g., changes that increase operator burden),*
- *Changes from manual to automatic initiation (or vice versa) of functions,*

- *Fundamental changes in data presentation (such as replacing an edgewise analog meter with a numeric display or a multipurpose CRT where access to the data requires operator interactions to display), or*
- *Changes that create new potential failure modes in the interaction of operators with the system (e.g., new interrelationships or interdependencies of operator actions and plant response or new ways the operator assimilates plant status information).”*

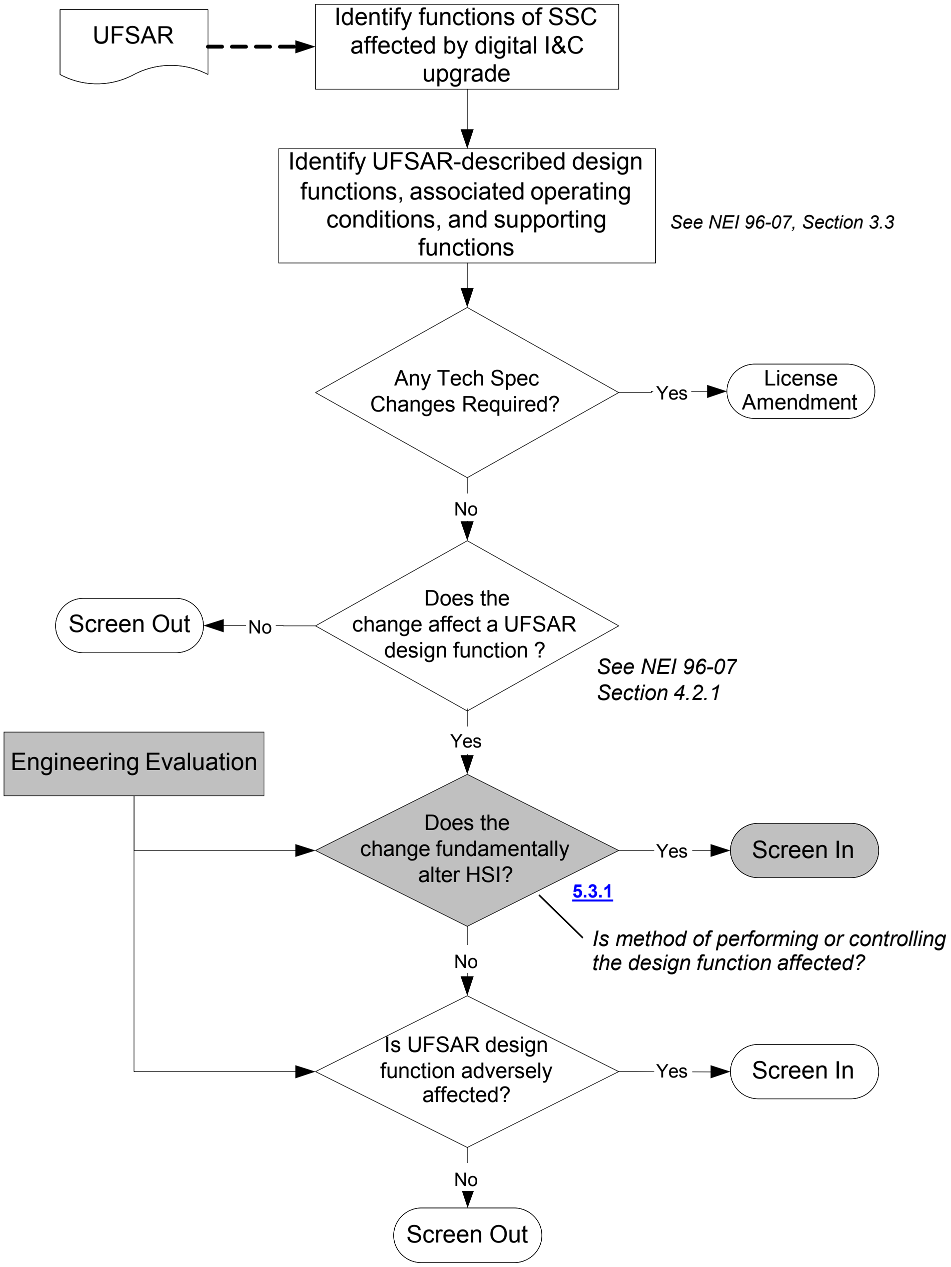

UFSAR
Identify functions of SSC affected by digital I&C upgrade
Identify UFSAR-described design functions, associated operating conditions, and supporting functions
See NEI 96-07, Section 3.3
Any Tech Spec Changes Required?
Yes
License Amendment
No
Does the change affect a UFSAR design function ?
No
Screen Out
See NEI 96-07 Section 4.2.1
Yes
Engineering Evaluation
Does the change fundamentally alter HSI?
Yes
Screen In
5.3.1
Is method of performing or controlling the design function affected?
No
Is UFSAR design function adversely affected?
Yes
Screen In
No
Screen Out

Figure 5-7
10 CFR 50.59 Screening – Addressing HSI Changes

Example 4-3 (TR-102348). Screening for a Recorder Upgrade (Screens Out)
An analog recorder is to be replaced with a new microprocessor based recorder. The recorder is used for various purposes including Post Accident Monitoring, which is an UFSAR-described design function. An engineering/technical evaluation performed on the change determined that the new recorder will be highly dependable (based on a quality development process, testability, and successful operating history) and therefore, the risk of failure of the recorder due to software is considered very low. The new recorder also meets all current required performance, HSI, and qualification requirements, and would have no new failure modes or effects at the level of the design function. The operator will use the new recorder in the same way the old one was used, and the same information is provided to support the Post Accident Monitoring function, so the method of controlling or performing the design function is unaltered. The licensee concludes that the change will not adversely affect any design function and screens out the change.

Example 4-4 (TR-102348). Screening for a Recorder Upgrade (Screens In)
Similar to Example 4-3, a licensee is planning to replace an analog recorder with a new microprocessor based recorder. However, in this instance, the engineering/technical evaluation determined that the new recorder does not truly record continuously. Instead it samples at a rate of 10 hertz, then averages the 10 samples and records the average every one second. This frequency response is lower compared to the original equipment and may result in not capturing all process variable spikes or short-lived transients. In this case, the licensee concludes that there could be an adverse effect on an UFSAR-described design function and screens in the change. In the 50.59 evaluation, the licensee will evaluate the magnitude of this adverse effect.

TR-102348 notes that for HSI changes not exhibiting these characteristics, it may be reasonable to conclude that the method of performing or controlling the design function is not adversely affected, and thus those changes would screen out (no 10 CFR 50.59 evaluation required). However, it also points out that these characteristics focus on potential adverse effects due to changes in the interface itself. They do not address changes to procedures or other changes that may affect human performance, for example, modifications to the I&C or mechanical systems that may affect system response, required operator action times, etc., for credited human actions. Changes to procedures that may be required to implement HSI changes, and changes to credited human actions (regardless of whether the HSI is changed) also need to be screened per 10 CFR 50.59.

Example 4-5 (TR-102348). Human-System Interface Change (Screens In)
Component controls for a redundant safety-related system are to be replaced with PLCs. The existing HSI for these components is made up of redundant hard-wired switches, indicator lights and analog meters. The new system consolidates the information and controls on two flat panel displays (one per redundant train), each with a touch screen providing "soft" control capability. The flat panel can present any of several selectable display pages, depending on what the operator is doing (e.g., starting/initiating the system, monitoring the system during operation, or changing the system line-up). To operate a control, the operator must (via the touch screen) select the appropriate display page, select the component to be controlled, select the control action (e.g., start or stop), and execute it.

The new HSI will provide better support of operator tasks and reduced risk of errors due to:

- *Consolidation of needed information onto a single display that provides a much more effective view of system operation when it is called into action.*

- *Elimination of the need for the operator to seek out meter readings or indications, saving time and helping to prevent errors.*
- *Integration of cautions and warnings with the display to help detect and prevent potential errors in operation (e.g., warnings about incorrect system lineup during a test).*

However, potential adverse effects include:

- *Increased time required to perform some control actions, due to the need to call up the appropriate display and operate the "soft" control.*
- *Fundamental change in the way information is presented to the operator, and different means of interacting with the controls and indications.*

The design was developed using a human factors engineering design, with a verification and validation process consistent with current industry and regulatory standards and guidelines. The goal of the design is to provide a more effective HSI that is less prone to human error than the existing design. However, because of the possible adverse effects noted above, the change is conservatively screened in and will undergo a 10 CFR 50.59 evaluation.

Use of a disciplined HFE design process in which human factors issues are considered by qualified personnel and evaluated using HFE analyses and verification and validation techniques should be credited for minimizing the likelihood of human errors or inadvertently introducing a new behavior or problem that did not previously exist for the old interface. This is discussed in Sections 4.3.4 and 5.3.4.2 of TR-102348. Guidance on incorporating appropriate HFE design and evaluation activities into the plant modification process is given in Section 2.4 and Section 3.1 of this document.

TR-102348 provides examples of HSI changes that would screen in and screen out under 10 CFR 50.59. Examples 4-3, 4-4 and 4-5 of TR-102348 are reproduced here for convenience.

5.3.2 CFR 50.59 Evaluation

This section discusses the 10 CFR 50.59 evaluation criteria and provides guidance on addressing HFE issues when performing the evaluation.

5.3.2.1 10 CFR 50.59 Evaluation Criteria

Section 4.4 of TR-102348 provides basic guidance on performing 10 CFR 50.59 evaluations for digital I&C upgrades. TR-102348 expresses the criteria in the 10 CFR 50.59 regulation in the form of eight questions that must be answered:

1. Does the activity result in more than a minimal increase in the frequency of occurrence of an accident?
2. Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety?
3. Does the activity result in more than a minimal increase in the consequences of an accident?
4. Does the activity result in more than a minimal increase in the consequences of a malfunction?

5. Does the activity create a possibility for an accident of a different type?
6. Does the activity create a possibility for a malfunction of an SSC important to safety with a different result?
7. Does the activity result in a design basis limit for a fission product barrier being exceeded or altered?
8. Does the activity result in a departure from a method of evaluation described in the UFSAR used in establishing the design bases or in the safety analyses?

If the answer is yes to any one or more of these questions, then the change requires a license amendment and prior NRC review and approval. The questions that are most relevant for HSI changes and other changes affecting human actions have to do with whether the change results in "more than a minimal increase" in the likelihood or consequences of accidents or malfunctions considered in the SAR, and whether the change creates the possibility of a new type of accident or a malfunction with a new result that has not been previously analyzed (questions 1-6).

5.3.2.2 HFE-Related Considerations in Performing and Documenting the Evaluation

The guidance in TR-102348 should be used when performing 10 CFR 50.59 evaluations for digital I&C upgrades, including changes to the HSI or other I&C changes that may impact human functions or tasks. The information in this section supplements the guidance provided in TR-102348 and points out some specific items that should be considered when performing and documenting the evaluation.

5.3.2.2.1 Compliance with Accepted Standards and Guidelines

TR-102348 emphasizes the importance of compliance with accepted standards and guidelines as part of demonstrating that properly-designed changes should not present more than a minimal increase (if any) in the likelihood or consequences of malfunctions or accidents. For HSI changes, compliance with key human factors guidelines such as NUREG-0711, NUREG-0700, and the HFE guidelines in this document can be credited when making these claims. See Section 5.1.2 for a discussion of how NRC uses these documents when reviewing a change for HFE compliance.

5.3.2.2.2 Addressing HFE Issues in Failure Analysis and Dependability Evaluations

Failure analysis and dependability evaluations are key elements in determining whether a change creates the possibility of a new accident or malfunction with new results. See Section 5.2.2, Section 5.2.4, and Section 3.6 for guidance on addressing human error as part of these evaluations.

5.3.2.2.3 HSI Considerations in Answering the Eight Questions

Appendix A in TR-102348 provides some supplemental questions for evaluating digital upgrades according to the 50.59 criteria, including questions related to the HSI. These cover items such as possible increased operator burden with the new interface during off-normal or failure mode conditions, possibility of new failures being introduced inadvertently through the interface, and potential for constraints or delays in operator response with the new interface due to difficulty in accessing needed controls. Hybrid HSI issues also should be addressed when answering the 10 CFR 50.59 questions – see Section 5.2.1 for guidance on evaluation of hybrid issues.

5.3.2.2.4 Addressing Both Positive and Negative Aspects of the Change

It is important to consider the positive impacts of the change along with the negative aspects that caused the change to screen in. Modernization of the HSI can provide significant benefits that help offset potential adverse effects. The 10 CFR 50.59 evaluation should address the overall impact resulting from both positive and negative influences. The NRC staff has emphasized this in their interactions with the industry – evaluations should not just focus on the negatives associated with digital upgrades, especially where benefits can be demonstrated that improve plant safety.

5.3.2.2.5 Cumulative Effects of Changes

It is also important to consider the cumulative effects of changes. The 10 CFR 50.59 rule, including the assessment of whether there is “more than a minimal” increase in likelihood or consequences of malfunctions or accidents, is applied to individual changes. NEI 96-07 (Section 4.3) says that changes should be linked and evaluated together only if they are interdependent (one change depends on another) or they collectively address a single design or operational issue. However, from an engineering and operational standpoint it is important to step back and look at the overall effect of a series of changes, particularly with regard to the more subtle or indirect effects such as impact on overall operator workload and impact on crew coordination and communication. Although the change brought about by any one modification may be small, the total impact could reach a point that some additional attention needs to be paid to the cumulative effects.

5.3.2.2.6 NRC Interaction on Major Changes

Individual changes to the HSI made as part of modernization typically will be designed such that they improve human performance – most of these will not increase the probability or consequences of accidents or malfunctions, nor create new accidents or malfunctions with different results. However, it is important to remember that a major control room modification, or the accumulation of many individual changes made as part of a modernization program, can impact the way in which the operators interact with each other and with the plant (the Concept of Operations). It is recommended that such changes be discussed with the NRC early in the project even if a license amendment is not strictly required per 10 CFR 50.59. This can significantly reduce licensing risk and the costs associated with potential NRC interactions.

5.3.2.2.7 Documentation

The bases for engineering judgments made as part of answering the 10 CFR 50.59 questions should be documented. TR-102348, Appendix B, provides guidance on the content and structure of the documentation for 10 CFR 50.59 screening and evaluations. As indicated in that appendix, the documentation of engineering evaluations should include evaluations of the human-system interface. Also, the industry and regulatory guides and standards that have been used or are met by the modification should be documented.

5.4 Licensing Submittals and Other NRC Interactions

5.4.1 License Amendment Requests

5.4.2 Other NRC Interaction for Major HSI Changes

This section discusses licensing submittals that may be required based on the outcome of the 10 CFR 50.59 evaluation or for other reasons (e.g., changes to the Technical Specifications). It also discusses the importance of having other interaction with the NRC staff, beyond just the required licensing submittals, when major modifications are to be made affecting the control room and the functions and tasks performed by human operators and maintainers.

5.4.1 License Amendment Requests

TR-102348 provides guidance on license amendment requests (LAR) that may be required for digital I&C upgrades. It is based on the general guidance and standard format proposed by NEI for license amendment requests (see Section 4.5, *License Amendment Process*, of TR-102348).

For modifications to the control room or other HSIs, and for other changes that impact human functions and tasks (e.g., changes to operator actions credited in the licensing basis), it is recommended that the LAR describe the HFE program and associated activities performed in support of the change. If the plant's HFE program has been reviewed previously by the NRC, then the previous review may be referenced and the submittal can focus only on any differences or deviations from the previously-reviewed program and the basis for those deviations.

It is suggested that the HFE program or process used by the plant, including the approach used for grading the HFE activities (see Section 2.4 and Section 3.1), be mapped to the review elements that are laid out in Chapter 18 of NUREG-0800 and in NUREG-0711. Those review elements are discussed in Section 5.1.2. If the submittal describes the program using a structure and terminology that are consistent with the pertinent regulatory guidance and familiar to the NRC reviewer, this can help expedite the regulatory review process.

For changes that affect human actions credited in the safety analysis, the submittal should address the regulatory review criteria described in Section II.C of NUREG-0800 Chapter 18, and in NUREG-1764. The NRC staff will apply risk insights in determining the extent of their review as described in NUREG-1764. Therefore, it is helpful if the submittal provides information on the risk significance of the affected human actions based on the plant-specific PRA, even if the submittal itself is not risk-informed per Reg. Guide 1.174.

5.4.2 Other NRC Interaction for Major HSI Changes

For major modernization programs, it is recommended that the plant communicate with the NRC staff early and often about both the planning and the implementation of the changes. Experience has shown that such communication can help reduce licensing risk and costs.

Figure 5-8 shows the HFE plans and activities that may be involved in a large-scale control room modernization program, and which might be discussed in interactions with the NRC. Note that not all of these activities are required, and some may not be applicable to a given plant's modernization program depending on the scope of the planned changes. For a major modernization program, all of these may apply.

Each of the plans and activities shown in Figure 5-8 might be discussed with NRC, including:

- The scope of the modernizations that are planned, including the endpoint design concept envisioned for the control room, and the migration plan for achieving the endpoint through a series of planned modification steps or phases
- Plans regarding licensing submittals and other NRC interactions expected during the course of the modernization program, based on the overall licensing plan
- HFE program support activities that go beyond those normally called for by the plant's modification process; examples might be the establishment of a control room design team with responsibilities extending across the planned modifications, and development of prototypes and mockups to support design and evaluation of new HSIs
- The HFE program and procedures that are part of the plant's modification process and will be applied to each change made during the migration
- HFE implementation plans for the individual modifications (as called for by the modification process)
- Descriptions of HFE activities performed and the results of those activities for each modification or phase.

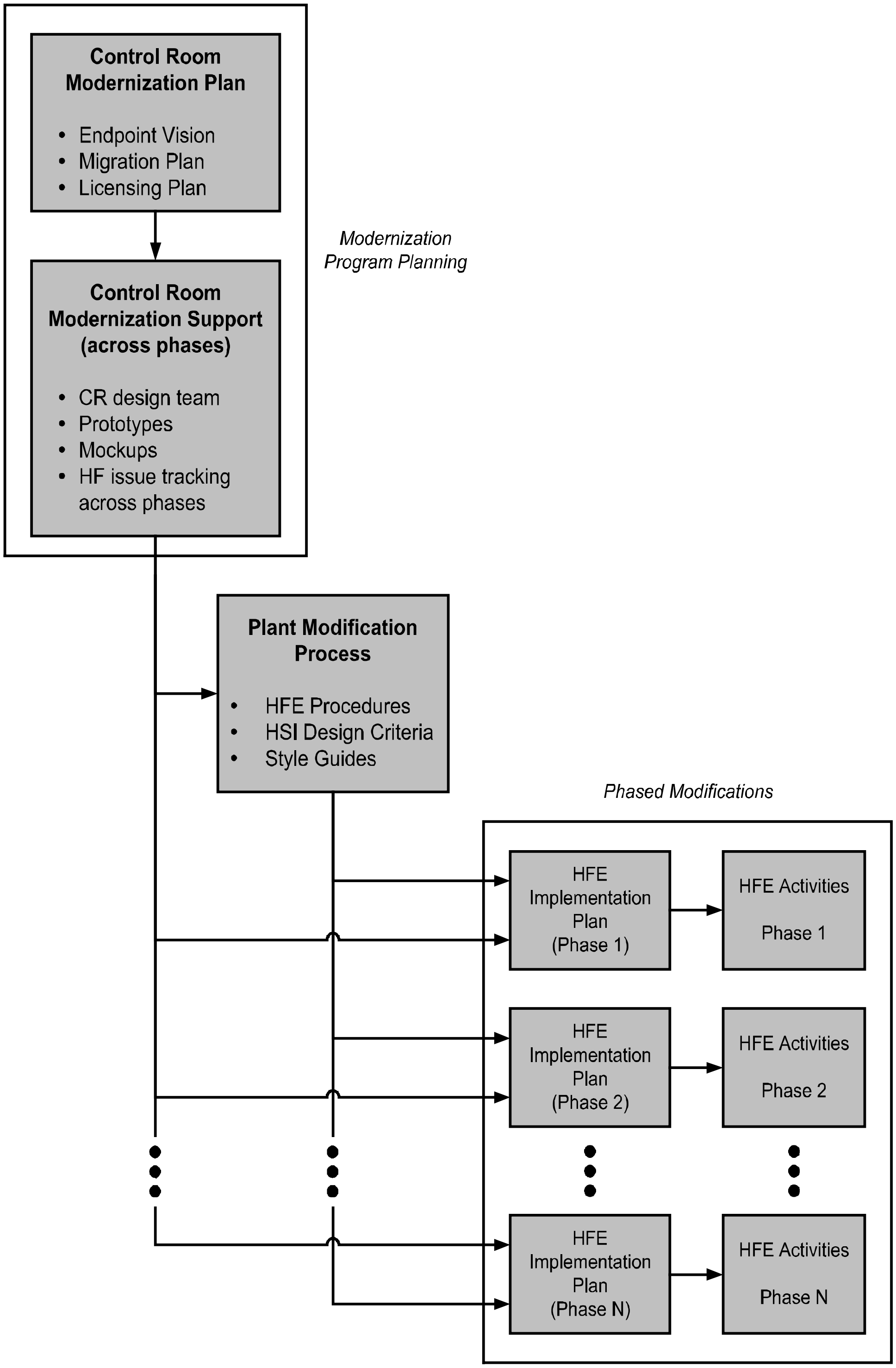

Control Room Modernization Plan
• Endpoint Vision
• Migration Plan
• Licensing Plan
Control Room Modernization Support (across phases)
• CR design team
• Prototypes
• Mockups
• HF issue tracking across phases
Modernization Program Planning
Plant Modification Process
• HFE Procedures
• HSI Design Criteria
• Style Guides
Phased Modifications
HFE Implementation Plan (Phase 1)
HFE Activities Phase 1
HFE Implementation Plan (Phase 2)
HFE Activities Phase 2
HFE Implementation Plan (Phase N)
HFE Activities Phase N

Figure 5-8
HFE Plans and Activities for a Large-Scale Modernization Program

5.5 Appendix – Roadmap to HFE-Related Regulatory Requirements and Guidance

This appendix provides a roadmap to regulatory requirements, NRC expectations, and applicable guidance documents for the HFE-related aspects of the following topics:

1. Determining When an HSI Change Needs Prior NRC Review and Approval (10 CFR 50.59)
2. Human Factors Engineering
3. HSI Design
4. Operator Licensing
5. Failure Analysis and Dependability Evaluations for Digital I&C Systems
6. Defense-in-Depth and Diversity (D3) Evaluations
7. Remote Shutdown
8. Emergency Plans and Notifications
9. Change to Risk-Important Human Actions
10. Risk-Informed Licensing Submittals
11. Technical Specifications and LCOs

The roadmap addresses only those aspects of the documents that relate to HSI changes or other I&C changes affecting human functions and tasks. It does not attempt to address other aspects such as I&C licensing issues that are strictly I&C related.

Sections of this document that provide relevant guidance are shown in bold face under the Guidance heading in the roadmap, and they are preceded by a special character (▶) to make them easily distinguishable from the references to other (external) documents.

1. Determining When an HSI Change Needs Prior NRC Review and Approval (10 CFR 50.59)

Regulatory Requirements

10 CFR 50.59 *Changes, tests and experiments* – defines what changes fall under the 50.59 rule and thus require a 10 CFR 50.59 evaluation; provides a set of questions that must be answered in the evaluation to determine whether a license amendment is required, which would then be submitted to NRC for review and approval prior to the change.

NRC Expectations

Reg. Guide 1.187, *Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments* – endorses NEI 96-07 Rev. 1

Regulatory Issue Summary (RIS) 2002-22, *Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule"* – endorses TR-102348/NEI 01-01 including its coverage of human factors and HSI considerations, and adds these clarifications:

- The Staff considers it likely that upgrades to RTS or ESFAS will require prior NRC review and approval per 10 CFR 50.59 criteria, and
- Engineering judgments made as part of the evaluation should be documented.

Guidance

NEI 96-07 Rev. 1, *Guidelines for 10 CFR 50.59 Implementation* – industry consensus guideline for implementing the 10 CFR 50.59 rule.

EPRI TR-102348 Rev. 1 (NEI 01-01), *Guideline on Licensing Digital Upgrades* – gives industry consensus guidance on design and licensing of digital I&C upgrades, consistent with NEI 96-07. Includes:

- Guidance on using accepted standards and guidelines for human factors engineering of modifications
- Guidance on "screening" HSI changes to determine whether a 10 CFR 50.59 evaluation is required
- Examples of HSI changes that screen in and screen out
- Guidance on performing the 10 CFR 50.59 evaluation, including supplemental questions that address HSI issues.

► **Section 5.3**

2. Human Factors Engineering

Regulatory Requirements

10 CFR 50.34(f), *Additional TMI-related requirements* – includes the following:

- 10 CFR 50.34(f)(2)(iii) requires a "control room design that reflects state-of-the-art human factor principles"
- 10 CFR 50.55a(h) Protection and safety systems – incorporates requirements of IEEE 279 and IEEE 603-1991 (plus correction sheet dated January 30, 1995) for plants constructed after January 1, 1971 – protection systems must meet the requirements in either IEEE 279 or IEEE 603-1991
- IEEE 603-1991 Criteria for Protection Systems for Nuclear Power Generating Stations – "Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988." (§5.14)

NRC Expectations

NUREG-0800 Chapter 18, II.B, *Review of the HFE Aspects of Control Room Modifications* – provides guidance to NRC reviewers for HFE review of control room modifications, according to the 12 HFE program elements described in NUREG-0711. Covers all the same elements as in Section II.A for review of new plants, but provides in II.B some supplemental guidance for review of modifications to existing plants.

NUREG-0711, *Human Factors Engineering Program Review Model* – provides detailed guidance for review of an HFE program, cover 12 program elements (see Section 5.1.2).

NUREG-0700, *Human-System Interface Design Review Guidelines* – provides detailed guidelines for HFE review of human-system interfaces, including both conventional and computer-based interfaces. The guidelines are written primarily to support HFE review as opposed to design of an HSI. The guidelines in Section 4 of this document update and expand on the guidelines in NUREG-0700 and address design of HSIs as well as review.

Guidance

► **Section 2.4**, HF Program Planning

► **Section 3**, Process Guidance

► **Section 4**, Detailed HFE Guidelines

3. HSI Design

Regulatory Requirements

10 CFR 50 Appendix A, *General Design Criteria*

- GDC 13 *Instrumentation and control* – requires instrumentation to monitor plant variables and systems and controls to maintain variables and systems within prescribed operating ranges.
- GDC 19 *Control room* – requires a control room from which actions can be taken to operate the unit safely under normal conditions and maintain it in a safe condition under accident conditions; also requires equipment at appropriate locations outside the control room with capability for prompt hot shutdown of the reactor and necessary instrumentation and control to maintain the unit in a safe condition during hot shutdown, and with potential capability for subsequent cold shutdown.

10 CFR 50.34(f) Additional TMI-related requirements

- 50.34(f)(2)(iv) SPDS
- 50.34(f)(2)(v) Bypass and operable status indication for safety systems

- 50.34(f)(2)(xii) Automatic and manual AFW system initiation and flow indication in control room (PWRs only)
- 50.34(f)(2)(xviii) Indication of inadequate core cooling such as saturation meters in PWRs, and signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs and BWRs
- 50.34(f)(2)(xix) Post-accident monitoring instrumentation
- 50.34(f)(2)(xxiv) Capability to record reactor vessel water level in one location on recorders that meet normal post-accident recording requirements (BWRs only)
- 50.34(f)(2)(xxv) Onsite Technical Support Center (TSC), onsite Operational Support Center (OSC), and nearsite Emergency Operations Facility (EOF)
- 50.34(f)(2)(xxvii) Inplant radiation monitoring for a broad range of routine and accident conditions

10 CFR 50.54, *Conditions of licenses*, paragraph m(2)(iii) – requires that in all modes other than cold shutdown and refueling, a licensed senior reactor operator must be in the control room at all times, and a licensed reactor operator or senior operator must be present "at the controls" at all times.

10 CFR 50.55a(h) *Protection and safety systems* – incorporates requirements of IEEE 279 and IEEE 603-1991 (plus correction sheet dated January 30, 1995) for plants constructed after January 1, 1971 – protection systems must meet the requirements in either IEEE 279 or IEEE 603-1991.

IEEE 603-1991 *Criteria for Protection Systems for Nuclear Power Generating Stations* – includes requirements on control room indication and manual control:

- Displays needed for manual protective actions must be part of the safety systems (thus qualified) and must meet requirements of IEEE 497-1981 (5.8.1)
- Safety system status indication must be provided, but need not be part of the safety system (5.8.2)
- Continued indication of bypasses must be provided but need not be part of the safety system; requires automatic activation of this display under certain circumstances, and requires capability to manually activate the indication at any time (5.8.3)
- Requires that information displays be accessible to the operator, and displays for manually controlled protective actions be visible from the location of the controls used to effect the actions (5.8.4)
- "Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988." (5.14)
- Requires capability in the control room to implement manual initiation at the division level of the automatically initiated protective actions; minimize the number of discrete operator manipulations required consistent with redundancy requirements (6.2.1)

- Requires capability in the control room to manually initiate and control protective actions not selected for automatic control (6.2.2)
- Requires capability to implement manual actions necessary to maintain safe conditions after the protective actions are completed, with the associated displays and controls located in areas that are accessible, in a suitable environment, and suitably arranged for operator surveillance and action (6.2.3)

NRC Expectations

NUREG-0737 Supplement 1, *Clarification of TMI Action Plan Requirements* – clarifies post-TMI requirements of NUREG-0737, including the Safety Parameter Display System (SPDS), Reg. Guide 1.97 application to emergency response facilities, upgraded emergency operating procedures (EOPs), and Emergency Response Facilities (ERF) – ERF include Technical Support Center (TSC), Operational Support Center (OSC), and Emergency Operations Facility (EOF).

Regulatory Guide 1.47 *Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems* – describes an acceptable way to meet IEEE 279 requirements – includes:

- Indication should be at the system level (regardless of whether indication is also provided at the component or channel level)
- The indication should be activated automatically when a bypass or other inoperability is induced deliberately for the protection system, the system it actuates to perform safety-related functions, or any auxiliary or supporting system that effectively bypasses or renders inoperable the protection system or actuated systems
- States the conditions under which such automatic activation must be provided based on expected frequency of occurrence and need for the affected system to be operable when it occurs
- Manual capability should exist in the control room to activate each system-level indicator (allows the operators to activate it when a condition occurs that is not automatically sensed and thus does not automatically activate the indication).

Regulatory Guide 1.97 Rev. 3 Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident – describes an acceptable method to meet regulatory requirements as they relate to post-accident monitoring instrumentation, based in part on ANSI/ANS-4.5-1980 – includes:

- Defines types of variables to be monitored and lists specific variables of each type, along with associated ranges, for BWRs and PWRs
- Defines categories of instrumentation, specifies what category should be used for each variable, and identifies design and qualification criteria for each category; criteria cover equipment qualification, redundancy, power source, channel availability, quality assurance, display and recording, range equipment identification, interfaces, servicing, testing and calibration, human factors, and direct measurement criteria.

- Human factors criteria are the same for all categories: instrumentation should be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules; instrumentation design should minimize conditions that would cause anomalous indications; human factors analysis should be used in determining type and location of displays; and to the extent practicable, the same instruments should be used for accident monitoring as are used for normal operation.
- Calls for "continuous real-time display" for Category 1 instrumentation; allows signals to be "processed for display on demand" for Categories 2 and 3.

NUREG-0800 Chapter 7, Branch Technical Position (BTP) HICB-10, *Guidance on Application of Regulatory Guide 1.97* – provides supplemental guidance that clarifies the Staff position and identifies alternatives acceptable to the Staff for satisfying the guidelines identified in Reg. Guide 1.97.

Regulatory Guide 1.62 *Manual Initiation of Protective Actions* – describes an acceptable way to meet IEEE 279 requirements on manual initiation at the system level – includes:

- Means should be provided for manual initiation of each protective action at the system level, regardless of whether means are also provided to initiate at the component or channel level
- Manual initiation should perform all actions performed by automatic initiation (e.g., including valve sequencing, interlocks, etc.)
- Switches for manual initiation should be located in the control room and be easily accessible to the operator so that action can be taken in an expeditious manner
- The amount of equipment common to both manual and automatic initiation should be kept to a minimum and no single failure within the manual, automatic, or common portions should prevent initiation
- Manual initiation should depend on the operation of a minimum of equipment
- Manual initiation should be designed to go to completion.

Regulatory Guide 1.153 Rev. 1, *Criteria for Safety Systems* – endorses IEEE 603-1991; references Reg. Guide 1.97 Rev. 3 as acceptable method of meeting requirements for accident monitoring instrumentation, as opposed to IEEE 497-1981 referenced in IEEE 603. Also, in Section D, Implementation, it states that in addition to review of applications for new plants, this regulatory guide "…will also be used to evaluate submittals from operating reactor licensees who voluntarily propose to initiate system modifications if there is a clear nexus between the proposed modifications and this guidance."

NUREG-0800 Chapter 7, Appendix 7.1-C, *Guidance for Evaluation of Conformance to IEEE Std 603*, item 13 states that: "The review of information displays should…confirm that the information displayed and the characteristics of the displays (e.g., location, range, type, and resolution) support operator awareness of system and plant status and will allow plant operators to make appropriate decisions."

Regulatory Guide 1.114 Rev. 2, *Guidance to Operators at the Controls and to Senior Operators in the Control Room of a Nuclear Power Unit* – describes an acceptable method for meeting the regulations requiring presence of an operator at the controls and a senior operator in the control room. Includes, among other items, the following provisions that have implications for control room and workstation design:

- Describes intent of the regulations (section B – Discussion).
- States that the operator at the controls "should have an unobstructed view of and access to the operational control panels, including instrumentation displays and alarms, to be able to initiate prompt corrective action when necessary on receipt of any indication (instrument response or alarm) of a changing condition." Defines operational control panels as "control panels that enable the operator at the controls to perform required manual safety functions and equipment surveillance and to monitor plant conditions under normal and accident conditions."
- States that the senior operator in the control room "is expected to spend most of the time in that portion of the control room where there is direct and prompt access to information on current unit conditions and where the senior operator can directly supervise and communicate with the operator at the controls."
- States that the senior operator can move briefly to other areas of the control room but must remain in the control room "in sight of or in the audible range of the reactor operator at the controls, or in the audible range of the control room annunciators."

Guidance

IEEE 497-2002, *IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations* – provides updated criteria for post-accident monitoring instrumentation intended to apply a more flexible and less prescriptive approach for identifying variables to be monitored and associated qualification requirements, and to address use of advanced instrumentation designs and solutions using modern digital technology. Not endorsed by NRC, but can be used as a source of information and criteria for digital post-accident monitoring systems.

► **Section 5.2.5**, **Section 6.4**

4. Operator Licensing

Regulatory Requirements

10 CFR 55, *Operators' Licenses*

- 10 CFR 55.45, *Operating tests* – describes operating tests to be administered using the plant-referenced simulator (55.46), another simulation facility approved for this use by NRC, or the plant if approved for the testing by NRC
- 10 CFR 55.46, *Simulation facilities* – describes how to request approval for simulation facilities other than plant-referenced simulator; gives requirements for plant-referenced simulator scope and fidelity ("Simulator fidelity has been demonstrated so that significant

control manipulations are completed without procedural exceptions, simulator performance exceptions, or deviation from the approved training scenario sequence."); requirements for continued assurance of simulator fidelity via performance testing (no mention of plant modifications)

10 CFR 55.59, Requalification

- Gives requirements for operator requalification program (requires NRC approval), and operators to be requalified via written examination and annual operating test
- Gives detailed list of tasks/scenarios to be tested in requal's
- Indicates "a simulator may be used in meeting the requirements…if it reproduces the general operating characteristics of the facility involved and the arrangement of the instrumentation and controls of the simulator is similar to that of the facility involved"
- Gives similar requirement regarding simulator used for "observation and evaluation of the performance and competency…" – I&C must "closely parallel" that of the facility involved.

NRC Expectations

Regulatory Guide 1.8 Rev. 3 *Qualification and Training of Personnel for Nuclear Power Plants* – endorses ANSI/ANS-3.1-1993, "Selection, Qualification, and Training of Personnel for Nuclear Power Plants" with some exceptions/clarifications (not germane here).

Regulatory Guide 1.149 Rev. 3 *Nuclear Power Plant Simulation Facilities for Use in Operator Training and License Examinations* – endorses ANSI/ANS-3.5-1998, including its provisions "for upgrading simulators to reflect changes to reference plant response or control room configuration." Exceptions/clarifications do not have impact here.

NUREG-1220 Rev. 1 *Training Review Criteria and Procedures* – gives criteria for evaluation of training programs including simulator training – no specific information or criteria on simulator fidelity.

Guidance

ANSI/ANS-3.5-1998 Requirements for simulators used for operator training, testing and requalification

- Requires a "training needs assessment" for any deviations between simulator and reference plant (4.2.1.4)
- Requires that "reference unit modifications determined to be relevant to the training program shall be implemented on the simulator within 24 months of their reference unit in-service dates, or earlier if warranted by a training needs assessment."

► **Section 6.3**

5. Failure Analysis and Dependability Evaluations for Digital I&C Systems

Regulatory Requirements

No specific requirements for digital systems – just those addressing I&C and protection systems in general.

NRC Expectations

NUREG-0800 Chapter 7, Appendix 7.0-A, Review Process for Digital Instrumentation and Control Systems.

Regulatory Issue Summary (RIS) 2002-22, Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule" – endorses TR-102348/NEI 01-01 for both design and licensing of digital I&C systems, including its discussion on use of failure analysis and methods for demonstrating adequate dependability of digital I&C systems.

Guidance

EPRI TR-102348 Rev. 1/NEI 01-01

► **Section 5.2.2**

► **Section 5.2.4**

6. Defense-in-Depth and Diversity (D3) Evaluations

Regulatory Requirements

The D3 evaluation addresses the potential for common cause failure of digital protection systems, which is a "beyond design basis" concern. There is no specific regulatory requirement, other than the basic requirements for reliability and independence of protection systems – see NUREG-0800 Chapter 7, BTP/HICB-19 for a list of these.

NRC Expectations

SECY 93-087, Staff Requirements Memorandum – describes the NRC position on defense-in-depth and diversity.

NUREG-0800 Chapter 7, Appendix 7.0-A, *Review Process for Digital Instrumentation and Control Systems* – indicates that NRC expects a D3 evaluation to be performed for digital upgrades "…that involve a reactor trip system (RTS) or an engineered safety features actuation system (ESFAS)…"

NUREG-0800 Chapter 7, BTP/HICB-19, *Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems:*

- Describes the NRC position on the potential for common cause failure of digital systems ("software common mode failure") and the need for a D3 evaluation to assess the vulnerability to such failures and how they would be mitigated.
- Indicates when a D3 evaluation should be performed and provides criteria for judging acceptability of the results – criteria are more relaxed than those applied to the licensing basis analyses described in the SAR and allow use of best-estimate methods and assumptions.
- Allows reliance on manual operator actions as part of mitigating the events evaluated in the D3 assessment, as long as the operator has sufficient information and time to take the action – the HSI used for this purpose may be non-safety related, as long as it is not subject to the same common cause failure.
- For new plants, states in item 4 of the NRC four-point position on D3: "A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above."
- States that: "*Human-factors engineering principles and criteria should be applied to the selection and design of the displays and controls. The human-performance requirements should be described and related to the plant safety criteria. Recognized human-factors standards and design techniques should be employed to support the described human-performance requirements.*"

Guidance

NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems* – presents details on the method for performing the D3 evaluation described in BTP-19, and includes discussion of different types of diversity and how they might be combined to demonstrate adequate overall diversity

EPRI 1002835, *Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades* – this guideline, which is expected to be completed in 2004 and sent to NRC for review and potential endorsement, provides guidance on performing D3 evaluations using any of three methods including an extended deterministic method based largely on BTP-19, and two alternative risk-informed methods using risk insights from the plant PRA to perform the evaluation.

► **Section 5.2.3**

7. Remote Shutdown

Regulatory Requirements

10 CFR 50 Appendix A – General Design Criteria:

- GDC 19, *Control room* – in addition to the main control room, requires equipment at appropriate locations outside the control room with capability for prompt hot shutdown of the reactor and necessary instrumentation and control to maintain the unit in a safe condition during hot shutdown, and with potential capability for subsequent cold shutdown.

10 CFR 50 Appendix R, *Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979:*

- Requires alternative or dedicated safe shutdown capability in the event of a fire in the control room and provides specific requirements for this capability.

NRC Expectations

Regulatory Guide 1.101 Rev. 4 *Emergency Planning and Preparedness for Nuclear Power Reactors* – endorses any of three methods for meeting 10 CFR 50.47 and defining Emergency Action Levels (EALs): NUREG-0654/FMA-REP-1, NUMARC/NESP-007, or NEI 99-01 (Rev. 4, January 2003).

Guidance

None identified.

8. Emergency Plans and Notifications

Regulatory Requirements

10 CFR 50.47 *Emergency plans* – basic requirements for emergency plans, including requirement for “a standard emergency classification and action level scheme” (10 CFR 50.47(b)(4)).

10 CFR 50 Appendix E *Emergency Planning and Preparedness for Production and Utilization Facilities* – establishes minimum requirements for emergency plans – requires that emergency action levels be described as part of plan content.

10 CFR 50.72 *Immediate notification requirements for operating nuclear power reactors*:

- Requires immediate (<1 hr) notification of declaration of any of the emergency classes in the emergency plan.
- For non-emergency events, requires: 1-hour report of any deviation from Tech Specs, 4-hour report of any initiation of shutdown required by Tech Specs, or demand for reactor trip or ECCS actuation, and 8-hour report of any of a number of other conditions including “any event that results in a major loss of emergency assessment capability, offsite response capability, or offsite communications capability (e.g., significant portion of control room indication, Emergency Notification System, or offsite notification system).”

NRC Expectations

Regulatory Guide 1.101 Rev. 4 *Emergency Planning and Preparedness for Nuclear Power Reactors* – endorses any of three methods for meeting 10 CFR 50.47 and defining Emergency Action Levels (EALs): NUREG-0654/FMA-REP-1, NUMARC/NESP-007, or NEI 99-01 (Rev. 4, January 2003).

Guidance

NUREG-0654/FEMA-REP-1, *Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants:*

- Provides Emergency Action Level guidelines, and lists in Appendix 1 example initiating conditions
- For Notification of Unusual Event, lists: "Indications or alarms on process or effluent parameters not functional in control room to an extent requiring plant shutdown or other significant loss of assessment or communication capability (e.g., plant computer, Safety Parameter Display System, all meteorological instrumentation)"
- For declaration of an Alert, lists the initiating condition: "Most or all alarms (annunciators) lost."

NEI 99-01 (Rev. 4), *Methodology for Development of Emergency Action Levels*:

- Gives overall guidance on EALs, defines terms, and lists Initiating Conditions and corresponding EALs for all four Emergency Classes
- Calls for a Notice of Unusual Event if there is an "unplanned loss of most or all safety system annunciation or indication in the control room for greater than 15 minutes" during certain modes of operation; this escalates to higher emergency classes if a transient is in progress and/or backup instrumentation is not available
- Discusses what "most" means, and provides some additional guidance
- Points out that loss of indications may cause an LCO to be reached per Tech Specs

9. Changes to Risk-Important Human Actions

Regulatory Requirements

10 CFR 50.55a(h), *Protection and safety systems* – incorporates requirements of IEEE 279 and IEEE 603-1991 (plus correction sheet dated January 30, 1995) for plants constructed after January 1, 1971 – protection systems must meet the requirements in either IEEE 279 or IEEE 603-1991.

IEEE 603-1991, *Criteria for Protection Systems for Nuclear Power Generating Stations* – requirements related to manual protective actions – see discussion under 3 HSI Design.

NRC Expectations

Regulatory Guide 1.153 Rev. 1, *Criteria for Safety Systems* – endorses IEEE 603-1991.

NRC Information Notice (IN) 97-78, Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times.

- Describes several instances in which operator actions were substituted or modified without adequate consideration of human performance issues and potential for operator errors of omission or commission, and which the NRC concluded represent changes to the licensing basis for which prior NRC review and approval should have been obtained per 10 CFR 50.59
- Discusses the need for careful analysis of these types of changes including potential human errors, and describes what an NRC review of such a change would consider.

NUREG-0800 Chapter 18, II.C, Review of HFE Aspects of Modifications Affecting Risk-Important Human Actions

- Uses both qualitative and quantitative risk factors to place the change into one of three categories, and defines the levels of review to be performed for each category
- Consistent with Reg. Guide 1.174 for risk-informed licensing submittals (NRC will use this risk categorization method regardless of whether the licensee uses risk insights in their submittal – see the section of this Roadmap on Risk-Informed Licensing Submittals)

NUREG-1764, *Guidance for the Review of Changes to Human Actions* – provides detailed guidance and basis for NUREG-0800 Chapter 18, II.C review criteria.

Guidance

► **Section 5.2.6**

► **Section 5.3**

10. Risk-Informed Licensing Submittals

Regulatory Requirements

None

NRC Expectations

Regulatory Guide 1.174 Rev. 1, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis:*

- Describes an approach for assessing any licensing basis changes that are supported by risk information

- Provides acceptance criteria based on the change in Core Damage Frequency and Large Early Release Frequency, as compared to the values prior to the change, plus other criteria including maintaining adequate defense in depth, adequate PRA quality, and others.

Guidance

EPRI 1002835 *Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades; Applying Risk-Informed and Deterministic Methods:*

- Provides guidance on performing these assessments using any of three methods: extended deterministic method (based largely on BTP-19), a standard risk-informed method (using updated PRA and Reg. Guide 1.174 acceptance guidance), and a simplified risk-informed (using existing PRA and Reg. Guide 1.174 acceptance guidance).
- This guideline is expected to be completed in 2004 and to be sent to NRC for their review and potential endorsement.

► **Section 5.2.6**

11. Technical Specifications and LCOs

Regulatory Requirements

10 CFR 50.36, *Technical Specifications* – contains basic requirements for Tech Specs and LCOs

10 CFR 50.72, *Immediate notification requirements for operating nuclear power reactors*:

- Requires immediate (<1 hr) notification of declaration of any of the emergency classes in the emergency plan
- For non-emergency events, requires: 1-hour report of any deviation from Tech Specs, 4-hour report of any initiation of shutdown required by Tech Specs, or demand for reactor trip or ECCS actuation, and 8-hour report of any of a number of other conditions including "any event that results in a major loss of emergency assessment capability, offsite response capability, or offsite communications capability (e.g., significant portion of control room indication, Emergency Notification System, or offsite notification system)."

NRC Expectations

None identified.

Guidance

Standard Technical Specifications for each reactor type – these list standard Tech Specs, LCOs and associated actions. For instrumentation, limited primarily to safety function actuations plus post-accident monitoring:

- NUREG-1430 B&W plants
- NUREG-1431 Westinghouse plants
- NUREG-1432 CE plants
- NUREG-1433 and NUREG-1434 GE BWR plants

6
SPECIAL TOPICS RELATED TO OPERATIONS AND MAINTENANCE

In developing the guidance given in this document on modernization planning (Section 2), design process (Section 3), detailed HFE guidelines (Section 4), and licensing (Section 5), a number of topics were identified for which guidance was needed but did not fit directly into any of the previous sections, or which cut across the subjects that are covered there. Guidance to address these additional topic areas is provided in this section, as described briefly below:

Human Factors Engineering for the Maintenance of Digital Systems (Section 6.1) – A key driver for the transition from analog to digital systems is the potential for reduced operations and maintenance costs. These reductions may be in the form of labor savings, hardware savings, or reduced threats to plant availability or safety during maintenance operations. For digital systems to achieve these improvements in the most cost efficient manner, maintainability must be emphasized in all phases of the design process. This section provides human factors guidance for the maintenance of digital systems, the effects of I&C modernization on maintenance of human system interfaces, and special considerations for the design of maintainers' HSIs. It provides:

- Guidance on the new or changed maintenance tasks and responsibilities that come with a digital upgrade and how the new maintenance needs can be integrated into existing plant maintenance practices.
- Guidance on what features should be included in a modification to minimize the impact on plant maintenance tasks and, in addition, potentially improve the performance of those maintenance tasks.

These guidelines do not address what is commonly referred to as "software maintenance." The maintenance of software related to the HSI is similar to maintenance of other plant software used for operation and control. The focus here is on maintenance of plant and control system hardware.

Human Factors Engineering for Configuration Management (Section 6.2) – Digital I&C systems and computer-based control and display systems present new capabilities for flexible information processing and presentation and new challenges for configuration management of information display. This section provides guidance to ensure that these capabilities and challenges are managed in a way that is governed by good human factors engineering principles and that supports effective use of the information and the associated HSIs. Specifically, this section addresses:

- Those aspects of configuration management of a digital upgrade modification that may affect the performance of human tasks at the system interfaces

- HSI features that can be configured by the operators and other users, e.g., special displays or selectable alarms. Those features are not part of the plant's configuration management system per se; however, they are important to the tasks that are performed at the human-system interfaces. This section addresses the human factors issues in controlling the configuration and use of these user-definable features.

Training Considerations Unique to Digital I&C Modernization Programs (Section 6.3) – New digital I&C and computer-based HSIs will impose new demands on training programs to address their operation and maintenance. The new systems may significantly alter the way tasks are performed and may result in new tasks for which training needs to be developed. Two unique aspects need to be considered:

- New issues that need to be addressed in training related to the impact of digital I&C and computer-based HSIs on operations and maintenance
- Managing and scheduling changes to the simulator while supporting training and qualification of the operators on the existing and modified designs, especially when changes extend over multiple outages and multi-unit plants are involved.

This section addresses the training considerations related to new digital I&C systems and computer-based HSIs.

Safety Monitoring and Control in Modernized Control Rooms (Section 6.4) – In most plants there are many different systems that have HSI aspects related to monitoring and control of plant safety functions, including SPDS, PAMS (PAMI), RPS (RTS), ESFAS, and BISI. There has not been a uniform or consistent approach applied to the design of these HSIs. As a result, they tend to be separate and isolated systems, some of which are rarely used and may not follow the conventions of the other control room HSIs. Also, the regulatory guidance applicable to these areas was written long ago and was based primarily on the analog technology prevalent in control rooms at that time. With I&C and HSI modernization, better and more integrated approaches are possible.

Section 6.4 also considers the need to provide diverse HSI capabilities that allow the operators to cope with postulated failures or degradation of the HSIs that are normally used, while still providing a well-integrated HSI for both normal and emergency plant operating conditions.

6.1 Human Factors Engineering for the Maintenance of Digital Systems

6.1.1 Overview

6.1.1.1 Purpose and Scope

6.1.1.2 Maintenance Tasks and Human Factors Engineering

6.1.1.3 Impact of Digital Upgrades on Maintenance

6.1.1.4 Section Content and Organization

6.1.2 Maintainability Checklist

6.1.3 General Design for Maintainability

6.1.3.1 Maintenance-Related Tasks

- 6.1.3.2 Redundant Components and Hot Spares
- 6.1.4 Detailed Design Features for Maintainability
- 6.1.5 Diagnosis and Testing
  - 6.1.5.1 Self-Diagnosis
  - 6.1.5.2 Error Detection and Indication
  - 6.1.5.3 Application Level Testing
- 6.1.6 Maintenance Performance
  - 6.1.6.1 Maintenance Tools
  - 6.1.6.2 Security
  - 6.1.6.3 Maintenance Personnel Responsibility
- 6.1.7 Maintainability in Procurement and Plant Changes
- 6.1.8 Sources of Additional Information
  - 6.1.8.1 Reference List
  - 6.1.8.2 Reference Content and Use

6.1.1 Overview

6.1.1.1 Purpose and Scope

This section provides human factors guidance for the maintenance of digital systems, and the affects of I&C modernization on maintenance of operator human system interfaces and special considerations for the design of maintainers' HSIs. It provides:

- Guidance on the new or changed maintenance tasks and responsibilities that come with a digital upgrade and how the new maintenance needs can be integrated into existing plant maintenance practices; and
- Guidance on what features should be included in a modification to minimize the impact on the plant maintenance tasks and, in addition, potentially improve the performance of those maintenance tasks.
- These guidelines do not address what is commonly referred to as "software maintenance." The focus is on maintenance of plant and control system hardware. The maintenance of the software related to the HSI is not different from the activities to maintain the other plant software for operation and control. Consequently, this section will not cover software maintenance as a separate subject.
- A key driver for the transition from analog to digital systems is the potential for reduced operations and maintenance costs. These reductions may be in the form of labor savings, hardware savings, or reduced threats to plant availability or safety during maintenance operations. However, features to improve maintainability are very costly to back-fit. For digital systems to achieve these improvements in the most cost efficient manner, maintainability must be formally emphasized in all phases of the design process. Irrespective of the potential improvements in maintainability, the maintenance of digital I&C systems will be markedly different from the maintenance of the conventional analog systems that they replace. Accordingly, instituting a digital upgrade will impact a plant's existing maintenance program and change the tasks performed at the HSIs.

6.1.1.2 Maintenance Tasks and Human Factors Engineering

This section emphasizes the aspects of the digital modification that directly affect what the operators and technicians do at the interfaces with the system. However, it will also address more general maintenance issues where the unique features of a digital upgrade have the potential to make significant changes to the existing plant maintenance practices.

Maintenance tasks tend to fall into the following broad categories and generally take place in the order indicated.

- Detection or Initiation Tasks – recognizing that equipment is not operating as intended for corrective maintenance or establishing that the time of operation or similar criterion for action has been reached for preventive maintenance,
- Diagnosis Tasks – establishing the specific condition that must corrected and determining the maintenance activities that must be performed,
- Preparation Tasks – removing equipment or systems from service or placing them in a condition that the maintenance can be performed,
- Performance Tasks – performing the maintenance,
- Confirmation Tasks – establishing that the maintenance has been correctly completed,
- Restoration Tasks – putting equipment or systems back in service or configuring them for normal operation, and
- Monitoring Tasks – establishing whether the maintenance was successful.

The guidance in this section will generally apply to one or several of these broad categories of maintenance tasks. For example, many of the guidelines on design features for testing are directly related to detecting that maintenance is needed and determining what maintenance should be performed. Testing features can also be used to confirm that the maintenance has been completed correctly. Guidelines relative to bypasses and interlocks are important to the preparation for and restoration from maintenance. Obviously, many design features such as those related to access, labeling, modularization, etc. have direct impact on the performance of the maintenance tasks. It should be recognized that these tasks are not all performed by maintenance technicians, the plant operators will also perform some of the tasks related to detection, preparation, and restoration. Engineering support will be particularly important in the diagnosis and monitoring tasks.

Many of the human factors principles and guidance for the operational interfaces are also applicable to interfaces utilized for maintenance. For example, labels and terminology need to be clear, population stereotypes need to be followed, anthropometric limits need to be respected, etc. In general, the human factors guidance in other sections of these guidelines and in other sources for system operational interfaces should be applied to system maintenance interfaces. Although human factors analyses may not be needed for the design of many maintenance interfaces, those techniques can and should be used to resolve human factors issues or uncertainties with maintenance task performance. Note that there may be maintenance tasks that are implicit or even explicitly considered in risk assessment, for example, time to repair a component. Those tasks may need a formal human factors evaluation to substantiate assumptions on their performance that have been made in other analyses.

A significant problem in applying sound human factors principles to maintenance tasks is to identify the tasks in a systematic fashion early enough in the design process that correction of human factors problems can be practically accomplished. This requires that any additional practices for maintenance-related interfaces be an integral part of the human factors design guidelines that are applied to the digital upgrade and that maintenance-related activities be included in human factors reviews.

6.1.1.3 Impact of Digital Upgrades on Maintenance

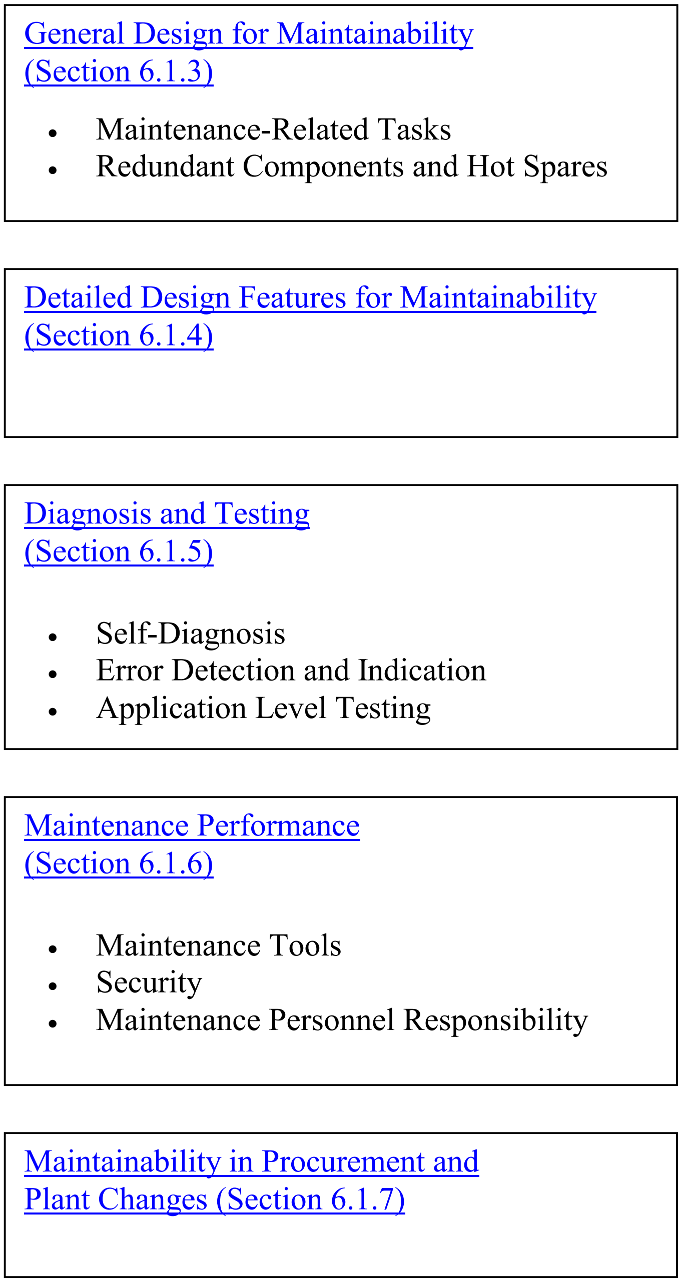
In a digital upgrade program it is essential that maintenance be considered from the very beginning of the project. For example, the endpoint vision should identify those improvements in maintenance that the program intends to institute, such as on-line testing, standardization of modules, and operator aids for maintenance. The planning will need to outline how the maintenance of the new equipment will be phased in and co-exist with the maintenance of equipment that is not modified. Trained personnel and equipment to service the existing analog systems will still be needed while new skills, procedures, and equipment will be needed for the digital equipment. Poorly designed maintenance interfaces can defeat the improvements in operation that can be achieved by a digital upgrade modification.

6.1.1.4 Section Content and Organization

The general arrangement of this section is shown schematically in Figure 6-1.

The first two parts of this section provide guidance on general and detailed design features needed to provide for maintenance in digital system upgrades. These discussions of design features are followed by discussions of diagnosis, testing, and other maintenance performance activities, including maintenance tools. The guidelines address how the plant maintenance program may need to be changed to accommodate the new digital systems. Guidance on incorporating the maintenance-related human factors guidance in procurement and change packages is also provided.

The information in these guidelines focuses on the major human factors aspects of those maintenance-related tasks performed at the HSIs that may be involved in a digital upgrade modification. However, the guidelines presented in this section may be only a fraction of the total number of maintenance-related design guidelines that could figure in a particular modification. Because of the wide range of possible modifications and the large number of potential guidelines, it is impractical for this section to include every detailed design guideline related to maintenance that may prove to be applicable. Some of that detailed design guidance will already be represented by the existing plant maintenance practices and design features and they should generally be followed. If those existing practices do not adequately cover the modified design, there is a relatively limited group of key references that present very comprehensive guidance on maintainability. It is expected that the information in these references will be used as necessary to establish the detailed design features of a modification to achieve high maintainability. To assist the guideline user in accessing this large amount of additional and more general information, Section 6.1.8 discusses the material in each of these key references and describes how they may be applicable to the design of a digital upgrade modification. In addition to the existing references discussed in Section 6.1.8, an EPRI report is in preparation (Reference 9) that covers many of the subjects covered in these guidelines in more detail and, in addition, provides guidance on the broader design aspects of a digital upgrade modification.



General Design for Maintainability (Section 6.1.3)

- Maintenance-Related Tasks
- Redundant Components and Hot Spares

Detailed Design Features for Maintainability (Section 6.1.4)

Diagnosis and Testing (Section 6.1.5)

- Self-Diagnosis
- Error Detection and Indication
- Application Level Testing

Maintenance Performance (Section 6.1.6)

- Maintenance Tools
- Security
- Maintenance Personnel Responsibility

Maintainability in Procurement and Plant Changes (Section 6.1.7)

Figure 6-1
Maintainability

6.1.2 Maintainability Checklist

The purpose of this checklist is to summarize the guidance in the remainder of this section in a concise form. It provides a way for a user who is familiar with maintenance and digital upgrade designs to rapidly establish the portions of the broad subject of maintenance that need special attention. It references the specific portion of these guidelines that applies. Citations to specific portions of the other extensive detailed guideline information that is available in the references for this section are not provided in the checklist. It is expected that the User of this document will have directly available the major applicable references discussed in Section 6.1.8. These references, particularly the explanations that they very often provide, will be useful for the development of the detailed design features and to identify specific requirements that need to be incorporated in procurement-related documents. As discussed further in Section 6.1.8, there are extensive detailed checklists in Reference 6. These checklists may be used to ensure that maintenance-related issues are adequately considered.

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
6.1.3	General Design for Maintainability							
	6.1.3.1	Maintenance-Related Tasks						
		=>	6.1.3.1-1	Human factors analyses that are used to support the design of the human-system interface used for the upgraded system should include maintenance-related tasks as well as tasks needed to operate the modified systems.				
	6.1.3.2	Redundant Components and Hot Spares						
		=>	6.1.3.2-1	For redundant components in hot standby configurations, there should be unambiguous indication of which component is operating and which is in standby.				
		=>	6.1.3.2-2	Testing of redundant equipment should include testing to confirm all potential fail-over and recovery situations.				
		=>	6.1.3.2-3	Alarms should be provided for any processor failure, prioritized based on consistent criteria, and clearly presented to the operators or maintenance technicians who have to take action.				
		=>	6.1.3.2-4	Where modules are installed in the system as “hot spares,” the maintenance procedures and labeling should distinguish the installed hot spares from the primary operating modules.				
6.1.4	Detailed Design Features for Maintainability							
	=>	6.1.4-1	The system, module or equipment should provide indication to technicians and operators that modules have been inserted into the correct slot or rack location.					

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	6.1.4-2	Modules should not normally have configuration jumpers, switch settings or uniquely embedded software that must be configured prior to putting that module into operation. Where that cannot be avoided, the operating system software should confirm that these settings are correct.				
	=>	6.1.4-3	Different interfaces (e.g. connectors, fittings, etc.) should be provided for each type of test or service equipment to minimize the likelihood of error.				
	=>	6.1.4-4	The I/O module terminations should accommodate the testing tasks, and the field connections should not introduce unreliability or trouble shooting complexity.				
	=>	6.1.4-5	Blown fuses, or open circuits of any kind, should be automatically detected and reported by the system diagnostics. The system's HSI should direct maintenance personnel to the specific point affected.				
	=>	6.1.4-6	All modules should have readily observable indications to show that the module is operational.				
	=>	6.1.4-7	For I/O modules, front panel indicators should distinguish unused points. They should not be displayed with a particular status or error state. Where this is not possible, other labeling means should be used to clearly indicate that these points are not in use.				
	=>	6.1.4-8	When output modules are configured to go to a predetermined state or to freeze as-is on failures of the controlling CPU or failure of the communication to the controlling CPU, appropriate information on failure state should be displayed to maintainers and operators in addition to information that there has been a failure.				
	=>	6.1.4-9	All modules should have labels that are keyed to system documentation.				
	=>	6.1.4-10	Module labels or cabinet maps should be such that they can be correctly updated as an integral part of any system design change.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	6.1.4-11	If geographically distributed components are used, the digital platform and system should provide communication and operation diagnostics, automatic fault detection, isolation capability, and appropriate indication to maintenance technicians and operators. The system's centrally located HSI should clearly diagnose failures to the replaceable module level.				
	=>	6.1.4-12	Displays should be configured to show system errors in graphic format. The self-diagnostic features of the platform should isolate a problem down to the component level (e.g. specific module I/O point).				
	=>	6.1.4-13	Local controls should be provided to permit component maintenance operations without the coordination between remote and local personnel.				
	=>	6.1.4-14	Local controls should include switches to disconnect all remote control actuation symbols. Adequate indications of alarms should be provided in the main control room to ensure operators are aware that they have lost control of that component.				
	=>	6.1.4-15	If remote switches are located in the main control room, additional isolation and transfer/disconnect capability for these control interfaces should be provided.				
	=>	6.1.4-16	Failed sensors in safety monitoring systems should be alarmed and logged and the out-of-service times monitored for technical specification compliance.				
	=>	6.1.4-17	Protection system bypasses should have controls to ensure they are not implemented in a way that can totally bypass all trip and actuation functionality.				
	=>	6.1.4-18	Administrative controls and security access restrictions such as passwords or key locks should be built into the system to control the use of bypasses.				
	=>	6.1.4-19	Bypasses should be clearly indicated and alarmed.				
	=>	6.1.4-20	Where plants are vulnerable to spurious trips and actuations until a bypass is manually activated, the HSI associated with activating and displaying bypasses should be easily and quickly accessible by plant operators.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	6.1.4-21	If a value is substituted in a calculation, then the calculated result should have a clearly distinguishable quality flag. Such a substitution should be treated as a bypass and the previous guidelines should be applied.					
6.1.5	Diagnosis and Testing							
	6.1.5.1	Self-Diagnosis						
		=>	6.1.5.1-1	Malfunction messages should be displayed at the HSIs and archived.				
	6.1.5.2	Error Detection and Indication						
		=>	6.1.5.2-1	The digital platform should provide the capability to automatically detect and indicate the following out-of-service conditions. However, since the functional impairment is different for each of these conditions, distinct indication should be provided.				
		=>	6.1.5.2-2	For important control or protection applications, out-of-range detection should be provided.				
		=>	6.1.5.2-3	In digital platforms, CPU and communication should incorporate error detection methods at power up and at the request of the operator.				
		=>	6.1.5.2-4	Where communication redundancy is employed, the method and coverage of automatic error detection and self-testing of these peripheral devices should be carefully reviewed; manual testing is sometimes required.				
		=>	6.1.5.2-5	The determination of the significance of errors and how they are alarmed or presented should be consistent across the various digital platforms.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	6.1.5.2-6	In redundant systems, sustained faults should be alarmed. Operators should be able to acknowledge the alarm, but the alarm should remain activated until the system becomes operable again.				
		=>	6.1.5.2-7	If the plant general alarm system employs multiple levels of alarm prioritization, the process effect of each error should be consistent with the plant's general alarm prioritization criteria.				
		=>	6.1.5.2-8	Out-of-service indications should be provided at the normal control location as an integral part of the component status display in all formats for which that status is displayed.				
		=>	6.1.5.2-9	Out-of-service conditions should be alarmed at the normal control location to ensure operators are aware of the abnormal event and the conditions should be logged in the plants historical recording system.				
		=>	6.1.5.2-10	The capability to manually identify an out-of-service condition for any plant component should be provided.				
		=>	6.1.5.2-11	The capability for operators and maintenance personnel to manually enter notes regarding the out-of-service conditions should be provided.				
		=>	6.1.5.2-12	In addition to the out-of-service condition, component position status should always be displayed.				
		=>	6.1.5.2-13	The human system interfaces should not combine detailed information needed by diagnostic technicians into the same set of displays as are used by the end-users.				
		=>	6.1.5.2-14	Replacement modules should require a minimum of special handling precautions.				
		=>	6.1.5.2-15	Replacing equipment should not create a hazardous condition for technicians or equipment.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	6.1.5.3		Application Level Testing					
		=>	6.1.5.3-1	Where customized application level testing is required, test features should be built into the system so that all tests can be conducted without the addition of temporary modifications, such as shorting contacts or opening circuit loops.				
		=>	6.1.5.3-2	Procedures and interlocks should be provided to ensure the system is in an acceptable bypassed mode before allowing manual tests to be initiated. Operations personnel should be provided with indications that the bypasses have been instituted.				
		=>	6.1.5.3-3	Tests of output devices should normally be manually initiated. The HSI should be specifically designed for the testing to be conducted and should not contain other unrelated information that can cause confusion and errors.				
		=>	6.1.5.3-4	For output interface tests, adequate indication and interlocks to avoid spurious plant disturbances should be provided.				
		=>	6.1.5.3-5	Digital platforms should provide the capability of taking inputs and outputs out-of-scan, and the ability to manually insert values for testing. When points are out-of-scan there must be clear indication that a value has been manually inserted.				
		=>	6.1.5.3-6	To ensure points are not unintentionally left in an out-of-scan condition summary displays should provide a listing of all points utilizing substituted values. If a value is manually substituted for a true process input, then calculated results should have a clearly distinguishable quality flag.				
		=>	6.1.5.3-7	System security features, such as passwords or keylocks, should ensure forced value functionality, e.g., taking a point out-of-scan, is only available to authorized users.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
6.1.6	Maintenance Performance							
	6.1.6.1	Maintenance Tools						
		=>	6.1.6.1-1	Digital platform maintenance tools should be available only at designated workstations.				
		=>	6.1.6.1-2	Digital platform maintenance tools should allow plant personnel to monitor system performance and maintain the system software without software programming expertise.				
		=>	6.1.6.1-3	System security features, such as passwords, should ensure that maintenance tools are only available to authorized users.				
		=>	6.1.6.1-4	The user should be able to specify the extent of testing to be performed (i.e., all or any combination of the included tests) and the number of times the test(s) should be repeated.				
		=>	6.1.6.1-5	Both the status and result of off-line diagnostics test should be indicated at the maintenance workstation and, if requested by the user, to a printer or file.				
	6.1.6.2	Security						
		=>	6.1.6.2-1	Any user action which might result in permanent changes to existing data or yield significant consequences to the computer or controlled system should be executed only after explicit user confirmation. The confirmation should not be a component of a routine command sequence and should present a sufficient safeguard against inadvertent actions.				
	6.1.6.3	Maintenance Personnel Responsibility						

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	6.1.6.3-1	The existing practices for repair and troubleshooting and the existing assignments and responsibilities of personnel for maintenance-related tasks should be re-evaluated for the modified digital equipment.				
6.1.7		Maintainability in Procurement and Plant Changes						
	=>	6.1.7-1	Specifications and other procurement documents should include or specifically cite maintainability-related human engineering requirements of the modification.					
	=>	6.1.7-2	Where a maintenance human-system interface will be provided by a vendor as part of an entire component package, human factors requirements should be included in the procurement specification or these interfaces should be required to be completely described by the vendor’s proposal.					
	=>	6.1.7-3	The planning for the modification should explicitly identify and include the completion of the maintenance-related tasks needed to close the related change package.					
	=>	6.1.7-4	Where maintenance tasks are implicitly or explicitly considered in a risk assessment, changes in the maintenance involved should have a human factors evaluation and this should be reflected in the change package.					
	=>	6.1.7-5	Instructions for preventive maintenance, testing and trouble-shooting tasks should be provided by the suppliers. The procedures should cover each step in sequence with an explanation of how each step is performed, which parameters can be adjusted, and the effects obtained by varying each parameter.					

6.1.3 General Design for Maintainability

6.1.3.1 Maintenance-Related Tasks

⇒ 6.1.3.1-1 Human factors analyses that are used to support the design of the human-system interface used for the upgraded system should include maintenance-related tasks as well as tasks needed to operate the modified systems.

Maintenance-related tasks are just as much a part of what takes place at the human-system interfaces as are the tasks that are performed to operate the systems. To the degree that these maintenance-related tasks can be defined they can be included in the design process in the same manner as any other task. The major difficulties are that unplanned maintenance, by its very nature, is not easy to define and can occur under a variety of plant conditions. Failure analyses (e.g., FMEAs) can be a source of information as to what unplanned maintenance tasks need to be addressed in the design process.

6.1.3.2 Redundant Components and Hot Spares

The most common design approach for enhancing system reliability and maintainability is through built-in component redundancy. The main benefit of redundancy is that continuously energized spares are built into the system to minimize the effects of module failures. In some cases redundancy also allows software to be updated with the system on-line by changing the software in one part of the system at a time. Redundancy can be applied to all important system components, including controllers or central processing units, communications modules, I/O etc. Hot spares are continually self-tested and can be moved into other locations as needed to accommodate primary module failures. This scheme simplifies on-line maintainability since spares that are known to be good are always available.

⇒ 6.1.3.2-1 For redundant components in hot standby configurations, there should be unambiguous indication of which component is operating and which is in standby.

⇒ 6.1.3.2-2 Testing of redundant equipment should include testing to confirm all potential fail-over and recovery situations.

It is equally important to test not only the fail-over to the standby device, but also the recovery to the original device. In some platforms either device can be considered the primary. When a fail-over occurs, the device that has taken over is now the new primary. Once a module is installed to replace the device that failed originally, that device now becomes the standby device.

⇒ 6.1.3.2-3 Alarms should be provided for any processor failure, prioritized based on of consistent criteria, and clearly presented to the operators or maintenance technicians who have to take action.

If systems switch between automatic and manual modes during a processor failure, the mode switching should be alarmed and clearly displayed. Where alarms are prioritized, the alarms for failures that have no redundant backup are generally given a higher priority than when there are redundant systems; however, failure consequences should still be the basic priority criterion. Alarms that are primarily for the use of maintenance technicians may still have to be presented to operators to assure that operators are made aware of the condition. This can often be done effectively by using a group or trouble alarm. The detailed alarm information that can only be used by maintenance technicians should not be presented directly to the operators unless it affects the response of the operators.

⇒ 6.1.3.2-4 Where modules are installed in the system as "hot spares," the maintenance procedures and labeling should distinguish the installed hot spares from the primary operating modules.

6.1.4 Detailed Design Features for Maintainability

This section discusses detailed design features of a digital upgrade modification that can have major impact on the maintenance-related tasks performed at the human-system interfaces. In some cases these features are provided in standard digital platforms; other features are engineered at the system application level. Depending on the scope of the modification there may be other detailed design features that impact maintenance and that should be considered in the design process. Section 6.1.8 discusses some of the major sources of information from which these other detailed design features can be derived.

⇒ 6.1.4-1 The system, module or equipment should provide indication to technicians and operators that modules have been inserted into the correct slot or rack location.

⇒ 6.1.4-2 Modules should not normally have configuration jumpers, switch settings or uniquely embedded software that must be configured prior to putting that module into operation. Where that cannot be avoided, the operating system software should confirm that these settings are correct.

⇒ 6.1.4-3 Different interfaces (e.g. connectors, fittings, etc.) should be provided for each type of test or service equipment to minimize the likelihood of error.

Test points and service points are provided throughout the plant to make signals available to maintenance personnel for checking, adjusting, and troubleshooting. One of the problems technicians can face is compatibility of these points and the tools or equipment to be used for these tasks. The designer must also establish a proper trade off between the desire for standardization of configuration and components and the need to provide deliberate and obvious differences to avoid human errors.

⇒ 6.1.4-4 The I/O module terminations should accommodate the testing tasks, and the field connections should not introduce unreliability or trouble shooting complexity.

When evaluating I/O modules, it is important to carefully examine the actual field interface connection scheme.

⇒ 6.1.4-5 Blown fuses, or open circuits of any kind, should be automatically detected and reported by the system diagnostics. The system's HSI should direct maintenance personnel to the specific point affected.

Blown fuse indicators can enhance maintenance, since they quickly direct the attention of maintenance personnel to the failed device. However, blown fuse indicators should be applied with caution since they can create sneak paths that can interfere with low energy circuits. For example, on a 4-20ma circuit a blown fuse indication circuit can supply enough loop current to prevent a failed circuit from being detected by the system's normal out-of-range detection.

⇒ 6.1.4-6 All modules should have readily observable indications to show that the module is operational.

Diagnostic LED's on all modules significantly enhance system troubleshooting. If a module is "operational," it should mean that the CPU has confirmed that the correct module type is positioned in rack, communication between the module and the CPU is successful and no internal errors or I/O errors are being reported. Input modules typically have LEDs for each input, which indicate the on/off state of the input. LEDs on more advanced modules may display error conditions such as ground faults, open circuits and low input sensing voltages.

⇒ 6.1.4-7 For I/O modules, front panel indicators should distinguish unused points. They should not be displayed with a particular status or error state. Where this is not possible, other labeling means should be used to clearly indicate that these points are not in use.

It may be appropriate to provide covers over potentially misleading status or error indicators that cannot be eliminated.

⇒ 6.1.4-8 When output modules are configured to go to a predetermined state or to freeze as-is on failures of the controlling CPU or failure of the communication to the controlling CPU, appropriate information on failure state should be displayed to maintainers and operators in addition to information that there has been a failure.

It has been common to configure output modules so they go to a predetermined state upon failure of input signals. This philosophy was based primarily on the inability to predict what state the outputs should be in over an extended period of system inoperability. But with the advanced diagnostics of digital systems, very short repair times are common. Therefore, outputs that fail as-is may be more appropriate to avoid unnecessary process disturbances due to failures and during maintenance. This may result in different failure states for similar modules and make it important to indicate that fact to the operators or maintainers.

⇒ 6.1.4-9 All modules should have adequate labels that are consistent with the system documentation.

Adequate and consistent labels will simplify trouble shooting and avoid maintenance errors. Labels should indicate module type, module number and module name (if the module is named in the system documentation). In addition, I/O modules should provide labels for each I/O point. Although space for labeling may be limited, the labeling should at least contain a number that can be referenced to the system documentation. Longer signal names and descriptions are an added benefit and their use is encouraged. Where the density of components does not permit individual labeling, an alternate approach to module labeling is to include a module map within the cabinet. This map provides a physical representation of the cabinet so that module locations and I/O points can be easily located.

⇒ 6.1.4-10 Module labels or cabinet maps should be such that they can be correctly updated as an integral part of any system design change.

The methods used and the controls applied will need to be consistent with the practices of the plant configuration management system; however, it is essential that the labels or maps correctly represent the actual configuration at all times. That is, the design change is not complete until the labeling is brought up-to-date.

⇒ 6.1.4-11 If geographically distributed components are used, the digital platform and system should provide communication and operation diagnostics, automatic fault detection, isolation capability, and appropriate indication to maintenance technicians and operators. The system's centrally located HSI should clearly diagnose failures to the replaceable module level.

With this capability maintenance personnel can travel to the remote location with the correct replacement module in hand, rather than requiring two trips to the remote location – one to diagnose the problem and a second to actually replace the module.

⇒ 6.1.4-12 Displays should be configured to show system errors in graphic format. The self-diagnostic features of the platform should isolate a problem down to the component level (e.g. specific module or I/O point).

Most digital systems provide I&C fault indications in the form of text messages. Many platforms also allow entry of text comments concerning repair. Some platforms generate these displays automatically. In others the displays need to be manually configured just like any other custom graphic display. Graphic presentations guide the maintenance staff to the component display relevant to the fault. Overall, a well designed graphical user interface can significantly minimize the time and effort needed to perform corrective maintenance. Many error conditions are detected at the component level, therefore component level indication is inherently provided by the digital platform. However, for more global abnormal conditions such as power supply, controller and I/O card failures, or interfaced system failures, application engineering is required to determine the many components that may be affected by those failures.

⇒ 6.1.4-13 Local controls should be provided to permit component maintenance operations without the coordination between remote and local personnel.

Local controls provide the capability to manually control plant components without reliance on remote personnel, remote HSI or remote CPUs. Local controls are important for initial system commissioning as well as periodic maintenance and testing. During initial system installation verification there are scheduling advantages to being able to test the connections from the digital system to controlled plant components before the remote HSI becomes fully operational. This becomes even more important for geographically distributed installations where the local I/O may be installed before the remote CPUs. To accommodate this, the local controls must function without dependence on remote controllers or HSI.

⇒ 6.1.4-14 Local controls should include switches to disconnect all remote control actuation signals. Adequate indications or alarms should be provided in the main control room to ensure operators are aware that they have lost control of that component.

During local component maintenance operations there should be no unexpected component operation due to signals from remote HSI or automation signals from controllers. For safety components the HSI must meet RG 1.47 compliance for inoperable display at the system level. While local switches provide the capability to disconnect remote control signals, component status feedback will need to remain operable so that operators can maintain awareness of component state changes and the resulting process affects.

⇒ 6.1.4-15 If remote switches are located in the main control room, additional isolation and transfer/disconnect capability for these control interfaces should be provided.

Remote switches that operate independent of the system's digital controllers can also be located in the Main Control Room, if quick access is necessary. However, technicians should understand this feature and how to replace components without creating abnormal or hazardous conditions.

⇒ 6.1.4-16 Failed sensors in safety monitoring systems should be alarmed and logged and the out-of-service times monitored for technical specification compliance.

⇒ 6.1.4-17 Protection system bypasses should have controls to ensure they are not implemented in a way that can totally bypass all trip and actuation functionality

⇒ 6.1.4-18 Administrative controls and security access restrictions such as passwords or key locks should be built into the system to control the use of bypasses.

⇒ 6.1.4-19 Bypasses should be clearly indicated and alarmed.

⇒ 6.1.4-20 Where plants are vulnerable to spurious trips and actuations until a bypass is manually activated, the HSI associated with activating and displaying bypasses should be easily and quickly accessible by plant operators.

⇒ 6.1.4-21 If a value is substituted in a calculation, then the calculated result should have a clearly distinguishable quality flag. Such a substitution should be treated as a bypass and the previous guidelines should be applied.

If the failed sensor is one of many inputs to a calculation, it is often desirable to include bypass capability so the remaining portions of the calculation can continue to be processed. These types of bypasses typically allow values to be substituted for the failed sensor. Substitutions can be other properly functioning sensor inputs or manual values. Some technical specifications will require the calculated value to be reported as failed, with clearly distinguishable bypass indication.

6.1.5 Diagnosis and Testing

6.1.5.1 Self-Diagnosis

Self-diagnostic features that are built-in to basic digital platforms play a significant role in identifying equipment failures and reduce trouble-shooting and replacement time (i.e. mean time to repair). This section discusses some of these self-diagnostic features that impact maintenance tasks, the extent of self-diagnostic coverage typically built-in to digital platforms, and the features of the HSI that support the understanding of the information provided.

⇒ 6.1.5.1-1 Malfunction messages should be displayed at the HSIs and archived.

More advanced archiving systems will also record other related parameters at the time the malfunctions occurs. This can be especially helpful in diagnosing transient errors that may only occur with a particular combination of input conditions. Advanced archiving systems will also generate reports that show failures over time so that adverse trends can be easily identified. For some platforms, these errors are automatically transmitted to remote HSI devices so they can be displayed and alarmed. For other platforms, the error buffers must be configured for display in the application software. Platforms that require alarm configuration require more application engineering effort.

6.1.5.2 Error Detection and Indication

⇒ 6.1.5.2-1 The digital platform should provide the capability to automatically detect and indicate the following out-of-service conditions. However, since the functional impairment is different for each of these conditions, distinct indication should be provided.

- *Disabling of normal operator control functionality*

  This can occur as a result of transfer switches activated at local panels or at object based control modules.

- *Disabling of normal automated control functionality*

  For safety components, automated controls can originate in the safety digital platform as well as other sources such as the diverse protection system or even the non-safety digital platform (typical of designs with advanced HSI). For components with this type of control source complexity an out-of-service condition is created when the functionality of any of these control sources is disabled

- *Digital platform conditions*

  These are conditions within the platform itself that impair its ability to operate.

⇒ 6.1.5.2-2 For important control or protection applications, out-of-range detection should be provided.

Self-diagnostic coverage is typically limited to wire breaks and errors in communication to controllers; however, for some applications it may also be important to detect other abnormalities such as not operating within tolerance limits.

⇒ 6.1.5.2-3 In digital platforms CPU and communication should incorporate error detection methods at power up and at the request of the operator.

⇒ 6.1.5.2-4 Where communication redundancy is employed, the method and coverage of automatic error detection and self-testing of these peripheral devices should be carefully reviewed; manual testing is sometimes required.

For example, internal diagnostic for networks and data-link communication interfaces typically do not specifically cover media devices such as fiber optic converters, network hubs or switches. These devices are inherently checked as part of the communication path, but all failures are reported at the communication interface level.

⇒ 6.1.5.2-5 The determination of the significance of errors and how they are alarmed or presented should be consistent across the various digital platforms

⇒ 6.1.5.2-6 In redundant systems, sustained faults should be alarmed. Operators should be able to acknowledge the alarm, but the alarm should remain activated until the system becomes operable again.

⇒ 6.1.5.2-7 If the plant general alarm system employs multiple levels of alarm prioritization, the process effect of each error should be consistent with the plant's general alarm prioritization criteria.

For example, some digital systems have been installed without evaluating error conditions. As a result, all errors are treated as important alarms and operators become quickly overloaded with unnecessary information.

⇒ 6.1.5.2-8 Out-of-service indications should be provided at the normal control location as an integral part of the component status display in all formats for which that status is displayed.

⇒ 6.1.5.2-9 Out-of-service conditions should be alarmed at the normal control location to ensure operators are aware of the abnormal event and the conditions should be logged in the plant's historical recording system.

⇒ 6.1.5.2-10 The capability to manually identify an out-of-service condition for any plant component should be provided.

All out-of-service conditions cannot be anticipated and therefore cannot be automatically detected.

⇒ 6.1.5.2-11 The capability for operators and maintenance personnel to manually enter notes regarding the out-of-service conditions should be provided.

Notes capability should include the following attributes:

- Notes should be directly entered and linked with the associated plant object.
- Normal component status displays, such as process mimics, should indicate that a maintenance note exists for that component. Simple navigation techniques should allow direct access to these notes.
- Notes should be automatically time tagged and logged with the author's name or role designation.
- Notes should be permanently logged in the historical record file.
- The ability to delete the notes for on-line display should be limited to plant personnel with this designated role.

⇒ 6.1.5.2-12 In addition to the out-of-service condition, component position status should always be displayed.

If reliable component status indication is not available because of the out-of-service condition itself, that should be reflected in the display.

⇒ 6.1.5.2-13 The human system interfaces should not combine detailed information needed by diagnostic technicians into the same set of displays as are used by the end-users.

The users interface is typically suitable to identify the failed module, but does not necessarily provide details on the cause of the failure. For detailed diagnostics, it is often necessary to interrogate a controller's internal error buffer. This type of diagnostic task is not meant for the general user and is typically useful only to maintenance technicians or engineers. Display of such information on displays normally used for operating the plant is distracting, adds clutter, and may increase the potential for human error.

⇒ *6.1.5.2-14 Replacement modules should require a minimum of special handling precautions.*

Since special handling precautions can add time and complexity to equipment replacement procedures, platforms should be evaluated for their susceptibility to static discharge failures and the supplier's maintenance and handling recommendations. Handling precautions must also be considered to minimize problems during failed equipment replacement.

⇒ *6.1.5.2-15 Replacing equipment should not create a hazardous condition for technicians or equipment.*

6.1.5.3 Application Level Testing

There are two types of automatic application level testing: passive and active. Passive testing is the process of monitoring the operations of the application and annunciating any anomalies. Active testing is the process of injecting test signals and observing the corresponding response by the application. Both can be designed into the system so that all testing can be conducted without any temporary modifications. In passive testing techniques, corresponding data from redundant control processors is periodically compared. Any deviations or errors are displayed and logged. Passive testing is typically used to compare input values (process measurements) and output values (trip and pre-trip) between redundant channels or between redundant processors within a channel.

⇒ *6.1.5.3-1 Where customized application level testing is required, test features should be built into the system so that all tests can be conducted without the addition of temporary modifications, such as shorting contacts or opening circuit loops.*

These types of temporary modifications have proven to cause configuration control errors and should be avoided.

⇒ *6.1.5.3-2 Procedures and interlocks should be provided to ensure the system is in an acceptable bypassed mode before allowing manual tests to be initiated. Operations personnel should be provided with indications that the bypasses have been instituted.*

⇒ *6.1.5.3-3 Tests of output devices should normally be manually initiated. The HSI should be specifically designed for the testing to be conducted and should not contain other unrelated information that can cause confusion and errors.*

⇒ *6.1.5.3-4 For output interface tests, adequate indication and interlocks to avoid spurious plant disturbances should be provided.*

For example, when performing a test that causes a reactor trip circuit breaker (RTCB) to open, the system must receive positive indication that the breaker has been re-closed before a permissive is generated to allow the same test in another RPS channel.

⇒ 6.1.5.3-5 Digital platforms should provide the capability of taking inputs and outputs out-of-scan, and the ability to manually insert values for testing. When points are out-of-scan there must be clear indication that a value has been manually inserted.

⇒ 6.1.5.3-6 To ensure points are not unintentionally left in an out-of-scan condition summary displays should provide a listing of all points utilizing substituted values. If a value is manually substituted for a true process input, then calculated results should have a clearly distinguishable quality flag.

⇒ 6.1.5.3-7 System security features, such as passwords or key locks, should ensure forced value functionality, e.g., taking a point out-of-scan, is only available to authorized users.

6.1.6 Maintenance Performance

6.1.6.1 Maintenance Tools

These "tools" are generally functionalities and software features. They may not involve conventional test equipment of hand tools.

⇒ 6.1.6.1-1 Digital platform maintenance tools should be available only at designated workstations

⇒ 6.1.6.1-2 Digital platform maintenance tools should allow plant personnel to monitor system performance and maintain the system software without software programming expertise.

⇒ 6.1.6.1-3 System security features, such as passwords, should ensure that maintenance tools are only available to authorized users.

⇒ 6.1.6.1-4 The user should be able to specify the extent of testing to be performed (i.e., all or any combination of the included tests) and the number of times the test(s) should be repeated.

⇒ 6.1.6.1-5 Both the status and result of off-line diagnostics test should be indicated at the maintenance workstation and, if requested by the user, to a printer or file.

6.1.6.2 Security

Providing security in maintenance activities typically involves control of functional access in the following increasing levels of security:

- Call-up of standard display formats and the information contained thereon.
- Access to alarm acknowledgement and control functions.

- Call-up of detailed information such as individual parameters used in computing a derived variable, unprocessed sensor values, individual parameters, or creation of temporary graphics displays on a one time basis.
- Modification of attributes of a database point.
- Removing a point from scan processing or alarm processing, inserting a value or state, restoring a point to alarm, scan processing. Some database points will need to have more restricted security access than other database points.
- Writing and execution of simple programs which can be executed on line but which are subordinate to and do not modify the primary program functions.
- Writing and execution of programs which modify the on line program functions.

⇒ 6.1.6.2-1 Any user action which might result in permanent changes to existing data or yield significant consequences to the computer or controlled systems should be executed only after explicit user confirmation. The confirmation should not be a component of a routine command sequence and should present a sufficient safeguard against inadvertent actions.

Feedback from users has shown there have been designs where the HSI contains unnecessary buttons that operators could accidentally push and reconfigure system parameters.

6.1.6.3 Maintenance Personnel Responsibility

The use of digital technology presents new opportunities, as well as a need to examine traditional roles for plant personnel performing maintenance and testing operations.

⇒ 6.1.6.3-1 The existing practices for repair and troubleshooting and the existing assignments and responsibilities of personnel for maintenance-related tasks should be re-evaluated for the modified digital equipment

Probably the most significant change brought about through digital technology is that modules fail significantly less often than analog systems. Another fundamental change is that end-users will no longer repair failed modules. This is due somewhat to the complexity and miniaturization of digital modules that make historical repair shop operations impractical. But it is also due to the proprietary nature of these designs. Most manufacturers do not provide the level of documentation, diagnostic tools, training, or parts for module repairs. Digital technology also changes the way troubleshooting is accomplished. For most common failures, trouble shooting is from workstations as compared to current practices of local trouble shooting of analog devices within cabinets using meters and oscilloscopes. Since workstations for maintenance can be located in centralized maintenance rooms or even in the main control room, there is now potential to question the traditional assignment of troubleshooting responsibility. Although there is a potential to migrate some level of system troubleshooting away from maintenance technicians and make it within the capability of control room operators, there is some potential for a loss of situation awareness by operators when they are performing non-operational tasks. This should be considered in any re-evaluation of maintenance task assignments.

6.1.7 Maintainability in Procurement and Plant Changes

In order to achieve high maintainability in a digital upgrade modification, the plant owner and system designers will need to devote effort to ensuring that maintainability features are adequately specified as part of the procurement of the equipment and that the actual changes to the plant support the maintainability features. There is a wide spectrum of changes and existing plant conditions that have to be considered. Accordingly, specific detailed guidance is not generally appropriate. However, the fundamental principle is that the human factors aspects of maintainability should be covered in both procurement documents and change packages. In addition to the guidelines in this subsection, there are numerous guidelines in the previous subsections that need to be considered in the procurement phase of a project and in carrying out the changes.

⇒ 6.1.7-1 Specifications and other procurement documents should include or specifically cite maintainability-related human engineering requirements of the modification.

The guidelines in this document will need to be translated into specific requirements in procurement-related documents. Because of the wide spectrum of possible modifications and the variation in existing maintenance practices from plant to plant it is not practical to identify a standard set of such requirement in these guidelines. If there are relatively standardized maintenance requirements for existing plant equipment, these standard maintenance requirements will have to be identified, evaluated for applicability to the modification, and appropriately reflected in the procurement documents for the modified equipment. The users of these guidelines should check the referenced material for specific detailed guidance that has not been included in these guidelines. Useful detailed requirements can often be derived from some of the more detailed guidelines in the cited references. Information has been provided in the Section 6.1.8.2 of these guidelines to assist in locating detailed guidelines on specific subjects in the referenced material.

⇒ 6.1.7-2 Where a maintenance human-system interface will be provided by a vendor as part of an entire component package, human factors requirements should be included in the procurement specification or these interfaces should be required to be completely described by the vendor's proposal.

In cases where commercial equipment is being used or adapted, the maintenance human-system interface may be standardized and difficult to change. It is important that the potential vendors be required to describe the interface in enough detail that a meaningful evaluation can be made by the system designers in selecting the components. Changes to relatively standard interfaces may be expensive and may have major schedule impacts if they have to be made after contracts are let.

⇒ 6.1.7-3 The planning for the modification should explicitly identify and include the completion of the maintenance-related tasks needed to close the related change package.

The content of change packages will vary from plant to plant; however, they generally cover specifically such maintenance-related issues as: maintenance personnel training, maintenance procedure changes, new maintenance facilities or test equipment, added spare parts, etc. These associated changes have to be completed at the same time as the modification is placed in service. Considerable effort to coordinate the various groups involved and to generate the necessary information and complete the work on an acceptable schedule will be required. This task in the modification process needs to be recognized and adequate support provided in the project effort.

⇒ 6.1.7-4 Where maintenance tasks are implicitly or explicitly considered in a risk assessment, changes in the maintenance involved should have a human factors evaluation and this should be reflected in the change package.

An example would be where time to repair is explicitly considered in a risk assessment. Other example would be time to diagnose a failure or actions to bring standby equipment on line. Some factors that are applied to account for human errors may also need to be re-evaluated. Liaison with individual responsible for risk assessment will be needed to ensure impacts on the PRA conclusions are evaluated in the design process. Note that this issue may directly affect the licensing of a digital upgrade (see Section 5 of these guidelines).

⇒ 6.1.7-5 Instructions for preventive maintenance, testing and trouble-shooting tasks should be provided by the suppliers. The procedures should cover each step in sequence with an explanation of how each step is performed, which parameters can be adjusted, and the effects obtained by varying each parameter.

The type of standard documentation available from suppliers is largely based on the demands placed on them by previous customers. Since this technology may be used throughout the world and in numerous industries, the quality of standard manuals and documentation varies considerably between suppliers. For example, sample printouts from the diagnostic programs should be required from the suppliers.

6.1.8 Sources of Additional Information

Although there is substantial reference information on the general subject of maintainability, the bulk of the applicable information can be found in a relatively limited set of references. In addition to listing important references, this section provides guidance as to what topics are covered in each of the cited references and how the information may be useful in developing a digital upgrade design that supports maintenance.

Even though the list of references is limited, the documents themselves tend to be voluminous and to cover a wide spectrum of subjects. It is recommended that all these references be readily available to the designers, particularly during the development of specification and procurement requirements.

6.1.8.1 Reference List

1. O’Hara, J. M., Brown, W. S., Lewis, P. M., and Persensky, J. J., *Human-System Interface Design Review Guidelines*, Section 13, Maintainability of Digital Systems, NUREG-0700, Revision 2, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, D.C., (pp 507-545) May 2002.

2. Stubler, W. F., Higgins, J. C., and Kramer, J., *Maintainability of Digital Systems: Technical Basis and Human Factors Review Guidance*, NUREG/CR-6636, BNL-NUREG-52566, Brookhaven National Laboratory, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, D.C., March 2000.
3. *Advanced Light Water Reactor Utility Requirements Document, Volume II, ALWR Evolutionary Plant,* Chapter 10, Man-Machine Interface Systems, Revision 6, Electric Power Research Institute, Palo Alto, CA: December 1993.
4. *NRC Review of Electric Power Institute's Advanced Light Water Reactor Utility Requirements Document*, Chapter 10, Man-Machine Interface Systems, NUREG-1242, Vol. 3, Part 2, U.S. Nuclear Regulatory Commission, Washington, D.C., 1994.
5. *Human Factors/Ergonomics Handbook for the Design for Ease of Maintenance*, DOE-HDBK-1140-2001, U.S. Department of Energy, Washington, D.C., Area HFAC, February 2001.
6. Pack, R. W., Seminara, J. L., Shewbridge, E. G., and Gonzalez, W. R., *Human Engineering Design Guidelines for Maintainability*, NP-4350, Final Report, Electric Power Research Institute (EPRI), Palo Alto, CA: December 1985. Research Project 2166-4.
7. *Dependability Management – Part 3-10: Application guide –Maintainability* , IEC 60300-3-10, First Edition, International Electrotechnical Commission, Geneva 2001.
8. *Human Factors Design Standard (HFDS) for Acquisition of Commercial-Off-The-Shelf Subsystems, Non-Developmental Items (NDI), and Developmental Systems*, Section 4, Designing equipment for maintenance, HF-STD-001, DOT/FAA/CT-03/05, U.S. Department of Transportation, Federal Aviation Administration Headquarters, Human Factors Division, Washington, May 2003.
9. *Maintainability of Digital Systems,* EPRI, Palo Alto, CA: October 2004. 1008124.

6.1.8.2 Reference Content and Use

6.1.8.2.1 References 1 and 2, NUREG-0700 and NUREG/CR-6636

These documents are a pair of very closely related documents which have been issued by the Nuclear Regulatory Commission. The cited section 13 in NUREG-0700 is specifically directed at identifying the maintainability considerations in digital systems. It is part of the much broader general human factors design review guidelines for the entire human system interface in nuclear power plants that is addressed by the total NUREG-0700 document. It represents an effort by the NRC to define what aspects of the plant human factors they will review and what criteria will be used in the evaluations. As such, it represents issues which will need to be addressed in any digital upgrade design – certainly for safety systems and where licensing is involved (see Section 5, Licensing). Section 13 of Reference 1 provides general guidance on maintainability in digital systems, including such high-level topics as minimization of maintenance, on-line maintenance, the role of humans, and avoiding hazards. In addition, it also provides guidance on a large number of specific individual topics that an NRC Reviewer will be expected to cover in their review. This includes topics such as:

- Instrument cabinets and racks,
- Equipment packaging (modularization, layout, mounting, etc.),
- Fuses and circuit breakers,
- Labeling and marking,
- Adjustment controls,
- Test and service points, and
- Test equipment (manual and automatic).

Reference 2 (NUREG/CR-6636) is a companion document that provides background, rationale, and further explanation of the material in Section 13 of NUREG-0700. It can be of considerable use in applying the information in Reference 1. It also provides extensive references to other information and identifies the source(s) of the specific review guidelines in Reference 1.

6.1.8.2.2 References 3 and 4, EPRI ALWR URD Chapter 10 and NUREG-l242

As for References 1 and 2, these two documents should be treated as a pair. The EPRI URD (Reference 3) provides a number of relatively high level requirements related to maintainability as well as some important detailed requirements. These requirements are presented along with the rationales for their inclusion in the document. The NUREG (Reference 4) provides the results of NRC's review of the URD. The basic portions of Chapter 10 of the URD that pertain to maintainability of digital systems are the following:

• 3.5.4	Reliability and Maintainability Analysis
• 3.6	Testability Requirements
• 3.7	Maintainability
• 5.6.3	Computer-Aided Plant Diagnostics, Maintenance, and Testing
• 6.1.7	Maintainability and Serviceability (software)
• 6.3.6	Maintainability and Serviceability (control systems)

For the general subject of maintainability, there were no significant comments from the NRC review and it is unlikely that reference to NUREG-1242 will be needed. It has been listed for completeness. Both References 3 and 4 are cited in Reference 2 as sources for the material in Reference 1. The EPRI URD provides a somewhat different perspective from that of the NRC in Reference 1, since it applies to the entire plant (not just safety-related aspects) and represents a rather broad industry consensus of what requirements should be specified for a new advanced nuclear power plant.

6.1.8.2.3 Reference 5, DOE-HDBK-1140-2001

This is a recently published handbook that DOE expects their contractors to apply to the design and maintenance programs for DOE facilities. Since many of their facilities are closely related to nuclear power plants, this handbook provides a valuable resource for specific maintenance practices. Many of the requirements are quite detailed and, although a large number are directed at general maintenance issues, a substantial number are either directly or indirectly pertinent to maintainability of a digital upgrade. In addition to specific design guidance there is also substantial information on the programmatic aspects of maintainability. This information will be useful in evaluating the impact of the digital technology on existing plant maintenance practices and programs. This reference also has an extensive listing of additional reference material. Unfortunately, it has no index.

The major topics covered include:

- Design for maintainability – the section covers such topics as layout, labeling, connectors, controls, displays, racks, handles, etc. It will be useful in establishing specific design requirements or evaluating existing designs.
- Workspace, storage, and workshop design – this section may be of some use in evaluating impact on existing facilities.
- Maintenance support equipment – This section tends to be directed largely at physical facilities and equipment (cranes, jacks, ladders, etc.). It has only limited application to a digital upgrade modification.
- Maintenance aids – This section deals with instructions, training, and related issues. It will be of some use; however, it is not focused on digital upgrades.
- Developing maintenance programs – This section deals with such subjects as preventive maintenance programs, monitoring, information management, software maintenance, and the design process. As for the other sections it is obviously not focused on digital upgrades; however, it provides information that may be useful in assessing the impact of a digital upgrade on overall plant maintenance practices and in integrating maintenance-related issues in the design process.

6.1.8.2.4 Reference 6, EPRI NP-4350

Although this reference was issued in 1985, it represents a very comprehensive source of guidelines directed at obtaining adequate maintainability. It is from the human factors perspective; however, it is obviously not narrowly focused on a digital upgrade project. A substantial part of the information is most directly applicable to new plant design; however, much of the guidance could also be applied to a digital modification project. It is a particularly valuable reference because it gives extensive examples and explanations of most of the recommendations. This makes it relatively straightforward in many cases to establish whether the guideline would be applicable to a particular digital upgrade project. The format of the document is such that most of the major sections include a checklist of the specific guidelines. These checklists can provide a valuable tool in establishing what guidelines may be applicable to a digital upgrade and, thereby, helping to select specific requirements for the design and procurement of equipment. Checklists are included in the following chapters:

- III-A Plant Design Factors
- III-B Workshop Design
- III-C Hazards and Protection Aspects of Facility Design
- III-D Environmental Factors
- III-E Movement of People and Equipment
- III-F Maintenance Communications

(These first six chapters are directed at facility design and are less likely to be directly applicable to a digital upgrade than the subsequent six chapters.)

- IV-A Equipment and System Maintainability
- IV-B Preventive and Predictive Maintenance
- IV-C Hazards and Protection Aspects of Equipment Design
- V-A Technical Manuals and Procedures
- V-B Labeling and Coding
- V-C Tools, Stores, and Test Equipment

This reference also includes an extensive list of additional references and an index of topics.

6.1.8.2.5 Reference 7, IEC 60300-3-10

This reference is part of a series of standards and guides which "explain the procedures for implementing a Dependability Programme during the design and development of a product in order to achieve specified levels of dependability." Its scope is broader than maintainability, although maintainability is a major factor. It has a number of high-level requirements and guidance and especially focuses on the programmatic aspects. It has few detailed design requirements; however, it addresses a number of subjects that can be impacted by a digital upgrade modification or which figure in the design process for the upgrade. It also references numerous other sources of guidance. It provides discussions of the following topics:

- Description of the product life cycle
- General discussion of a maintainability program, including
  - Planning and constraints
  - Maintainability studies
  - Project management
  - Design for maintainability (includes a section on human factors)
  - Externally provided products
  - Analysis and prediction methods
  - Verification, validation, and test

- Life cycle cost
- Maintenance support planning
- Improvements and modifications
- Collection and analysis of maintenance data

This reference is unlikely to provide significant assistance in establishing design details; however, it provides a somewhat different perspective on maintainability from the other references. It is relatively concise (only about 30 pages of English text) and its different point of view can help ensure that no important consideration is left out of the design process.

6.1.8.2.6 Reference 8, FAA Human Factors Design Standard

This is a recently published standard that was “developed as a comprehensive reference tool to help FAA and contractor human factors professionals carry out FAA human factors policy.” It represents a major revision of a previous HFDG (Human Factors Design Guide) that was last issued in 1996. Although it is directed at general human factors and covers a broad range of topics, it includes a specific (and extensive) section directed requirements for Designing Equipment for Maintenance (Section 4). In addition, other sections may be pertinent to maintainability, for example, Section 8 on Computer-human interface and Section 12 on Personnel Safety. It is very extensive document (over a hundred pages in Section 4 alone) and covers a great many detailed design features related to maintenance. Although it repeats much of the information in References 1, 5, and 6, it has a different perspective in that it is not a guideline, rather it is a standard. It may prove to be valuable in setting requirements on vendor supplied items and in selecting detailed design features. The following major topics are covered in Section 4:

- Designing equipment for handling
- Packaging, arrangement, and mounting of equipment
- Access openings
- Cases, covers, guards, and shields
- Fasteners
- Connectors
- Lines and Cables
- Fluid and Gas lines
- Packaging, layout, and mounting of internal components
- Adjustment controls
- Fuses and circuit breakers
- Test points and service points
- Test equipment
- Tools

6.1.8.2.7 Reference 9, EPRI 1008124, Maintainability of Digital Systems

This reference expands upon the information in the guidelines. It also goes into more detail on many of the subjects, and gives examples. It provides information on design features to provide maintainability in digital systems that is not within the scope of the HSI guidelines.

6.2 Human Factors Engineering for Configuration Management

6.2.1 Overview

6.2.2 Configuration Management Guidelines Checklist

6.2.3 General Configuration Control Guidance

6.2.4 Configuration Change Control Guidance

6.2.5 Control of User-Defined Interface Features

6.2.1 Overview

These guidelines address those aspects of configuration management of a digital upgrade modification that may affect the performance of human tasks at the system interfaces. In addition to configuration information that is part of the data included in the formal configuration management system, there will usually be some other information or data that are used in the tasks at the human system interfaces to operate or service the plant. This information may change periodically or depend upon specific plant conditions that are variable. These guidelines will address that additional type of configuration information. In the human-system interfaces provided as part of digital upgrade modification, there may be features that can be configured by the operators and other users. For example, special displays or selectable alarms are potential features. Those features are not part of the plant's configuration management system; however, they are important to the tasks that are performed at the human-system interfaces. These guidelines will address the human factors issues in controlling the configuration and use of these user-definable features. In some cases, the necessary configuration control can be established by features of the technology such as automatic recording of changes; however, some control may best be achieved by administrative approaches similar to that used for conventional HSIs. For some simple digital upgrades, existing practices may be adequate and should not be changed. The guideline user should focus on the concern that underlies each guideline and not on how new technology might be used.

A digital upgrade modification will change the information that is included in the configuration management system. The modification design team will have to identify that information and provide that information to the plant staff responsible for the configuration management system. This will include establishing what new information must be included in the design basis documents due to the modification. This can be a major effort for the design team and one that requires careful consideration in planning for the modification. However, it is not closely related to the human-system interface tasks and to human factors engineering and, consequently, that activity is not within the scope of these guidelines. The content of this section is shown schematically in Figure 6-2.

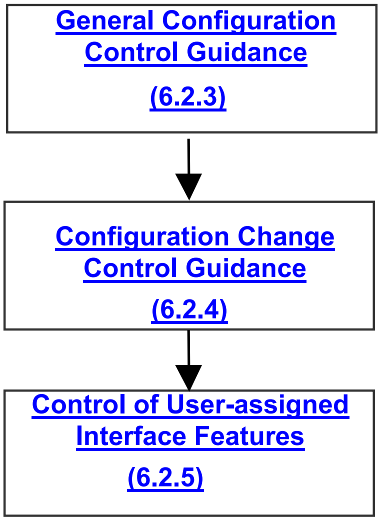

General Configuration Control Guidance
(6.2.3)
Configuration Change Control Guidance
(6.2.4)
Control of User-assigned Interface Features
(6.2.5)

Figure 6-2
Configuration Management

6.2.2 Configuration Management Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining sections. For additional information, please consult the sections and guidelines referenced.

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
6.2.3		General Configuration Control Guidance					
	=>	6.2.3-1	Where operation or servicing of the digital upgrade modification results in human tasks that require information from the configuration management system and similar data sources, those tasks should be identified in the design process and appropriate human factors review provided.				
	=>	6.2.3-2	Where human tasks involve consulting configuration information, some way to confirm expeditiously that the version of the requested information is up-to-date should be provided.				
6.2.4		Configuration Change Control Guidance					
	=>	6.2.4-1	If the human-system interfaces involved in the upgrade modification provide means by which information in the configuration management or similar data bases can be directly changed, control methods comparable to that for other similar configuration information should be provided.				
	=>	6.2.4-2	Procedures should be established that ensure that human factors engineering review of HSI and plant configuration changes that affect the tasks performed at the modified human-system interfaces is done when necessary.				
	=>	6.2.4-3	Where the human tasks require operators or technicians to access configuration information, practical methods for temporary changes and corrections should be provided.				
	=>	6.2.4-4	Generating a temporary change or correction and incorporating it in the currently used information should comply with existing administrative procedures. Where the technology has changed how this is accomplished, the intent of the previously used controls should be maintained.				
	=>	6.2.4-5	The human system interfaces in the digital upgrade modification should incorporate limitations on making temporary changes or corrections equivalent to those required by plant administrative change control procedures.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	6.2.4-6	A temporary change or correction to an item of configuration information should be available to all users of the information.				
	=>	6.2.4-7	Means should be provided to identify all outstanding temporary changes or corrections. Temporary changes should have a limited life. A temporary change or correction should not be allowed to become a de facto permanent feature of the HSI.				
6.2.5		Control of User-Defined Interface Features					
	=>	6.2.5-1	Methods to provide for the management of user-defined features of the human-system interface that are provided as part of the upgrade modification should be established and the interface designed to support that management.				
	=>	6.2.5-2	Protocols should be established as to what will be done with special displays of information when shifts change or operators are relieved.				
	=>	6.2.5-3	Means should be provided so that supervisors can know what special displays are being used by the persons that they supervise. Furthermore, the supervisors should have easy access to the identical display.				
	=>	6.2.5-4	Methods should be provided to monitor and record the use of special displays. These records should provide information on who created the special display and when it was in use. The records should also provide the ability to reconstruct the display itself. (Additional guidelines related to the use of these records are provided below.)				
	=>	6.2.5-5	The records should be configured so that they could be used as indications of the need for changes in the plant or the human-system interface.				
	=>	6.2.5-6	Enough information should be recorded so that all special displays that were used by the operators in the course of an event can be reconstructed and properly placed in time.				
	=>	6.2.5-7	Information should be recorded in a form that training personnel can evaluate the displays that were used for possible incorporation in the standard training program.				

6.2.3 General Configuration Control Guidance

⇒ 6.2.3-1 Where operation or servicing of the digital upgrade modification results in human tasks that require information from the configuration management system and similar data sources, those tasks should be identified in the design process and appropriate human factors review provided.

How information is obtained from the configuration management system is generally the responsibility of the plant's configuration management staff. However, where the operators or technicians who operate or service the modified systems interface directly with a configuration management system, the tasks involved need to be addressed by the modification design team. It should not be expected that the configuration management staff will provide human factors review in the context of the modification. It may be necessary to work directly with those responsible for configuration management in the earliest concept and planning phases to assure that the impacts are thoroughly examined.

Design changes involved in the modification may make accessing the configuration information different – both in what information is obtained and how the access is accomplished. Those cases where access may become more difficult or less efficient should be identified in the design process and evaluated from a human performance standpoint. For example, the institution of compact workstations may reduce the room available to consult hard-copy information and result in accessing electronic versions of the information. Similarly, the presentation of some procedures in electronic format will markedly change how those procedures are accessed.
In some cases, especially for operators and maintenance technicians, accessing the information in the configuration management system or similar information in a data base will be an integral part of the tasks performed at the human-system interface and, therefore, need human factors engineering evaluation.

⇒ 6.2.3-2 Where human tasks involve consulting configuration information, some way to confirm expeditiously that the version of the requested information is up-to-date should be provided.

Although all configuration management systems will have controls on the versions of information in their system (see the next section on changes), the user of the system should have a way to confirm easily that the information is current. This is not for the purpose of independent verification. It is to address the human factors consideration that users (an operator, for example) should have a means to resolve concerns that may arise in their minds if they receive information that does not seem to be correct or to make sense. It is important that the operator have an expeditious way to resolve those doubts.

6.2.4 Configuration Change Control Guidance

Any configuration management system or base of data will provide methods by which changes to the configuration are controlled. The upgrade modification itself will obviously be a change and it will have to be done in accordance with the standard plant administrative change control procedures. Those changes are not directly the focus of these guidelines. However, there are some aspects of configuration change control that are closely related to the tasks performed at the human-system interfaces. In addition to permanent changes to the configuration information that may affect human tasks, these guidelines address the following closely-related issues that involve temporary changes or correction:

- Some systems involve the use of so-called “tuned parameters.” These are configuration data that are not fixed in the long term, but are changed in response to particular plant conditions. Typically, they include such items as set points that are selected by the operators or others and provide the means to optimize performance or maintain stability margins. These can also be the result of the operators or technicians running a test or following a particular procedure.
- There are also instances where errors are discovered in configuration data. Typically error reports are generated; however, there is usually some way for operators or technicians (with appropriate supervisory controls) to make an immediate temporary change. Another situation that can result in a temporary change is when a sensor failure results in a constant alarm situation and the point is put “out-of-scan.”

⇒ 6.2.4-1 If the human-system interfaces involved in the upgrade modification provide means by which information in the configuration management or similar data bases can be directly changed, control methods comparable to that for other similar configuration information should be provided.

Changes in the documents and records that form the managed configuration are controlled by the administrative procedures of the configuration management system. These may no longer be completely appropriate for the modified interfaces. The increased use of information in electronic format provides the potential for changes to be effected rather easily and without the safeguards that are provided for hard-copy documents. This can be a security issue and the plant security provisions may impact how the configuration changes are controlled. It may also affect how the information is presented at the interface and how the tasks are conducted at the interface. Changes to so-called “tunable parameters” also may be accomplished differently as a result of a digital upgrade modification and existing change control methods may no longer be appropriate.

⇒ 6.2.4-2 Procedures should be established that ensure that human factors engineering review of HSI and plant configuration changes that affect the tasks performed at the modified human-system interfaces is done when necessary.

Implementation of this guideline requires that criteria for HFE review are established, that procedures to obtain this review are in place, and that persons qualified to perform those reviews are identified and available. A variety of specific criteria may be established; however, the basic test is whether the change affects the human tasks at the interfaces.

⇒ 6.2.4-3 Where the human tasks require operators or technicians to access configuration information, practical methods for temporary changes and corrections should be provided.

In the course of actual power plant operation it often becomes necessary to make temporary or short term changes to some of the information that is covered by the configuration management system or which is in similar data sources. One common example would be a temporary change to a procedure because of a component being out-of-service. There also may be changes to drawings or diagrams or even parameters that are stored in the configuration description that need to be noted immediately in case the information is used. In conventional plant interfaces, such temporary changes or corrections are addressed in such simple fashions as handwritten notes in execution copies of procedures or "red-lining" of a record copy of the diagrams. As more of the interface between the personnel and plant is presented in electronic format, these past techniques are no longer practical. The need for the capability to cope with the temporary changes still remains and the electronic presentations have to incorporate some means to deal with temporary changes. Where the configuration information used in tasks at the modified human-system interfaces is affected by a temporary change or correction, the design has to make the users aware of the temporary changes without degrading the task performance. Caution must be exercised in setting up a change procedure or protocol to ensure that temporary changes are not unnecessarily inhibited – some changes will always be necessary.

⇒ 6.2.4-4 Generating a temporary change or correction and incorporating it in the currently used information should comply with existing administrative procedures. Where the technology has changed how this is accomplished, the intent of the previously used controls should be maintained.

In existing plants temporary changes and corrections are always controlled in some manner. Those control practices need to be maintained or, where new technology or configurations make that impractical, equivalent methods need to be instituted. Special security provisions (in software or hardware) may be needed to assure that the limitations are not circumvented.

⇒ 6.2.4-5 The human system interfaces in the digital upgrade modification should incorporate limitations on making temporary changes or corrections equivalent to those required by plant administrative change control procedures.

As an example, the modification to the interface in the upgrade may inadvertently permit changes to be made without proper controls or authorization or without proper records of when and by whom the changes were made. In some cases the use of new technology and providing information in electronic form may make it substantially easier to make changes than was the case before the modification. It may be necessary to include special provisions in some commercial equipment to comply with the limitation on who can make changes and the character of those changes, i.e., commercial equipment may not include adequate security provisions.

⇒ 6.2.4-6 A temporary change or correction to an item of configuration information should be available to all users of the information.

For example, if the operators have made a temporary change to a procedure, it should be possible for the operations supervisors, the training department, engineering or others to view the procedure and recognize the change. It should not be possible to access the information in such a manner that the user is not aware of the existence of a temporary change or correction.

⇒ 6.2.4-7 Means should be provided to identify all outstanding temporary changes or corrections. Temporary changes should have a limited life. A temporary change or correction should not be allowed to become a de facto permanent feature of the HSI.

Practices are undoubtedly already in place in an operating plant to address the issue covered by this guideline; however, changes resulting from the new technology used in a digital modification may make the methods used to accomplish the function no longer applicable. The modified system should not result in complications in making the change permanent that result in more temporary changes being maintained in a semi-permanent status.

6.2.5 Control of User-Defined Interface Features

It is expected that the new technology of the HSI for the modified systems will involve increased capability for the operators or users to tailor the information provided at the human-system interface to facilitate the particular operations in progress. This is a desirable feature; however, it raises a number of potential human factors problems that need to be considered in the design process. The user-defined displays should consider the tradeoff between benefits and the potential to introduce additional sources of human errors. There will also need to be design effort devoted to assuring the following:

- The tools used to create such displays are easy to use and result in valid information being displayed.
- The operators and other users are trained in how to create such displays.
- There are clearly defined limits to the access to plant data and software so that unintended effects are not produced in creating a display.

The issues surrounding the control of the configuration of these user-defined displays are clearly outside the scope of plant formal configuration management as it is currently defined. Although they are closely related to the design of displays covered in Section 4.1, they are also closely related to managing the plant configuration and to the human system interface and will be covered in this section of the guidelines. These guidelines are usually stated in terms of displays; however, any user-defined feature (such as selectable alarms) may involve similar issues and are intended to be covered by the guidelines.

⇒ 6.2.5-1 Methods to provide for the management of user-defined features of the human-system interface that are provided as part of the upgrade modification should be established and the interface designed to support that management.

Although user-assigned features may improve the effectiveness of the operators and the staff, they also may promote variability in operating practices. This, in turn, can result in individual-to-individual variations in how the plant is operated or how activities are performed. These individual variations may introduce desirable practices; however, they may also introduce ad hoc and unreviewed practices. This guideline is directed at ensuring that these user-interface features do not become a source of varying (and sometimes unpredictable) operational techniques or results.

⇒ 6.2.5-2 Protocols should be established as to what will be done with special displays of information when shifts change or operators are relieved.

For example, if the expectation is that special displays will be left in place for use by the next shift or the relief operator, that capability should be provided. However, this capability might be unavailable if each special display is associated with a particular operator and the operators are logged on or off the system.

⇒ 6.2.5-3 Means should be provided so that supervisors can know what special displays are being used by the persons that they supervise. Furthermore, the supervisors should have easy access to the identical display.

Effective supervision of a highly technical task requires that supervisors know what information their workers are using as a basis for their actions. The supervisors are generally more senior and experienced and may recognize the fallacy in a display that a worker is using. For some simple modifications, the supervisor may be able to view the operator’s activities and displays directly; however, as the displays or controls become more compact, this may not be practical and special provisions to permit the supervisors to see what the individual operators are using will have to be provided.

⇒ 6.2.5-4 Methods should be provided to monitor and record the use of special displays. These records should provide information on who created the special display and when it was in use. The records should also provide the ability to reconstruct the display itself. (Additional guidelines related to the use of these records are provided below.)

There are a number of reasons to keep careful and complete records of what special displays are in use. Some of them are discussed in subsequent guidelines. These purposes should be used as a guide to establish the specific methods of monitoring and recording. In many ways these records supplant the records in a conventional human-system interface that would be found in the operators’ log entries. They are not intended to be a means to “spy” on the operators. Such provisions need not be automatically provided; however, they should also not burden the operators with record keeping chores. For example, it may be adequate to note the time and date a display was used to establish who created it, since other records would show which operators were on duty.

⇒ 6.2.5-5 The records should be configured so that they could be used as indications of the need for changes in the plant or the human-system interface.

Consistent or repeated use by several operators of the same or similar special display of information could be the indication that existing display information is deficient or that there are operational problems that need attention. In order to provide the data from which the determination of the need for change can be made, the system should provide the means for others (such as engineers, trainers, or procedure writers) to determine what special displays or definable features have been used and by whom.

⇒ 6.2.5-6 Enough information should be recorded so that all special displays that were used by the operators in the course of an event can be reconstructed and properly placed in time.

It should be possible to go back to any time and determine the displays that were actually in use. An essential part of the evaluation of a plant event is the determination of what information the operators or others on the plant staff used to make their decisions. Unless the special, user-defined displays are tracked and recorded so that they can be reproduced, meaningful human factors evaluation of events will be difficult.

⇒ 6.2.5-7 Information should be recorded in a form that training personnel can evaluate the displays that were used for possible incorporation in the standard training program.

Special user-assigned displays that are found to be useful should be available and known to all operators or users. This will assure consistency of operations. It will also assist in ensuring that such displays are based on valid technical precepts.

6.3 Training Considerations Unique to Digital I&C Upgrades

6.3.1 Introduction

6.3.2 Objectives

6.3.3 New Training Topics

6.3.3.1 Operations Personnel

6.3.3.2 Maintenance Personnel

6.3.4 Use of Full Scope Simulator and Other Training Tools

6.3.4.1 Requirements for Training, Licensing, and Simulator Fidelity

6.3.4.2 Training Simulators: Challenges and Options

6.3.4.3 Guidance on Use of Simulators for Training

6.3.5 Sources of Additional Information

6.3.6 Case Study: Training and Simulation for a Turbine Controls Upgrade

6.3.6.1 Operator Familiarization and Training

6.3.6.2 New Operator Training and Operator Requalification

6.3.6.3 Full-Scope Simulator Upgrade

6.3.6.4 Other Simulations and Tools

6.3.6.5 Engineering Design and Testing

6.3.6.6 Procedure Development and Validation

6.3.6.7 Maintenance Training

6.3.6.8 Conclusion and Plans for Future Modifications

6.3.1 Introduction

This section discusses training considerations and challenges related to digital I&C upgrades and the introduction of computer-based HSIs. It does not describe how training programs should be developed or modified. Utilities routinely conduct training and develop new or modified training courses using a systems approach to training (SAT) per 10 CFR 50.120. The foundations of such an approach are (see 10 CFR 55.4):

- A systematic analysis of tasks and jobs to be performed
- A systematic analysis of tasks and jobs to be performed
- Development of learning objectives derived from an analysis of desired performance
- Design and implementation of training based on the learning objectives
- Evaluation of trainee mastery of the objectives during training, and
- Evaluation and revision of the training based on the performance of trained personnel in the job setting.

This approach is applicable to training on digital upgrades just as it is for other plant modifications to which it is routinely applied. Because modernization does not result in the need for a fundamentally different approach to training, this section does not describe how training programs should be developed or modified to support modernization. Rather, it discusses specific training considerations and challenges that should be addressed in training some of which are unique to digital I&C upgrades and the introduction of computer-based HSIs. New operations and maintenance issues that should be addressed are identified, and challenges associated with modifying and using the plant reference simulator to support training are discussed.

Experience at plants that have undergone modernization has shown that the introduction of digital technology presents some new issues that should be addressed in training, both for operations and maintenance personnel. Modernization can result in a significant change to how personnel perform their tasks. Some of the changes stem from aspects of performance that may not be fully addressed in current training programs, such as how to interact with computer-based

HSIs. For example, since the functionality of analog HSIs was fairly limited, it was relatively straightforward to address these in formal training. However, computer-based HSIs introduce a range of new "secondary tasks", requiring new knowledge and skills merely for the purpose of interacting with the HSIs. These interfaces require more attention during training so that personnel can understand how they process information and commands, the flexibility that is built into them, their failure modes, and how the interfaces should be managed to best support the required tasks.

Also, there are some significant challenges involved in using the plant simulator to provide training on the modifications while still supporting other training needs. The simulator must be modified to reflect the changes made in the plant, and it plays an important role in familiarizing and training the operators on the new systems and training issues discussed above. This leads to a need to modify the simulator well before the changes are made in the actual plant. But at the same time, the simulator must allow for training and re-qualification of operators on the existing configuration, particularly for a multi-unit plant sharing a single simulator. This results in some challenges related to scheduling of the simulator modifications, and the potential need for use of other simulation and training tools.

New training issues are discussed in Section 6.3.3. Use of the plant simulator and other tools, and scheduling challenges associated with simulator modification are covered in Section 6.3.4. The latter includes a Case Study that describes how training and simulation were handled for a turbine control system upgrade.

6.3.2 Objectives

The objectives of this section are:

- To identify operational and maintenance topics to be addressed in personnel training programs that arise from the transition to digital technology and, therefore, may be new to utilities, and
- To address the coordination of plant modifications, training facility modifications, and ongoing personnel training.

6.3.3 New Training Topics

Training is a very important part of ensuring proper and efficient use of digital I&C systems and computer-based HSIs. This section identifies new training topics that may be introduced by the change from analog to digital I&C systems and HSIs. Topics are identified separately for operations and for maintenance personnel.

Each topic is defined in terms of what a training program should address (not how to address it), followed by a technical discussion of the topic that provides additional information and examples illustrating the issues.

6.3.3.1 Operations Personnel

This section discusses important training topics for operations personnel, including:

- Changes in crew roles, responsibilities, and teamwork
- Understanding the characteristics and functions of computer-based HSIs
- Interacting with automatic systems and decision aids
- Recognizing and handling failures
- Dealing with hybrid HSIs
- Working with temporary, interim configurations

Note that these topics are related and the issues associated with them overlap. In discussing them separately, we are trying to isolate considerations to be addressed in crew training.

6.3.3.1.1 Changes in Crew Roles, Responsibilities, and Teamwork

Crews should be trained on how their roles and responsibilities may be changed by the availability of increased automation and HSI functionality. A very important aspect of this training should include how to maintain teamwork and effective communication.

Discussion

NPP crews work as teams. Behaviors that are typically identified as important elements of teamwork include having common and coordinated goals, maintaining shared situation awareness, engaging in open communication, and cooperative planning. Successful teams monitor the status of others, back each other up, actively identify errors, and question improper procedures. In Section 3.5 the effects of plant modifications, automation, and technology on teamwork and team processes were discussed. Technology can impact the roles and responsibilities of crewmembers and teamwork. For example, experience has shown that when crewmembers operate at individual compact workstations, communication among the crewmembers is diminished and each operator is less aware of what other team members are doing. Measures may be taken in the design to help foster team communications, and training can reinforce the need and approaches for maintaining team communications.

Any changes to teamwork brought about by the new technologies need to be addressed in training, including changes to:

- Individual crewmember roles and responsibilities
- Ability to maintain communication and team situation awareness
- Strategies for supervision and peer checking.

6.3.3.1.2 Understanding the Characteristics and Functions of Computer-Based HSIs

Crews should to be trained on the functions, capabilities, and limitations of the new computer-based HSIs. Crews should be trained on the interface management features of the HSIs and on effective strategies for their use in various situations. The training should address topics such as navigation within and between screen displays, manipulation of on-screen features such as windows, and use of user-definable characteristics and features. Crews should also be trained to understand the relationships between HSI features.

Discussion

The discussion of this topic is broken into four areas:

- HSI Capabilities and Functions
- General Interface Management Strategies
- Use of User-Defined Features
- Understanding the Relationships Between HSI Features.

HSI Capabilities and Functions

In Section 3.7, the differences between analog and computer-based HSIs were discussed, including for example greater integration of HSI resources, more processing of lower-level data into higher-level information, and greater flexibility to customize the way HSIs appear and are used. While these are very useful features, they do add to the general complexity of the interface. While there was a fairly close link between the meter face on the control board and the sensor it was linked to, there may be considerable software processing between the information presented in a computer-based display and the sensors themselves. This needs to be addressed in training more so than it did for analog HSIs. A couple of examples will illustrate the point.

A computer-based alarm system is likely to use a number of techniques to reduce alarms and alarms may be presented on a number of different displays (see Section 4.4 for a detailed discussion of alarm processing and display). When the new alarm system is used, its behavior may be different from the old alarm system. For example, in a particular scenario an expected alarm may not be seen because it was suppressed by the alarm system. The actions of the software processing may not be obvious to operators unless they are sufficiently trained on what the processing is doing. Alarms may also appear in multiple places, such as in a process display and on a message list. Operators need to be trained on the relationship between the same alarms as they appear in different displays.

Another example is higher-level information displays. In a “one sensor-one display” control room, operators have to integrate parameter information themselves to make sense of what the indicators are telling them. In computer-based control rooms some of the integration takes place in the HSIs. Where large amounts of information at various levels of abstraction are consolidated into one or more graphic formats, training in the interpretation of the displays becomes very important. Operators should be trained on the relationship between (1) the display and the plant states it represents understanding of the plant. The basic characteristics and functions of computer-based HSIs are sufficiently different from analog HSIs that training in their use and interpretation is needed. The training should address all features of the user interface, including those that are infrequently used.

General Interface Management Strategies

Many computer-based HSIs provide multiple ways of doing the same thing. The HSIs typically provide a great deal of flexibility. This enables the HSI to be tailored to meet personnel preferences or to better meet the operator's information needs for a particular task. For example, information can be retrieved in many ways on a display: by clicking an icon on a mimic display, selecting it from a pull-down menu, or inputting the display designation through a keyboard command. Once retrieved, this information can be viewed in many ways.

There are often preferred strategies for particular situations that can minimize the workload associated with information access and management. However, the focus of simulator training is usually on plant operations and handling emergencies properly. There is usually little training on how the HSIs should be used during a scenario. It is up to the individual crewmembers to decide how to use the HSIs. This results in individual variability between crewmembers with respect to the extent to which they use the different HSI resources and how they use them. Without proper training, HSI use may become burdensome and inefficient.

This training does not necessarily have to be conducted on the plant's full-scope simulator. In fact, it may be more effectively accomplished using other simulation means – see Section 6.3.4.2 for further discussion.

Use of User-Defined Features

Computer-based HSIs may provide special features for individual users to define functions for their own use, e.g., to define a temporary alarm setpoint on a troublesome parameter to support monitoring. The appropriate use of such features and their control should be addressed in training. Operators should understand the value of such features and when to use them. They also should be trained to prevent misuse or for such features to provide misleading or confusing information to other crewmembers.

Another example is the use of operator-defined displays. Even in plants with the most well conceived display systems, situations may arise that could not be anticipated by the display designers. To assist crews in managing these situations, the display system can provide tools for the easy creation of user-defined displays. Examples of such situations include:

- Monitoring a combination of plant parameters that are not presented on a single display
- Monitoring an important maintenance activity that is being performed in the plant from the CR, using closed-circuit television with an onscreen task sequence list and timer

Such flexibility needs to be designed and used with caution to ensure that users cannot negatively impact existing operational displays and that the quality and correctness of new displays is assured. Users also need to be trained on potential problems that can be created, such as omitting important information. Providing some controls over user-defined displays and training in their use can help address these issues. See Section 6.2 for further guidance on appropriate control of user-defined features.

Understanding the Relationships Among HSI Features

Training should also address the relationships among HSI resources, such as alarms, controls, and procedures. There may be significant overlap of functionality among these different resources, for example:

- The ability to perform a control action from a soft control screen or from a computerized procedure
- The presence of an alarm on an alarm display, on a mimic display, on a soft control, or a computerized procedure
- The display of parameter information in information displays, procedures, etc.

Operators should be trained about the consistency and inconsistencies across similar HSI functions.

6.3.3.1.3 Interacting with Automatic Systems and Decision Aids

Crews should be trained on the proper use of automation and decision aids. They should also be trained on supervision of these aids, including the need to verify the correctness of key analyses and assessments using independent information. Finally, they should be trained on the potential for over-reliance and complacency in the use of automation and decision aids.

Discussion

Many of the considerations discussed in the previous topic (Understanding the Characteristics and Functions of Computer-Based HSIs) apply to automatic systems and decision aids. In this discussion the focus is more on the human role in interacting with them. In Section 3.3.1.2, The Changing Concept of Automation, there was a discussion of how digital systems offer the opportunity to extend concepts of automation to more flexible process control (such as shared control) and to cognitive processes that are typically crew activities. The CBP example described in Example 3-1 is an example of a DA. DAs also include computerized operator support systems (see Section 4.6 for examples of such systems). For simplicity, we will refer to all such systems collectively as decision aids (DAs).

DAs offer a great potential to improve overall performance, reduce workload, and minimize errors. One way they do this is to provide support for difficult or complex tasks. Another way is by automating lower-level activities, such as data collection (e.g., accessing plant parameters), thus freeing operators up for more high-level supervisory activities. To achieve this benefit, personnel require training on the proper use and limitations of DAs. Important considerations involve DA supervision and guarding against over-reliance and complacency.

The first step in supervising DAs is to know when they should be used and under what circumstances their effectiveness may be limited. Most DAs are designed with the recognition that the user is the cognizant decision-maker. Training needs to foster the ability of crews to detect that a DA is off-track and how to redirect it. For example, DAs should contain features that enable users to query the basis for a conclusion and to allow operators to override them at any point and redirect them in some way. This includes having (1) multiple diverse sources of information available to operators in the control room, and (2) effective communication among the operators in order to detect and correct cases where the DA is off-track.

While DAs provide valuable support, it is important for crews to know their limitations. For example, DAs might provide incorrect information because their interpretation of information may not be as complete or reflect the depth of understanding of human crews. For example, a DA may make an assessment as to whether a parameter is "stable or increasing" based on a limited scope of information such as an analysis of trend data. However, operators making the same assessment may consider not only the behavior of the parameter in question, but also: (1) other current situational factors (such as a cooldown that is temporarily decreasing pressurizer level), and (2) changes that are likely to occur in the near future (such as if the crew is about to take some action that will increase the cooldown rate) that will affect the behavior of the parameter. A prime example is that cooldown will affect RCS level and pressure, as well as SG level and pressure. The training implication is that crews should thoroughly understand the potential limitations of the technology and should verify DA guidance if they question the accuracy of the guidance. This discussion highlights the importance of training operators to utilize multiple independent sources of information in the control room (e.g., alarms, graphic displays, and board indicators) to double-check a DA. Operators should be trained to verify DA analyses and conclusions at key points using independent methods.

Maintaining a supervisory role is also important after operators become familiar with and trust automation and DAs. Sometimes this trust leads to a tendency to accept their assessments without sufficient oversight. Training can help reinforce the importance of the operators' supervisory responsibilities.

6.3.3.1.4 Recognizing and Handling Failures

Crews should be trained to understand the ways in which I&C systems and HSIs can degrade and how to recognize and handle such failures. This training should include how to cope with complete failures of the systems.

Discussion

Failures of sensors, communications, and computer systems can have significant effects on the associated I&C systems and on plant behavior. Failures of digital I&C may have different and more extensive impact on the plant because of the potential for multiple functions to be affected (e.g., multiple automatic control loops failing simultaneously). Operators should be trained on these differences from the old systems and how to detect and respond to digital I&C failures.

Also, instrumentation failures can have significant effects on displays, especially as the information presented is a synthesis of lower level information. The failure modes of the display, the sources of information used in the display, and the systems that produce the display should be carefully examined for their effects on the operators' use and interpretation of the displayed information and the potential effect on plant operations.

For example, the effects of instrumentation failures need to be understood to ensure that they do not lead to incorrect situation assessment; i.e., operators mistakenly interpreting a display change as a change in process state when it is due to an instrument failure. Displays should be designed using the guidelines given in Section 4.1.7, Data Quality and Update Rate, for indicating the quality of information displayed. Related training considerations include:

- How to detect instrumentation failures
- How to discriminate failures from real process failures
- When failures are detected that affect a display, how the operational use of that display should be changed
- How to detect control failures

6.3.3.1.5 Dealing with Hybrid HSIs

Operators should be trained in the use of hybrid HSIs, i.e., HSIs that contain both computer-based and analog alarms, displays, and/or controls. This training should address:

- Tasks requiring use of both analog and digital HSIs
- Different behavior of analog and digital HSIs
- HSIs that exist in both an analog and digital form
- Non-functional HSIs

Discussion

After the completion of one or more digital I&C upgrades most plants will have hybrid HSIs; i.e., HSIs that contain both computer-based and analog alarms, displays, and/or controls. This can pose challenges to operators that should be addressed in training. In addition to the items specifically mentioned below, Section 2.3.4.1, Hybrid HSI Issues, should be consulted. It contains a list of issues pertaining to the use of hybrid HSIs and provides some additional detail.

Tasks Requiring Use of Both Analog and Digital HSIs

When operators perform tasks, they often have to use HSIs from several different systems. When some of these systems have been upgraded while others have not, they will have to transition back and forth between them. This could include performing some aspects of the task at a workstation, while others are performed at a control board. While from a design perspective, this situation should be minimized, it could happen for unavoidable reasons. Operators should be trained on the best strategy for managing the transitions between technologies during integrated task performance.

Different Behavior of Analog and Digital HSIs

The differences in the characteristics of analog and digital HSIs are a potential source of misunderstanding and confusion. A few examples will illustrate these differences.

- Displays – Digital information displays often provide digital values to the level of several decimal places. This can be misinterpreted as greater accuracy that analog gauges and meters. Such is not necessarily the case. Further, digital values are often changing as the measured parameter drifts slightly up and down. By contrast, the same drifts may be hardly noticeable on an analog meter, which under the same circumstances appears relatively stable. These different behaviors should be addressed in operator training.
- Controls – Analog controls have physical characteristics that provide important feedback that helps the operator regulate control actions. These include the feel of the control and the feedback obtained when manipulating the control (called proprioceptive feedback). These features help prevent errors. Soft controls often lack these features but may have additional error protective features, such as confirmation steps. Operators should be trained in the proper use of these features and to not defeat them by, for example, accepting confirmation steps without ever thinking about them (as frequently happens in desk-top computing – for example, the automatic response to "Are you sure you want to delete this file?")
- Failure modes – Analog and digital equipment may behave differently when failures occur and these differences should be addressed in training.

HSIs That Exist in Both an Analog and Digital Form

In hybrid control rooms, there may be HSIs for the same parameter or controls that exist in both analog and digital form. These may seem to operators that they should be the same; however, they may not for a number of reasons, including the processing that occurs in a digital system. For example, the same high temperature alarm may be available as an analog alarm and a digital alarm. However, under certain circumstances, one may come in but not the other. This may be due to digital alarm processing, a result of which may be to suppress the alarm. Another similar issue is that digital information displays will probably not show exactly the same value as an analog display. Operators should be trained on what to do in these circumstances and to understand when the difference between the two is meaningful.

Non-Functional HSIs

There may be reasons why deactivated HSIs are left in place, but are non-functional.
The presence of any such HSIs should be addressed during operator training so that operators do not inadvertently try to use them.

6.3.3.1.6 Working with Temporary, Interim Configurations

Operators should be trained for proper task performance and HSI/procedure use during temporary interim configurations.

Discussion

Many large digital I&C modernization programs take many years to complete. The program may be accomplished over several outages, each representing a temporary configuration that will be in place only until the next outage. Thus, between the current design and achieving the endpoint vision, there are a series of interim configurations of systems, HSIs, and procedures. Also, during the time that a given modification is being performed, there may be temporary HSI configurations that are needed during the transition as the new equipment is being installed and before the new interface is fully operational.

Operators should be trained for these interim configurations. The changes to the configuration of plant systems may alter the way tasks are performed in unique ways that will only be in effect for the time that that configuration exists. Operators will also have to accomplish tasks with a unique arrangement of HSIs and procedures. Thus, operators will need to be trained on these unique task, HSI, and procedure configurations.

6.3.3.2 Maintenance Personnel

Specific training will be needed to address the changes in administrative control over how maintenance on digital equipment is performed and the necessary changes to the maintenance work process itself. Important training topics for maintenance personnel include:

- Workstation Operations
- Advanced Maintenance Support
- Enhanced Operations/Maintenance Communications Interface
- Effects of Digital I&C Failure on Plant Operations
- Differences in Maintenance Testing Between Analog and Digital Systems

There is some overlap associated with the above topics. However, by discussing them separately, unique considerations to be addressed in maintenance training can be identified.

With digital systems there is a significant reduction in the amount of preventive maintenance that is required for the I&C equipment. Most of the maintenance that is performed is corrective in nature. As a result, that is the primary focus of the discussion here.

6.3.3.2.1 Maintenance Workstation Operations

Maintenance personnel should be trained on the shift to workstation–based operations and on the new functionality such workstations offer.

Discussion

Maintenance is performed differently in a facility with digital equipment and these differences should be addressed in training. With analog equipment, the work process involves going to the equipment location, locally isolating the component, possibly removing it to a maintenance area for testing, making the repair, returning it to service, and having operations verify it functionally.

Many maintenance activities on digital systems are performed from specific maintenance/diagnostic workstations. Workstation oriented operations bring new functionality and significant changes to how maintenance personnel perform their tasks, some of which is explained in more detail in the sections below. This is a major change to standard maintenance work practices.

Maintenance crews will need to be trained to change their work planning, flow, and operations to workstation-based operations. This training should address many of the issues noted above for operations staff, such as:

- Changes to their roles and responsibilities and the availability of increased automation and more functional HSIs
- New functions, capabilities, and limitations of the new systems
- The ways in which the HSIs can degrade and how to recognize and handle such failures
- The interface management features of the HSIs.

With respect to this list, training for workstation based operations will entail many of the same considerations as training operations personnel in the use of new HSIs. Therefore, maintenance training should incorporate the considerations discussed under training topic “Understanding the Characteristics and Functions of Computer-Based HSIs” discussed above.

6.3.3.2.2 Advanced Maintenance Support

Maintenance personnel should be trained on the application of advanced maintenance support functionality that will be increasingly available at maintenance workstations.

Discussion

Effective testing and maintenance of plant systems and equipment are major drivers for the safety, reliability, and economics of nuclear power. The application of more advanced technology to maintenance decision making, planning, and execution has a great potential impact. Some candidate approaches are: (1) condition-monitoring sensor technology and software systems that can provide the information needed to make reliability and risk-based decisions for plant maintenance; (2) on-line monitoring and assessment using advanced instrumentation and computational technology; (3) on-line maintenance, i.e., performance of maintenance while the system or component is operating, as contrasted to waiting for the system to come off-line; and (4) virtual reality and simulation for maintenance planning.

Many of the advances rely on fairly advanced and automated diagnostics and prognostics that will be increasingly available to maintenance staffs. These technologies will enable safer and more reliable operation and extended intervals between outages to be achieved. Integration of multiple sensor data outputs through data fusion will provide signals for control and fault diagnostics of actuators and predictions of system element remaining life. The use of prognostics will provide for a proactive approach to maintenance that reduces unplanned outages, optimizes staff utilization, and provides smart self-diagnostic systems that operate with high reliability. Real-time risk models will be improved and may allow operations and maintenance personnel to optimize surveillance testing and maintenance to ensure risk due to off-normal alignments is minimized.

Training in the use of these sophisticated aids will entail many of the same considerations as for training operations personnel in the use of decision aids, thus, maintenance training should incorporate the considerations discussed under training topic "Interacting with Automatic Systems and Decision Aids" discussed above.

Thus training on the use of these more advanced support systems is very important. Training in the use of advanced HSIs and supporting systems for testing and maintenance should seek to minimize:

- Unnecessary maintenance activities
- Time to maintain
- Impact on production
- Impact on risk
- Exposure to radiation and other toxic materials

6.3.3.2.3 Enhanced Operations/Maintenance Communications Interface

Maintenance personnel should be trained on changes in communication necessitated by incorporating digital technology into the plant design basis. A very important aspect of this training is addressing changes to the work control process and the importance of communication links with operations personnel.

Discussion

There is more emphasis on communications between operations and maintenance when working on digital systems and this communication should be addressed in training. Although good communications is necessary when working on analog systems, most data from digital devices is shared among various plant systems. Work control has to be carefully coordinated to ensure that malfunctioning digital devices are not causing operators to change the status of equipment in the plant based on potentially erroneous data. This would also apply when doing calibrations or performing surveillance testing. An example of the need for enhanced communications is provided in Example 6-1 below.

Example 6-1: Example of the Impact of Technology on Teamwork
An event at a NPP that illustrates the need for enhanced communications involved a plant operating at full power when it experienced an automatic reactor scram on low reactor water level. The low level resulted from an unexpected runback of two of the three reactor feedwater pumps, which occurred while software parameters were being changed by I&C technicians in a recently installed digital feedwater control system. The cause of this event was attributed to inadequate communications between operations and I&C, and control over the control system's software. A design weakness, which was known to operations but not I&C personnel, caused the control system to automatically reinitialize to zero output when parameters were changed in certain software blocks. This drove the feedwater pump's speed-demand signal to zero for a few seconds. Incorporating and emphasizing the necessity for enhanced communications in the facility work control process training of maintenance personnel when working on digital equipment should address this need.

6.3.3.2.4 Effects of Digital I&C Systems on Plant Operations

Maintenance personnel should be trained to understand the ways in which failures in digital I&C systems can degrade plant operations and impact safety. This training should include how specific work activities on key components can impact the plant systems.

Discussion

Techniques used for isolation to achieve the needed independence and redundancy capability are different for digital and analog systems. Digital I&C systems share data transmission and combine multiple functions in a single piece of equipment (e.g., a processor module), to a greater extent than was done with analog systems. This places significant emphasis on defense-in-depth against propagation of common cause failures within and between system functions. The outputs from digital components can be used as inputs to multiple control systems. Isolation becomes difficult because these outputs may affect more than one system or train. Also, digital system maintenance or configuration errors can affect large portions of the control room HSI. An example of this involved a failure of a digital annunciator system as described in Example 6-2 below.

Example 6-2: Example of the Broad Impact of a Digital System Maintenance Error
The failure caused the overhead annunciator system in the plant control room to be inadvertently configured so that it did not update the annunciators to indicate the true alarm status but did not alert the operators to this. The overhead annunciator design allowed maintenance personnel using a remote workstation to place an event recorder in a mode other than the usual operating mode, and then enter password-protected software without encountering warning messages. The incorrect mode was set when a switch was incorrectly positioned. Then an operator, who was attempting to obtain data on system status, mis-keyed the characters of a command in a way that happened to result in what would be a valid command in that mode for some implementations of the system. In this particular implementation it placed the overhead annunciator system in a state in which it was no longer processing any alarms, making the entire system inoperable.

These types of design differences and their impact on plant operations should be addressed in the configuration control process training given to facility maintenance personnel (for additional information on configuration control, see Section 6.2 of this document).

6.3.3.2.5 Differences in Maintenance Testing Between Analog and Digital Systems

Maintenance personnel will require training on the different testing capabilities associated with digital systems, any new operability requirements, and operation of any test equipment specific to digital systems.

Discussion

Testing of digital I&C systems is markedly different than testing analog systems. Some digital devices have internal self-test or calibration capability, whereas analog devices almost always require external testing and calibration. As stated earlier, digital device testing and calibration may be performed from a workstation, not locally. If some form of local testing or calibration is necessary for the digital devices, the type of testing and the form of the testing for digital I&C devices would also be very different. Two examples that illustrate these differences are provided in Examples 6-3 and 6-4 below.

Example 6-3: Example of a Digital System Testing Error Due to Incorrect Input
In one event, testing of a recently installed digital adjustable-speed-drive modification to the reactor recirculation pumps caused a rapid reduction in reactor power of 15 percent within 40 seconds. This event was attributed to a keyboard (soft control) error in the set point of the reactor recirculation flow. A test engineer intended to type a setpoint value of 51 percent, which an operator could execute, if needed, by pressing the "Enter" key. However, the test engineer inadvertently transposed the digits (i.e., typed 15) and pressed the "Enter" key. This caused the rapid decrease in power which, when recognized and corrected by operations, was followed by an increase in reactor power. This resulted in a power excursion reportable event.

Example 6-4: Example of a Digital System Testing Error Due to Inadequate Restoration
This example involved an automatic start of the motor-driven auxiliary feedwater pumps while personnel were resetting the central processing units in the digital main feedwater pump turbine control system. While I&C technicians and a vendor representative were resetting the third of three central processing units, an inadvertent trip signal was generated for two feedwater pumps caused by inadequate restoration of the second central processing unit before rebooting the third unit. The main feedwater trip signal was generated because the system sensed that two of the three central processing units were not functional.

Replacement of an inoperable digital sensor or transmitter can be different from an in-kind replacement of an analog component. Digital components may have internal logic or software that is unique. There may also be differences in internal logic between like components of a different production series. These differences could result in failure modes and system malfunctions that were not evaluated in sufficient detail in the safety analysis report or even considered in the initial design of the facility. Effects may include common mode failures due to common software being used in redundant channels or different sensitivity characteristics to electromagnetic interference. An example of this problem is provided in Example 6-5 below.

Example 6-5: Example of the Impact of a Maintenance Related Failure
An event at a BWR involved an inoperable torus temperature monitoring system. Plant personnel found that circuit cards in one channel were defective. Maintenance replaced the circuit cards and the channel was declared operable. Subsequent checkouts showed that a module in this channel was loaded with an incorrect software algorithm that could result in potentially non-conservative output. This problem was addressed by loading the correct software. Training of maintenance personnel in the area of spare parts requisition and quality assurance was modified to emphasize these characteristics of digital systems.

6.3.4 Use of Full Scope Simulator and Other Training Tools

U.S. nuclear plants use full-scope, plant-specific simulators for training and licensing of new operators, and for refresher training and periodic re-qualification of operators who are already licensed. These simulators replicate the control board instrumentation and the main control room and workstation layout. They include models of the plant's dynamic behavior to provide high-fidelity simulation of normal operation and emergency conditions, including design basis accidents and other plant malfunctions.

Section 6.3.4.1 discusses the requirements for maintaining fidelity of the full-scope training simulator as changes are made. Section 6.3.4.2 discusses scheduling and other challenges associated with use of the full-scope simulator to support training on the new system, while maintaining capability to train and re-qualify operators on the present configuration. That section also identifies other simulation options and tools that might be considered in order to meet these challenges. Finally, Section 6.3.4.3 provides guidance on identifying specific training needs and selecting simulation options and tools that can be used to meet those needs.

6.3.4.1 Requirements for Training, Licensing, and Simulator Fidelity

As discussed in Section 2.5, operator licensing is governed by 10 CFR 55. Licensees are required to provide adequate training and maintain qualifications of the operators as changes are made to the plant, control room, or other HSIs. This is done now when small changes are made to the control room from time to time. Major control room changes made as part of an I&C modernization program can have a much greater impact on training and qualification exams. However, there is no “re-licensing threshold.” The same requirements apply as for any other change that affects operator training and qualification – these must be kept up to date with the control room so that the operators are always satisfactorily trained and qualified on the plant they are operating and the training program retains its accreditation by INPO and approval by NRC.

The regulation 10 CFR 55.46 contains requirements on simulation facilities. It gives the basic requirements for scope and fidelity of the plant-referenced simulator. Regulatory Guide 1.149 addresses simulation facilities for use in operator training and license examinations. It endorses ANSI/ANS-3.5-1998, including its provisions “for upgrading simulators to reflect changes to reference plant response or control room configuration.”

The ANSI standard provides requirements for simulators used for operator training, testing and requalification. It requires a “training needs assessment” for any deviations between the simulator and the reference plant (§4.2.1.4). It also requires that “reference unit modifications determined to be relevant to the training program shall be implemented on the simulator within 24 months of their reference unit in-service dates, or earlier if warranted by a training needs assessment” (§5.3.1.2). See the Roadmap to HFE-Related Regulatory Requirements and Guidance in Section 5.5 for more information and pointers to regulatory guides and related information.

NRC and INPO expect that training programs will be updated as necessary in accordance with a systems approach to training (SAT), and that the reference simulator will be maintained such that it meets the requirements of 10 CFR 55.46 and ANSI/ANS-3.5. They have not provided any additional guidance or requirements on training and simulator modification to support I&C and control room modernization.

6.3.4.2 Training Simulators: Challenges and Options

Modernization of the I&C systems and the control room presents several challenges with regard to the plant simulator and support of operator training:

- The plant simulator is typically used nearly full-time to support initial operator training and qualification, refresher training, and re-qualification of operators. As a result, it is difficult to find the time to make any significant modifications to the simulator while still supporting the routine training needs.
- The changes made during modernization can be significant in terms of their impact on operations, and the differences between analog and digital technologies raise new training issues that should be addressed (see Section 6.3.3). As a result, there is a need to start familiarizing and training operators on the new system well in advance of the actual installation. Trainers often would like to have nine months to a year in which to accomplish the training prior to making major analog-to-digital upgrades affecting the control room.
- The challenges are even greater when a utility has a multi-unit site at which the plants are being upgraded on different schedules, which is often the case.

All of this leads to the need for additional simulation capability to support parallel training activities. One solution is to procure a second full-scope simulator; however, this is an expensive option. In addition, it may not provide the best solution. Some aspects of training benefit from use of a partial scope or part-task simulator focusing on specific training objectives (e.g., learning to manage the user interface to a digital system) without the distractions associated with having the rest of the control room (all the controls, indications, and alarms) and control room environment active at the same time. Also, trainees can do more independent exploring and trial-and-error exercises using a stand-alone system than they would do when the interface is in an instructor-led or group exercise using the replica simulator.

A number of advancements in computing and simulation technologies have occurred that allow for other options beyond purchasing a second full-scope simulator. These advancements and related trends in the use of various types of simulation for operator training are discussed below:

6.3.4.2.1 Portability of Plant Dynamic Models

The computing capability of desktop computers (e.g., Windows™ based PCs) has advanced to the point that they can run full plant dynamic models. This allows for much more flexibility and portability of training simulators. A PC-based simulator can provide simulated plant behavior that is of the same fidelity as the full-scope simulator, because it uses the same models.

6.3.4.2.2 Expanded Application of Models

Utilities can leverage their investment in the dynamic models that were developed for the replica simulator. For example, in addition to various uses for training, the dynamic models also can be used to support engineering design and evaluation of new control algorithms, or to check out new digital implementations of existing control logic, without having to use the full-scope simulator or the actual plant to verify them.

6.3.4.2.3 Use of a Range of Simulator Types to Meet Different Training Needs

Since the original introduction of full-scope, replica training simulators there has been an international trend toward use of a wider range of simulator types in order to meet different needs related to operator training. These can supplement (but not replace) the use of the full-scope simulator. They include part-task simulators, basic principles simulators, compact simulators, and other training devices that provide cost-effective training for specific purposes and reduce the demand on the full-scope simulator (see IAEA-TECDOC-995 for more information).

6.3.4.2.4 Modular and Reconfigurable Simulators

Another trend is toward more modular designs that allow simulators to be reconfigured to simulate different HSIs. As modern computer-based HSIs are introduced, this enables greater flexibility in what can be simulated and how quickly a simulator can be reconfigured. Even hard control panels can be fabricated in a modular fashion with "plug-and-play" capability to swap out one design for another, each interfaced to the same plant model when it is made active. Flat panel displays can be overlaid or mounted above a section of a hard panel and activated when a new interface (emulated on the display) is to be tested or used in training. Workstations can be mounted on rolling carts so they can be wheeled in or out as needed, again with plug-and-play interfaces to the rest of the simulator.

6.3.4.2.5 Improved Emulation of DCS Control Logic and Operator Interface

When building a simulator, or modifying the existing simulator, decisions must be made regarding whether to "simulate," "emulate," or "stimulate" the equipment and systems that are to be represented. Here we use these three words to distinguish between the following options:

- Simulation – write software (possibly custom code) that simulates the behavior of the actual system or equipment as an integral part of the simulator
- Emulation – use a software tool that can "translate" the configuration of the actual system and produce an emulation of its behavior (without having to write software to do this); the emulation is then interfaced to the rest of the simulator software
- Stimulation – use actual equipment that is "stimulated" by (receives simulated variable inputs from) the plant models.

Of course, for the most part the behavior of the plant systems (pumps, valves, processes) is simulated in software (the plant dynamic models). But I&C systems and HSIs can be represented as software simulations, emulations, or actual equipment that is stimulated by the plant models. This choice can be made separately for the I&C control logic/automation and the HSI. Either can be simulated or emulated with good fidelity using modern PCs and graphical displays.

For either of these portions of the system, simulation using custom hard-coding can be very expensive. It also can create a maintenance problem, as the simulation software must be revised each time a change is made in the control logic (e.g., settings, loop configurations), or in the operating displays, or when the DCS vendor modifies the system software. However, technology has advanced such that emulations are now available with "translators" that read the configuration database from the DCS platform and configure the emulation accordingly. Thus, when changes are made in the plant they can also be made relatively easily in the simulator.

There still can be some difficulty when the DCS vendor makes fundamental changes in its system as this may require a revision to the emulation software, introducing additional cost and delay in implementing these changes on the simulator.

Of course, there are costs to consider for the stimulation option as well. For example, there is the initial cost of purchasing the required DCS hardware and the cost of interfacing this hardware to the simulator. Also, there can be costs associated with updating the DCS hardware when the vendor makes changes; hardware and software interfaces also may have to be updated to reflect the changes. Both the initial costs and recurring cost of maintaining the simulator should be considered when deciding between simulation, emulation and stimulation.

An additional consideration is that with emulation a simulator can be quickly changed from one software version/build to another. This can allow new versions to be evaluated while still providing for training on the previous version. It can facilitate direct comparisons of the two versions, and difference training on the changes from one version to the next.

Finally, a potentially significant advantage of modern emulations with respect to training is that they often include simulator features and instructor capabilities that are not easily implemented when actual equipment is stimulated. Examples are capabilities such as freeze, backtrack, replay, fast/slow time, and initialize for new scenario.

See Brookes 2002, Fryer 2003, and Meloni 2003 for additional information on emulation technologies.

6.3.4.2.6 Virtual Reality

This technology has advanced to the point that it is being applied in a number of maintenance and training applications, and could potentially be used for simulating the plant control room and interaction with the HSIs. It could also be used to support the design and evaluation process, thus leveraging its cost. Virtual reality (VR) technology could be used to create a virtual control room containing interactive workstations and controls and displays. The virtual control room would be linked with the plant simulator. Trainees could practice with the virtual control room in the simulator center, in a classroom, and at other locations because virtual systems can interface with the simulator software by use of Web technology. In fact, trainees and the instructor could collaborate from various locations with existing Web-based capabilities.

The plant's current and upgraded control room configurations (based on the planned I&C changes) may be incorporated into different versions of the VR software. Although not proven feasible as yet, in the future this capability may permit operators to undergo training on the upgraded virtual control room before the upgrades are completed and the simulator is modified to reflect the changes. Also, it may be possible to use virtual control rooms to train on control room configurations that are no longer represented on the plant simulator.

EPRI report 1008232 provides additional information about virtual reality capabilities.

6.3.4.3 Guidance on Use of Simulators for Training

Consider the following guidance related to modification of the plant full-scope simulator and development of other simulations to support training. See the Case Study given at the end of this section for an example of how operator training and simulation were approached for an upgrade to a plant's turbine control system. Each guidance statement is followed by a discussion that provides additional information and explanation of the guidance.

6.3.4.3.1 Training Needs and Options for Simulation Support

Examine the training needs associated with the planned upgrade and determine what types of simulation are most appropriate to support meeting those needs.

Discussion

Use of the full-scope replica simulator may not be required for much of the initial familiarization and training needed to support the upgrade. In fact, other types of simulations may provide more effective training for some aspects of the change than would be achieved with the full-scope simulator. Table 6-1 lists potential needs for operator familiarization and training, and provides information on possible simulation options to support these training needs. These are examples only – the training program and specific simulation options chosen should be based on a systems approach to training (SAT) and a training needs assessment for the specific change. (As discussed in Section 6.3.1, initial development and modification of training programs should be based on SAT per 10 CFR 50.120.) See the Case Study for an example of how training was accomplished for a turbine control upgrade and the types of simulations that were used.

Note that the training requirements will vary widely depending on the scope, complexity, level of experience with the equipment/HSI, and importance or criticality of the tasks that are impacted. See Section 2.4 for a discussion of factors that can be used to grade the modification and would likely influence the training regimen needed for a given change.

For modifications that make significant changes to the HSI, the familiarization and training may best be done in stages, beginning with basic information on the change, through hands-on use of the interface and learning how to interact with the computer-based system, to full crew complement exercises covering normal and emergency operations. Various stages of simulation can be used to support this, with increasing fidelity of the interface and the operating environment as the training progresses.

This type of progression may be most important for the first significant implementation of digital controls, when digital I&C and computer-based HSIs are first introduced. For subsequent modifications, especially those involving use of the same digital platform, the training needs would likely be reduced. They could focus primarily on the specifics of the current application.

6.3.4.3.2 Additional Training Tools

Develop additional training tools and facilities that meet the training needs and allow for parallel training activities to help meet schedule requirements.

Discussion

Examine the full range of options for providing additional simulation capability, including:

- Portable desktop simulators
- Classroom simulators
- Other part-task simulators that may already be available or could be developed
- Prototypes and development systems used for developing the I&C/HSI design or for full-scope simulator software development.

Table 6-1
Examples of Potential Operator Training Needs for an Analog-to-Digital System Upgrade Includeing a Modernized HSI

Training Need/Objective	Focus of Training	Approach and Options
Gain an understanding of the change, its purpose, and basic differences between the old (analog) and new (digital) system	Differences in the hardware and the system configuration versus the old system; any differences in basic functionality (e.g., in level of automation); any changes in crew roles or responsibilities	Classroom training (no hands-on simulation)
Gain familiarity with basic operation of the new plant systems (I&C and other equipment) and their HSIs	How tasks are performed on the new system; basic organization and functionality of the interface (e.g., display structure, user interface management features, the alarm system, and any operator aids that are provided)	Classroom training Use of portable simulators, prototype workstations, or development systems by operators to gain familiarity (may be ad hoc) Self-study by individual operators using a standalone machine, perhaps guided through operation of the system by an intelligent tutoring tool but also allowing free-form exercising of the new system

Table 6-1
Examples of Potential Operator Training Needs for an Analog-to-Digital System Upgrade Includeing a Modernized HSI (Continued)

Training Need/Objective	Focus of Training	Approach and Options
Gain familiarity with operating screens, important displays and their content	General layout of screens, symbols and colors; content and arrangement of specific displays for monitoring and control; basis for high-level displays, their information content and how to interpret them and query for additional detail	Classroom training Mockups or photographs/images of important displays used to build familiarity prior to actual hands-on use Self-study (see above)
Gain familiarity with user-defined features of the HSI	Basic understanding of the configurable and user-definable aspects of the interface, their purpose, restrictions on their use, and configuration control impacts	Classroom training Use of portable (part-task) simulators, prototype workstations, or development systems by individual operators to gain familiarity (may be ad hoc) Self-study (see above)
Develop skills in operating the system using the new interface and new/modified procedures	Details of the user interface; developing individual skills in navigating through displays, menus and other selections; skills in performing basic control operations, obtaining information to support tasks; understanding and using any decision aids that are provided	Classroom training Formal hands-on training using a simulator – may be accomplished using a classroom simulator, portable desktop (part-task) simulators or prototype workstations, prior to moving to the full-scope simulator Self-study (see above)
Develop skills in normal and abnormal operations with the new system and HSI in a crew environment in the control room	Normal and emergency operations (e.g., plant startup, shutdown, post-trip, design basis events); hybrid issues such as use of both old (analog) and new (digital) interfaces to perform tasks	Some of this may be accomplished initially using a classroom simulator if it supports crew-based exercises Full-scope replica simulator ultimately will provide full fidelity of crew environment and control room layout including full complement of controls, displays and alarms

Table 6-1
Examples of Potential Operator Training Needs for an Analog-to-Digital System Upgrade Includeing a Modernized HSI (Continued)

Training Need/Objective	Focus of Training	Approach and Options
Understand system failure modes and develop skills in distinguishing between and managing I&C/HSI system failures versus plant equipment malfunctions	Effects of plausible I&C and HSI failures; interpreting alarms; recognizing specific failure modes; proper response to these failures; use of backups for HSI failures; alarm response procedures and other procedures related to failures and malfunctions	Classroom training Use of a classroom simulator if it supports simulation of I&C/HSI failures; prototype or stimulated hardware may also provide a vehicle for demonstrating failure modes Self-study (see above) guided by an intelligent tutoring or computer-based training system Ultimately, exercises on the full-scope simulator will provide full fidelity in a crew environment
Develop skills in crew coordination, communication, and teamwork with the new system and new HSI	Impact of the change on teamwork or ability to maintain crew coordination; working as a team; peer checking; supervision; responding as a crew to major plant malfunctions	Exercises on the full-scope simulator will provide full fidelity of control room layout, crew member locations, crew communication and coordination

6.3.4.3.3 Simulator Flexibility

Consider building in flexibility or ability to support multiple configurations when modifications are made to the full-scope simulator.

Discussion

Ultimately the full-scope simulator will require modification to reflect the changes made in the plant (see ANSI/ANS 3.5 for requirements). It may be possible to make the changes in a way that allows switching between the old and the new configurations to support training on either of these. Examples of features that might be considered include:

- Use of overlays, ranging from a simple cover over control board instrumentation to be removed or de-activated, to flat panel displays overlaid on standoffs with emulation of new controls and/or displays with plug-in interfaces to the simulator computer. Pull-down screens might be considered to go over or in front of displays or alarms on vertical panels (see the Case Study for an example of how simple covers can be used for instrumentation that is being removed or de-activated).
- Modular panel sections with “plug-and-play” capability to swap between old and new design configurations.

- Workstations on carts that can be rolled into place and connected to the simulator to make them active.

See the Case Study for an example of simulator modifications made to allow reconfiguration for a turbine controls upgrade.

6.3.4.3.4 Simulation Support for Other Non-Training Related Activities

Consider other needs for simulation to support activities beyond training, and the potential for an integrated simulation facility to provide a more cost-effective overall solution.

Discussion

Other activities that may benefit from simulation include:

- Operating procedure development
- Engineering evaluation and verification of the digital I&C logic and HSI – simulation can allow closed-loop testing of control algorithms, help ensure translation of the old analog logic to the new platform provides the desired functionality, and facilitate demonstration and testing of operating displays to obtain operations input and review (Note: A training simulator typically would not be used as the sole means for QA design verification, but simulation can be a very beneficial aid in performing evaluations and design verifications along with other methods that may be needed to satisfy overall QA requirements)
- Factory acceptance tests or other testing of the I&C and HSI designs, which often involves at least some rudimentary simulation to exercise the new control system but might benefit from a full plant simulation
- HFE evaluations of the new interface (e.g., HFE design verification – see Section 3.8, and tests and evaluations – see Section 3.10), and human performance evaluations to validate the overall design
- Ongoing activities to support design and operational improvements.

At a minimum, these activities should be planned and coordinated to take maximum advantage of the training simulations that are developed. Combining some of these activities through use of an integrated simulation facility may be beneficial to all of them and may reduce overall costs.

6.3.5 Sources of Additional Information

ANSI/ANS 3.5. Nuclear Power Plant *Simulators for Use in Operator Training and Examination, American Nuclear Society*. ANSI/ANS 3.5-1998.

Brookes 2002. ARJ Brookes, *Emulation Technology for a Classroom Simulator, Proceedings of the 2002 Western MultiConference*. Society for Computer Simulation International, January 2002.

EPRI 1008232. *Application of 'Modern"Visualiza tion Technology to Improve Human Decision-Making*. EPRI, Palo Alto, CA: 2004. 1008232.

Fryer 2003. G. Fryer, *Nuclear Simulators –Practical Advice for I&C Upgrades, International Conference on Simulation Training for Nuclear Power Plants and Systems. Society for Computer Simulation International*, January 2003.

IAEA-TECDOC-995. *Selection, Specification, Design and Use of Various Nuclear Power Plant Training Simulators, International Atomic Energy Agency*. IAEA-TECDOC-995, January 1998.

Meloni 2003. R. Meloni, P. Gaffuri, and D. Pathe, *Technical Advances in Operator Training Simulator Systems, ERTC Computing Conference.* Milan, Italy, June 2003.

6.3.6 Case Study: Training and Simulation for a Turbine Controls Upgrade

This case study describes the approach that was taken by the Comanche Peak nuclear station for training and simulation in support of a turbine control system upgrade. The focus of the example is on operator training, although some information is provided on the approach used for training of maintenance personnel.

In this project, the main turbine electro-hydraulic control (EHC) system was replaced using a standard DCS platform that the utility had selected for non-safety related applications. The modification was made initially on one unit of a two-unit plant, which is supported by a single reference plant simulator. In addition to EHC, the modification also replaced the turbine-generator voltage regulator and other related controls including the controls for the moisture separator-reheater (MSR). This was the first implementation of the chosen DCS platform at this plant.

Familiarization and training of the operators was accomplished using a combination of tools, including:

1. The full-scope reference simulator, modified to allow simulation of both the existing and upgraded (digital) turbine controls,
2. A classroom simulator that incorporated plant dynamic models from the full-scope simulator and an emulation of the DCS, and
3. Ad hoc use of a simulator development system to help familiarize the operators with the new turbine controls.

This example describes the approach used for training on this modification. Figure 6-3 shows an approximate timeline for the training-related activities.

6.3.6.1 Operator Familiarization and Training

Planning for operator training began approximately 18 months prior to implementation of the upgrade, as part of planning for the overall modification. At this point the modification was sufficiently well defined that the training needs could be scoped and initial plans developed.

A target training schedule for the simulator (e.g., what scenarios are planned for various times) is set five years in advance for this plant. Because scenarios related to turbine control were not scheduled prior to the time of the modification, it was necessary to modify the simulator training schedule to move this training up on the schedule. Also, the project team coordinated with Operations and Training management to set overall requirements for operator training including a rough idea of the scope of the training, the facilities that would be needed, and the types of simulator exercises that would be required.

Familiarization and training of the operators on the new DCS interface was accomplished through the activities described below.

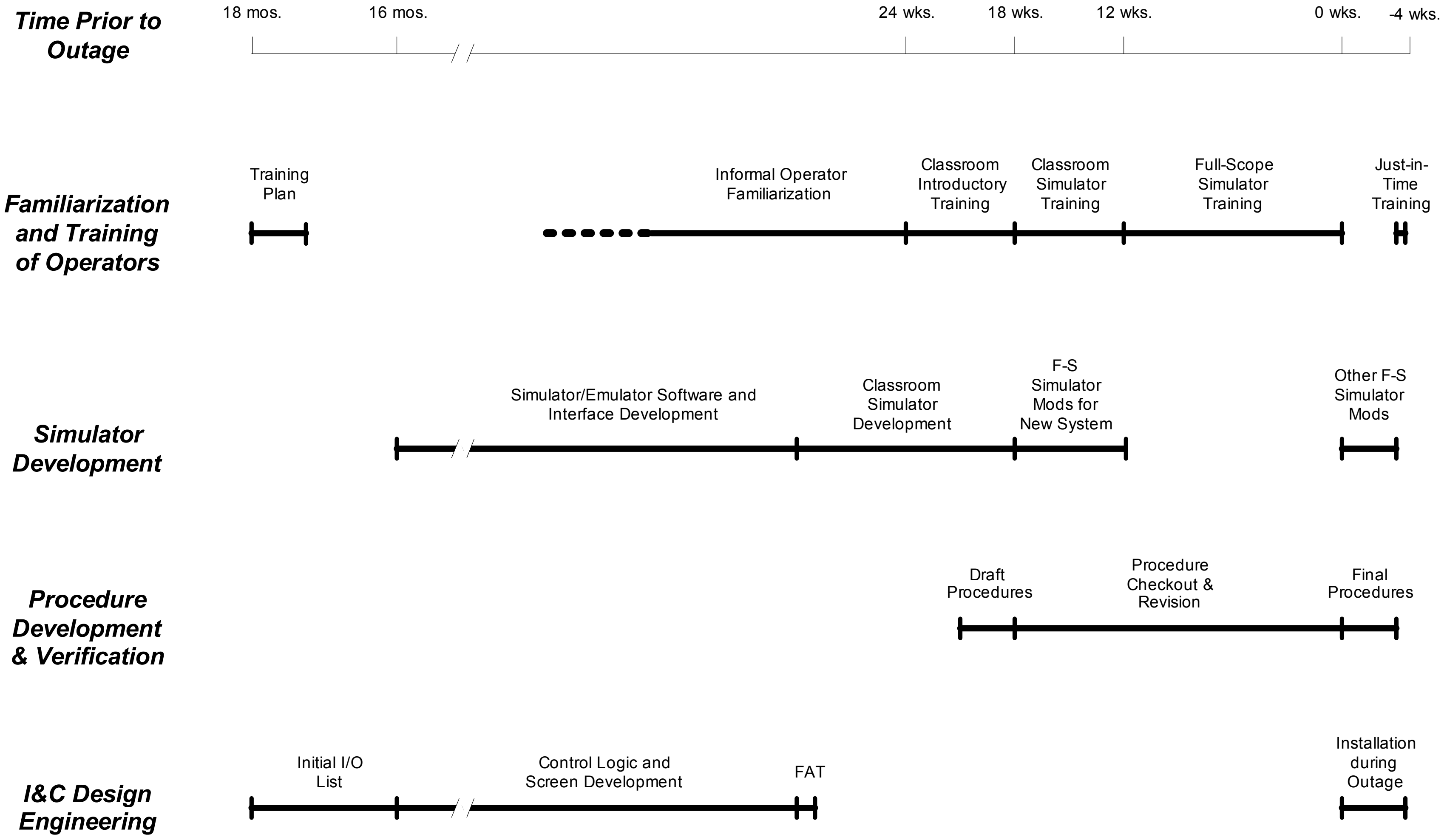


Figure 6-3
Timeline of Training and Related Activities for the Turbine Controls Upgrade

6.3.6.1.1 Informal Familiarization

Operators gained familiarity with the new control system through a variety of activities:

- An experienced operator was placed on the design team and was heavily involved in development of the turbine control displays and the alarm response procedures for new alarms generated by the system. In addition to providing crucial operations input to the design, this provided an Operations representative who was very knowledgeable on the system and could act as a liaison to the rest of the Operations staff.
- During development of the simulator changes including emulation of the operator interface, a few operators observed the activities being performed on the simulator development system to gain some early familiarity with the overall upgrade and the DCS interface.
- A copy of the development machine also was placed at a temporary location in the plant, allowing individual operators to explore and gain familiarity with the new interface at their leisure. The development machine uses a software emulation of the DCS coupled to a dynamic model of the plant derived from the full-scope simulator. This provides a realistic simulation of the turbine controls, including the DCS human-system interface, and the overall plant behavior. It can be run on any modern computer with a Microsoft Windows™ operating system. This type of self-paced familiarization allows operators to explore various features of the interface in ways that could not be done during instructor-led classroom or full-scope simulator training. For example, operators can try different things that they would not attempt during an instructor-led exercise for fear of disrupting the scenario, but which give them a much better understanding of the many features of the new HSI.

6.3.6.1.2 Formal Introduction to New System

Formal training was conducted in the classroom to introduce the operators to the new turbine control system, focusing mainly on the new hardware. The training, which was conducted in two-hour sessions, provided operators with an understanding of:

- The basis for the modification
- The operational benefits it provided
- The hardware configuration
- The differences between how the old and new systems operate.

To a degree, this was a “change management” class. It helped the operators manage and feel comfortable with the change from an analog to a digital control system for equipment that is very important to economic operation of the plant.

6.3.6.1.3 Classroom Simulator Training

Two-hour training sessions were held in the classroom to provide formal, hands-on training on operation of the new turbine control system. The training was conducted over a period of six weeks. This training was supported by a classroom simulator, which included a dynamic model of the plant (from the full-scope simulator) and a software emulation of the DCS including the operator interface. (The classroom simulator is described in more detail below in the section entitled *Other Simulations and Tools*.) Operators could each individually perform simulated startup and operation of the turbine-generator from a desktop computer screen. This training focused on normal operations – no failure modes were involved at this stage. Also, although the classroom simulator provided capability for multiple operators to work together from individual workstations, which would have allowed for some limited crew exercises, these sessions focused on training the operators to perform tasks individually using the new DCS.

There were several observers present during the training sessions who served functions other than training:

- A representative of the design team observed the operators' use of the system and identified any design deficiencies that needed correction
- The procedure writer observed the exercises to identify any corrections or improvements needed to the operating procedures
- A human factors engineer observed as part of HFE evaluation of the new interface, identifying any human factors engineering discrepancies in the design.

6.3.6.1.4 Full-Scope Simulator Training

Training exercises were conducted on the full-scope reference plant simulator. The simulator was first modified to incorporate the new control system including the DCS HSI, which was emulated through software. The training, which occurred over a time period of twelve weeks, was conducted in two parts:

1. Operation in a crew environment – this was similar to the classroom simulator training in that it focused on normal operations, but in this case it included a full crew complement rather than individual operator training. Also, the full set of controls, displays and alarms was active and available to the operators as opposed to just the turbine control system interface used during the classroom training.
2. Training on failures and abnormal operating conditions – this covered plant malfunctions and some limited training on control system failure situations. Malfunctions included automatically-initiated turbine runbacks, conditions that required a manual runback, and conditions requiring a turbine trip. Control system failures included failure of one of the operator terminals, forcing the operator to go to another terminal that remained functional.

Observers were again present during the training sessions to perform the non-training related functions listed above.

6.3.6.1.5 Just-in-Time Training

Additional training was performed using the full-scope simulator just prior to the time during the outage at which operators were to perform specific evolutions in the plant. This "just-in-time" (JIT) training was conducted about three to four days prior to the actual evolutions. Repeated startups were performed on the simulator over a six-hour time frame, covering turbine warm-up, MSR operation, generator synchronization, and some parts of the test procedures that were to be performed as part of startup testing (e.g., step changes). It was about this time that a copy of the simulator development system was placed at a temporary location in the plant, as discussed above, so that operators could gain additional contact time with the simulated system (beyond what could be done during the formal training) and obtain greater familiarity and experience in operating with the new interface.

Because the earlier simulator training lasted until just prior to the outage, and this training occurred prior to the end of the outage, this left a period of only about three weeks during the 26-day outage in which the full-scope simulator was not being used. All other simulator modifications that were needed had to be accomplished during this limited time window.

6.3.6.2 New Operator Training and Operator Requalification

Training and licensing examinations for new operators were completed before the control system modifications were made in Unit 2. In the future, new operators will be trained on Unit 1 and will receive difference training on Unit 2 (including difference training on the new control system until such time as Unit 1 has been upgraded with the new system). Requalification of existing operators will be handled in a similar manner.

6.3.6.3 Full-Scope Simulator Upgrade

The full-scope training simulator is referenced to Unit 1. Difference training is routinely conducted to address the relatively small differences between Unit 1 and Unit 2 during training of the operators.

Typically, it is preferable to make any significant modifications to Unit 1 before they are made in Unit 2, so that similarity is maintained between the simulator and the actual Unit 1 plant. However, for reasons unrelated to training, the turbine control modification was made first to Unit 2. Because the simulator required modification to support training on the new Unit 2 configuration, this resulted in a significant difference between the modified simulator and the actual reference unit (Unit 1). Also, this change presented the problem of how to accommodate training and qualification of operators on both units during the time period in which one unit was modified and the other was not.

To address this, a scheme was developed that allows training on either unit's configuration by making some relatively simple changes to the simulator to switch from one configuration to the other. The new DCS workstations for the turbine control modification were installed in the operator's desk area and not on the control boards. Figure 6-4 shows this. In the plant, the old controls and indications on the control boards were removed. For the simulator, however, these were retained and temporary covers were made that fit over the affected control board instrumentation. The covers can be attached or removed quickly. With this scheme, changing from the old to the new configuration requires simply turning on the new workstations at the desk area, covering the old controls and indications on the control board, and loading the updated plant model. Thus usually takes less than one hour. Covers over selected portions of the control board instrumentation can be seen in the photograph of Figure 6-4.

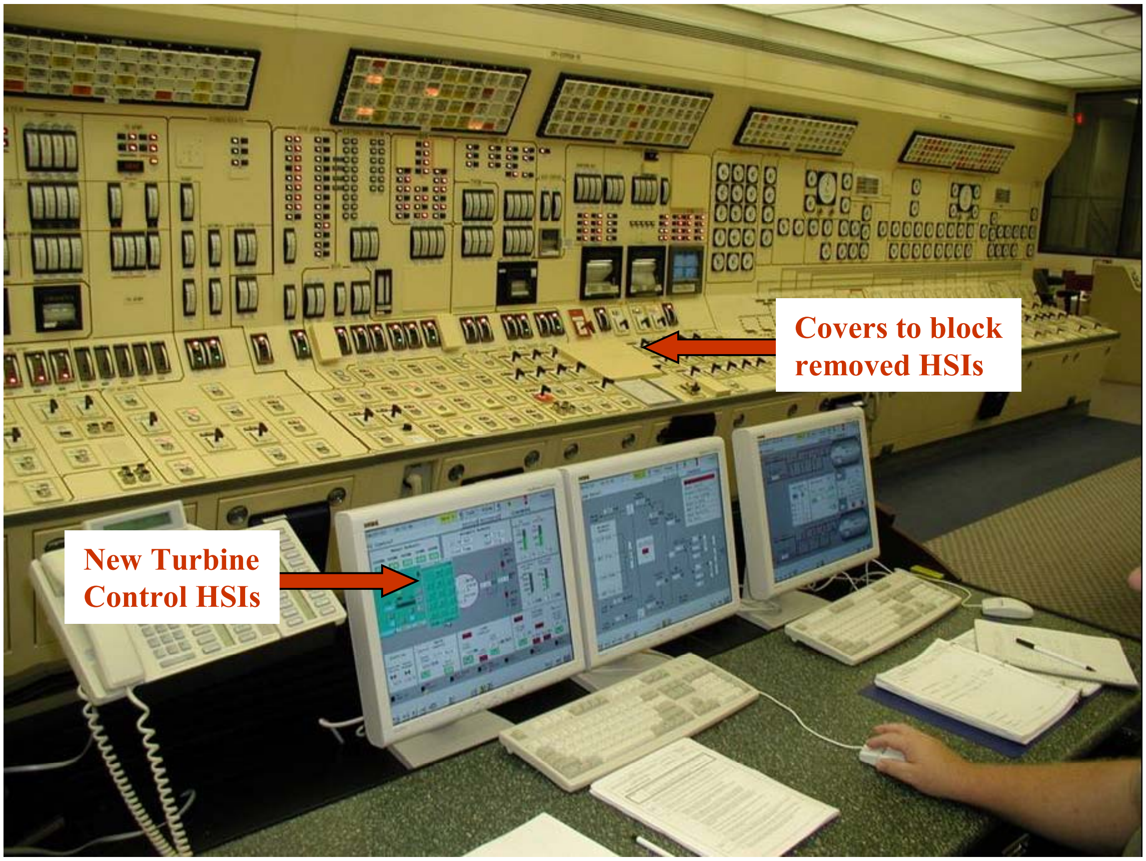


Figure 6-4
Full-Scope Training Simulator Configured for Training on New DCS-Based Turbine Control System

Modification to the simulator's software models began more than a year before to the outage, when the new control system input/output (I/O) list was reasonably well defined. There was significant software interface work required to interface the plant dynamic models with the emulation of the new control system. Some iteration was required during the time the engineering work was being completed prior to factory acceptance testing (FAT), as some items did change that impacted the simulator.

A simulator development system (see *Other Simulations and Tools* below) was used to develop and verify the new software interfaces and the DCS emulation software itself. Software to emulate the operating screens was a new product that had to be developed by the emulation software vendor.

6.3.6.4 Other Simulations and Tools

A classroom simulator was developed for hands-on training of the operators on the new turbine control system. Shown in Figure 6-5, this system provides emulated DCS workstations at each student's desk and a large overview screen at the front of the classroom. The workstations are networked to a shared plant dynamic model, providing realistic simulation of the behavior of the plant. Software emulation provides an accurate simulation of the DCS turbine controls implementation and the operator interface.

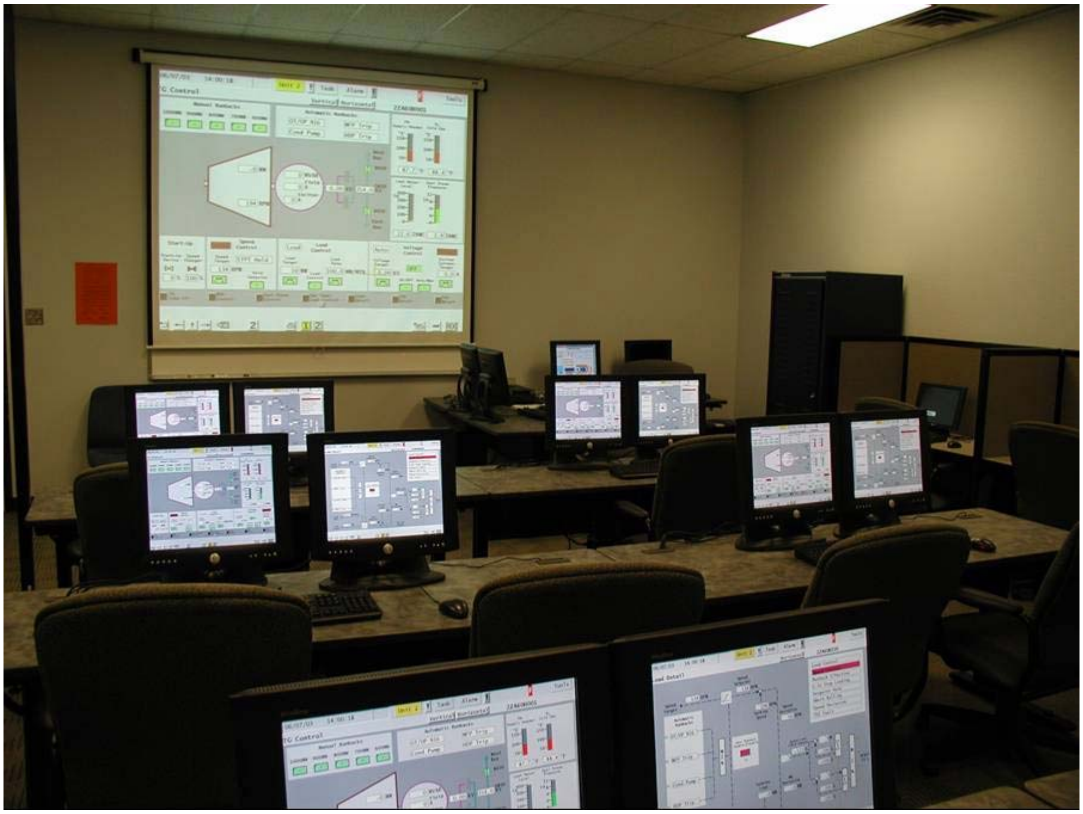


Figure 6-5
Classroom Simulator for Hands-On Training

With this simulator, all operators in the classroom can individually control the turbine-generator from their workstations. This allows individual hands-on training in evolutions such as turbine roll-up and generator synchronization (see the Classroom Simulator Training discussion above). The simulator also will be able to support crew exercises, in which operators can act together as a team using their individual workstations with the plant model reflecting the individual actions taken at each workstation. However, this feature was not used for the turbine controls classroom training.

A simulator development system was used to support development and verification of the simulator software including the DCS emulation. As discussed above, this system also was used for some ad hoc familiarization and training of operators. The development system included an actual, stimulated operator’s terminal along with an emulation of the operator interface. The DCS control logic (automation) was emulated rather than stimulating actual equipment. Use of actual control logic (DCS control hardware) would not have provided simulation features that were needed such as freeze and back-track. The system was used to test the software emulation of the DCS control logic and the emulation of the operator interface. The emulated operator interface could be displayed alongside the actual, stimulated interface to allow a direct comparison for full checkout of the newly developed emulation software.

The emulations required two basic sets of input from the engineering design activity:

1. Database defining the control logic and automation, and
2. Screen database that defined the operating displays.

The emulation software used these as inputs to generate the emulation.

6.3.6.5 Engineering Design and Testing

Engineering design work to develop and test the turbine controls application was performed using an engineering workstation purchased from the DCS vendor. The engineering workstation (actually several interconnected computers working together) provided tools for developing both the control logic (including automation) and the displays that make up the operator interface.

To support testing of the control logic and the displays, a full set of actual DCS equipment was purchased including control racks, power supplies, and operator interface terminals. These were used along with rudimentary simulations of input signals to support factory acceptance testing (FAT) of the equipment on-site. The FAT was completed approximately seven months prior to the outage.

Utility engineering personnel were heavily involved in the FAT along with vendor personnel. The vendor provided a detailed model of the turbine-generator, but the FAT facility did not include a full plant dynamic model. Inputs to the test system were simulated and some simple closed-loop simulations were developed to respond to outputs and provide simulated feedback signals so that the control system logic could be tested in closed-loop operation. In the future, the engineering/FAT testing facility and the simulator development system may be combined, allowing a complete simulation of the plant behavior to be used in testing new control systems being developed.

6.3.6.6 Procedure Development and Validation

Important aspects of procedure development and validation are noted below:

- The procedure writer was given basic training on the new turbine control system and the DCS interface. This training did not cover hardware and software; it focused only on the operation of the new system.
- The classroom simulator was used as an aid to support development and verification of the procedures.
- The alarm response procedures required the greatest effort, as they were quite different and much more extensive than the existing procedures. Other operating procedures did not require such significant changes.
- The procedure writer was directly involved in both the classroom and full-scope simulator training exercises, identifying any problems or corrections needed to the procedures or improvements that could be made based on the operators' experience in using them during the training evolutions. Comments provided by the operators in each training session resulted

in changes to the procedures used in the next session. In addition to ensuring that the resulting procedures were valid and effective, this process gave all of the operators a feeling of ownership in the procedures when they were completed.

- The timeline shows the schedule followed for procedure development. The engineering work had to be substantially complete prior to starting development of the procedures. At least a draft of the procedures was needed for the classroom simulator training, so the development had to start at least one month prior to that in order to ensure a draft would be ready. As mentioned above, the procedures were checked and refined during the classroom and full-scope simulator exercises. Final procedures were needed for the JIT training.

6.3.6.7 Maintenance Training

Training of maintenance personnel was done separate from the operator training. The control system vendor provided this training using a mobile laboratory (trailer that could be moved from plant to plant). No simulation capability was provided, as this training focused on hardware and software maintenance. Although the plant recognizes that with digital systems the demarcation between operator and maintainer responsibilities can become somewhat blurred, the traditional distinction between the two was maintained for this modification. Operators do not perform any maintenance-related activities (e.g., swapping out cards or modules to quickly restore functionality). I&C maintenance personnel are called in for this work, and the controls are placed in manual if necessary until repairs are performed.

The relative roles of operators and maintainers could change in the future as greater use is made of digital systems in the plant.

6.3.6.8 Conclusion and Plans for Future Modifications

The modification was installed successfully and the operators were able to start up and operate the new turbine control system without any significant difficulties. Some key aspects of the approach taken to training on this modification, which were considered important contributors to its success, were:

- Involvement of Operations personnel in many aspects of the change – through participation in the design effort, observing and using the development system to become familiar with the change, and helping to refine the new operating procedures based on their trial use in simulator training exercises
- Use of a classroom simulator for training on the new DCS – this simulator proved to be very effective in providing initial hands-on training without requiring time on the full-scope training simulator, for which availability is very limited
- A staged approach to operator familiarization and training, starting with general familiarization on the modification, progressing to classroom training on the differences from the previous analog system, followed by hands-on training in basic operations using the new HSI, then full-scope simulator exercises in a crew environment, and finally just-in-time training on startup and pre-operational testing evolutions

- Taking advantage of operator training evolutions to accomplish other activities associated with the project, such as development and checkout of operating procedures and human engineering reviews of the new interface in action; and
- Modification of the full-scope simulator in a way that provided flexibility for operator training and qualification on either the old or the new control system configuration.

Based on the experience and lessons learned from this modification, plant personnel expect to consider the following when planning for training and simulation support of future digital controls modifications:

- Additional training of operators on I&C system malfunctions – some of this was done for the turbine controls upgrade, but training personnel felt that more should be done in the future to better prepare operators for the various failure scenarios they could potentially face with the new digital systems. This training would help operators understand what transients can be caused by different I&C failures (module failures, failure of communication links, etc.), how to interpret the alarms that occur during these situations, and how to respond.
- Making a closer tie between engineering design and testing activities on the one hand, and training simulator development and testing on the other. For example, the plant models that are part of the training simulator could be used to support closed-loop testing of the new control system by providing simulation of plant systems and equipment, reducing the need for special input-output simulations. In the future, the simulator development system and the engineering workstation and testing facilities may be combined to support integrated simulation and testing that will serve the needs of both engineering and simulator software development and verification.

  This type of integration will become more important for future modifications that involve new control systems that interact closely with one or more systems already implemented in the plant. For example, for any new control systems that will interact closely with the turbine controls, it may be impractical to stage a complete set of stimulated DCS hardware to support integrated testing such as the FAT. Emulation of the turbine controls could be used to allow integrated tests and only require staging of actual equipment for the new system(s) to be installed.
- Potential development of a second simulator – when future modifications are made that require more extensive changes to the main control boards and control room, there is the potential that an additional simulator will be needed. At least one simulator needs to be available nearly full-time to support the heavy demand for regular operator (re-)training and (re-)qualification. The modifications required to update the full-scope simulator and the time needed to support special training on the new controls may simply be too much to handle along with the other routine training demands. However, a part-task simulator may be sufficient as a second simulator for this purpose. It could be made re-configurable to support training on the old and new control system configurations. Operators could be rotated between the two simulators as necessary.

6.4 Safety Monitoring and Control in Modernized Control Rooms

6.4.1 Introduction

6.4.2 Key Documents

6.4.2.1 Regulatory Requirements and Guidance

6.4.2.2 Industry Standards and Guidelines

6.4.3 Designing Modernized HSIs for Safety Monitoring and Control

6.4.3.1 Obtain Design Inputs

6.4.3.2 Identify Safety Monitoring and Control Tasks

6.4.3.3 Identify HSI Resources Needed

6.4.3.4 Design for Conditions in Which All HSIs are Available

6.4.3.5 Design for Conditions in Which HSIs are Failed or Degraded

6.4.3.6 Minimizing the Number of Different Types of HSIs

6.4.1 Introduction

This section addresses a number of challenging issues related to the design of modernized HSIs that provide for effective monitoring and control of plant safety functions, and meet the relevant regulatory requirements for safety monitoring and control. It also considers the need to provide diverse HSI capabilities that allow the operators to cope with postulated failures or degradation of the HSIs that are normally used, while still providing a well-integrated HSI for both normal and emergency plant operating conditions.

Specific design issues that are addressed in this section include the following:

Modern, Integrated Design Solutions for Meeting post-TMI Requirements

Following the accident at Three-Mile Island plant, the NRC and the nuclear industry established requirements aimed at providing better support to plant personnel for accident monitoring and control. This led to the identification of many different safety-related systems that have HSI aspects, e.g., SPDS, PAMS (PAMI), and BISI. In some cases the HSIs provide information about the status or availability of safety functions, systems, components, and parameters. In other cases, HSIs provide for the manual initiation of safety systems that have failed to operate as designed. Currently there is not a uniform and consistent approach to how these HSIs are designed. As a result, they tend to be separate and isolated systems that are rarely used and that may not follow the conventions of the other control room HSIs. Also, the regulatory guidance for these features was written long ago and was based primarily on the analog instrumentation installed in the plants at that time. With I&C and HSI modernization, better and more integrated approaches are possible in these areas. Some interpretation of the regulatory guides is needed in certain areas to show how more modern solutions meet the intent of the original requirements.

Qualification Requirements for HSIs

As the control room is modernized and conventional instruments and controls are replaced with newer digital implementations, design decisions must be made regarding which HSIs or HSI components must be qualified as safety-related equipment, and which ones can be implemented using non-safety equipment such as a non-safety DCS. Plants currently have qualified HSIs (typically qualified meters and switches) that can be used to control safety equipment, but in many cases this was done more as a matter of expediency than because of any specific regulatory requirements or guidance. The regulations are clear on the need for qualified HSIs to perform actions credited in the SAR safety analyses. However, they are not so clear on the level of qualification needed for HSIs used to support other emergency operations called out in the plant's EOPs. (An exception is post-accident monitoring instrumentation for which there is relatively detailed guidance on qualification requirements.) If some HSIs that are presently qualified as safety-related equipment are to be moved to non-safety interfaces or to a lesser grade qualified platform, this may require regulatory justification.

For controls that are to be qualified/safety-related, these can be retained as safety-related hard controls or they can be implemented on safety-related soft controls (e.g., using a qualified flat panel display).

Other HSI Design Requirements Including Provision of a 'Minimum Inv entory"

In addition to deciding which HSIs must be qualified, decisions must also be made on other HSI design requirements, including identifying which HSIs should be located in fixed positions, which ones should be continuously displayed, and those that can be selected by the operator on demand. The regulatory requirements and guidelines in these areas are not always clear and thus require some interpretation. A related topic is the concept of a "minimum inventory." It relates to decisions on what should be fixed position, and also what backup capabilities should be provided for when HSIs that are normally used by the operators have failed (see the next issue listed below). The concept of a minimum inventory arose as part of the NRC's reviews of advanced reactors. While the inventory pertains to advanced plants and not existing plants, it is useful to consider the issues involved and their operational consequences.

Diversity in the HSIs and Provision of Backup Capabilities

Another factor that must be considered is the need for diversity in the HSIs. Operator actions that are credited in a defense-in-depth and diversity (D3) evaluation must not be subject to the postulated common cause failures of the protection systems that they are intended to address. Potential failures of the HSIs used in normal operation also should be considered, and may lead to the need for some HSI capabilities to be implemented on equipment that is diverse from the normal HSIs. In that case, the diverse HSI capabilities that are needed are not driven by regulatory requirements, but depend on the operating philosophy or concept of operations chosen by the plant for operating under these conditions.

Competing Design Influences

The design considerations identified above can often drive the design in different and competing directions, resulting in the need to make tradeoffs. For example, in order to address credible failure modes it is necessary to provide multiple ways of accomplishing key functions using separate HSIs that are not subject to the same failures. On the other hand, it is desirable for the operators to use HSIs with which they are familiar when they are confronted with failed or degraded conditions, rather than switching to backup HSIs that are used infrequently or only in training evolutions. Also, effectiveness of the HSIs used during normal operation may be reduced if they are cluttered with backup controls and indications installed for situations that are very infrequently if ever encountered during plant operation.

This section briefly summarizes the key regulatory requirements and guidelines that relate to these issues and discusses the intent of these documents. It also identifies other design and operational considerations that should be addressed along with the regulatory requirements when designing modernized HSIs for safety monitoring and control.

Following this, a set of definitions is provided. Defining terms is essential to understanding how to approach safety monitoring and control. Many of the key documents identify HSI design requirements using different terms, such as dedicated display, continuous display, and continuously available that are not precisely defined, and hence different interpretations are possible.

Finally, this section identifies design activities that should be carried out to examine the tradeoffs and develop HSIs that meet the overall design objectives. The discussion is directed primarily at design efforts for major modernization programs for which most of the control room HSIs are involved, but the concepts and approaches also can be used as appropriate for less extensive modernization programs.

The guidance in this section should be considered when developing a control room endpoint design concept as discussed in Section 2.2 Endpoint Definition. Also, the issues covered here should be addressed when evaluating interim control room designs produced during the "migration" toward the endpoint, as discussed in Section 2.3 Migration Strategy.

This section does not provide details of the design process or specify the design solutions that should result – these will depend on the plant's specific modernization plans and control room endpoint, the I&C architecture, and the current design of the control room. Regardless of the design solution selected, the design process described in Section 3 of this document should be followed, and the HFE guidelines in Section 4 should be used to specify the detailed implementation of HSI characteristics and functions.

6.4.2 Key Documents

For the purpose of this section, the key documents fall into two categories: (1) regulatory requirements and guidance, and (2) industry guidance. The reader is referred to Section 5.5, Roadmap to the Relevant Documents, which contains a more comprehensive list of documents and their implications for HSI design. Key portions of the roadmap that are relevant to the present discussion are repeated here for the reader's convenience. Discussion of the intent of the regulatory guidance documents is provided here where appropriate.

6.4.2.1 Regulatory Requirements and Guidance

In 10 CFR 50.34(f), several Post-TMI requirements to improve safety monitoring and control were established, including:

- 50.34(f)(2)(iv) Safety Parameter Display System (SPDS)
- 50.34(f)(2)(v) Bypass and operable status indication for safety systems
- 50.34(f)(2)(xii) Automatic and manual AFW system initiation and flow indication in control room (PWRs only)
- 50.34(f)(2)(xviii) Indication of inadequate core cooling such as saturation meters in PWRs, and signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs and BWRs
- 50.34(f)(2)(xix) Post-accident monitoring instrumentation
- 50.34(f)(2)(xxiv) Capability to record reactor vessel water level in one location on recorders that meet normal post-accident recording requirements (BWRs only)
- 50.34(f)(2)(xxvii) Inplant radiation monitoring for a broad range of routine and accident conditions

The regulations, however, provided little guidance on how these systems, functions, and capabilities were to be implemented. In order to provide guidance on meeting these requirements, numerous NRC documents were developed. The key points of several are discussed below, including:

- NUREG-0800, Standard Review Plan - Chapter 18, Human Factors Engineering (and related NRC guidance on SPDS)
- Regulatory Guide1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident (Rev. 3, ML003740282)-5/1983
- Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
- Regulatory Guide 1.62, Manual Initiation of Protective Actions
- Branch Technical Position HICB-19 (BTP-19), Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (NUREG-0800 Chapter 7)

6.4.2.1.1 NUREG-0800, Standard Review Plan – Chapter 18, Human Factors Engineering

The intent of the SPDS requirement was to improve the ability of plant personnel to monitor critical safety functions and rapidly determine when safety challenges arise. Numerous guidelines were published in NUREG-0800 specifically addressing the characteristics of safety parameter displays. Additional guidance was provided in Supplement 1 of NUREG-0737 (NRC, 1980) and NUREG-1342 (NRC, 1988). The NRC review criteria for the HFE aspects of SPDS were subsequently moved from NUREG-0800 to NUREG-0700, Rev 2 (Section 5, Safety Function and Parameter Monitoring System). The NRC's HFE review guidance for SPDS is summarized in Section 4.1, Table 4-2 of this document.

NUREG-1342 notes that SPDS parameters should be continuously displayed, not just continuously available. However, the NRC has accepted SPDS systems that provide either a dedicated, single display of plant variables or a hierarchy of display pages on a single display device, with perceptual cues to alert the user to changes in the safety status of the plant (such as when safety functions are challenged).

6.4.2.1.2 NUREG-0800, Standard Review Plan –Chapter 18, Human Factors Engineering Regulatory Guide1.97 Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident (Rev. 3, ML003740282) - 5/1983

This regulatory guide addresses instrumentation for accident monitoring and describes an acceptable method to meet regulatory requirements as they relate to post-accident monitoring instrumentation, based in part on ANSI/ANS-4.5-1980. It defines types of variables to be monitored and lists specific variables of each type, along with associated ranges, for BWRs and PWRs. It also defines the categories of instrumentation, specifies what category should be used for each variable, and identifies design and qualification criteria for each category; criteria cover equipment qualification, redundancy, power source, channel availability, quality assurance, display and recording, range, equipment identification, interfaces, servicing, testing and calibration, human factors, and direct measurement criteria.

Table 2 of Regulatory Guide 1.97 identifies types of variables based on their use by operations personnel. They are:

Type A – Those variables to be monitored that provide the primary information required to permit the control room operator to take specific manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accidents.

Type B – Those variables that provide information to indicate whether plant safety functions are being accomplished.

Type C – Those variables that provide information to indicate the potential for being breached or the actual breach of the barriers to fission product releases.

Type D – Those variables that provide information to indicate the operation of individual safety systems and other systems important to safety.

Type E – Those variables to be monitored as required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.

The human factors considerations given in the regulatory guide, applicable to all categories, include:

- instrumentation should be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules
- instrumentation design should minimize conditions that would cause anomalous indications; human factors analysis should be used in determining type and location of displays
- to the extent practicable, the same instruments should be used for accident monitoring as are used for normal operation

For each variable listed, Table 2 of Regulatory Guide 1.97 identifies which of three categories of design and qualification criteria are needed for the instrumentation providing the variables. The aspects of these criteria directly related to HSI design are summarized below in terms of the need for qualified HSIs, information redundancy, and continuous information presentation.

For Category 1 instrumentation:

- *Qualification* – "Qualification applies to the complete instrumentation channel from sensor to display where the display is a direct indicating meter or recording device. If the instrumentation channel signal is to be used in a computer-based display, recording, or diagnostic program, qualification applies from the sensor up to and including the channel isolation device."
- *Redundancy* – For Category 1 instrumentation - "Where failure of one accident-monitoring channel results in information ambiguity (that is, the redundant displays disagree), that could lead operators to defeat or fail to accomplish a required safety function, additional instrumentation should be provided to allow the operators to deduce the actual conditions in the plant. This may be accomplished by providing additional independent channels of information on the same variable (addition of an identical channel) or by providing an independent channel to monitor a different variable that bears a known relationship to the multiple channels (addition of a diverse channel)."
- *Display and Recording* – Continuous real-time display should be provided. The indication may be on a dial, digital display, CRT, or strip chart recorder.

For Category 2 instrumentation:

- *Qualification* – Same as Category 1
- *Redundancy* – No specific provisions
- *Display and Recording* – The instrumentation signal may be displayed on an individual instrument or it may be processed for display on demand.

For Category 3 instrumentation:

- *Qualification* – No specific provisions
- *Redundancy* – No specific provisions
- *Display and Recording* – Same as Category 2

6.4.2.1.3 Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

Regulatory Guide 1.47 describes an acceptable way to meet IEEE 279 requirements regarding status indication for safety systems. It includes the following provisions:

- Indication should be at the system level (regardless of whether indication is also provided at the component or channel level)
- The indication should be activated automatically when a bypass or other inoperability is induced deliberately for the protection system, the system it actuates to perform safety-related functions, or any auxiliary or supporting system that effectively bypasses or renders inoperable the protection system or actuated systems
- States the conditions under which such automatic activation must be provided based on expected frequency of occurrence and need for the affected system to be operable when it occurs
- Manual capability should exist in the control room to activate each system-level indicator (allows the operators to activate it when a condition occurs that is not automatically sensed and thus does not automatically activate the indication).

Note that there are no qualification or redundancy requirements stated in this regulatory guide.

6.4.2.1.4 Regulatory Guide 1.62 Manual Initiation of Protective Actions

This document describes an acceptable way to meet IEEE 279 requirements for manual initiation of protective actions, including:

- Means should be provided for manual initiation of each protective action at the system level, regardless of whether means are also provided to initiate at the component or channel level
- Manual initiation should perform all actions performed by automatic initiation (e.g., including valve sequencing, interlocks, etc.)
- Switches for manual initiation should be located in the control room and be easily accessible to the operator so that action can be taken in an expeditious manner
- The amount of equipment common to both manual and automatic initiation should be kept to a minimum and no single failure within the manual, automatic, or common portions should prevent initiation
- Manual initiation should depend on the operation of a minimum of equipment
- Manual initiation should be designed to go to completion.

6.4.2.1.5 BTP-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

BTP-19 provides acceptance guidelines for Defense-in-Depth & Diversity (D3) assessments of digital I&C system designs. The purpose of a D3 evaluation is to assess the vulnerability of the I&C systems to common cause failures due to software design errors and ensure that the plant has adequate coping capability to deal with such failures should they occur. As stated in the Standard Review Plan (NUREG-0800) Chapter 7, Appendix 7.0-A, the NRC expects that a D3 evaluation will be performed for digital upgrades involving the reactor trip system (RTS) or engineered safety features actuation system (ESFAS). Section 5.2.3 of this document discusses D3 evaluations and the associated HSI implications. EPRI 1002835, *Guideline for Performing Defense-in-Depth & Diversity Assessments for Digital I&C Upgrades,* provides more detailed industry guidance for performing D3 evaluations, including use of risk-informed methods that are alternatives to the method described in BTP-19 (see the discussion of the EPRI document below under Industry Standards and Guidelines).

BTP-19 reiterates NRC's four-point position on defense-in-depth and diversity (see Section 5.2.3 for further discussion). Points 1-3 apply to modifications to existing plants and call for the D3 evaluation discussed above. Such evaluations typically lead to identification of a small number of specific manual actions that operators should take to cope with postulated common cause failures of digital safety systems.

Point 4, which applies to advanced reactors, indicates that "A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above." Acceptance criteria are provided, including specific capabilities that should be provided, how they should be implemented in order to ensure they are not subject to common cause failures of the protection systems, and the need for HFE principles and criteria to be applied in their design. NRC concluded this instrumentation was needed because in advanced reactors all of the protection and control systems are digital computer-based and thus potentially subject to common cause failure. Although as stated it is applicable only to advanced reactors, there is some uncertainty as to whether the same concern could be raised for existing plants that plan extensive modernization of the protection and control systems.

6.4.2.2 Industry Standards and Guidelines

This section briefly summarizes important provisions of industry standards and guidance documents that relate to safety monitoring and control.

6.4.2.2.1 IEEE 603 – IEEE Standard Criteria for Safety Systems for Nuclear Power Plants (1998)

This document includes the following requirements on control room indication and manual control (IEEE 603 section indicated in Parentheses):

- Displays needed for manual protective actions must be part of the safety systems (thus qualified) and must meet requirements of IEEE 497-1981 (5.8.1)
- Safety system status indication must be provided, but need not be part of the safety system (5.8.2)
- Continued indication of bypasses must be provided but need not be part of the safety system; requires automatic activation of this display under certain circumstances, and requires capability to manually activate the indication at any time (5.8.3)
- Requires that information displays be accessible to the operator, and displays for manually controlled protective actions be visible from the location of the controls used to effect the actions (5.8.4)
- "Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988." (5.14)
- Requires capability in the control room to implement manual initiation at the division level of the automatically initiated protective actions; minimize the number of discrete operator manipulations required consistent with redundancy requirements (6.2 paragraph a)
- Requires capability in the control room to manually initiate and control protective actions not selected for automatic control (6.2 paragraph b)
- Requires capability to implement manual actions necessary to "maintain safe conditions" after the protective actions are completed, with the associated displays and controls located in areas that are accessible, in a suitable environment, and suitably arranged for operator surveillance and action (6.2 paragraph c).

The 1991 version of IEEE 603, which contained similar requirements, was endorsed by the NRC in Regulatory Guide 1.153 Rev. 1. It is also referenced in 10 CFR 50.55a(h) along with its predecessor, IEEE 279. That regulation states that protection systems constructed after January 1, 1971, must meet the requirements in either IEEE 279 or IEEE 603. Regulatory Guide 1.153 states that IEEE 603-1991 will be used by the NRC when reviewing license applications for new plants. It states further that IEEE 603 "will also be used to evaluate submittals from operating reactor licensees who voluntarily propose to initiate system modifications if there is a clear nexus between the proposed modifications and this guidance."

NUREG-0800 Chapter 7, Appendix 7.1-C, *Guidance for Evaluation of Conformance to IEEE Std 603*, item 13 states that: "The review of information displays should…confirm that the information displayed and the characteristics of the displays (e.g., location, range, type, and resolution) support operator awareness of system and plant status and will allow plant operators to make appropriate decisions."

6.4.2.2.2 IEEE 497 - IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations (2002)

This revision of the standard was intended to provide a consolidated source of post-accident monitoring requirements and bases for the new generation of advanced nuclear plant designs, and to provide guidance allowing a flexible basis (less prescriptive than Reg. Guide 1.97) for making changes to such systems in older plants; it also was specifically intended to provide criteria for advanced instrumentation systems designs, and for design modifications based on modern digital technology. Plants can use (and some have used) the guidance in this standard to help address design issues that are not adequately addressed in Reg. Guide 1.97.

6.4.2.2.3 EPRI 1002835, Guideline for Performing Defense-in-Depth & Diversity Assessments for Digital I&C Upgrades (2004)

This document was prepared by an industry Working Group to provide guidance and alternative methods for performing D3 evaluations, including risk-informed methods that make use of risk insights from the plant-specific PRA. The methods recommended in EPRI 1002835 are considered to be acceptable alternatives to the deterministic method described in BTP-19 and NUREG/CR-6303.

The EPRI document also provides guidance in the following areas:

- Examining the I&C system design to determine where there are susceptibilities to digital common cause failure that warrant consideration in the D3 evaluation. It suggests crediting defensive measures that, if present in the digital system design and implementation, may limit susceptibility to common cause failures.
- Using the PRA to determine where diversity in the I&C systems is of value in terms of overall plant risk. This includes determining what manual operator actions can be of value, and the diversity that may be needed between the associated HSIs and other portions of the I&C systems.

Use of the guidance in this document should help in defining what manual operator actions are needed to cope with digital common cause failures, and the diversity that will be needed for the associated HSIs. Also, the approach described for evaluation of defensive measures taken in the digital system design and implementation may be helpful when evaluating susceptibility of other digital systems (e.g., control systems and HSIs) and determining what HSI failure modes or degraded conditions are credible and should be addressed in the modernization design. Finally, the EPRI guidance document discusses use of the PRA to examine overall risk associated with digital I&C and HSI upgrades early in the design process, and using the risk insights obtained to help determine the I&C architecture. Risk insights may also be obtained that could influence the HSI design for safety monitoring and control.

6.4.3 Designing Modernized HSIs for Safety Monitoring and Control

This section describes activities that should be performed to develop modernized design concepts for safety monitoring and control and to identify design requirements for the associated HSIs.

6.4.3.1 Obtain Design Inputs

6.4.3.1.1 Previous Licensing Commitments

Identify all previous licensing commitments that relate to safety monitoring and control and control room HSIs, including post-TMI requirements.

6.4.3.1.2 Current Implementations of Safety Monitoring and Control Features

Examine current implementations of safety monitoring and control capabilities, including SPDS, PAMI, BISI, etc. Identify aspects of these that are desirable to retain or to change. Determine which HSIs are presently implemented using qualified equipment or systems.

Input from the Defense-in-Depth & Diversity (D3) Evaluation

Examine the results of the D3 evaluation (if applicable), which addresses postulated common cause failures of the automatic protection systems (RTS and ESFAS). Identify manual operator actions that may be needed to back up the automatic protection system actuations and the HSIs that would be required to support those actions (including prompting indications, alarms, controls, and performance feedback). In addition to identifying the manual actions that are credited, the D3 evaluation should also specify requirements for diversity of the associated HSIs to ensure that they are not affected by the same postulated failures. This should include consideration of the potential for the failure to affect the signals or data sources as well as the HSIs themselves.

Input from I&C and HSI Failure Analyses

Examine the results of failure analyses of the I&C systems and HSIs to define other specific failed or degraded conditions that need to be considered in the design, how often these might be expected to occur, and their duration (as appropriate). **The I&C systems and HSIs should be designed to maximize the availability of these systems and minimize the likelihood of substantial loss of capability due to single failures or credible common cause failures.** However, the design and the associated concept of operations should allow for credible failure situations, including, if appropriate, substantial loss or degradation of the HSIs.

The guidance given in EPRI 1002835 can be used for evaluating potential susceptibilities to digital failures and identifying defensive design measures that may be taken to reduce those susceptibilities. Although that guidance was written primarily to support D3 evaluations, which address common cause failures of digital safety systems, it also can be applied in analyzing potential for failure of other digital systems, including non-safety systems and HSIs.

6.4.3.2 Identify Safety Monitoring and Control Tasks

Identify the tasks involved in safety monitoring and control. It is helpful to group these into categories based on the importance of the tasks in responding to emergencies as described in the safety analysis and the plant’s EOPs, and their importance to overall plant safety. EOPs typically identify multiple ways of accomplishing safety functions, or multiple success paths for recovering from abnormal events or accidents. Some of these use safety systems (“safety success paths”) to accomplish the function, while others make use of non-safety systems (“non-safety success paths”). When multiple success paths are identified, the first one specified is typically the “preferred success path.” The operators would choose this success path first if it is available.

Placing the tasks in categories can help identify and group together important HSI resources that are needed to perform safety monitoring and control functions, and lead more directly to a determination of appropriate qualification levels and other design requirements for those HSIs.

For example, the following categories of tasks might be considered:

- Manual operator actions that are credited in the SAR as part of the response to events analyzed as part of the licensing basis.
- Manual actions that are needed to accomplish the first manual “safety success paths” called out in the EOPs, for which there are no automated success paths.
- Tasks involved in monitoring and, when necessary, backing up automatic protective actions or automated success paths called out in the EOPs (this may also include monitoring conditions that could lead to automatic actions, potentially allowing pre-emptive action to prevent the need for automatic actuations)
- Tasks involved in carrying out preferred EOP success paths (those that are not safety success paths already covered above)
- Tasks involved in carrying out alternate manual safety success paths called out in the EOPs (those that are not the first safety success paths already covered above)
- Monitoring and control tasks required to sustain a steady power level, monitor the safety status of the plant, detect the need to shut down, and perform an orderly shutdown of the plant (these may become important when designing for potential loss or degradation of HSIs normally used during power operation, depending on the plant’s chosen concept of operations for those conditions).

The plant PRA also should be consulted to ensure that all risk-significant operator actions and tasks have been identified. See Section 5.2.6 for further discussion on use of the PRA.

As noted earlier, the need for use of qualified HSIs to perform the first category of tasks listed above is clear in the regulations, but the level of qualification needed and other design requirements that should be applied to the other categories are not as clear. Defining the design and qualification requirements for different categories is discussed further in Section 6.4.3.4 below.

6.4.3.3 Identify HSI Resources Needed

Identify the HSI resources needed to support the tasks that were categorized in Section 6.4.3.2 above using the HFE activities described in Section 3. For manual actions, these include prompting indications and alarms, controls, and information that provides feedback on performance of the action. For a large-scale modernization program, it can be helpful to perform both a “top-down” and a “bottom-up” review to identify the needed HSIs. The top-down review starts with the tasks and tries to identify the HSI resources needed to support them. A bottom-up review examines the existing controls, indicators, and alarms provided in the control room to ensure that all those needed or the safety monitoring and control tasks have been identified. This review also can be used to capture all the current HSI components in an inventory or database for use in identifying an appropriate disposition for each of these in the final endpoint design (e.g., retain, move, transfer to DCS, etc.).

6.4.3.4 Design for Conditions in which All HSIs are Available

Modernization programs provide an opportunity to improve the design of HSIs for safety monitoring and control and to better integrate them into the overall control room. The intent of this section is to consider these systems from an HFE standpoint to identify options for their implementation. The specific goals of the HFE design effort are to:

- Provide better consistency in the way HSIs are used from normal to emergency operations
  - the differences in the way personnel use HSI in emergencies from every day HSI usage should be minimized
  - the use of HSIs during normal operations should reinforce the knowledge and skills necessary for using HSIs during emergency operations
- Provide greater consistency in information and control design for HSIs used for normal and emergency operations
  - Differences in the look, feel, and functional characteristics of HSIs used in emergencies, versus those used every day, should be minimized
  - All HSIs should follow the same HFE principles and guidelines
  - Wherever possible, requirements for I&C diversity should not lead to diverse HSIs in terms of their look, feel, and functional characteristics
  - When diverse HSI equipment is needed to address specific failure modes, the HSI should, to the extent practical, have similar look, feel, and functional characteristics as the rest of the HSIs
- Provide better integrated support for emergency and post-accident operations across HSI resources. For example:
  - Information in computer-based displays should map well to the specific information needed by crews using EOPs
  - Alarms should be provided to support the recognition of conditions requiring EOP use and transitions

Ideally, the look and use of HSIs should be consistent and provide seamless transitions between all normal plant evolutions (from startup to power operation, to low power and cold shutdown) and abnormal and emergency conditions. Such standardization and consistency helps make the HSI transparent to the users. This maximizes their skill in HSI use and interpretation and minimizes the distractions and workload associated with using HSIs that are, by comparison, much less familiar.

6.4.3.4.1 Monitoring Information Related to Plant Safety

The general approach to monitoring information related to safety, including SPDS and PAMI displays, should be to follow the guidance in Section 4.1.3, Display Functions, of this document. That is, provide computer-based displays arranged in a display hierarchy that supports high-level monitoring and easy, rapid access to more detailed information. This approach is briefly discussed below.

Computer displays provide the opportunity to present information in a hierarchal fashion and apply coding techniques, thus making it very easy to determine overall function, system, or parameter status (status-at-a-glance functionality) and to rapidly access more detailed information when challenges or problems arise. Design approaches to accomplish this are provided in Section 4.1.3.1, Display Design for Plant Monitoring, Detection, and Situation Assessment. Using a common approach to information design and presentation across all plant situations will reduce operator burden associated with secondary tasks in using the HSIs, and make operations more seamless and less likely to lead to error.

The original SPDS concept was a stand-alone backfit system for control rooms having conventional HSIs. The limitations of conventional HSI technology made monitoring overall plant status difficult. Further, safety function information was located in various locations in the control room, thus it was difficult to access all function information at one time. More modern SPDS implementations provide a computer-based presentation of this information, providing overall status information as well as detailed information in a single location. In many acceptable SPDSs, high-level status of each safety function was continuously displayed; however, each of the individual parameters contributing to that overall status was not. In fact, that approach is preferred because it enables superior monitoring of overall status, rapid detection of challenges, and rapid retrieval of detailed information. Section 4.1.3 discusses the rationale for this type of information presentation in greater detail. Further, SPDS information can be integrated into the operating crew's primary displays, e.g., in overview displays, thus achieving a design approach that is consistent with the purpose of the SPDS. The approach to achieving this objective is provided in Section 4.1.3 (see Guideline 4.1.3.1.2-4).

The same approach can be extended to the display of PAMI information, monitoring of automatic actuations, and other safety monitoring requirements. PAMI parameters should be also situated in the spatially dedicated, continuously visible overview display. They should be graphically grouped and labeled to satisfy the requirement for their identification. However, it is not necessary to provide all PAMI parameters in the overview display. Those only used for post accident situations can be placed in a second level display that is immediately accessed from the overview display. This second level display should provide the full set of PAMI parameters, grouped and labeled, along with other supporting information and controls (as determined through evaluation of EOPs and task analyses).

For safety monitoring, a shallow hierarchy should be used. High-level monitoring of safety information using status indication is provided at the top level overview display. This display is *spatially dedicated* and *continuously visible*. From that display, the operator should be able to access more detailed information on a selected safety function in a second level display that addresses safety systems and success path information. This second level display is *continuously available*. The second level display may also provide access to manual controls, if needed (see the discussion of controls below). A third level display can provide detailed component-level information and controls.

6.4.3.4.2 Controls for Safety-Related Actions

Similarly, safety-related controls, such as those used for manual backup of failed automatic safety actuations, should be designed in the same manner as all computer-based soft controls following the general guidance provided in Section 4.3, Soft Controls. The guidance provides a general approach for identifying which should be spatially dedicated and which can be retrievable and provides guidance for detailed design features.

Soft controls offer a number of advantages over conventional control devices (as is discussed in detail in Section 4.3). Important considerations from a safety standpoint include:

- Soft control can be easily co-located in the HSI display with the relevant status and parameter information or can be continuously available (i.e., retrievable with only one user action). Thus all safety-related monitoring and control can be performed from the same location, minimizing the need to access and retrieve information and take control actions from multiple control panels.
- Control can be provided at a function or system level, in addition to providing individual component controls should they become necessary
- The soft control display can provide direct and immediate information about control status and feedback on the success of the control action.

6.4.3.4.3 HSI Organization

The organization of safety-related information and controls should follow a task-based display approach. Information and controls should be grouped together in individual displays thus making safety monitoring and control more effective. Guidance for this type of integration is provided in Section 4.1.3.2, Display Design for Task Performance. For example, a task-based display of ESFAS monitoring and manual initiation can be provided, using all of the advantages of high-salience coding to indicate problems and immediate access to manual controls. The display can also provide feedback on the success of manual operations and provide ready access to more detailed information if needed.

6.4.3.4.4 Additional Considerations

There are several unique considerations for safety monitoring, including

- bypassed and inoperable status indication
- need for redundant information
- availability of trend displays
- need for qualified HSIs

Bypassed and Inoperable Status Indication

With respect to Regulatory Guide 1.47 guidance on indication of bypassed and inoperable status, Section 4.1.3 of this document provides guidance for such indication as part of general status indication (see Guideline 4.1.3.1.2-3). In addition, the following specific guidance from the Regulatory Guide should be followed:

- Indication should be at the system level (regardless of whether indication is also provided at the component or channel level)
- The indication should be activated automatically when a bypass or other inoperability is induced deliberately for the protection system, the system it actuates to perform safety-related functions, or any auxiliary or supporting system that effectively bypasses or renders inoperable the protection system or actuated systems
- Automatic activation should be provided under the conditions stated in the Regulatory Guide, which are based on expected frequency of occurrence and need for the affected system to be operable when it occurs
- Manual capability should exist in the control room to activate each system-level indicator (allows the operators to activate it when a condition occurs that is not automatically sensed and thus does not automatically activate the indication).

Need For Redundant Information

Requirements for redundancy and protection against single failures can lead to multiple redundant indications for a single plant variable or parameter. This places the burden on the operators to combine the readings to determine the actual value, and compare them to identify and resolve any discrepancies between the readings. However, one of the advantages of digital systems is that data validation can be performed, which removes some of this burden from the operators and provides more accurate information. Further, information concerning data uncertainty can be provided. Access to individual parameter values can be provided as well as the validated result. The guidance in Section 4.1 addresses the use of data validation and quality coding (see Guidelines 4.1.7-9 through 4.1.7-14).

These design approaches can be used in the presentation of safety-related information, while still meeting redundancy and single failure requirements.

Availability of Trend Displays

With respect to providing trend information, computer-based displays provide the capability to trend almost any parameter in ways that are better and more flexible than traditional chart recorders. If trends are determined through task analysis to be the primary means by which a parameter is monitored, then a trend graph can be its primary presentation mode in the display. Section 4.1.5.6, Graphs, provides guidance on the design of trend graphs.

Need for Qualified HSIs

Determine the minimum set of HSIs that need to be qualified in order to meet regulatory requirements and ensure that HSIs needed to cope with design basis events will be available, including post-accident monitoring per Regulatory Guide 1.97. Note that the minimum required set of qualified HSIs may be a reduced set as compared to those that are presently qualified. This is because many of the existing controls and indicators used to interface with safety systems and components were implemented using qualified equipment because it was expedient to do so, as opposed to being driven by any specific regulatory requirement.

For HSIs that need to be qualified and are already implemented using qualified equipment, one option is to retain the existing equipment (in the current location or moved to another location). However, the information and controls can alternatively be placed on qualified computer-driven displays. Tradeoffs between use of existing or new qualified HSIs are presented in Table 6-2.

Table 6-2
Tradeoffs Between Use of Existing (Conventional) or New (Computer-Based) Qualified HSIs

HSI Technology	Advantages	Disadvantages
Conventional	New devices do not need to be purchased Operators are already familiar with their use	May be necessary to relocate many of the devices in order to accomplish other design objectives, such as removing old control panels Will require maintenance of the old equipment Increased training burden associated with having a mix of both types of HSIs
Computer-Based	Can use the same computer-based presentation techniques as other displays and controls, obtaining the basic advantages of computer-based HSIs (e.g., see discussion above on advantages of soft versus hard controls). Lower training burden since all HSIs work in a similar way	Qualified equipment must be purchased

Based on these considerations, for extensive modernization programs it may be most effective to replace the conventional HSIs with qualified computer-displays. For less extensive programs, either alternative may be chosen.

Graded Approach to Qualification

Different levels of qualification may be provided for HSIs performing functions with different levels of criticality or importance to safety. The plant may already have established a graded approach for digital systems qualification, and this might be used to set appropriate qualification levels for HSIs or HSI components. Full 1E qualification of hardware and software will be required based on regulations or the plant's licensing commitments (e.g., for HSIs used to take manual actions credited in the SAR safety analyses, which must be considered as part of the safety systems per IEEE 603). However, lower levels of qualification may be acceptable for other HSIs. The plant PRA might be used to help determine the needed level of qualification for HSIs based on the risk associated with the tasks for which they are needed. (See the categorization of tasks defined in Section 6.4.3.2).

Reduced levels of qualification that might be considered include:

- Full hardware qualification but somewhat relaxed software qualification – for example, HSIs used to support some important EOP success paths may not require full qualification per regulatory requirements, but are still important to safety and may be needed to demonstrate adequate capability to mitigate certain events. Relaxed software qualification requirements for selected systems have been accepted by the NRC for some advanced plant designs.
- Non-qualified but highly reliable hardware and software with a level of documented software quality assurance – some HSIs that do not require qualification but are nevertheless important to the operator's ability to handle abnormal or emergency situations warrant a level of assurance beyond that applied to other non-safety systems. Examples of this treatment in some existing plants include SPDS, ATWS mitigation systems, and critical non-safety control systems. Computer-based procedure systems implementing EOPs might be candidates for this level of "qualification" in a modernized control room.

Consider each of the categories of safety monitoring and control tasks defined in Section 6.4.3.2 above and the associated HSIs identified in Section 6.4.3.3 as part of establishing appropriate levels of qualification. Note that application of a graded approach to HSI qualification and demonstrating its adequacy is an area of potential licensing risk. Early interaction with the NRC on this topic is recommended to help minimize this risk.

6.4.3.5 Design for Conditions in which HSIs are Failed or Degraded

Based on the results of the failure analysis of the I&C and HSI systems, the design may need to incorporate diverse HSI capabilities to address situations in which the HSIs normally used are lost or degraded. The extent of the diverse HSI capability that is needed depends to a great extent on how the plant wants to respond to loss of the normal HSIs. A variety of options are possible, including:

- Immediately shut down the plant
- Maintain the current state for a specified period of time (assuming the reactor is at power and no secondary event has occurred) and monitor plant safety functions for the need to shut down
- Support power maneuvers
- Handle plant upsets and emergencies

Note that this addresses an issue that is beyond the regulatory requirement for qualified HSIs need for accident mitigation and safe shutdown. (See the discussion in Section 6.4.3.4 above on need for qualified HSIs and use of graded approaches to qualification.) This issue is driven largely by the plant's desired concept of operations for situations in which HSIs are failed or degraded.

This issue has been extensively discussed with respect to the design and regulatory review of advanced reactors. The concept of a "minimum inventory" was established in part to address this situation. (The minimum inventory concept also relates to the need for spatially dedicated HSIs; over time, it has been associated both with spatial dedication and backup for HSI failure.) While the concept was not precisely defined and was implemented somewhat differently across the individual design reviews, the basic concept was as follows. A minimal set of HSIs would be provided to accomplish the following types of safety-related considerations:

- Alarms for performing actions needed in response to design basis events for which there is no automatically actuated safety function
- Regulatory guide 1.97 Type A, B, and C Category 1 parameters
- Controls for manual safety system actuation (e.g., reactor and turbine trip and ESF actuation)
- Controls, displays and alarms for performing important human actions as defined by the PRA
- Controls, displays and alarms for maintaining critical safety functions and safe shutdown conditions

While the concept of a "minimum inventory" is applicable only to advanced reactors and not plants modernizing the I&C and control rooms, it does provide ideas as to the capabilities that should be evaluated for inclusion in the functional design of the backup HSIs. With each added functional capability, additional HSIs are needed.

Backup HSIs can be implemented using a conventional or computer-based design as long as the equipment is not subject to the same failures for which it is intended to provide backup.

6.4.3.6 Minimizing the Number of Different Types of HSIs

The need for some HSIs to be implemented using qualified equipment, and the need for some HSIs to be diverse from others in order to cope with potential HSI failure modes, can result in the operator having to use a number of different types of HSIs under different circumstances. In order to achieve the highest level of integration and consistency practical, it is important to try to consolidate as much as possible and minimize differences in the functional characteristics of the various HSI resources provided to the operators. Designers should take advantage of opportunities to consolidate HSIs to meet multiple requirements. Examples include:

- If one or more overview displays are to be incorporated into the design to provide high-level information to the entire crew (e.g., via relatively large continuous displays mounted on a wall or vertical panel), it may be possible to take advantage of this feature to meet other requirements as well. For example, using qualified flat panel displays for the overview may allow requirements for Category 1 PAMI displays to be met, and also support other safety monitoring requirements that require spatially dedicated and/or qualified displays.

- If the design incorporates the capability to monitor and control safety as well as non-safety equipment through non-safety workstations (e.g., some designs are able to accomplish this using a non-safety DCS with features that effectively prevent DCS failures from compromising the safety systems), then these workstations might be used to accomplish other functions. For example, indications and controls needed to support manual actions credited in the D3 evaluation might be accomplished using the non-safety workstations as opposed to providing separate controls and indicators for D3, as long as the postulated safety system failures they are intended to cope with do not also affect the data sources, control outputs or the workstations themselves.
- If the design incorporates the capability to monitor and control non-safety equipment as well as safety equipment through safety-related (qualified) HSIs, then these qualified HSIs might be used to allow limited continued operation during normal HSI failure conditions (e.g., failure of DCS workstations).

A
ACRONYMS

AFW	Auxiliary Feedwater
AH	Abstraction Hierarchy
ALWR	Advanced Light Water Reactor
ANN	Artificial Neural Networks
ANS	American Nuclear Society
ANSI	American National Standards Institute
AO	Auxiliary Operator
AOA	Axial Offset Anomalies
ARP	Alarm Response Procedures
ATWS	Anticipated Transient without Scram
BISI	Bypassed and Inoperable Status Indication
BOP	Balance Of Plant
BTP	Branch Technical Position
BWR	Boiling Water Reactor
CBP	Computer-Based Procedure
CCF	Common Cause Failure
CCTV	Closed-Circuit Television
CCW	Closed Cooling Water
CDD	Conceptual Design Document

CDF	Core Damage Frequency
CFR	Code of Federal Regulations
CHR	Containment Heat Removal
CMFDD	Condition Monitoring and Fault Detection and Diagnosis
COMPRO	Computerized Procedure System (Westinghouse)
COPMA	Computerized Operation Manual (OECD Halden Reactor Project)
COSS	Computerized Operator Support Systems
CPU	Central Processing Unit
CR	Control Room
CRD	Control Rod Drive
CRDR	Control Room Design Review
CReDITS	Concept Development, Requirements Definition, Design, Implementation, Testing, Support
CRT	Cathode Ray Tube
CSCW	Computer Supported Cooperative Work
CSF	Critical Safety Functions
CST	Condensate Storage Tank
CTA	Cognitive Task Analysis
D3	Defense-in-Depth and Diversity
DA	Decision Aid
DCRDR	Detailed Control Room Design Review
DCS	Distributed Control System
DG	Diesel Generator
DNBR	Departure from Nucleate Boiling Ratio

DOE	Department of Energy (US)
EAL	Emergency Action Level
ECCS	Emergency Core Cooling Systems
EdF	Electricité de France
EHC	Electro-hydraulic Control
EID	Ecological Interface Design
EOF	Emergency Operations Facility
EOP	Emergency Operating Procedure
EOPTS	EPRI BWR Emergency Operating Procedure Tracking System
EPRI	Electric Power Research Institute
ERF	Emergency Response Facility
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
F/T	Functions and Tasks
F-V	Fussel-Vesely
FAT	Factory Acceptance Test
FDA	Fisher Discriminant Analysis
FDI	Fault Detection and Isolation Stages
FMEA	Failure Modes and Effects Analysis
GDC	General Design Criterion
HA	Human Actions
HED	Human Engineering Discrepancies
HEP	Human Error Probability
HFE	Human Factors Engineering

HFIS	Human Factors Information System (NRC)
HP	Human Performance
HRA	Human Reliability Analysis
HSI	Human-System Interface
HTA	Hierarchical Task Analysis
HVAC	Heating, Ventilation, Air Conditioning
HX	Heat Exchanger
I&C	Instrumentation and Control
I/O	Input/Output
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute of Nuclear Power Operations
IPE	Individual Plant Examination
ISD	Initial Scoping Document
ISO	International Standards Organization
ISV	Integrated System Validation
JIT	Just-in-Time Training
KSA	Knowledge, Skills and Abilities
LA	Link Analysis
LAR	License Amendment Request
LCD	Liquid Crystal Display
LCO	Limited Conditions of Operations
LCS	Local Control Station

LED	Light Emitting Diode
LERF	Large Early Release Frequency
LME	Lead Modification Engineer
LOCA	Loss of Coolant Accident
MCR	Main Control Room
MSIV	Main Stream Isolation Valve
MSR	Moisture Separator-Reheater
N/A	Not Applicable
NASA	National Aeronautics and Space Administration
NEA	Nuclear Energy Agency
NEI	Nuclear Energy Institute
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OECD	Organization for Economic Co-operation and Development
OER	Operating Experience Review
OSA	Operational Sequence Analysis
OSC	Operational Support Center
P&ID	Piping and Instrumentation Design
PAMI	Post-Accident Monitoring and Indication
PAMS	Post-Accident Monitoring Systems
PBP	Paper-Based Procedure
PCA	Principal Component Analysis
PLC	Programmable Logic Controller
PLS	Partial Least Squares

PORV	Power-Operated Relief Valve
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PWR	Pressurized Water Reactor
QA	Quality Assurance
RAW	Risk Assessment Worth
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RFP	Request for Proposal
RHR	Residual Heat Removal
RO	Reactor Operator
ROP	Reactor Oversight Process
RPS	Reactor Protection System
RSP	Remote Shutdown Panel
RSR	Remote Shutdown Room
RTCB	Reactor Trip Circuit Breaker
RTS	Reactor Trip System
RWST	Radioactive Waste Storage Tank
SAGAT	Situation Awareness Global Assessment Technique
SAR	Safety Analysis Report
SART	Silence, Acknowledge, Reset and Test
SAT	(1) Site acceptance test; (2) Systems Approach to Training
SDCA	Spatially-Dedicated and Continuously-Available (control)

SDCV	Spatially-Dedicated Continuously Visible
SEE-IN	Significant Event Evaluation-Information Notice (INPO)
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SLC	Standby Liquid Control
SME	Subject Matter Expert
SPC	Suppression Pool Cooling
SPDS	Safety Parameter Display Systems
SRO	Senior Reactor Operator
SRP	Standard Review Plan
SSC	Structure, System or Component
TLX	Task Load Index
TMI	Three Mile Island Nuclear Power Station
TSC	Technical Support Center
TSV	Task Support Verification
UFSAR	Updated Final Safety Analysis Report
V&V	Verification and Validation
VDU	Video Display Unit
VR	Virtual Reality
W&W	Workstations and Workplaces

B
GLOSSARY

Analytical redundancy – The calculation of expected parameter values using a model of system performance.

Best-estimate analysis – Analysis that uses realistic inputs and assumptions – this is in contrast to the plant licensing basis safety analysis, which uses conservative values for inputs and makes worst-case assumptions. Best estimate analysis is intended to provide a realistic, as opposed to conservative, estimate of what the actual behavior of the plant will be for a given scenario.

Capture error – An error of execution (slip) that occurs when an infrequently performed action requires a sequence of operations, some of which are the same as or similar to those of a frequently performed action. In attempting the infrequent action, the more frequent action is performed instead. For example, an operator intends to perform task 1, composed of operations A, B, C, and D, but instead executes the more frequently performed task 2, composed of operations A, B, C, and E.

Common cause failures – Failures of equipment or systems that occur as a consequence of the same cause. The term is usually used with reference to redundant equipment or systems or to uses of identical equipment in multiple systems. Common cause failures can occur due to design, operational, environmental, or human factor initiators. Common cause failures in redundant systems compromise safety if the failures are concurrent failures, that is, failures which occur over a time interval during which it is not plausible that the failures would be corrected.

Common mode failure – By strict interpretation, has a meaning that is somewhat different from common cause failure because failure mode refers to the manner in which a component fails rather than the cause of the failure. However, because the discussions in this guideline are concerned with failures that can compromise safety and disable redundant systems or disable multiple systems using the same equipment, regardless of whether they are common mode or common cause, the two terms are used interchangeably in this document.

Computer-based HSI – An HSI that is presented on a VDU or other computer-driven presentation medium. (See Conventional HSI).

Computer-based procedures – presentation of plant procedures in computer-based rather than paper-based formats for the purpose of helping personnel achieve the procedures' aims.

Concept of operations – How the plant is operated (operational philosophy) – includes items such as crew size and makeup, how the crew operates the plant under normal and abnormal conditions, roles and responsibilities of individual crew members, crew coordination and supervision.

Configural display – A display in which information dimensions are uniquely represented, but where new emergent properties are created from interactions between the dimensions. Configural display representations often use simple graphic forms, such as a polygon.

Continuous-adjustment interfaces – Computer-based formats that have continuous ranges usually accessed with some type of slewing motion requiring a gross movement followed by a fine adjustment. Their operation is similar to that of continuous-adjustment controls, such as rotary dials or slider switches.

Continuously available – Information or controls that can be accessed directly (with only one user action) from a continuously visible display.

Conventional HSI – An HSI that is presented using non-computer-based hardware. Information is displayed on a meter, gauge, indicator light, or other device. Controls are physical switches such as a push button or "J" handle). A conventional HSI may or may not be linked to a digital I&C system. (See Computer-Based HSI).

Core damage frequency – Expected number of core damage events per unit time.

Defense in depth – A concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. For instrumentation and control systems, the application of the defense in depth concept includes the control system; the reactor trip or scram system; the Engineered Safety Features Actuation System (ESFAS); and the monitoring and indicator system and operator actions based on existing plant procedures. The echelons may be considered to be concentrically arranged in that when the control system fails, the reactor trip system shuts down reactivity; when both the control system and the reactor trip system fail, the ESFAS continues to support the physical barriers to radiological release by cooling the fuel, thus allowing time for other measures to be taken by reactor operators to reduce reactivity.

Dependability – A broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others.

Description error – An error of execution (slip) that involves performing the wrong set of well-practiced actions for the situation. Description errors occur when the information that activates or triggers the action is either ambiguous or undetected.

Discrete-adjustment interfaces – Computer-based formats with individual settings that usually can be accessed using fairly gross movements. Their operation is similar to discrete-adjustment controls, such as push buttons.

Display devices – The media used to present information to personnel, including meters, gauges, VDUs, and hard-copy display devices (printers and plotters).

Display element – The basic building blocks used to make up display formats, such as abbreviations, labels, icons, symbols, coding, and highlighting.

Display format – The general class of information presentation. Examples of general classes are continuous text (such as a procedure display), mimics and piping and instrumentation diagram (P&ID) displays, trend graphs, and flowcharts.

Display network – A group of display pages within an information system and their organizational structure.

Display page – A defined set of information that is intended to be displayed as a single unit. Typical NPP display pages may combine several different formats on a single VDU screen, such as putting bar charts and digital displays in a graphic P&ID format. Display pages typically have a label and designation within the computer system so they can be accessed by operators as a single "display."

Display screen – the entire software-controlled display surface of a display device (e.g., a VDU).

Diverse – Accomplish a task or function by a means different from its primary means, such that the two are not subject to the same common cause failure.

Diversity – The use of at least two different means for performing the same function. This can include diversity in how the function is performed (e.g., different algorithms, different variables sensed or physical principles applied, manual versus automatic) or in the equipment (different technologies, different hardware and/or software, different actuation means) used to perform the function.

Density – (Screen Density) The amount of the display screen that contains information; often expressed as a percentage of the total area.

Emergent feature – A high-level, global perceptual feature produced by the interactions among individual parts or graphical elements of a display (e.g., lines, contours, and shapes).

Endpoint – Concept for the final control room after modernization has been completed – a target or vision that can be used to guide the design of modifications over time so that they work toward the desired final product.

Error-tolerant features – Characteristics of the HSI that minimize the effects of operators' errors.

Feedback – System or component response (e.g., visual or aural) which indicates the extent to which the user's desired effect was accomplished. Feedback can be either intrinsic or extrinsic. The former is that which the individual senses directly from operating the control devices (e.g., clicks, resistance, control displacement). The latter is that which is sensed from an external source that indicates the consequences of the control action (e.g., indicator lights, display changes, aural tones).

Function allocation – The process of assigning responsibility for function accomplishment to human or machine resources, or to a combination of human and machine resources.

Function analysis – The examination of system goals to determine what functions are needed to achieve them.

Hardwired – A direct path from an HSI to a sensor or control, not involving digital equipment in the communication path.

Human engineering discrepancy (HED) – A departure from some benchmark of system design suitability for the roles and capabilities of the human operator. This may include a deviation from a standard or convention of human engineering practice, an operator preference or need, or an instrument/equipment characteristic that is implicitly or explicitly required for an operator's task but is not provided to the operator.

Human factors engineering (HFE) – The application of knowledge about human capabilities and limitations to plant, system, and equipment design. HFE provides reasonable assurance that the design of the plant, systems, equipment, human tasks, and the work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support the plant (see "Human factors").

Human-system interfaces (HSIs) – A human-system interface (HSI) is that part of the system through which personnel interact to perform their functions and tasks. In this document, "system" refers to a nuclear power plant. Major HSIs include alarms, information displays, controls, and procedures. Use of HSIs can be influenced directly by factors such as, (1) the organization of HSIs into workstations (e.g., consoles and panels); (2) the arrangement of workstations and supporting equipment into facilities such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility; and (3) the environmental conditions in which the HSIs are used, including temperature, humidity, ventilation, illumination, and noise. HSI use can also be affected indirectly by other aspects of plant design and operation such as crew training, shift schedules, work practices, and management and organizational factors.

Information system – Those aspects of the HSI that provide information on the plant's systems to the operator.

Integral Display – A display that depicts the integration of information in such a way that the individual parameters used to generate the display are not explicitly represented in it.

Integrated system validation – Integrated System Validation is an evaluation using performance-based tests to determine whether an integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and acceptably supports safe operation of the plant.

Interface management – Actions performed by the operator to control the human-system interface rather than the plant, including finding and retrieving displays and adjusting display windows. Operators typically navigate through displays and retrieve needed controls and displays.

Loss-of-activation error – An intended action is not carried out due to a failure of memory (i.e., the intention has partially or completely decayed from memory). A special case of loss-of-activation errors involves forgetting part of an intended act while remembering the rest (e.g., retrieving a display while not being able to remember why it is needed).

Level of abstraction – A hierarchy consisting of levels increasing in abstraction, e.g.,

- Physical form – the appearance and spatial location of the components
- Physical function – the characteristics of the components and their interconnections
- Generalized function – the basic functions a system was designed to achieve
- Abstract function – the causal structure of the process in terms of mass, energy, information or value flows
- Functional purpose – the purpose for which the system was designed; the functional characteristics of the plant as opposed to physical characteristics.

Menu – A type of dialogue in which a user chooses one item out of a list of displayed alternatives. Selection may be made by actions such as pointing and clicking and by depressing an adjacent function key.

Migration path – A series of changes to the control room to be accomplished in steps that lead toward the final control room endpoint (also *migration plan*, *migration strategy*).

Mimic – A display format combining graphics and alphanumerics used to integrate system components into functionally oriented diagrams that reflect the components' relationships.

Misordered components of an action sequence – A slip involving skipped, reversed, or repeated steps. Soft controls may be prone to this type of slip because they require sequential operations for accessing and using controls and displays.

Mode error – Performing an operation that is appropriate for one mode when the device is in another mode. Mode errors occur when the user believes the device is in one mode when it is in another one.

Maintainability – The design of equipment to support effective, efficient maintenance activities.

Maintenance – A process with the objective of preserving the reliability and safety of plant structures, systems, and components or restoring that reliability when it is degraded.

Mockup – A static representation of an human-system interface (see "Simulator" and "Prototype").

Object display – A type of integral display that uses a geometric object to represent parameter values graphically, but where the individual information dimensions or data contributing to the object are not displayed.

Operating experience review – A review of relevant history from the plant’s on-going collection, analysis, and documentation of operating experiences and from interviews with plant staff.

Performance shaping factors (PSFs) – Factors that influence human reliability through their effects on performance. PSFs include factors such as environmental conditions, HSI design, procedures, training, and supervision.

Probabilistic risk assessment – A qualitative and quantitative assessment of the risk associated with plant operation and maintenance that is measured in terms of frequency of occurrence of risk metrics, such as core damage or a radioactive material release and its effects on the health of the public (also referred to a probabilistic safety assessment).

Primary tasks – Those tasks performed by the operator to supervise the plant; i.e., monitoring, detection, situation assessment, response planning, and response implementation.

Qualified HSI – A computer-based or conventional HSI that is implemented using qualified class 1E equipment (hardware and software).

Reference plant – The specific nuclear power plant from which a simulation facility’s control room configuration, system control arrangement, and design data are derived [from 10 CFR 55.4].

Reference simulator (or plant-referenced simulator) – A simulator modeling the systems of the reference plant with which the operator interfaces in the control room, including operating consoles, and which permits use of the reference plant’s procedures [from 10 CFR 55.4].

Risk-important human action – An action that must be performed successfully by operators to ensure plant safety.

Selection display – Any display from which the operator may make a selection, such as choosing a plant variable, plant component, or a command. Two formats commonly used for selecting plant components and variables are the menu and mimic.

Separable display – Each process parameter is presented individually and no relationships between the parameters are shown by the representation itself. The key aspect of separable displays is not that individual parameters are presented, but that no interaction or relationship between them is perceived.

Soft control – A control device that has connections with the control or display system that are mediated by software rather than direct physical connections. As a result, the functions of a soft control may be variable and context dependent rather than statically defined. Also, the location of a soft control may be virtual (e.g., within the display system structure) rather than spatially dedicated. Soft controls include devices activated from display devices (e.g., buttons and sliders on touch screens), multi-function control devices (e.g., knobs, buttons, keyboard keys, and switches that perform different functions depending upon the current condition of the plant, the control system, or the HSI), and devices activated via voice input.

Soft slider – An input format used to directly manipulate a variable over a set range of values (also called a slider bar or a scroll bar). A soft slider resembles a barchart with a pointer directed toward the current value. They are typically manipulated via pointing interfaces, such as a touch screen or mouse. Input is provided by sliding the pointer along the length of the barchart scale to the desired value. It is used when the range of possible values and the ratio of a value to that range must be displayed.

Spatially dedicated and continuously visible – An HSI that is in a fixed position and is directly observable without a user action. [1]

Systems approach to training (SAT) – A training program that includes the following five elements [from 10 CFR 55.4]:

1. Systematic analysis of the jobs to be performed.
2. Learning objectives derived from the analysis which describe desired performance after training.
3. Training design and implementation based on the learning objectives.
4. Evaluation of trainee mastery of the objectives during training.
5. Evaluation and revision of the training based on the performance of trained personnel in the job setting.

Secondary tasks – Those tasks that the operator perform when interfacing with the plant, but are not directed to the primary task. Secondary tasks may include: navigating through and paging displays, searching for data, choosing between multiple ways of accomplishing the same task, and making decisions regarding how to configure the interface.

Simulator – A facility that physically represents the human-system interface configuration and that dynamically represents the operating characteristics and responses of the plant in real time. (see “Mockup” and “Prototype”).

Style guide – A document that contains guidelines that have been tailored so they describe the implementation of human factors engineering guidance to a specific design, such as for a specific plant control room.

Task – A group of activities that have a common purpose, often occurring in close temporal proximity.

Task analysis – A method of detailing the components of a task in terms of the demands placed upon the human operator, the information required by the operator, the extent to which the task requires reliance on or coordination with other personnel, and the relation of the task to other tasks.

[1] Note that spatially dedicated means that the display is always available in the same location in the control room. It does not mean that that location is the only location at which such information can be retrieved. A DCS or other computer-based information system may provide access to the same displays at other locations as well, such as other workstations or remote shutdown facilities.

Top-down process – In a top down design approach, the design starts at the “top” with high-level plant mission goals that are broken down into functions that are allocated to human and system resources and are further broken down into tasks performed to accomplish function assignments. Tasks are arranged into meaningful jobs and the human-system interface is designed to best support job task performance. The detailed design is the “bottom” of the top-down design process.

Unintentional activation – A slip that occurs when a set of actions (schema) that is not part of a current action sequence becomes activated and then triggered for extraneous reasons. It can lead to the unintended actuation of an input device.

Verification – The process by which the human-system interface design is evaluated to determine whether it acceptably satisfies personnel task needs and human factors engineering design guidance.

C
REFERENCES

1. *Human Factors Guide for Nuclear Power Plant Control Room Development,* Electric Power Research Institute, Palo Alto, CA: (EPRI NP-3659). EPRI (1984).
2. NUREG-0700 Revision 2. *Human-System Interface Design Review Guidelines*, U.S. Nuclear Regulatory Commission, Washington, DC: 2002.
3. IEEE 1220-1998 IEEE Standard for Application and Management of the Systems Engineering Process. New York: Institute of Electrical and Electronics Engineers, 1998.
4. IEEE (1999). IEEE guide for the evaluation of human-system performance in nuclear power generating stations [IEEE Std 845-1999]. New York: Institute of Electrical and Electronics Engineers.
5. *Technical Material for a Workshop on Control Room Upgrades,* Electric Power Research Institute, Palo Alto, CA: 2003. EPRI TR 1007795.
6. ISO 13407:1999. Human-Centred Design Processes for Interactive Systems, International Organization for Standardization, Geneva, Switzerland: 1999.
7. ISO (2000). *Ergonomic Design of Control Centres* (ISO 11064-1). Geneva, Switzerland: International Standards Organization.
8. IEC (1989). *Design for Control Rooms of Nuclear Power Plants* (IEC-964). Geneva, Switzerland: Bureau Central de la Commission Electrotechnique International.
9. NUREG-0711 Revision 1. *Human Factors Engineering Program Review Model*, U.S. Nuclear Regulatory Commission, Washington, DC: 2002.
10. EPRI TR-102348 Revision 1 – NEI 01-01. *Guideline on Licensing Digital Upgrades: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule*, EPRI, Palo Alto, CA: 2002. 1002833.
11. 10 CFR 50.59. *Changes, Tests and Experiments*, Code of Federal Regulations Title 10, Part 50.59, U.S. Nuclear Regulatory Commission, Washington, DC: 2000.
12. RIS 2002-22. NRC Regulatory Issue Summary 2002-22, Use of EPRI/NEI Joint Task Force Report, 'Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,' U.S. Nuclear Regulatory Commission, Washington, DC: November 2002.
13. NUREG-0800. Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, U.S. Nuclear Regulatory Commission, Washington, D.C.: 1987.
14. IEEE Std 1023-1988. IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, New York: 1988.

15. IEC 62096 CDV. *Nuclear Power Plants - Instrumentation and Control - Guidance for the Decision on Modernization*, 45A/429/CDV (Committee Draft for Vote), International Electrotechnical Commission, Geneva, Switzerland: July 2001.

16. Regulatory Guide 1.97 Revision 3. Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, U.S. Nuclear Regulatory Commission, Washington, DC: 1983.

17. Regulatory Guide 1.47. *Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems*, U.S. Nuclear Regulatory Commission, Washington, DC: 1973.

18. IEEE 279-1971 Protection Systems for Nuclear Generating Stations. New York: Institute of Electrical and Electronics Engineers, 1971.

19. IEEE 603-1991. *Criteria for Protection Systems for Nuclear Power Generating Stations*, Institute of Electrical and Electronics Engineers, New York, NY: 1991.

20. NUREG-1764. *Guidance for the Review of Changes to Human Actions*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

21. 10 CFR 50 Appendix A. *General Design Criteria for Nuclear Power Plants*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

22. 10 CFR 50.34(f). *Contents of applications; technical information; Additional TMI-related requirements*, Code of Federal Regulations Title 10, Part 50.34, U.S. Nuclear Regulatory Commission, Washington, DC.

23. 10 CFR 50 Appendix R. *Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

24. 10 CFR 55. *Operators' Licenses*, Code of Federal Regulations Title 10, Part 55, U.S. Nuclear Regulatory Commission, Washington, DC.

25. NEI 96-07 Revision 1. *Guidelines for 10 CFR 50.59 Implementation*, Nuclear Energy Institute, Washington, DC: November 2000.

26. Regulatory Guide 1.174 Revision 1. An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, U.S. Nuclear Regulatory Commission, Washington, DC: April 2002.

27. BTP-19 BTP HICB-19 "Evaluation of Defense in Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Standard Review Plan (NUREG-0800) Chapter 7, Rev. 4. Washington, DC: Nuclear Regulatory Commission, 1997.

28. NUREG-0737 Supplement 1. Clarification of TMI Action Plan Requirements – Requirements for Emergency Response Capability, U.S. Nuclear Regulatory Commission, Washington, DC: January 1983.

29. Regulatory Guide 1.62. *Manual Initiation of Protective Actions*, U.S. Nuclear Regulatory Commission, Washington, DC: 1973.

30. EPRI 1002835. *Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades*, EPRI, Palo Alto, CA: 2004. 1002835.

31. NUREG-0654 (FEMA-REP-1) Rev. 1. Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, Appendix 1, Emergency Action Level Guidelines for Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, DC.

32. Higgins, J. and Nasta, K. (1996). HFE Insights For Advanced Reactors Based Upon Operating Experience (NUREG/CR-6400). Washington, DC: U.S. Nuclear Regulatory Commission.

33. O'Hara, J. Pirus, D., Beltracchi, L., *Information Display: Considerations for Designing Modern Computer-Based Display Systems,* Electric Power Research Institute, Palo Alto, CA: 2003. (EPRI-1002830).

34. International Electrotechnical Commission (2000). *Nuclear Power Plants - Design of Control Rooms - Function Analysis and Assignmen*t (IEC 61839). Geneva, Switzerland: Bureau Central de la Commission Electrotechnique Internationale.

35. Kirwan, B. and Ainsworth L. (Eds). (1992). *A Guide to Task Analysis*. London: Taylor and Francis.

36. Shraagen, J., Chipman, S., and Shalin, V. (2000). *Cognitive Task Analysis*. New Jersey: Lawrence Erlbaum Associates.

37. Vicente, K., (1999). Cognitive Work Analysis. Toward Safe, Productive, and Healthy Computer-Based Work. New Jersey: Lawrence Erlbaum Associates.

38. Burgy, D., Lempges, C., Miller, A., Schroeder, L. Van Cott, H., Paramore, B. (1983). *Task Analysis of Nuclear Power Plant Control Room Crews* (NUREG/CR-3371, Volumes 1 and 2). Washington, DC: U.S. Nuclear Regulatory Commission.

39. 10 CFR 50.54. *Conditions of licenses*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

40. Plott, C., Engh, T., and Barnes, V. (2004). Technical Basis for Regulatory Guidance for Assessing Exemption Requests from the Nuclear Power Plant Licensed Operator Staffing Requirements Specified in 10 CFR 50.54(m) (NUREG/CR-6838). Washington, DC: U.S. Nuclear Regulatory Commission.

41. Kirwan, B. (1994). A Guide to Practical Human Reliability Assessment. London: Taylor & Francis.

42. IEC-964: Design for Control Rooms of Nuclear Power Plants (International Electro-technical Commission, 1989).

43. ISO 11064, Ergonomic Design of Control Centers.

44. ANSI (2001). *Common Industry Format for Usability Test Reports* (NNSI NCITS 354-2001). New York: American National Standards Institute, Inc.

45. ISO 9241-14:1997 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 14: Menu dialogues. and ISO 9241-15:1997 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 15: Command dialogues.

46. IEEE 1012-1998, IEEE Standard for Software Verification and Validation, March 1998.

47. O'Hara, J, Stubler, W., Higgins, J., and Brown, W. (1997). Integrated system validation: Methodology and review criteria (NUREG/CR-6393). Washington, DC: U.S. Nuclear Regulatory Commission.

48. ANSI (1993). Guide to human performance measurements [ANSI/AIAA G-035-1992]. Washington, DC: American National Standards Institute.

49. Endsley, M. (1995). Measurement of situation awareness in dynamic systems. *Human Factors*, 37, 65-84.

50. Hogg, D., Folleso, K., Torralba, B., and Volden, F. (1994). *Measurement of the Operator's Situation Awareness for Use Within Process Control Research: Four Methodological Studies* (HWR-377). Halden, Norway: OECD Halden Reactor Project.

51. Rasmussen, J. (1986). *Information processing and human-machine interaction*. New York, NY: North Holland.

52. NUREG-1342 Status Report Regarding Industry Implementation of Safety Parameter Display Systems. Washington, DC: Nuclear Regulatory Commission, 1988.

53. Tani, M., Masato, H., Yamaashi, K., Tanikoshi, and Futakawa, M., Courtyard: Integrating Shared Overview on a Large Screen and Per-User Detail on Individual Screens. *Proceedings of CHI '94, ACM Conference on Human Factors in Computing Systems*. New York, NY: Association for Computing Machinery, Inc., 1994.

54. *Frey, P.R., Sides, W.H., Hunt, R.M., and Rouse, W.B. (1984). Computer-Generated Display System Guidelines – Volume 1: Display Design*, Electric Power Research Institute, Palo Alto, CA: EPRI NP-3701.

55. Danchak, M.M. (1981). Techniques for Displaying Multivariate Data on Cathode Ray Tubes with Applications to Nuclear Process Control. NUREG/CR-1994. Washington, DC: U.S. Nuclear Regulatory Commission.

56. Galitz, W.O. (1993). User Interface Screen Design. Wellesley, MA: QED Publishing Group.

57. ANSI/ISA-S5.5, *Graphic Symbols for Process Displays,* Instrument Society of America, 1985.

58. ISO/IEC 11581-1:2000(E), Information technology – User system interfaces and symbols – Icon symbols and function – Part 1: Icons – General, International Organization for Standardization, First edition, 2000.

59. IEC-1227 Nuclear Power Plants, Control Rooms, Operator Controls. Geneva, Switzerland: International Electrotechnical Commission, 1993.

60. Fink, R. (1990). *A procedure for reviewing and improving power plant alarm systems,* Electric Power Research Institute, Palo Alto, CA: (EPRI NP-3448-L-R1).

61. IEEE (1988). IEEE standard criteria for the periodic surveillance testing of nuclear power plant generation station safety systems (ANSI/IEEE 338-1987). New York: The Institute for Electrical and Electronics Engineers, Inc.

62. ISA (2000a). *Setpoints for safety-related instrumentation* (ISA-RP67.04.01-2000). North Carolina: Instrument Society of America.

63. ISA (2000b). Methodologies for determination of *setpoints for nuclear- related instrumentation.* (ISA-RP67.04.02-2000). North Carolina: Instrument Society of America.

64. *Alarm Processing Methods – Improving Alarm Management in Nuclear Power Plant Control Rooms*, Electric Power Research Institute Palo Alto, CA: (EPRI 1003662). EPRI (2003).

65. O'Hara, J., Higgins, J., Stubler, W., and Kramer, J. (2000). *Computer-based procedure systems: Technical basis and human factors review guidance* (NUREG/CR-6634). Washington, DC: U.S. Nuclear Regulatory Commission.

66. O'Hara, J., Pirus, D., Nilsen, S., Bisio, R., Hulsund, J-E., and Zhang, W. (2001). *Computerisation of procedures - Lessons learned and future perspectives* (HPR-355). Halden, Norway: OECD Halden Reactor Project.

67. Roth, E. and O'Hara, J. (2002). Integrating digital and conventional human system interface technology: Lessons learned from a control room modernization program. (NUREG/CR-6749). Washington, D.C.: U.S. Nuclear Regulatory Commission.

68. U.S. Nuclear Regulatory Commission (1982). *Guidelines for the preparation of emergency operating procedures* (NUREG-0899). Washington, DC: U.S. Nuclear Regulation Commission.

69. O'Hara, J. Stubler, W., and Higgins, J. (1996). Hybrid human-system interfaces: Human factors considerations (BNL Report J6012-T1-4/96). Upton, NY: Brookhaven National Laboratory.

70. Wieringa, D., Moore, C., and Barnes, V. (1993) *Procedure writing: Principles and practices*. Piscataway, NJ: IEEE Press.

71. Davis, E., Funk, D., Hooten, D., and Rusaw, R., *On-line Monitoring of Instrument Channel Performance*, EPRI, Palo Alto, CA: 1000604. (2000).

72. Heo, G., Chang S. (2003). Comparative study on state analysis of BOP in NPPs, IEEE Trans. on Nuclear Science, 50 (4): 1271-1281 Part 2.

73. Chiang, L. H., Russel, E. L., and Braatz, R. D. (2001). Fault Detection and Diagnosis in Industrial Systems, Springer-Verlag, London.

74. Rasmussen, B., Hines, J.W., and Uhrig, R. (2003). A novel approach to process modeling for instrument surveillance and calibration verification, Nuclear Technology, 143 (2): 217-226.

75. Upadhyaya, B., Zhao, K., and Lu, B. (2003). Fault monitoring of nuclear power plant sensors and field devices, Progress in Nuclear Energy, 43 (1-4): 337-342.

76. Gou, Z., and Uhrig, R. (1992). "Nuclear Power Plant Performance Study by Using Neural Networks", IEEE Trans. Nucl. Sci., 39, 915.

77. Sunde, S., Berg, O., Dahlberg, L., and Fridquist, N-O. (2003). Data reconciliation in the steam turbine cycle of a boiling-water reactor, Nuclear Technology, 143.

78. Dorr, R., Kratz, F., Ragot, J., Loisy, F., and Germain, J-L. (1997). Detection, Isolation, and Identification of Sensor Faults in Nuclear Power Plants, IEEE Trans. Contr. Sys. Techn., 5, 42.

79. Chou, G.-H., Lee, K.-H., and Chao, H.-J. (1994). The Development of a Thermal Performance Diagnostics Expert System for Nuclear Power Plant, IEEE Transactions on Nuclear Science, 41, 1729 – 1735.

80. Por, G., Kiss, J., Sorosanszky, I., and Szappanos, G. (2003). Development of a false alarm free, Advanced Loose Parts Monitoring System (ALPS), Progress in Nuclear Energy, 43 (1-4): 243-251.

81. Nabeshima, K., Suzudo, T., Seker, S., Ayaz, E., Barutcu, B., Turkcan, E., Ohno, T., and Kudo, K. (2003). On-line neuro-expert monitoring system for Borssele nuclear power plant, Progress in Nuclear Energy, 43 (1-4): 397-404 2003.

82. Lefvert, T., et al. (1999). “Core Monitoring for Commercial Reactors: Improvements in Systems and Methods”, NEA Workshop Proceedings, Stockholm, Sweden, 4-5 October 1999. ISBN 92-64-17659-4.

83. Human Factors and Ergonomics Society (2002). Human factors engineering of computer workstations [BSR/HFES 100]. Santa Monica, CA: Human Factors and Ergonomics Society.

84. NUREG/CR-6303. Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, U.S. Nuclear Regulatory Commission, Washington, DC: December 1994.

85. 10 CFR 100 Reactor Site Criteria, Code of Federal Regulations Title 10 Part 100, U.S. Nuclear Regulatory Commission, 2004.

86. NUMARC 93-01, Rev. 3. *Maintenance Rule Implementation*, Nuclear Energy Institute (formerly NUMARC), Washington, DC: 1996.

87. NEI 00-02. *10 CFR 50.69 Option 2 Categorization*, Nuclear Energy Institute, Washington, DC.

88. 10 CFR 50.55a (h). *Protection and safety systems*, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

89. IEEE 497-2002. IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, New York, NY: September 2002.

90. ANSI/ANS-4.5-1980 Criteria for Accident Monitoring Functions in Light-Water Cooled Reactors. La Grange Park, IL: American Nuclear Society, 1980.

91. Regulatory Guide 1.153 Revision 1. *Criteria for Safety Systems*, U.S. Nuclear Regulatory Commission, Washington, DC: June 1996.

92. Regulatory Guide 1.114 Revision 2. Guidance to Operators at the Controls and to Senior Operators in the Control Room of a Nuclear Power Unit, U.S. Nuclear Regulatory Commission, Washington, DC: May 1989.

93. Regulatory Guide 1.8 Revision 3. *Qualification and Training of Personnel for Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: May 2000.

94. Regulatory Guide 1.149 Revision 3. *Nuclear Power Plant Simulation Facilities for Use in Operator Training and License Examinations*, U.S. Nuclear Regulatory Commission, Washington, DC: October 2001.

95. NUREG-1220 Revision 1. Training Review Criteria and Procedures, U.S. Nuclear Regulatory Commission, Washington, DC: 1993.

96. ANSI/ANS-3.5-1998. Requirements for Simulators Used for Operator Training, Testing and Requalification, American National Standards Institute, La Grange Park, IL: 1998.

97. SECY 93-087. Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, U.S. Nuclear Regulatory Commission, Washington, DC: July 1993.

98. Regulatory Guide 1.101 Revision 4. Emergency Planning and Preparedness for Nuclear Power Reactors, U.S. Nuclear Regulatory Commission, Washington, DC: July 2003.

99. 10 CFR 50.47. Emergency plans, Code of Federal Regulations Title 10, Part 50, U.S. Nuclear Regulatory Commission, Washington, DC.

100. NUREG-0654 (FEMA-REP-1) Rev. 1. Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, Appendix 1, Emergency Action Level Guidelines for Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, DC.

101. NUMARC/NESP-007, Rev. 2 Methodology for Development of Emergency Action Levels. Washington, DC: Nuclear Management and Resources Council (NUMARC), 1992.

102. NEI 99-01 Revision 4. *Methodology for Development of Emergency Action Levels*, Nuclear Energy Institute, Washington, DC: January 2003.

103. Information Notice (IN) 97-78. Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times, U.S. Nuclear Regulatory Commission, Washington, DC: October 1997.

104. NUREG-1430. *Standard Technical Specifications, B&W Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

105. NUREG-1431 Revision 2. *Standard Technical Specifications, Westinghouse Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: 2001.

106. NUREG-1432. *Standard Technical Specifications, CE Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

107. NUREG-1433 and NUREG-1434. *Standard Technical Specifications, GE Plants*, U.S. Nuclear Regulatory Commission, Washington, DC: 2004.

108. Stubler, W. F., Higgins, J. C., and Kramer, J., *Maintainability of Digital Systems: Technical Basis and Human Factors Review Guidance,* NUREG/CR-6636, BNL-NUREG-52566, Brookhaven National Laboratory, Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission, Washington, D.C., March 2000.

109. *Advanced Light Water Reactor Utility Requirements Document, Volume II, ALWR Evolutionary Plant, Chapter 10, Man-Machine Interface Systems, Revision 6,* Electric Power Research Institute, Palo Alto, CA: December 1993.

110. *NRC Review of Electric Power Institute's Advanced Light Water Reactor Utility Requirements Document*, Chapter 10, Man-Machine Interface Systems, NUREG-1242, Vol. 3, Part 2, U.S. Nuclear Regulatory Commission, Washington, D.C., 1994.

111. *Human Factors/Ergonomics Handbook for the Design for Ease of Maintenance,* DOE-HDBK-1140-2001, U.S. Department of Energy, Washington, D.C., Area HFAC, February 2001.

112. Pack, R. W., Seminara, J. L., Shewbridge, E. G., and Gonzalez, W. R., *Human Engineering Design Guidelines for Maintainability,* NP-4350, Electric Power Research Institute (EPRI), Palo Alto, CA: Research Project 2166-4, Final Report, December 1985.

113. *Dependability Management – Part 3-10: Application guide –Maintainability* , IEC 60300-3-10, First Edition, International Electrotechnical Commission, Geneva 2001.

114. Human Factors Design Standard (HFDS) for Acquisition of Commercial-Off-The-Shelf Subsystems, Non-Developmental Items (NDI), and Developmental Systems, Section 4, Designing equipment for maintenance, HF-STD-001, DOT/FAA/CT-03/05, U.S. Department of Transportation, Federal Aviation Administration Headquarters, Human Factors Division, Washington, May 2003.

115. *Maintainability of Digital Systems,* EPRI, Palo Alto, CA: October 2004. 1008124.

116. 10 CFR 50.120 Training and Qualification of Nuclear Power Plant Personnel, Code of Federal Regulations Title 10 Part 50.120. Washington, DC: U.S. Nuclear Regulatory Commission, 2004.

117. 10 CFR 55.4 Operator's Licenses, Definitions, Code of Federal Regulations Title 10 Part 55.4. Washington, DC: U.S. Nuclear Regulatory Commission, 2004.

118. IAEA-TECDOC-995. Selection, Specification, Design and Use of Various Nuclear Power Plant Training Simulators, International Atomic Energy Agency. IAEA-TECDOC-995, January 1998.

119. Brookes 2002. ARJ Brookes, Emulation Technology for a Classroom Simulator, Proceedings of the 2002 Western MultiConference. Society for Computer Simulation International, January 2002.

120. Fryer 2003. G. Fryer, Nuclear Simulators – Practical Advice for I&C Upgrades, International Conference on Simulation Training for Nuclear Power Plants and Systems. Society for Computer Simulation International, January 2003.

121. Meloni 2003. R. Meloni, P. Gaffuri, and D. Pathe, *Technical Advances in Operator Training Simulator Systems, ERTC Computing Conference.* Milan, Italy, June 2003.

D
CHECKLISTS

D.1 Information Display

D.1.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.1.3	Display Functions								
	4.1.3.1	Display Design for Plant Monitoring, Detection, and Situation Assessment							
		4.1.3.1.1	Defining a Hierarchy to Serve as a Basis For Displays						
			=>	4.1.3.1.1-1	Displays for monitoring and situation assessment should be organized according to an abstraction hierarchy. The hierarchy should: • Completely describe the plant in terms of its main purposes or missions, i.e., supply power to the grid and maintain safety • Reveal goal status at each level • Reveal both physical and functional relationships • Reveal interactions and dependencies of the hierarchy elements • Be applicable to all operational situations and reflect differences associated with different operating modes • Be meaningful to the users				
			=>	4.1.3.1.1-2	Displays should reflect the hierarchy and provide information at various levels that are appropriate to the various operator functions and tasks. Higher level displays should support monitoring of plant status and situation assessment functions and increasingly detailed displays should support troubleshooting or more detailed status monitoring.				
			=>	4.1.3.1.1-3	Each display in the hierarchy should use the same general design principles.				
		4.1.3.1.2	Content of Individual Displays						
			=>	4.1.3.1.2-1	Displays should include a representation of the main functions, processes, systems, and component of the plant's AH and their relationships.				
			=>	4.1.3.1.2-2	Displays should indicate the key modes of operation that affect the user's interpretation of information.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.1.3.1.2-3	The important AH elements should be presented so the status can be determined at a glance, i.e., that status is very easily recognized. The types of information that should be considered include: • Goal attainment Status - the current function or system goal is being achieved or not. • Availability Status - available or not available (e.g., bypassed/inoperable; tagged-out; key locked) and whether an action is required for use (e.g., line-up). • Capability Status - the current capability to contribute to the satisfaction of the functional goal in question. This relates to the sufficiency of system or component to achieve a goal. For example, current operating conditions may be such that a system cannot achieve its function because it is not designed to operate under those conditions. Consider, for example, low-pressure safety injection as one of the alternatives that is available to satisfy the Control RCS Water Mass Inventory function. It is only effective in satisfying the goal if the RCS pressure is low enough.) • Service Status - in service or not in service (the element is ready to achieve its purpose). Being ready to achieve a purpose may require going through several stages of successful functional states. • Equipment Functional Status - (e.g., flow/no-flow, energized/de-energized, on/off, and open/closed).				
			=>	4.1.3.1.2-4	Important performance indicators for key AH elements should be provided. These may be measured parameters or derived values. Any analyses or information integration by which lower-level data are analyzed to produce higher-level performance indicators should be available to users so they can easily determine the meaning of higher-level indicators.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.1.3.1.2-5	The display should have information readily available on plant dynamics, i.e., indicate when the performance indicators are changing at significant rates.				
			=>	4.1.3.1.2-6	Overview displays should address safety parameter display system (SPDS) requirements.				
			=>	4.1.3.1.2-7	The display should indicate conditions requiring operator actions related to the main AH elements.				
			=>	4.1.3.1.2-8	Upon control actuation, a display should be immediately available to allow the operator to evaluate the performance of the system, e.g., information on the control input and output actuation signals and the resulting states of plant process components. Comparison of these states with expected states should also be made and deviations displayed in the abnormality indication portion of the HSI.				
			=>	4.1.3.1.2-9	To the extent possible, the functionality of the displays should be preserved at all power levels and plant operating modes.				
			=>	4.1.3.1.2-10	Higher-level overview display(s) should be available at the user workstations. If the control room layout will permit, the overview display(s) should also be located so that it can be seen from anywhere in the control room.				
			=>	4.1.3.1.2-11	Providing overviews not only supports monitoring but access to more detailed information as well (by means of navigation features to drill down to more detailed displays).				
			=>	4.1.3.1.2-12	Displays at each level should alert users to important changes to the plant that may be indicated in higher- and lower-level displays. The method of alert should communicate to the user whether the change is at higher levels or lower levels and facilitate navigation to the appropriate display showing the applicable plant changes.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.1.3.1.2-13	Displays in each level of the hierarchy should present information that effectively communicates the plant relationships at that level and which minimizes the need to access multiple displays.				
4.1.3.1.3		Navigation Within the Display Hierarchy					
	=>	4.1.3.1.3-1	Each display should be clearly labeled as to its contents and its relationship in the hierarchy.				
	=>	4.1.3.1.3-2	The system should provide on-screen navigational links to and from high-level and lower-levels of information with references and supporting information.				
	=>	4.1.3.1.3-3	Navigation tools should provide for flexible approaches to searching for information.				
	=>	4.1.3.1.3-4	The system should include a history function allowing users to keep track of the sequence of displays they have accessed to facilitate retracing their steps.				
	=>	4.1.3.1.3-5	A list of all displays, e.g., on a menu, should be available to provide access to displays that do not have on-screen links.				
	=>	4.1.3.1.3-6	Visual search within each display should be supported by coding and other display features that enable users to easily see associated information in the display.				
	=>	4.1.3.1.3-7	When conditions signal changes in display pages the user is not currently viewing that the user should attend to, special navigation aids should be presented to enable those displays to be easily retrieved. However, the displays should not be immediately displayed unless the user requests them.				
	=>	4.1.3.1.3-8	To be effective, sufficient display area should be provided for users to display needed information in parallel and to minimize the need for navigation.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.1.3.2	Display Design for Task Performance						
	4.1.3.2.1	Task Selection					
	=>	4.1.3.2.1-1	Tasks requiring highly-reliable human performance should be considered for task-based display support. These tasks are mostly: • Important to nuclear or personnel safety • Important to maintaining power generation • Important to equipment protection for significant items • Time critical • Complex				
	=>	4.1.3.2.1-2	Tasks that have high interface management and navigation demands (if performed without a specialized display) should be considered for task.based display support.				
	=>	4.1.3.2.1-3	Tasks for which improved efficiency is desired should be considered for task-based display support.				
	4.1.3.2.2	Task-Based Display Design					
	=>	4.1.3.2.2-1	The task display requirements should be identified.				
	=>	4.1.3.2.2-2	The system should provide notice of when the task is required.				
	=>	4.1.3.2.2-3	The display should indicate the conditions that must be met before a task or step can be undertaken. Information about preconditions should be displayed so that users will be informed before starting the task or step.				
	=>	4.1.3.2.2-4	Where the task is proceduralized, instructions and sequences should be provided for performing the task or step.				
	=>	4.1.3.2.2-5	Specific plant information needed to perform the task should be displayed in the order and organization in which it is needed, to minimize interface management demands.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.1.3.2.2-6	Cautions and warnings related to task performance should be displayed when the information is displayed to the user. Cautions or warnings should be distinctively presented, so that they are easily differentiated from each other and from other display elements.				
			=>	4.1.3.2.2-7	Any alarms related to the task or step that may impact the user's ability to perform, or may alter the actions the user should take, should be presented in the task-based display.				
			=>	4.1.3.2.2-8	If soft control capability is provided, controls needed to perform the task or step should be directly available in the display.				
			=>	4.1.3.2.2-9	When the task or steps requires operating systems/equipment/controls, then expected and actual feedback should be provided in the display.				
			=>	4.1.3.2.2-10	The task display should provide indication when a task or step can or should be terminated.				
			=>	4.1.3.2.2-11	The information presented in the task display should be conducive to efficient task execution.				
			=>	4.1.3.2.2-12	The task display should provide support for tracking task progress.				
			=>	4.1.3.2.2-13	The overall structure of the task elements (alarms, information, instructions, controls, etc.) reflecting the task requirements should be: • Sequentially structured when the task steps need to be completed in a specific order • Structured into groups of parallel information when no specific sequence is needed				
			=>	4.1.3.2.2-14	When a task requires more than one display, onscreen navigation aids should be provided to easily access the displays.				

Guidelines			Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	4.1.3.3	Display Design for Teamwork, Crew Coordination, and Collaborative Work				
=>	4.1.3.3-1	Displays should include functionality to support teamwork when the following conditions exist: • There is a high need for users to work together on the same task/problem (e.g., complex diagnoses of plant failures) • Face-to-face interaction/collaboration is difficult due to the arrangement of the workplace and the demands of concurrent tasks (e.g. multi-location coordinated activities)				
=>	4.1.3.3-2	A common frame of reference for plant status should be provided.				
=>	4.1.3.3-3	A user-addressable frame-of-reference should be provided if users have to collaborate to perform an activity.				
=>	4.1.3.3-4	A CSCW display should support each crewmember's understanding of the others' activities. This can be accomplished by providing information for common team activities, such as in shift turnovers and for maintenance activities.				
=>	4.1.3.3-5	Supervisor workstations should provide the capability to access the same displays as those at operator workstations.				
=>	4.1.3.3-6	A coding scheme or designation system should be used to identify users when they manipulate information on a group-view display.				
=>	4.1.3.3-7	When multiple users have to work together on the same task, displays should provide a collaborative workspace.				
=>	4.1.3.3-8	The display should provide tools that enable users to interact with the HSI or the plant. Other users should be able to infer information about the nature of the task and the specific actions taken by observing the HSI.				
=>	4.1.3.3-9	Display controls should prevent individuals from making changes to CSCW displays in ways that would reduce their usefulness to others.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.3.3-10	When multiple users have access to on-screen pointing devices (such as cursors) for interacting with the group-view display, features should be provided to manage access to the cursor and indicate current user.				
		=>	4.1.3.3-11	When transferring information between individual displays and the CSCW displays, the information should be presented promptly and with minimal delay.				
4.1.4	Display Pages							
	4.1.4.1	Identification of Information						
		=>	4.1.4.1-1	A title or header should be placed at the top of every display page, briefly describing the contents or purpose of the display.				
		=>	4.1.4.1-2	Every display page should have a unique identification to provide a reference for use in requesting the display of that page.				
		=>	4.1.4.1-3	Where displays have several levels of titles (and/or labels), the system should provide visual cues to aid users in distinguishing among the levels in the hierarchy.				
		=>	4.1.4.1-4	General labels and row/column labels should remain along the edges of the display.				
		=>	4.1.4.1-5	When displays are partitioned into multiple pages, function/task-related data items should be displayed together on one page.				
		=>	4.1.4.1.6	Users working with multipage displays should be provided with a page location reference within the display sequence.				
		=>	4.1.4.1-7	Users viewing a portion of a larger display should be provided with an indication of the location of the visible position of a display (frame) in the overall display.				
	4.1.4.2	Organization of Information						
		=>	4.1.4.2-1	General HSI features (e.g., a data display zone, control zone, or message zone) should be displayed in consistent locations from one display to another.				

Guidelines			Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
=>	4.1.4.2-2	The HSI functional zones and display features should be visually distinctive from one another, especially for on-screen command and control elements (which should be visibly distinct from all other screen structures).				
=>	4.1.4.2-3	Information on a display should be grouped according to principles obvious to the user, e.g., by task, system, function, or sequence, based upon the user's requirements in performance of the ongoing task (see Table 4-1).				
=>	4.1.4.2-4	Information needed by the operator to accomplish a given task should be presented so that it is immediately seen to be related.				
=>	4.1.4.2-5	A uniform nondistracting background color should be used with a hue/contrast that allows the data (foreground) to be easily visible and which does not distort or interfere with the coding aspects of the display.				
=>	4.1.4.2-6	When information is grouped on a display, the groups should be made visually distinct by such means as color blocking or padding or separation using blanks or demarcation lines.				
4.1.4.3	Clarity of Presentation					
=>	4.1.4.3-1	Displays should present, in an immediately usable form, only the data needed for the task they are designed to support; data irrelevant to the task should not be displayed, and extraneous text and graphics should not be present.				
=>	4.1.4.3-2	Redundancy in the presentation of information items should be limited to cases where needed for backup or to avoid excessive movement.				
=>	4.1.4.3-3	Displays should be as uncluttered as possible.				
=>	4.1.4.3-4	Displayed information which temporarily overlays and obscures other display data should not erase the overlaid data.				
4.1.4.4	Coding and Highlighting of Information					

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.4.4-1	Highlighting should be used sparingly.				
		=>	4.1.4.4-2	The prominence of graphic features should reflect the importance of the information.				
		=>	4.1.4.4-3	Coding and highlighting should not interfere with the readability of displayed information nor delay its presentation.				
		=>	4.1.4.4-4	Highlighting should be removed if it no longer has meaning.				
		=>	4.1.4.4-5	When highlighting is not sufficient to indicate the specific nature of some outstanding or discrepant feature that merits attention by a user, supplementary text should be displayed to make it clear.				
		=>	4.1.4.4-6	Coding of important information should incorporate redundancy.				
		=>	4.1.4.4-7	Coding should be provided when a user must distinguish rapidly among different categories of displayed data.				
		=>	4.1.4.4-8	Meaningful or familiar codes should be used, rather than arbitrary codes.				
		=>	4.1.4.4-9	Consistent meanings should be assigned to codes across user interfaces in the plant (including existing interfaces).				
		=>	4.1.4.4-10	A characteristic used for coding should have only one meaning.				
		=>	4.1.4.4-11	Highlighting should be clear and easily recognizable and should attract the users' attention.				
		=>	4.1.4.4-12	Inverse video should be used only to show the selection of on-screen items or to highlight small segments in a larger block of text.				
4.1.5		Display Formats						
	4.1.5.1		Continuous Text Displays					
		=>	4.1.5.1-1	A standard text display format should be used from one display to another.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.1-2	VDU displays of textual data, messages, or instructions should generally follow design conventions for printed text.				
		=>	4.1.5.1-3	Text to be displayed should be worded so that it is quickly and easily understood.				
		=>	4.1.5.1-4	When a user must read continuous text on line, at least four lines of text should be displayed at one time.				
		=>	4.1.5.1-5	Continuous text should be displayed in wide columns, containing at least 50 characters per line.				
		=>	4.1.5.1-6	In display of textual material, words should be kept intact, with minimal breaking by hyphenation between lines.				
		=>	4.1.5.1-7	Conventional punctuation should be used in textual display.				
		=>	4.1.5.1-8	Consistent spacing between the words of displayed text should be maintained, with left justification of lines and ragged right margins. A minimum of one character width (capital N for proportional spacing) should be used between words.				
		=>	4.1.5.1-9	A minimum of two stroke widths or 15 percent of character height, whichever is greater, should be used for spacing between lines of text.				
		=>	4.1.5.1-10	Displayed paragraphs of text should be separated by at least one blank line.				
		=>	4.1.5.1-11	When tables and/or graphics are combined with text, each figure should be placed near its first citation in the text, preferably in the same display frame.				
		=>	4.1.5.1-12	When a line is placed under an item to mark or emphasize it, the line should not impair the legibility of the item, e.g., by obscuring the descenders.				
		=>	4.1.5.1-13	Within a text file or table, the use of a different font style should be preferred over the use of a different size for highlighting information.				

			Guidelines		Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.1-14	When a special symbol, such as an asterisk, is used to draw attention to a selected item in alphanumeric displays, the symbol should be separated from the beginning of the word by a space.				
		=>	4.1.5.1-15	When a user must read lengthy textual material, that text should be available in printed form.				
	4.1.5.2		Tables and Lists					
		=>	4.1.5.2-1	Information should be organized in some recognizable logical order to facilitate scanning and assimilation.				
		=>	4.1.5.2-2	A table should be constructed so that row and column labels represent the information a user has prior to consulting the table.				
		=>	4.1.5.2-3	Each row and column should be uniquely and informatively labeled and should be visually distinct from data entries.				
		=>	4.1.5.2-4	Labels should include the unit of measure for the data in the table; units of measurement should be part of row or column labels.				
		=>	4.1.5.2-5	Consistent column and row spacing should be maintained within a table, and from one table to another. Similarly, spacing between rows should be consistent within a table and between related tables.				
		=>	4.1.5.2-6	The spacing between columns should be greater than any internal spaces that might be displayed within a tabulated data item.				
		=>	4.1.5.2-7	In dense tables with many rows, a blank line, dots, or some other distinctive feature (to aid horizontal scanning) should be inserted after a group of rows at regular intervals.				
		=>	4.1.5.2-8	The font and size of alphanumeric characters should be consistent within a table and between related tables.				
		=>	4.1.5.2-9	Columns of alphabetic data should be displayed with left justification to permit rapid scanning.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.2-10	Columns of numeric data should be justified with respect to a fixed decimal point; if there is no decimal point, then numbers should be right justified.				
		=>	4.1.5.2-11	Arabic rather than Roman numerals should be used when listed items are numbered.				
		=>	4.1.5.2-12	Item numbers should begin with one rather than zero.				
		=>	4.1.5.2-13	When a list of numbered items exceeds one display page, the items should be numbered continuously in relation to the first item on the first page.				
		=>	4.1.5.2-14	Complete numbers should be displayed for hierarchic lists with compound numbers, i.e., repeated elements should not be omitted.				
		=>	4.1.5.2-15	Lists should be formatted so that each item starts on a new line.				
		=>	4.1.5.2-16	When a single item in a list continues for more than one line, items should be marked in some way so that the continuation of an item is obvious.				
		=>	4.1.5.2-17	Where lists of items extend over more than one display page, the last line of one page should be the first line on the succeeding page.				
		=>	4.1.5.2-18	For a long list, extending more than one displayed page, a hierarchic structure should be used to permit its logical partitioning into related shorter lists.				
		=>	4.1.5.2-19	If a list is displayed in multiple columns, the items should be ordered vertically within each column rather than horizontally within rows and across columns.				
		=>	4.1.5.2-20	When lists or tables are of variable length and may extend beyond the limits of one display page, the user should be informed when data are continued on another page and when data are concluded on the present page.				
	4.1.5.3		Data Forms and Fields					

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.3-1	Data fields to be compared on a character-by-character basis should be positioned one above the other.				
		=>	4.1.5.3-2	The ordering and layout of corresponding data fields across displays should be consistent from one display to another.				
		=>	4.1.5.3-3	The format of a VDU data form should be similar to that of commonly used hardcopy source documents.				
		=>	4.1.5.3-4	When forms are used for data entry as well as for data display, the formats of these forms should be compatible.				
		=>	4.1.5.3-5	Clear visual definition of data fields should be provided so that the data are distinct from labels and other display features.				
		=>	4.1.5.3-6	The label and the data display area should be separated by at least one character space.				
		=>	4.1.5.3-7	At least three spaces should appear between the longest data field in one column and the rightmost label in an adjacent column.				
		=>	4.1.5.3-8	When label sizes are relatively equal, both labels and data fields should be left justified. One space should be left between the longest label and the data field column.				
		=>	4.1.5.3-9	When label sizes vary greatly, labels should be right justified and the data fields should be left justified. One space should be left between each label and the data field.				
		=>	4.1.5.3-10	If appropriate, labels should be used to help the user interpret the data displayed in a field.				
		=>	4.1.5.3-11	A field group heading should be centered above the labels to which it applies.				
		=>	4.1.5.3-12	At least five spaces should appear between groups of data fields.				
		=>	4.1.5.3-13	When headings are located on the line above related screen fields, the labels should be indented a minimum of five spaces from the start of the heading.				

Guidelines					**Complies**	**Does not Comply, but with Justification**	**Does not Comply, but without Justification**	**Not Applicable**
		=>	4.1.5.3-14	When headings are placed adjacent to the related fields, they should be located to the left of the topmost row of related fields. The column of labels should be separated from the longest heading by a minimum of three blank spaces.				
		=>	4.1.5.3-15	A data form should have a logical organization.				
		=>	4.1.5.3-16	The number of pages in a data form required to complete an activity should be minimized to reduce the amount of navigation.				
	4.1.5.4	Numeric Readouts						
	4.1.5.5	Bar Charts and Histograms						
		=>	4.1.5.5-1	Each bar on the display should have a unique identification label.				
		=>	4.1.5.5-2	When bars are displayed in groups, they should be labeled as a unit, with individual distinguishing labels for each bar.				
		=>	4.1.5.5-3	When data must be compared, bars should be adjacent to one another and spaced such that a direct visual comparison can be made without eye movement.				
		=>	4.1.5.5-4	In a related series of bar charts, a consistent orientation of the bars (vertical or horizontal) should be adopted.				
		=>	4.1.5.5-5	If one bar represents data of particular significance, then that bar should be highlighted.				
		=>	4.1.5.5-6	The zero reference should be the center of the deviation bar chart.				
		=>	4.1.5.5-7	On a deviation bar chart, the range of normal conditions for positive or negative deviations should represent no more than 10 percent of the total range.				
		=>	4.1.5.5-8	The magnitude of each variable should be displayed when a deviation bar display is used as a main display format for safety function parameters.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.5-9	Segmented bars, in which differently coded segments are shown cumulatively within a bar, should be used when both the total measures and the portions represented by the segments are of interest.				
		=>	4.1.5.5-10	The data categories should be ordered within each segmented bar in the same sequence, with the least variable categories displayed at the bottom and the most variable at the top.				
	4.1.5.6		Graphs					
		=>	4.1.5.6-1	Graphs should convey enough information to allow the user to interpret the data without referring to additional sources.				
		=>	4.1.5.6-2	When multiple curves are included in a single graph, each curve should be identified directly by an adjacent label, rather than by a separate legend.				
		=>	4.1.5.6-3	If a legend must be displayed, the codes in the legend should be ordered to match the expected or typical spatial order of their corresponding curves in the graph itself.				
		=>	4.1.5.6-4	Coding should be used when multiple variables are displayed in a single graph.				
		=>	4.1.5.6-5	Line coding should be used consistently across graphs.				
		=>	4.1.5.6-6	In displays of multiple curves, if one curve represents data of particular significance, then that curve should be highlighted (see Section 4.1.4.4).				
		=>	4.1.5.6-7	Trend displays should be capable of showing data collected during time intervals of different lengths.				
		=>	4.1.5.6-8	When the user must compare trend data represented by separate curves, the curves should be displayed in one combined graph.				
		=>	4.1.5.6-9	If operators must read exact parameter values from displayed curves, features should be provided to support this.				
		=>	4.1.5.6-10	Curves representing planned, projected, or extrapolated trend data should be distinctive from curves representing actual data.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.6-11	Combining several individual curves into a single average curve should only be done when users do not need to know the pattern of individual curves or when curves differ on the basis of minor irregularities.				
		=>	4.1.5.6-12	Where curves represent cyclic data, the scale should be selected so that at least one complete cycle is shown.				
		=>	4.1.5.6-13	The target area, preferred combination of X- and Y-axis values, should be graphically defined.				
		=>	4.1.5.6-14	Old data points should be removed after some fixed period of time to prevent clutter.				
		=>	4.1.5.6-15	A linear profile chart should form recognizable geometric patterns for specific abnormal conditions.				
		=>	4.1.5.6-16	The area below the profile line should be shaded to provide a more distinguishable profile.				
		=>	4.1.5.6-17	Labels should be provided along the bottom of a linear profile chart to identify each parameter.				
		=>	4.1.5.6-18	All segments in a segmented curve graph should be related to the total value.				
		=>	4.1.5.6-19	The data categories in a segmented curve graph should be ordered so that the least variable curves are displayed at the bottom and the most variable at the top.				
		=>	4.1.5.6-20	The different bands of segmented curve graphs should be made visually distinctive by coding, such as by the texturing or shading of bands (see Patterns).				
		=>	4.1.5.6-21	Where space permits, the different bands of segmented curve graphs should be labeled directly within the textured or shaded bands.				
		=>	4.1.5.6-22	If some plotted points represent data of particular significance, they should be highlighted to make them visually distinctive from others.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.6-23	When relations among several variables must be examined in scatterplots, an ordered group (matrix) of plots should be displayed, each showing the relation between just two variables.				
		=>	4.1.5.6-24	When scatterplots are grouped in a single display to show relations among several variables, an interactive aid should be provided for analysis so that if a user selects a set of data in one plot then the corresponding data points in other plots will be highlighted.				
	4.1.5.7		Pie Charts					
		=>	4.1.5.7-1	There should be no more than five partitions in a pie chart.				
		=>	4.1.5.7-2	Pie chart segments should be labeled directly rather than by a separate legend. If a segment is too small to contain the label, the label should be placed outside the segment with a line from it to the segment.				
		=>	4.1.5.7-3	If the task requires precise values, numbers should be added to pie chart segment labels to indicate the percentage and/or absolute values.				
		=>	4.1.5.7-4	If a particular segment of a pie chart requires emphasis, it should be highlighted by special hatching or displaced slightly from the remainder of the pie.				
	4.1.5.8		Flowcharts					
		=>	4.1.5.8-1	The available decision options should be displayed in logical order.				
		=>	4.1.5.8-2	Only a single decision should be required at each step.				
		=>	4.1.5.8-3	When a flowchart is designed so that a user must make decisions at various steps, the available options should be displayed in some consistent order from step to step.				

			Guidelines		Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.8-4	While flowcharts should display only the data immediately required by the user, more detailed data should be available by means of a simple action.				
		=>	4.1.5.8-5	Flowcharts should be designed so that the path of the logical sequence is consistent with familiar orientation conventions.				
		=>	4.1.5.8-6	There should be a standard set of flowchart symbols.				
	4.1.5.9		Mimics and Diagrams					
		=>	4.1.5.9-1	Mimics and diagrams should contain the minimum amount of detail needed for the task they were designed to support.				
		=>	4.1.5.9-2	Plant components represented on mimic lines should be identified.				
		=>	4.1.5.9-3	Indications of the actual status of plant systems and equipment, as opposed to demand status, should be provided when required by the task.				
		=>	4.1.5.9-4	All flow path line origin points should be labeled or begin at labeled components.				
		=>	4.1.5.9-5	All flow path line destination or terminal points should be labeled or end at labeled components.				
		=>	4.1.5.9-6	Flow directions should be clearly indicated by distinctive arrowheads.				
		=>	4.1.5.9-7	Flow paths should be coded (e.g., by color and/or width) to indicate important information (see Color).				
		=>	4.1.5.9-8	Overlapping of flow path lines should be avoided.				
		=>	4.1.5.9-9	Where symbols are used to represent equipment components and process flow or signal paths, numerical data should be presented reflecting inputs and outputs associated with equipment.				
		=>	4.1.5.9-10	When a graphic display contains some outstanding or discrepant feature that merits attention by a user, supplementary text should be displayed to emphasize that feature.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.9-11	When users must evaluate information in detail, computer aids for calculation and visual analysis should be provided.				
	4.1.5.10		Maps					
		=>	4.1.5.10-1	Significant features of a map should be labeled directly on the display unless cluttering or obscuring of other information would result.				
		=>	4.1.5.10-2	When several different maps will be displayed, a consistent orientation should be used so that the top of each map will always represent the same direction.				
		=>	4.1.5.10-3	The user should be able to select different map orientations and reference points.				
		=>	4.1.5.10-4	If the map orientation can be changed, the map labels and symbols should remain oriented to the user's position.				
		=>	4.1.5.10-5	When a map exceeds the capacity of a single display frame, users should be able to change the display in order to show different areas of current interest.				
		=>	4.1.5.10-6	Codes, such as texture patterns, color, or tonal variations, should be used when different areas of a map must be defined, or when geographic distribution of a particular variable must be indicated.				
		=>	4.1.5.10-7	Tonal codes (different shades of one color) rather than spectral codes (different colors) should be used when users must make relative judgments for different colored areas of a display.				
		=>	4.1.5.10-8	Where different areas of a map are coded by texture patterns or tonal variation, the darkest or lightest shades correspond to the extreme values of the coded variable.				
		=>	4.1.5.10-9	In applications where the geographic distribution of nongeographic data must be displayed, other graphic elements should be added to a map for that purpose.				
		=>	4.1.5.10-10	When changes in mapped data are significant for a user's task, auxiliary graphic elements should be included to highlight those changes.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.1.5.10-11	When the use of mapped data may be complex, computer aids should be provided for data analysis.				
	=>	4.1.5.10-12	The user should be able to rapidly remove non-critical information from a map or map overlay display.				
4.1.5.11	Integral and Configural Displays						
	=>	4.1.5.11-1	Integral displays should be used to communicate high-level, status-at-a-glance information where users may not need information on individual parameters to interpret the display.				
	=>	4.1.5.11-2	Configural displays should be used when users must rapidly transition between high-level functional information and specific parameter values.				
	=>	4.1.5.11-3	The methods by which lower-level data are analyzed to produce higher-level information and graphical elements should be understandable to users.				
	=>	4.1.5.11-4	Users should have access to the rules or computations that link process parameters and graphical features, and to an explanation of how the information system produces higher-level information.				
	=>	4.1.5.11-5	A perceptually distinct reference aid should be provided in an object display to support users in recognizing abnormalities in the object's characteristics.				
	=>	4.1.5.11-6	The display elements should be organized so that the emergent features that arise from their interaction correspond to meaningful information about the process or system, e.g., when the aspect of the system represented by the emergent is disturbed, the disturbance is visible in the emergent feature.				
	=>	4.1.5.11-7	The emergent features or patterns within the display should be nested (from global to local) in a way that reflects the hierarchical structure of the process.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.11-8	Each emergent feature should be clearly distinguishable from other emergent features and from information on individual parameters.				
		=>	4.1.5.11-9	Each relevant process parameter should be represented by a perceptually distinct element within the display.				
		=>	4.1.5.11-10	The display should support the user in performing tasks requiring lower-level information.				
		=>	4.1.5.11-11	The emergent features and their interactions should not be so complex as to be susceptible to misinterpretation.				
	4.1.5.12		Graphic Instrument Panels					
		=>	4.1.5.12-1	Zones indicating operating ranges should be color coded by edge lines or wedges for circular scales.				
		=>	4.1.5.12-2	When check-reading positive and negative values on rotary meters (circular displays), the zero or null position should be at 12 o'clock or 9 o'clock.				
		=>	4.1.5.12-3	The pointer on fixed scales should extend from the right of vertical scales and from the bottom of horizontal scales.				
		=>	4.1.5.12-4	The pointer on fixed scales should extend to but not obscure the shortest graduation marks.				
		=>	4.1.5.12-5	Tick marks should be separated by at least 0.07 inches (1.75 millimeters) for a viewing distance of 28 inches (71 centimeters) under low illumination.				
		=>	4.1.5.12-6	Scales should not be cluttered with more marks than necessary for the precision needed the tasks for which the scale is used.				
	4.1.5.13		Speech Displays					
		=>	4.1.5.13-1	Speech should be limited to provide only a few messages.				
		=>	4.1.5.13-2	The user should be able to have speech messages repeated.				
		=>	4.1.5.13-3	Messages should be short and simple.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.5.13-4	A distinctive and mature voice should be used.				
		=>	4.1.5.13-5	Spoken messages should be presented in a formal, impersonal manner.				
		=>	4.1.5.13-6	Words in a speech message should be concise, intelligible, and appropriate for the information presented.				
		=>	4.1.5.13-7	A speech message priority system should be established such that more critical messages override the presentation of messages having lower priority.				
		=>	4.1.5.13-8	If speech is used to provide warnings as well as other forms of user guidance, spoken warnings should be easily distinguishable from routine messages.				
		=>	4.1.5.13-9	Speech signal intensity should be clearly audible for the expected ambient noise environment.				
4.1.6		Display Elements						
	4.1.6.1		Alphanumeric Characters					
		=>	4.1.61-1	Text to be read (except labels) should be presented using upper and lower case characters.				
		=>	4.1.61-2	A clearly legible font should be utilized. Fonts should have true ascenders and descenders, uniform stroke width, and uniform aspect ratio.				
		=>	4.1.61-3	For a given font, it should be possible to clearly distinguish between the following characters: X and K, T and Y, I and L, I and 1, O and Q, O and 0, S and 5, and U and V.				
		=>	4.1.61-4	The height of characters in displayed text or labels should be at least 16 minutes of arc (4.7 mrad) and the maximum character height should be 24 minutes of arc (7 mrad).				
		=>	4.1.61-5	For fixed (as opposed to proportionally spaced) presentations, the height-to-width ratio should be between 1:0.7 to 1:0.9.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.1.61-6	A 4x5 (width-to-height) character matrix should be the minimum matrix used for superscripts and for numerators and denominators of fractions that are to be displayed in a single character position.				
	=>	4.1.61-7	Horizontal separation between characters or symbols should be between 10 and 65 percent of character or symbol height.				
4.1.6.2		Abbreviations and Acronyms					
	=>	4.1.6.2-1	Abbreviations should be avoided (except when terms are commonly referred to by their initialisms, e.g., SPDS).				
	=>	4.1.6.2-2	When defining abbreviations that are not common to the user population, a simple rule should be used that users understand and recognize.				
	=>	4.1.6.2-3	Abbreviations should be distinctive so that abbreviations for different words are distinguishable.				
	=>	4.1.6.2-4	Abbreviations and acronyms should not include punctuation.				
	=>	4.1.6.2-5	When arbitrary codes must be remembered by the user, characters should be grouped in blocks of three to five characters, separated by a minimum of one blank space or other separating character such as a hyphen or slash.				
	=>	4.1.6.2-6	The use of the letters O and I in a non-meaningful code should be avoided since they are easily confused with the numbers 0 (zero) and 1 (one), respectively.				
	=>	4.1.6.2-7	When codes combine letters and numbers, letters should be grouped together and numbers grouped together rather than interspersing letters with numbers.				
4.1.6.3		Numeric Data					
	=>	4.1.6.3-1	Numeric values should ordinarily be displayed in the decimal number system.				
	=>	4.1.6.3-2	Leading zeros in numeric entries for whole numbers should be suppressed.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.6.3-3	A number should be displayed at the number of significant digits required by users to perform their tasks; displays should not imply precision beyond the capabilities of the underlying sensors.				
		=>	4.1.6.3-4	Numeric displays should accommodate the variable's full range				
		=>	4.1.6.3-5	Numeric displays should change slowly enough to be readable.				
		=>	4.1.6.3-6	If users must rapidly discern directional change, numeric displays should be provided with arrows to indicate the direction of change.				
		=>	4.1.6.3-7	If users must evaluate the difference between two sets of data, the difference should be presented on the display.				
		=>	4.1.6.3-8	All numbers should be oriented upright.				
		=>	4.1.6.3-9	If more than four digits are required, they should be grouped and the groupings separated as appropriate by commas, by a decimal point, or by additional space.				
	4.1.6.4		Icons and Symbols					
		=>	4.1.6.4-1	Symbols and icons should be simple and immediately recognizable.				
		=>	4.1.6.4-2	The meanings of icons and symbols should be obvious.				
		=>	4.1.6.4-3	Icons and symbols used in interfaces should conform to existing conventions and users' expectations.				
		=>	4.1.6.4-4	The use and meanings of symbols should be consistent throughout the plant as well as within a given interface.				
		=>	4.1.6.4-5	Icons or symbols that can be interacted with (e.g., that cause an action when clicked) should be readily distinguishable from those the have no such function.				
		=>	4.1.6.4-6	Changes in the 'look' of icons or symbols that are intended to convey the state of equipment or status of control systems should be conspicuous.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.6.4-7	The layout and arrangement of groups of symbols should follow a consistent and defined logic.					
		=>	4.1.6.4-8	The primary use of icons in graphic displays should be to represent actual objects or actions.					
		=>	4.1.6.4-9	Icons should be designed to look like the objects, processes, or operations they represent, by use of literal, functional, or operational representations.					
		=>	4.1.6.4-10	Each icon and symbol should represent a single object or action, and should be easily discriminable from all other icons and symbols.					
		=>	4.1.6.4-11	Special symbols to signal critical conditions should be used exclusively for that purpose.					
		=>	4.1.6.4-12	Words and symbols should not be used alternately.					
		=>	4.1.6.4-13	Icons and symbols should be large enough for the user to perceive the representation and discriminate it from other icons and symbols.					
		=>	4.1.6.4-14	An icon or symbol should be highlighted when the user has selected it.					
		=>	4.1.6.4-15	Icons that may not be immediately and unambiguously recognized should be accompanied by a text label.					
		=>	4.1.6.4-16	If icons are used to represent control action options, a label indicating the action should be associated with the icon.					
	4.1.6.5	Labels							
		4.1.6.5.1	Labeling Principles						
			=>	4.1.6.5.1-1	Controls, indicators, and other individual display elements that must be located, identified, or manipulated, should contain appropriate, distinct, unique, and descriptive labels.				
			=>	4.1.6.5.1-2	A hierarchical labeling scheme should be used to reduce confusion and search time.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.1.6.5.1-3	Major labels should be used to identify major systems, subordinate labels should be used to identify subsystems or functional groups, and component labels should be used to identify each display element.				
			=>	4.1.6.5.1-4	Labels should be consistent within and across panels in their use of words, acronyms, abbreviations, and part/system numbers.				
			=>	4.1.6.5.1-5	All discrete functional control positions (for example, “ON” and “OFF” positions of a particular controller) should be labeled.				
		4.1.6.5.2		Label Location					
			=>	4.1.6.5.2-1	Control and indicator labels should be located consistently, either below or above the display element, especially on the same display.				
			=>	4.1.6.5.2-2	Avoid placing adjacent labels together. Labels should be separated one from another by at least two standard character spaces.				
			=>	4.1.6.5.2-3	The labels used to identify a group of controls and or indicators corresponding to major systems or functional groups (subsystems) should be located above that group.				
			=>	4.1.6.5.2-4	Curved patterns should not be used for labeling.				
			=>	4.1.6.5.2-5	Labels should not detract from or obscure any other information displayed on the screen that must be read by the user.				
			=>	4.1.6.5.2-6	Labels should not be obscured by other information displayed on the screen.				
			=>	4.1.6.5.2-7	The label for a specific graphical object (i.e., an icon) should be placed in close proximity to the object.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.1.6.5.2-8	Labels may be placed directly on certain types of components (e.g., pushbuttons) for the purpose of increasing the utility and efficiency of control identification.				
	=>	4.1.6.5.2-9	Control position information should be visible to the user before, during, and after operation of the control.				
	=>	4.1.6.5.2-10	The user should not be allowed to move or hide labels for any visual display components, excepting graph legends.				
4.1.6.5.3		Label Content					
	=>	4.1.6.5.3-1	Use common terms that originate form typical language usage and/or from standard terminology for nuclear power plants.				
	=>	4.1.6.5.3-2	Trade names and other irrelevant information should not appear on labels.				
	=>	4.1.6.5.3-3	Use whole words rather than abbreviations whenever space permits.				
	=>	4.1.6.5.3-4	Use standard abbreviations as created and used at the plant.				
	=>	4.1.6.5.3-5	Use standard acronyms if they have been well established.				
	=>	4.1.6.5.3-6	Avoid the use of words that may be interpreted as both a noun or adjective and as a verb (e.g., “OPEN” in the case of “OPEN VALVE”).				
	=>	4.1.6.5.3-7	Words and abbreviations of similar appearance should be avoided where an error in interpretation could occur.				
	=>	4.1.6.5.3-8	When special precautionary words are required, select ones that provide an appropriate sense of urgency, hazard, or danger.				
	=>	4.1.6.5.3-9	All danger, warning, and safety instruction labels should be designed in accordance with appropriate safety standards.				
	=>	4.1.6.5.3-10	The label should briefly and simply express the intended action of controls or the meaning of the given indication.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.6.5.3-11	Nomenclature printed on labels should be consistent with that used in procedures.				
		=>	4.1.6.5.3-12	When presenting a list of options, labels should reflect the question or decision being posed to the user.				
	4.1.6.5.4	Label Lettering						
		=>	4.1.6.5.4-1	Labels should be uniquely and consistently highlighted, boxed, or otherwise emphasized to differentiate them from other screen structures and data.				
		=>	4.1.6.5.4-2	Always use capital letters for labels and not a mix of capital and lowercase letters.				
		=>	4.1.6.5.4-3	The lettering for all labels should be oriented so that they read from left to right, not around corners, on their side, or up and down.				
		=>	4.1.6.5.4-4	Labels should be graduated in size such that the labels used for the group on the higher hierarchy level are about 25 percent larger than the labels used for the group on the preceding level of hierarchy.				
		=>	4.1.6.5.4-5	Absolute label size should be determined starting with the smallest lettering size that will be compatible with the display resolution and the typical average viewing distance.				
		=>	4.1.6.5.4-6	Lettering and background colors should provide high contrast and legibility.				
		=>	4.1.6.5.4-7	Ensure that all numbers and characters are clearly distinguishable.				
4.1.6.6	Scales, Axes, and Grids							
	=>	4.1.6.6-1	Numbers on a scale should increase clockwise, left to right, or bottom to top.					
	=>	4.1.6.6-2	Nine should be the maximum number of tick marks between numbers.					

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.6.6-3	Scales should have tick marks at a standard interval of 1, 2, 5, or 10 (or multiples of 10) for labeled divisions; intervening tick marks to aid visual interpolation should be consistent with the labeled scale interval.				
		=>	4.1.6.6-4	For one-revolution circular scales, zero should be at 7 o'clock and the maximum value should be at 5 o'clock.				
		=>	4.1.6.6-5	Axes should be clearly labeled with a description of what parameter is represented by the axis.				
		=>	4.1.6.6-6	The units of measurement represented by the scale should be included in the axis label.				
		=>	4.1.6.6-7	Conventional scaling practice should be followed, in which the horizontal X-axis is used to plot time or the postulated cause of an event, and the vertical Y-axis is used to plot the effect.				
		=>	4.1.6.6-8	If users must compare graphic data across a series of displays, the same scale should be used for each.				
		=>	4.1.6.6-9	The scales should be consistent with the intended functional use of the data.				
		=>	4.1.6.6-10	A linear scale should be used for displayed data, in preference to logarithmic or other non-linear methods of scaling, unless it can be demonstrated that non-linear scaling will facilitate user interpretation of the information.				
		=>	4.1.6.6-11	When users must compare aggregate quantities within a display, or within a series of displays, scaling of numeric data should begin with zero.				
		=>	4.1.6.6-12	When graphed data represent positive numbers, the graph should be displayed with the origin at the lower left, such that values on an axis increase as they move away from the origin of the graph.				
		=>	4.1.6.6-13	Only a single scale should be shown on each axis, rather than including different scales for different curves in the graph.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.6.6-14	If different variables on a single graph require different scales, they should be scaled against a common baseline index, rather than showing multiple scales.				
		=>	4.1.6.6-15	When a graphic display has been expanded from its normal coverage, some scale indicator of the expansion factor should be provided.				
		=>	4.1.6.6-16	Users should be able to manually change the scale to maintain an undistorted display under different operating conditions.				
		=>	4.1.6.6-17	If the system is designed to automatically change scale, an alert should be given to the user that the change is being made.				
		=>	4.1.6.6-18	If interpolation must be made or where accuracy of reading graphic data is required, computer aids should be provided for exact interpolation.				
		=>	4.1.6.6-19	When grid lines are displayed, they should be unobtrusive and not obscure data elements (e.g., curves and plotted points).				
		=>	4.1.6.6-20	Graphs should be constructed so that the numbered grids are bolder than unnumbered grids.				
		=>	4.1.6.6-21	When data comparisons of interest fall within a limited range, the scaled axis should emphasize that range, with a break in the displayed axis to indicate discontinuity with the scale origin.				
		=>	4.1.6.6-22	When scaled data will contain extreme values, duplicate axes should be displayed, so that the X-axis appears at both the top and bottom, and the Y-axis at both the left and right sides of the graph.				
		=>	4.1.6.6-23	Unless required, use of three-dimensional scales (i.e., where a Z-axis is added to the display) should be avoided.				
	4.1.6.7		Borders, Lines, and Arrows					
		=>	4.1.6.7-1	Meaningful differences between lines appearing in graphic displays, such as flow paths, should be depicted by using various line types, e.g., solid, dashed, dotted, and widths.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.6.7-2	In flow charts and other graphics displays, arrowheads should be used in a conventional fashion to indicate directional relations in the sequential links between various elements.					
		=>	4.1.6.7-3	Unnecessary borders should not be used in the display.					
		=>	4.1.6.7-4	A border should be used to improve the readability of a single block of numbers or letters.					
		=>	4.1.6.7-5	If several labels or messages are clustered in the same area, distinctive borders should be placed around the critical ones only.					
	4.1.6.8	Visual Characteristics							
		4.1.6.8.1	Color						
			=>	4.1.6.8.1-1	Color use and the meanings attached to colors should be consistent throughout the plant as well as within a specific upgrade project.				
			=>	4.1.6.8.1-2	Color should be utilized as part of the overall labeling and demarcation strategy.				
			=>	4.1.6.8.1-3	Color should be used as part of the overall strategy to emphasize particular items of information.				
			=>	4.1.6.8.1-4	Colors should be considered for use as part of the overall strategy to identify the status of components or systems.				
			=>	4.1.6.8.1-5	Color should be considered for use as part of the overall strategy to convey the magnitude of measured quantities.				
			=>	4.1.6.8.1-6	The number of colors should be limited to those that can be easily distinguished.				
			=>	4.1.6.8.1-7	Colors should have adequate contrast and luminance with respect to the surroundings.				
			=>	4.1.6.8.1-8	The uses of color as a coding should normally be backed up with another coding method.				
			=>	4.1.6.8.1-9	When a user must distinguish rapidly among several discrete categories of data, a unique color should be used to display the data in each category.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.1.6.8.1-10	When color coding is used, each color should represent only one category of displayed data.				
	=>	4.1.6.8.1-11	Color coding should not create unplanned or obvious new patterns on the screen.				
	=>	4.1.6.8.1-12	Colors and color combinations that may cause problems owing to the workings of color vision should be avoided.				
4.1.6.8.2		Size					
	=>	4.1.6.8.2-1	Use of size coding should be limited to avoid crowded displays.				
	=>	4.1.6.8.2-2	No more than three size levels should be used to represent for discrete information.				
	=>	4.1.6.8.2-3	Each discrete size should be between 50% and 100% larger than the smaller size.				
	=>	4.1.6.8.2-4	Image proportions should be maintained when varying an image's size.				
	=>	4.1.6.8.2-5	If size is used to convey quantitative information, the area should vary in proportion to the measurement.				
4.1.6.8.3		Shape					
	=>	4.1.6.8.3-1	Shape coding should be used to represent discrete, nominal information, as opposed to relative values.				
	=>	4.1.6.8.3-2	No more than 15 distinct and clearly identifiable shapes should be used.				
4.1.6.8.4		Pattern					
	=>	4.1.6.8.4-1	Pattern codes should be simple.				
	=>	4.1.6.8.4-2	When using pattern density to convey quantity, the least dense pattern should represent the lower extreme, and the densest pattern should represent the higher extreme.				
4.1.6.8.5		Brightness					

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.1.6.8.5-1	No more than two levels of brightness coding should be used on VDUs.				
	=>	4.1.6.8.5-2	Higher brightness levels should signify more importance and higher priority.				
4.1.6.8.6	Flashing						
	=>	4.1.6.8.6-1	Flash coding should be used very sparingly.				
	=>	4.1.6.8.6-2	Flash coding should not be used on text or detailed data that must be read.				
	=>	4.1.6.8.6-3	Only small area of the screen should flash at any time.				
	=>	4.1.6.8.6-4	No more than two flash rates should be used to ensure that the rates are clearly distinguishable.				
	=>	4.1.6.8.6-5	Faster flashing rates should correspond to more critical information.				
	=>	4.1.6.8.6-6	Some method of flash suppression or acknowledgement should be provided.				
	=>	4.1.6.8.6-7	Flashing should not be used with long-persistence phosphor displays.				
4.1.6.9	Auditory Coding						
	=>	4.1.6.9-1	Auditory signals should be provided to alert the user to situations that require attention, such as an incorrect input action or a failure of the HSI to process an input from the user.				
	=>	4.1.6.9-2	Systems used to transmit non-verbal auditory signals should be used only for that purpose.				
	=>	4.1.6.9-3	Auditory signals should provide localization cues that direct users to those control room workstations where attention is required.				
	=>	4.1.6.9-4	Auditory signals should be selected to avoid interference with other auditory sources, including verbal communication.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.6.9-5	Advisory or caution signals should be readily distinguishable from warning signals and used to indicate conditions requiring awareness, but not necessarily immediate action.				
		=>	4.1.6.9-6	Auditory alerts, as well as caution and warning sounds, should accompany visual displays.				
		=>	4.1.6.9-7	Once a particular auditory signal code is established for a given operating situation, the same signal should not be designated for some other display.				
		=>	4.1.6.9-8	If the audio signal varies on one dimension only (such as frequency), the number of signals to be identified should not exceed four.				
		=>	4.1.6.9-9	One audio signal may be used in conjunction with several visual displays, provided that immediate discrimination is not critical to personnel safety or system performance.				
		=>	4.1.6.9-10	Audio warning signals that might be confused with routine signals or with other sounds in the operating environment should not be used.				
		=>	4.1.6.9-11	The intensity, duration, and source location of the signal should be compatible with the acoustical environment of the intended receiver as well as with the requirements of other personnel in the signal area.				
		=>	4.1.6.9-12	Noncritical auditory signals should be capable of being turned off at the discretion of the user.				
		=>	4.1.6.9-13	When the signal must indicate which user (of a group of users) is to respond, a simple repetition code should be used.				
		=>	4.1.6.9-14	Sound sources (speakers or buzzers) should direct sound toward the center of the main operating area.				
		=>	4.1.6.9-15	When an audio signal must bend around major obstacles or pass through partitions, its frequency should be less than 500 Hz.				
		=>	4.1.6.9-16	Auditory alert and warning signals should be audible in all parts of the control room.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.1.6.9-17	The intensity of auditory signals should be set to unmistakably alert and get a user's attention.				
		=>	4.1.6.9-18	When an audio signal must travel over 1000 feet, its frequency should be less than 1000 Hz.				
		=>	4.1.6.9-19	When the noise environment is unknown or expected to be difficult to penetrate, audio signals should have a shifting frequency that passes through the entire noise spectrum and/or be combined with a visual signal.				
		=>	4.1.6.9-20	Audio warning signals should not interfere with any other critical functions or warning signals, or mask any other critical audio signals.				
		=>	4.1.6.9-21	The audio display device and circuit should be designed to preclude warning signal failure in the event of system or equipment failure and vice versa.				
		=>	4.1.6.9-22	Auditory alarm systems should be designed so that false alarms are avoided.				
		=>	4.1.6.9-23	Coding methods should be distinct and unambiguous, and should not conflict with other auditory signals.				
		=>	4.1.6.9-24	Similar auditory signals must not be contradictory in meaning with one another.				
		=>	4.1.6.9-25	Auditory signals may be pulse coded by repetition rate. Repetition rates should be sufficiently separated to ensure discrimination.				
		=>	4.1.6.9-26	If modulation of the frequency (Hz) of a signal denotes information, center frequencies should be between 500 and 1000 Hz.				
		=>	4.1.6.9-27	If discrete-frequency codes are used for audible signal coding, frequencies should be broad band and widely spaced within the 200 to 5000 Hz range (preferably between 500 and 3000 Hz).				
		=>	4.1.6.9-28	Using the intensity of a sound to convey information is not recommended.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.1.6.9-29	It should be possible to test the auditory signal system.				
4.1.7		Data Quality and Data Uprate					
	=>	4.1.7-1	The maximum update rate should be determined by the time required for the user to identify and process the changed feature of the display.				
	=>	4.1.7-2	The user should be capable of controlling the rate of information update on the display, but the allowable rate should not exceed that capable of being met by the information source and the processing equipment.				
	=>	4.1.7-3	Changing alphanumeric values that the user must reliably read should not be updated more often than once per second.				
	=>	4.1.7-4	When the computer generates a display to update changed data, the old items should be erased before adding new data items to the display.				
	=>	4.1.7-5	Items on a graphic display should not move faster than 60 degrees of visual angle per second, with 20 degrees per second preferred.				
	=>	4.1.7-6	The timeliness of displayed data should be such that, for the purposes of their tasks, users can consider it to represent current conditions at the time it is viewed.				
	=>	4.1.7-7	Data values displayed in any part of the workspace should be able to be considered, for purposes of users' tasks, consistent in time with all other displayed data.				
	=>	4.1.7-8	Each variable should be displayed with an accuracy sufficient for the users to perform their tasks.				
	=>	4.1.7-9	Variables that are subject to validation (e.g., checks for accuracy) should be identified and an indication should be provided when these data are invalid.				
	=>	4.1.7-10	When checks for accuracy could not be performed, the unvalidated status of the data should be clearly indicated.				
	=>	4.1.7-11	Data entered by personnel should be identified such that it is easily distinguished from validated data.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.1.7-12	Analytical redundancy should be considered to help ensure the appropriateness of displayed values.				
	=>	4.1.7-13	A display feature should be provided to indicate to the user that the system is operating properly (or that a system failure has occurred).				
	=>	4.1.7-14	Information system failures (due to sensors, instruments, and components) should result in distinct display changes that directly indicate that depicted plant conditions are invalid.				
	=>	4.1.7-15	When task performance requires or implies the need to assess currency of information within a display, the information should be annotated with time information.				
	=>	4.1.7-16	When task requirements dictate that current information changes be continuously viewed and the display is changing so rapidly that the information is difficult to read, the user should have the capability of simultaneously viewing the information in a supplemental ‘snapshot’ display (i.e., a display frozen to enhance readability) along with the continuous display.				
	=>	4.1.7-17	If a display has a freeze capability, the display should have an obvious reminder that it is in the freeze mode.				

D.2 User Interface Interaction and Management

D.2.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.2.4		General Interface Design Objectives						
	4.2.4.1		Simplifying Input					
		=>	4.2.4.1-1	User input actions should be simple, particularly for real-time tasks requiring fast user response.				
		=>	4.2.4.1-2	Input transactions and associated displays should be designed so that a user can stay with one method of entry, and not have to shift to another.				
		=>	4.2.4.1-3	For interpreting user-composed control entries, upper and lower case letters should be treated as equivalent.				
		=>	4.2.4.1-4	Unless otherwise required by processing or display requirements, alphabetic input should be left justified, and numeric input should be right justified for integer data or decimal point justified for decimal data.				
		=>	4.2.4.1-5	Automatic justification of tabular data entries should be provided.				
		=>	4.2.4.1-6	When a user must enter numeric values that will later be displayed, all significant zeros should be maintained.				
		=>	4.2.4.1-7	Numeric values should be displayed to the level of significance required of the data, regardless of the value of individual input data.				
		=>	4.2.4.1-8	Data entry by overwriting a set of characters within a field should be avoided.				
		=>	4.2.4.1-9	The user should not be required to enter data separators or delimiters, such as dashes and slashes.				
		=>	4.2.4.1-10	The user should not be required to enter units of measure.				
		=>	4.2.4.1-11	When data entry is a significant part of a user’s task, entered data should appear on the user’s main display.				
		=>	4.2.4.1-12	The same explicit ENTER action should be required for entry of corrections as used for the original entry.				
		=>	4.2.4.1-13	Users should be able to perform simple editing during text entry without having to invoke a separate edit mode.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.4.1-14	When appropriate (e.g., in menu-based systems where system response may be slow), the system should allow users to easily enter a sequence of commands or option codes as a single ‘stacked’ entry.				
		=>	4.2.4.1-15	All displays should be designed so that features relevant to user entries are distinctive in position and/or format.				
		=>	4.2.4.1-16	The means of entering information or commands should be compatible with user skills, permitting simple step-by-step actions by beginners, but permitting more complex entries by experienced users.				
	4.2.4.2		Ensuring User Control of the Interaction					
		=>	4.2.4.2-1	Users should be allowed to control the processing of information or execution of commands.				
		=>	4.2.4.2-2	If different kinds of user interrupts are provided, each interrupt function should be designed as a separate control option with a distinct name.				
		=>	4.2.4.2-3	User interrupts and aborts should not modify or remove stored or entered data.				
		=>	4.2.4.2-4	Users should be allowed to control the pace and sequence of their entry of information or commands.				
		=>	4.2.4.2-5	If PAUSE or SUSPEND options are provided, some indication of the status should be displayed whenever a user selects such an option.				
		=>	4.2.4.2-6	The HSI should provide visual and/or auditory reminders for interrupted tasks.				
		=>	4.2.4.2-7	The HSI should provide simple mechanisms for retrieving displays and controls for tasks that have been suspended.				
		=>	4.2.4.2-8	At any step in a defined transaction sequence, if there is only a single appropriate next step, then a consistent control option to continue to the next transaction should be provided.				
		=>	4.2.4.2-9	Transactions should never leave the user without further available action and should provide next steps or alternatives.				
	4.2.4.3		Establishing Consistency of Interface and Interaction					
		=>	4.2.4.3-1	Procedures for entering commands or information should be consistent in form and consequences.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.4.3-2	All terms employed in the user-system interface, and their abbreviations, should be consistent in meaning from one transaction to another, and from one task to another.				
		=>	4.2.4.3-3	The wording and required format of information or command entry functions should be consistently reflected in the wording of user guidance, including all operating procedures, labels, messages, and training material.				
		=>	4.2.4.3-4	Controls used for interface management tasks should have consistent locations.				
	4.2.4.4		Minimizing Demands on the User					
		=>	4.2.4.4-1	Entry of information or commands should not require the user to remember special codes or sequences or to perform translations or conversions.				
		=>	4.2.4.4-2	A user should not be required to re-enter information already available to the system.				
		=>	4.2.4.4-3	Information necessary to accomplish a specific entry (e.g., labels, annotations, prompts, or options lists) should be available to the user when that transaction action is appropriate.				
		=>	4.2.4.4-4	An information entry sequence should be designed so that its organization reflects the user's view of the task, and should provide all control options that may be required.				
		=>	4.2.4.4-5	Flexible means of entering information or commands should be provided so that users can accomplish necessary transactions, and can obtain guidance as needed in connection with any transaction.				
		=>	4.2.4.4-6	The results of any entry should be compatible with user expectations, so that the system changes in a 'natural' way in response to user actions.				
		=>	4.2.4.4-7	If entries are made by keying onto the display, such as by keyed menu selections or commands, they should be distinguishable from displayed text.				
		=>	4.2.4.4-8	Annotations added by users to displayed text should be distinguishable from the text itself.				
		=>	4.2.4.4-9	Travel distance for cursors across and between display pages and windows on a display screen should be minimized.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.4.4-10	Displays that can provide decluttering capabilities should also provide a means for the user to rapidly return the display to its original configuration.				
		=>	4.2.4.4-11	The user should be able to manipulate information without concern for internal storage and retrieval mechanisms of the system.				
		=>	4.2.4.4-12	When likely default values can be defined for the information to be entered in a particular task, those default values should be offered to speed entry.				
		=>	4.2.4.4-13	Preset and automated set-up features should be used to ensure that users do not have to perform these functions while operating the plant.				
		=>	4.2.4.4-14	When users must select options by code entry, the code associated with each option should be displayed in a consistent and distinctive manner.				
		=>	4.2.4.4-15	When several users must interact with the system simultaneously, control entries by one user should not interfere with those of another.				
	4.2.4.5		Maintaining Awareness of Context and Operations					
		=>	4.2.4.5-1	If the consequences of a user entry will differ depending upon context established by a prior action, then some continuous indication of current context should be displayed for reference by the user.				
		=>	4.2.4.5-2	Information displayed to provide context for user entries should be distinctive in location and format, and consistently displayed from one transaction to the next.				
		=>	4.2.4.5-3	Users should be permitted to request a summary of prior entries to help determine present status, and should be allowed to review the entries currently in effect.				
		=>	4.2.4.5-4	A general list of basic options should be provided and always be available to serve as a ‘home base’ or consistent starting point for user input.				
		=>	4.2.4.5-5	When a user is performing an operation on some selected display item, that item should be highlighted.				
		=>	4.2.4.5-6	The general options list should show control entry options grouped, labeled, and ordered in terms of their logical function, frequency, and criticality of use, following the general guidelines for menu design.				
		=>	4.2.4.5-7	Users should be provided with a list of the control options that are specifically relevant and available for any transaction.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.2.4.5-8	Only control options that are actually available for the current transaction should be offered to users.					
4.2.4.6	Guiding and Assisting Users							
	4.2.4.6.1	General						
		=>	4.2.4.6.1-1	System messages should appear in standard locations.				
		=>	4.2.4.6.1-2	Consistent grammatical construction should be used in system messages.				
		=>	4.2.4.6.1-3	System messages should use familiar terminology.				
		=>	4.2.4.6.1-4	System messages should be concise and clearly worded.				
		=>	4.2.4.6.1-5	Wording for system messages should be directed at the user.				
		=>	4.2.4.6.1-6	No extraneous information should be displayed.				
		=>	4.2.4.6.1-7	Presenting the system as a person should be avoided.				
		=>	4.2.4.6.1-8	Experienced users should be able to define when and how guidance will be provided by automated guidance/help systems.				
		=>	4.2.4.6.1-9	The content of help information should be oriented toward users' completion of their tasks; i.e., the information should be procedural.				
		=>	4.2.4.6.1-10	The display of online help should not obscure important information.				
		=>	4.2.4.6.1-11	Online help should accommodate users' differing levels of expertise and preferred interaction styles.				
		=>	4.2.4.6.1-12	Users should be able to request guidance information regarding requirements for information or command entry (e.g., syntax, parameters, and options).				

					Guidelines	Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.1-13	Users should be provided with whatever information may be needed to guide command entries at any point in a sequence of transactions, by incorporating prompts in a display and/or by providing prompts in response to requests for HELP.				
		4.2.4.6.2		Prompts					
			=>	4.2.4.6.2-1	Users should be provided with clear and specific information to guide entries during logon/logoff or command or information entry.				
			=>	4.2.4.6.2-2	When a user must specify the address for a message, prompting should be provided.				
			=>	4.2.4.6.2-3	Standard symbols should be used for input prompting.				
			=>	4.2.4.6.2-4	When a command entry is not recognized or is inappropriate, users should be prompted to correct, rather than re-enter the command.				
			=>	4.2.4.6.2-5	Cues should be provided to indicate the size of a fixed-length data entry field.				
			=>	4.2.4.6.2-6	Additional cuing of data format should be included in a field label when that seems helpful.				
			=>	4.2.4.6.2-7	Users should be able to request computer generated prompts to determine required parameters or available options for a command.				
			=>	4.2.4.6.2-8	Prompting should be provided for required formats and acceptable values for data entries.				
			=>	4.2.4.6.2-9	Graphic means may be provided for displaying prompting aids and other guidance pertaining to current control actions.				
		4.2.4.6.3		Advisory Messages					
			=>	4.2.4.6.3-1	Advisory messages should be distinctive.				
			=>	4.2.4.6.3-2	Information requiring prompt attention should be presented through both visual and auditory means.				
			=>	4.2.4.6.3-3	Protection against data loss should be provided.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.3-4	Users should be informed when a command will be time-consuming to process.				
		4.2.4.6.4		Error Messages					
			=>	4.2.4.6.4-1	When the computer detects an entry error, an error message should be displayed stating the error and possible subsequent operations.				
			=>	4.2.4.6.4-2	Error messages should be clearly worded, informative, and appropriate to the task.				
			=>	4.2.4.6.4-3	The computer should display an error message only after completion of an entry.				
			=>	4.2.4.6.4-4	Where an entry is invalid or inoperative at the time of selection, no action should result except a display of an advisory message indicating the error and the appropriate functions, options, or commands.				
			=>	4.2.4.6.4-5	Error messages should facilitate correction of the error.				
			=>	4.2.4.6.4-6	The means of notifying users of errors should remain effective when there are multiple errors.				
			=>	4.2.4.6.4-7	If an error is detected in a group of entries, the system should process correct commands until the error is displayed.				
			=>	4.2.4.6.4-8	Following the output of a simple error message, users should be able to request a more detailed explanation of the error.				
			=>	4.2.4.6.4-9	Error messages should be presented at the point of the error or in a consistent area of the display.				
		4.2.4.6.5		Validating User Input					
			=>	4.2.4.6.5-1	Displays and transactions associated with information entry should be designed so that users can review and confirm entries before they are processed by the system.				
			=>	4.2.4.6.5-2	The system should validate any item whose entry and/or correct format or content is required for subsequent data processing.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.5-3	In a repetitive data entry task, the data for each transaction should be validated as it is completed, and the user should be allowed to correct errors before beginning another transaction.				
			=>	4.2.4.6.5-4	Optional item-by-item data validation within a multiple-entry transaction should be provided.				
			=>	4.2.4.6.5-5	Validation features should accommodate deferred entries				
			=>	4.2.4.6.5-6	If data validation detects a probable error, an error message should be displayed to the user at the completion of data entry.				
			=>	4.2.4.6.5-7	When a data or command entry error is suspected but cannot be determined (in terms of system error logic), a cautionary message asking for confirmation should be displayed.				
		4.2.4.6.6		Correcting Information/Command Entries					
			=>	4.2.4.6.6-1	All error corrections by the user should be acknowledged by the system, either by indicating a correct entry has been made or by another error message.				
			=>	4.2.4.6.6-2	Any user action should be immediately reversible by an UNDO command.				
			=>	4.2.4.6.6-3	For all inputs, whether data entries or commands, users should be allowed to edit composed material before requesting computer processing.				
			=>	4.2.4.6.6-4	When the system detects an error in a user input, the user should be allowed to make an immediate correction.				
			=>	4.2.4.6.6-5	Following error detection, users should be allowed to edit entries by rekeying only those portions that were in error.				
			=>	4.2.4.6.6-6	Users should be required to take an explicit ENTER action for computer processing of error corrections.				
			=>	4.2.4.6.6-7	When inappropriate or unrecognized commands are detected, a list should be provided to the user showing permissible commands, anticipating the command intended.				

				Guidelines		Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.6-8	Users should be allowed to BACKUP easily to previous steps in a transaction sequence in order to correct an error or make any other desired change.				
			=>	4.2.4.6.6-9	If an error is detected in a stacked series of command entries, the computer should either consistently execute to the point of error, or else consistently require users to correct errors before executing any command.				
			=>	4.2.4.6.6-10	If only a portion of a stacked command can be executed, the user should be notified and provided appropriate guidance to permit correction, completion, or cancellation of the stacked command.				
			=>	4.2.4.6.6-11	If a user makes a command entry error, after the error message has been displayed, the user should be allowed to enter a new command.				
			=>	4.2.4.6.6-12	If a command entry is not recognized, the user should be allowed to revise the command rather than rejecting the command outright.				
		4.2.4.6.7		User Guidance/Help					
			=>	4.2.4.6.7-1	Reference material describing system capabilities, procedures, and commands and abbreviations should be available and easily accessed on-line.				
			=>	4.2.4.6.7-2	When a user requests HELP on a topic, the computer should accept synonyms and abbreviations.				
			=>	4.2.4.6.7-3	The information presented in response to a HELP request should be tailored to the task context.				
			=>	4.2.4.6.7-4	When a request for HELP is ambiguous in context, the computer should initiate a dialogue to specify what data, message, or command requires explanation.				
			=>	4.2.4.6.7-5	When a HELP display provides summary information, more detailed explanations should be available.				
			=>	4.2.4.6.7-6	A complete hardcopy set of computer system operating procedures and contingency procedures should be available in the control room.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.4.6.7-7	Procedures should be prepared from the point of view of the user.				
			=>	4.2.4.6.7-8	Cross-indices of the available data displays should be available in the control room in hardcopy form.				
	4.2.4.7		Allowing Flexibility						
		=>	4.2.4.7-1	Flexible HSI features should be provided when they provide specific benefits to user tasks and their use does not impair user performance.					
		=>	4.2.4.7-2	Users should not have to use flexible interface features to support tasks and circumstances that could have been anticipated and designed for.					
		=>	4.2.4.7-3	The system should be sufficiently flexible to enable users to respond to unanticipated situations or where personal preference can positively impact performance.					
		=>	4.2.4.7-4	Users' flexibility in configuring the interface should not be unlimited.					
		=>	4.2.4.7-5	Displays that can be modified by users should provide a means for the user to rapidly return the display to its default configuration.					
		=>	4.2.4.7-6	The design of flexible HSI features should provide capabilities that are consistent with the levels of expertise of the users.					
		=>	4.2.4.7-7	When information or command entry requirements may change, some means for the user (or a system administrator) to make necessary changes to available functions should be provided.					
4.2.5		Interface Management Functions							
	4.2.5.1		Entry of Commands and Information						
		4.2.5.1.1		Command Language					
			=>	4.2.5.1.1-1	The system should be designed to help users learn and remember the commands.				
			=>	4.2.5.1.1-2	The interaction should be designed to minimize the effort involved in entering the commands.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.1-3	A command language should be designed to minimize errors, and the system should tolerate types of errors that can be anticipated.				
		4.2.5.1.2		Menus					
			=>	4.2.5.1.2-1	User requested menus should be used whenever possible; the use of permanent menus should be minimized.				
			=>	4.2.5.1.2-2	If menu options are included in a display that is intended also for data review and/or data entry, the menu options should be distinct from other displayed information.				
			=>	4.2.5.1.2-3	When permanent menus are used, there should be one standard design for the input prompt that is used across all tasks.				
			=>	4.2.5.1.2-4	A menu should be designed to display all options appropriate to any particular transaction.				
			=>	4.2.5.1.2-5	Menus should display as selectable only those options that are actually available in the current context.				
			=>	4.2.5.1.2-6	Menus should be designed so that the function of the menu is evident to the user.				
			=>	4.2.5.1.2-7	When equivalent keyboard commands are provided, they should be displayed as part of the menu option label.				
			=>	4.2.5.1.2-8	If one option on a menu is selected more often than the others, then it should be highlighted.				
			=>	4.2.5.1.2-9	Where discrimination among options may be difficult for users, menus can provide a preview of options.				
			=>	4.2.5.1.2-10	Options that are critical or frequently chosen should be quickly accessible using as few steps as possible.				
			=>	4.2.5.1.2-11	Users should be able to select a menu or submenu directly, without going through intermediate selection steps.				
			=>	4.2.5.1.2-12	Users should have to take only one simple action to return to the next higher level in hierarchic menus.				
			=>	4.2.5.1.2-13	Users should have to take only one simple action to return to the general menu at the top level in hierarchic menus.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.2-14	When menu selection is accomplished by code entry, users should be able to combine a series of selections into a single “stacked” entry.				
			=>	4.2.5.1.2-15	Experienced users should be able to bypass a series of menu selections and make an equivalent command entry directly.				
			=>	4.2.5.1.2-16	When a menu is first displayed, the cursor should be positioned so that it may be readily located and used.				
			=>	4.2.5.1.2-17	A menu macro capability should be provided if it produces faster access.				
			=>	4.2.5.1.2-18	Multiple navigation paths should be provided to items in the display system.				
			=>	4.2.5.1.2-19	A visual representation of the menu structure should be provided.				
			=>	4.2.5.1.2-20	Menu options should be ordered and grouped logically.				
			=>	4.2.5.1.2-21	Where ordering cannot be determined by the above, alphabetic ordering should be used.				
			=>	4.2.5.1.2-22	The order of options on menus should be fixed.				
			=>	4.2.5.1.2-23	If meaningful categories cannot be developed for menu options then visual groups should be created for long menus.				
			=>	4.2.5.1.2-24	All menu items should be visible to the user without scrolling.				
			=>	4.2.5.1.2-25	When multiple menu options are displayed in a list, each option should be displayed on a new line, i.e., format the list as a single column.				
			=>	4.2.5.1.2-26	When menu selection must be made from a long list, and not all options can be displayed at once, a hierarchic sequence of menu selections should be provided rather than one long multipage menu.				
			=>	4.2.5.1.2-27	Menus should have a limited number of items in breadth and in depth.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.2-28	If menu options are grouped in logical subunits, each group should have a descriptive label that is distinctive in format from the option labels themselves.				
			=>	4.2.5.1.2-29	If menu options are grouped in logical subunits, the same color should be used for menus within the same group.				
			=>	4.2.5.1.2-30	The display format and selection logic of hierarchic menus should be consistent at every level.				
			=>	4.2.5.1.2-31	Hierarchic menus should be organized and labeled to guide users within the hierarchic structure.				
			=>	4.2.5.1.2-32	Users should be able to access a visual representation of their paths through a hierarchy of menus.				
			=>	4.2.5.1.2-33	When users must step through a sequence of menus to make a selection, the hierarchic menu structure should be designed to minimize the number of steps required.				
			=>	4.2.5.1.2-34	When hierarchic menus are used, the user should have some indication of current position in the menu structure.				
			=>	4.2.5.1.2-35	If hierarchical branching is used, each subordinate menu should be visually distinct from each previous superordinate menu.				
			=>	4.2.5.1.2-36	The display of hierarchic menus should be formatted so that options that actually accomplish actions can be distinguished from options that merely branch to other menu frames.				
			=>	4.2.5.1.2-37	The categories listed across the menu bar should be organized systematically.				
			=>	4.2.5.1.2-38	Category labels on menu bars should be centered in the vertical dimension. Horizontally, category labels on the menu bar should be separated by enough space to be distinguishable as separate items, i.e., by at least two standard character widths.				
			=>	4.2.5.1.2-39	The height of a menu bar should be sufficient to contain standard text characters that serve as menu category labels, as well as space above and below the text characters.				
			=>	4.2.5.1.2-40	Pull-down and pop-up menus should be activated only by a specific user action that requests the display of the menu.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.2-41	When a pull-down or pop-up menu item(s) has/have been selected, the menu should revert to its hidden state as the selected command is carried out.				
			=>	4.2.5.1.2-42	If menu items are selectable via activation of programmable function keys, the arrangement of the menu list should be compatible with the arrangement of the keys to the greatest degree possible.				
			=>	4.2.5.1.2-43	An explanatory title should be provided for each menu that reflects the nature of the choice to be made.				
			=>	4.2.5.1.2-44	Menus should be displayed in consistent screen locations for all modes, transactions, and sequences.				
			=>	4.2.5.1.2-45	When menu selection is accomplished by code entry, a standard command entry area (window) should be provided where users enter the selected code.				
			=>	4.2.5.1.2-46	Users should not be able to select menu items that are in conflict.				
			=>	4.2.5.1.2-47	If menu selection is accomplished by pointing, dual activation should be provided, in which the first action designates the selected option, followed by a separate second action that makes an explicit control entry.				
			=>	4.2.5.1.2-48	If menu selection is accomplished by pointing, the sensitive area for pointing should be as large as consistently possible, including at least the area of the displayed option label plus a half-character distance around that label.				
			=>	4.2.5.1.2-49	The system should provide feedback as users interact with menus.				
			=>	4.2.5.1.2-50	When menus are provided in different displays, they should be designed so that option lists are consistent in wording.				
			=>	4.2.5.1.2-51	Menu options should be consistently worded as commands.				
			=>	4.2.5.1.2-52	Letter codes used to designate menu options should be meaningful and should be used consistently.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		4.2.5.1.3		Function Keys					
			=>	4.2.5.1.3-1	Function keys should be provided for interim command entries, i.e., for actions taken before the completion of a transaction.				
			=>	4.2.5.1.3-2	Each function key should be labeled informatively to designate the function it performs.				
			=>	4.2.5.1.3-3	Function keys should be grouped in distinctive locations on the keyboard to facilitate their learning and use.				
			=>	4.2.5.1.3-4	A function assigned to a particular key in a given task context should be assigned to the same key in other contexts.				
			=>	4.2.5.1.3-5	When a function is continuously available, its function should be assigned to a single key.				
			=>	4.2.5.1.3-6	Frequently used functions should be executed by means of a single key action and should not require chord-keying (e.g., use of the shift key).				
			=>	4.2.5.1.3-7	When a function key performs different functions in different operational modes, equivalent or similar functions should be assigned to the same key.				
			=>	4.2.5.1.3-8	If chord-keying is used, the functions paired on one key should be logically related.				
			=>	4.2.5.1.3-9	If chord (e.g., control/shift) keying is used, the logical relation between shifted and unshifted functions should be consistent from one key to another.				
			=>	4.2.5.1.3-10	If a key is used for more than one function, the function currently available should always be indicated to the user.				
			=>	4.2.5.1.3-11	If the functions assigned to a set of keys change as a result of user selection, the user should be provided with an easy means to return to the initial, base-level functions.				
			=>	4.2.5.1.3-12	When function key activation does not result in any immediately observable natural response, users should be provided with some other form of computer acknowledgment.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.3-13	Function keys are not needed for a current transaction should be temporarily disabled.				
			=>	4.2.5.1.3-14	If some function keys are active and some are not, the current subset of active keys should be indicated in some noticeable way, such as by brighter illumination.				
			=>	4.2.5.1.3-15	The system should prompt the user for confirmation if a function key is pressed in a context unrelated to the function.				
			=>	4.2.5.1.3-16	The layout of function keys should be compatible with their use.				
		4.2.5.1.4		Macros/Programmable Function Keys					
			=>	4.2.5.1.4-1	Users should be allowed to assign a single name to a defined series of entries, and then to use that named “macro” for subsequent command entry.				
			=>	4.2.5.1.4-2	Users should have access to an index of their macros and programmable function keys with their respective composition of commands.				
			=>	4.2.5.1.4-3	The use of user definable macros and programmable function keys should be limited.				
			=>	4.2.5.1.4-4	A user should be restricted from modifying a macro or programmable function key as defined by a different originating user.				
			=>	4.2.5.1.4-5	Users should not be allowed to duplicate macro names.				
		4.2.5.1.5		Forms					
			=>	4.2.5.1.5-1	Form filling should be provided as an aid for composing complex command entries.				
			=>	4.2.5.1.5-2	Appropriate and readily modified default parameters should be displayed in forms used for composing complex command entries.				
			=>	4.2.5.1.5-3	Forms for command entry should be consistent in format.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.5-4	Form filling should be used for tasks where some flexibility in information entry is needed, such as the inclusion of optional as well as required items, and/or where computer response may be slow.				
			=>	4.2.5.1.5-5	Where no source documents or forms exist to support information entry, then fields should be logically grouped, by sequence and frequency of use, importance, and functional associations.				
			=>	4.2.5.1.5-6	Just one explicit entry action at the end of the transaction sequence should be required, rather than separate entry of each item.				
			=>	4.2.5.1.5-7	For each data field, an associated label should be displayed to help users understand what entries can be made.				
			=>	4.2.5.1.5-8	Whenever possible, entry of multiple data items should be allowed without keying special separator or delimiter characters.				
			=>	4.2.5.1.5-9	When a field delimiter must be used for data entry, a standard character should be employed consistently for that purpose.				
			=>	4.2.5.1.5-10	When multiple data items are entered as a single transaction, as in form filling, the user should be allowed to review, modify, or cancel the items before entering the form.				
			=>	4.2.5.1.5-11	When entry of information in a field is deferred or omitted, the system should identify the field by highlighting or other means. Before the information is filed or accessed, the user should be reminded that information has not been entered, if such entry is required.				
			=>	4.2.5.1.5-12	When sets of data items must be entered sequentially, in a repetitive series, a tabular display format should be provided where data sets can be keyed row by row.				
			=>	4.2.5.1.5-13	Users should not have to remove unused underscores or otherwise enter keystrokes for each position within a variable length entry area.				
			=>	4.2.5.1.5-14	Optional versus required data entries within fields on input forms should be distinct.				
			=>	4.2.5.1.5-15	Distinctive formats should be provided for column headers and row labels, so that users can distinguish them from data entries.				
			=>	4.2.5.1.5-16	For entry of tabular data, when entries are frequently repeated, users should be provided with some easy means to copy duplicated data.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.5-17	Where the number of fields is limited, screen traversal distances are short, and when data fields will be accessed sequentially, users should be allowed to tab directly from one data field to the next, so that the cursor can move freely back and forth across rows or columns.				
			=>	4.2.5.1.5-18	Direct pointing devices, such as a mouse or light pen, should be available (1) for selecting fields in complicated forms, or (2) when field entry will be less predictable (as in database update).				
			=>	4.2.5.1.5-19	For long forms, those with many rows, some extra visual cue should be provided to help a user scan a row accurately across columns.				
			=>	4.2.5.1.5-20	If certain information is used frequently, then it should be automatically entered into the form as a default; see guidance on defaults in Section 4.2.4.4.				
		4.2.5.1.6		Direct Manipulation					
			=>	4.2.5.1.6-1	Direct manipulation should be used primarily in tasks with actions and objects that lend themselves to pictographic representation, and in which the actions and objects need not be modified for the successful interpretation of the command by the system.				
			=>	4.2.5.1.6-2	When user input involves frequent pointing on a display surface, the interface should be designed so that other actions (e.g., display control) are also accomplished by pointing, in order to minimize shifts from one entry device to another.				
			=>	4.2.5.1.6-3	Selection of an icon, menu, or application-specific capability from a function area should be acknowledged by highlighting the selected item.				
			=>	4.2.5.1.6-4	The direct manipulation interface should include (1) windows for containing the data files, (2) menus for additional objects and actions that are not easily represented by pictographic icons.				
			=>	4.2.5.1.6-5	Direct manipulation should not be used when the computer response is slow.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.6-6	If icons are used to represent control actions in menus, a text label should be displayed with each icon to help assure that its intended meaning will be understood.				
			=>	4.2.5.1.6-7	Graphic means should be provided for displaying the context of current control actions to users.				
			=>	4.2.5.1.6-8	Prompting aids and other guidance pertaining to current control actions should be displayed graphically to the user.				
			=>	4.2.5.1.6-9	A user should be able to “open” an icon with a simple, explicit action.				
			=>	4.2.5.1.6-10	The size and separation of items on the screen that are displayed for selection should allow them to be pointed to easily (i.e., without requiring precise positioning of the pointer).				
			=>	4.2.5.1.6-11	When exact placement of graphic elements is required, users should be allowed to expand (“zoom”) the critical display area to make the positioning task easier.				
			=>	4.2.5.1.6-12	Users should be provided some means for designating and selecting displayed graphic elements for manipulation.				
			=>	4.2.5.1.6-13	All items currently selected should be highlighted in some way to minimize uncertainty about the objects or files to which subsequent actions will be applied.				
			=>	4.2.5.1.6-14	During graphic data entry/editing, the selected attributes that will affect current actions should be displayed for ready reference by the user.				
			=>	4.2.5.1.6-15	Automatic registration or alignment of computer-generated graphic data should be provided, so that variable data are shown properly with respect to fixed background or map data at any display scale.				
			=>	4.2.5.1.6-16	When complex graphic data must be entered quickly, computer aids should be provided to automate that process.				
			=>	4.2.5.1.6-17	Automated plotting of computer-stored data should be provided at user request, with provision for subsequent editing by a user.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.6-18	When graphic data must be plotted in predefined standard formats, templates or skeletal displays for those formats should be provided to aid data entry.				
			=>	4.2.5.1.6-19	When graphs must be constructed for data plotting, computer aids should be provided for that purpose.				
			=>	4.2.5.1.6-20	Computer aids should be provided to help users specify appropriate scales for graphic data entry.				
			=>	4.2.5.1.6-21	Users should be allowed to designate a group of elements to which graphic editing operations will be applied in common.				
			=>	4.2.5.1.6-22	The effects of operations performed on direct manipulation interfaces should be immediately visible.				
			=>	4.2.5.1.6-23	Explicit error messages should be provided for incorrect actions related to the process (as opposed to the interface).				
			=>	4.2.5.1.6-24	Representations used as icons should require minimal interpretation.				
		4.2.5.1.7		Natural Language					
			=>	4.2.5.1.7-1	A natural language interface should not be the sole means of taking actions that may have to be done very quickly or reliably.				
			=>	4.2.5.1.7-2	The outputs of a natural language system should be consistent with the types of entries required of users.				
		4.2.5.1.8		Query Language					
			=>	4.2.5.1.8-1	A query language should reflect a single, natural data structure or organization.				
			=>	4.2.5.1.8-2	The wording of a query should simply specify what data are requested.				
			=>	4.2.5.1.8-3	Users should be allowed to employ alternative forms when composing queries, corresponding to common alternatives in natural language.				
			=>	4.2.5.1.8-4	A query language should minimize the need for quantifiers in query formulation.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.8-5	A query language should include logic elements that permit users to link sequential queries as a single entry.				
			=>	4.2.5.1.8-6	If a query will result in a large-scale data retrieval, the user should be informed and required to confirm the transaction or to narrow the query before processing.				
			=>	4.2.5.1.8-7	A query language interface should not be the sole means of taking actions that may have to be done very quickly or reliably.				
		4.2.5.1.9		Question and Answer					
			=>	4.2.5.1.9-1	The system should provide the user with a specific request for information.				
			=>	4.2.5.1.9-2	Each question should be displayed separately.				
			=>	4.2.5.1.9-3	The system should indicate any constraints that apply to the user's response.				
			=>	4.2.5.1.9-4	The system should accept as much data as the user is willing to provide in an answer.				
			=>	4.2.5.1.9-5	When a series of computer-posed questions are interrelated, answers to previous questions should be displayed when those will provide context to help a user answer the current question.				
			=>	4.2.5.1.9-6	The user should have the ability to remove a question and answer from the screen or recall a question and answer to the screen.				
			=>	4.2.5.1.9-7	When questions prompt entry of data from a source document, the question sequence should match the data sequence in the source document.				
			=>	4.2.5.1.9-8	A question mark should be the delimiter of the question and answer dialogue.				
		4.2.5.1.10		Speech					
			=>	4.2.5.1.10-1	Spoken input should be used together with alternative methods such as keyed entry or pointing.				
			=>	4.2.5.1.10-2	The characteristics of the speech recognition function should be appropriate for the tasks it is intended to support.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.1.10-3	Feedback and simple error correction procedures should be provided for speech input, so that when a spoken entry has not been correctly recognized by the computer, the user can cancel that entry and speak again.				
			=>	4.2.5.1.10-4	When speech input is the preferred means of input, alternatives forms for critical entries should be allowed, so that if the system cannot recognize an entry after repeated attempts, another entry form can be substituted.				
			=>	4.2.5.1.10-5	Speech recognition systems should have a means of activation and deactivation (e.g., PAUSE and CONTINUE options) so that conversation between users is not taken as command input.				
			=>	4.2.5.1.10-6	The vocabulary items should (1) consist of words that are meaningful and familiar to the user, (2) be phonetically distinct from one another; and (3) consist of 2-5 syllables.				
			=>	4.2.5.1.10-7	Application vocabularies should be divided into sets based on the hierarchy of the application and recognition accuracy requirements.				
			=>	4.2.5.1.10-8	The user should be able to test the recognition of any individual vocabulary item without the entire interactive system being on-line. Feedback on the word recognized and the corresponding confidence score should be available immediately after each use of a word.				
			=>	4.2.5.1.10-9	When the consequences of errors are not significant, the speech amplitude and rejection levels required for input should be user-adjustable.				
			=>	4.2.5.1.10-10	Where word boundaries (pauses between words) are required for system interpretation, boundaries of 100 milliseconds or more should be allowed by the system.				
			=>	4.2.5.1.10-11	An indication of the similarity of each spoken command to the recorded template should be available to the user.				
			=>	4.2.5.1.10-12	If an application functions with a speaker-dependent voice recognizer, the user should be able to retrain or update any or all vocabulary templates at any time.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.2.5.2		Supporting Use of Individual Display Pages					
	=>	4.2.5.2-1	When requested data exceeds the capacity of a single display frame, users should be given some easy means to move (vertically, horizontally, or both, as needed) over displayed material by paging or scrolling.				
	=>	4.2.5.2-2	When users are required to integrate information across a large display, the HSI should be designed to minimize the effort associated with scrolling, paging, and zooming, and to maintain the users' orientation.				
	=>	4.2.5.2-3	The design of display pages should take into account limitation in users' abilities to effectively process visual information presented in a scrolling frame.				
	=>	4.2.5.2-4	Displays should be designed to avoid the need for excessive scrolling.				
	=>	4.2.5.2-5	An appropriate orientation for display framing should be chosen and used consistently throughout the interface.				
	=>	4.2.5.2-6	Display framing should be described (e.g., in user instructions and key labels) in functional terms, and wording that implies spatial orientation should be avoided.				
	=>	4.2.5.2-7	Display framing should be described (e.g., in user instructions and key labels) in functional terms, and wording that implies spatial orientation should be avoided.				
	=>	4.2.5.2-8	In addition to scrolling continuously or line-by-line, users should have the option of moving in larger increments (e.g., a display frame or 'page' at a time).				
	=>	4.2.5.2-9	Users should have the ability to scroll or page using different techniques.				
	=>	4.2.5.2-10	Users should be able to expand the size of (i.e., 'zoom') any selected area of the display.				
	=>	4.2.5.2-11	The interface should have features that help user remain oriented when 'zooming' displays.				
	=>	4.2.5.2-12	When users zoom a display, the system should compensate for changes in the size of symbols, labels, and other graphical objects.				
4.2.5.3		Supporting Navigation in Systems of Displays					

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.5.3-1	The organization of the display network should be readily understood by users.				
		=>	4.2.5.3-2	The display system should be represented so that the user's perception of the relatedness of displays is consistent with distance in the structure of the display hierarchy.				
		=>	4.2.5.3-3	Cues should be provided to help the user retain a sense of location within the information structure.				
		=>	4.2.5.3-4	Easily discernable features should appear in successive views and provide a frame of reference for establishing relationships across views.				
		=>	4.2.5.3-5	There should be physical or functional overlaps between displays that prevent the displays from appearing as disjointed views.				
		=>	4.2.5.3-6	A hypertext information system should show how a destination node is related to the point of departure.				
		=>	4.2.5.3-7	If the interpretation of displayed data depends on its context (i.e., the location in the display network), an explicit indication of the context should appear in the display.				
		=>	4.2.5.3-8	In spatial representations (such as maps or P&IDs), features should be included to help operators understand the depiction and to assist in way finding and maintaining orientation (especially when the representation is larger than a display page).				
		=>	4.2.5.3-9	During navigation, displays should support users' comprehension of the relationships between successive views or destinations.				
		=>	4.2.5.3-10	Wherever possible, the time and effort associated with navigation among display pages (especially those that are often used in succession) should be minimized.				
		=>	4.2.5.3-11	Use of various navigation strategies should be supported.				
		=>	4.2.5.3-12	The display network should provide more than one way to access displays.				
		=>	4.2.5.3-13	When multiple methods are provided for navigating in a hypertext system, they should function similarly.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.2.5.3-14	Backtrack capabilities should always be available in hypertext interfaces and should function in the same way.				
		=>	4.2.5.3-15	Selection points (e.g., navigation targets or links) should be easily detectable and readily distinguished from other displayed text or objects.				
	4.2.5.4		Controlling Displays					
		=>	4.2.5.4-1	Users should be able to specify the information to be displayed and select the format in which it is presented.				
		=>	4.2.5.4-2	Screen control locations and control options should be clearly and appropriately indicated.				
		=>	4.2.5.4-3	The rate at which displayed values are updated should be appropriate for the users' tasks.				
		=>	4.2.5.4-4	If a display can be frozen, it should contain features to ensure that users' remain aware of its state, and of the ongoing situation.				
		=>	4.2.5.4-5	If a display is suppressed, the interface should contain features to ensure that users' remain aware of its absence, and of the ongoing situation.				
		=>	4.2.5.4-6	Automated window management should be coordinated with the user's tasks.				
		=>	4.2.5.4-7	Automated interface management features should be designed such that their operation can be anticipated by users.				
		=>	4.2.5.4-8	The operation of automated interface management features should be apparent to the user.				
		=>	4.2.5.4-9	The operation of automated interface management features should not draw excessive attention from the user.				
	4.2.5.5		Providing Feedback					
		=>	4.2.5.5-1	The computer should acknowledge every entry immediately.				
		=>	4.2.5.5-2	Actions requested by users should be completed within an appropriate time.				
		=>	4.2.5.5-3	If processing time requires delay of concurrent user inputs (and no keyboard buffer is available), users should be kept aware of the status of processing.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.2.5.5-4	When slower-than-typical response time can be anticipated (e.g., owing to unusual demands on the system) the users should be given information that will allow them to adjust their interaction with the system.				
	=>	4.2.5.5-5	Response time deviations should not exceed more than half the mean response time.				
4.2.5.6	Protecting Information						
4.2.5.6.1	User Identification						
	=>	4.2.5.6.1-1	The logon process and procedures for user identification should be as simple as possible, consistent with protecting the system and associated data.				
	=>	4.2.5.6.1-2	When system security requires more stringent user identification than is provided by password entry, auxiliary tests should be devised that authenticate user identity without imposing impractical demands on users.				
	=>	4.2.5.6.1-3	Messages or signals should be provided in order to notify users (and system administrators) of potential threats to data security.				
	=>	4.2.5.6.1-4	If there are pending actions and the user requests a logoff, the system should inform the user that these actions will be lost and allow the user to cancel either the pending actions or the logoff.				
	=>	4.2.5.6.1-5	Where possible, in the event of automatic logoff, open files should be saved to some defined file name.				
	=>	4.2.5.6.1-6	Interactive timesharing systems should allow some specified time between keyboard actions before automatic logoff unless a longer period is requested by the user.				
	=>	4.2.5.6.1-7	An audible signal should be presented at specified intervals prior to automatic logoff.				
	=>	4.2.5.6.1-8	As required for security, procedures to control access to printed data should be established, rather than simply prohibiting the printing of sensitive data.				
4.2.5.6.2	Data Integrity						

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.6.2-1	Measures should be provided to minimize data loss from failures or errors in the data processing system.				
			=>	4.2.5.6.2-2	Data should be protected from damage as result of inadvertent or mistaken actions by the user.				
			=>	4.2.5.6.2-3	Display formatting features, such as field labels and delimiters, should be protected from accidental change by users.				
			=>	4.2.5.6.2-4	When users are not authorized to change displayed data, “read-only” status should be indicated on the display.				
			=>	4.2.5.6.2-5	Data should be protected from inadvertent loss caused by the actions of other users.				
			=>	4.2.5.6.2-6	When simulated data and system functions are displayed or provided (perhaps for user training), real data should be protected and real system use should be clearly distinguished from simulated operations.				
			=>	4.2.5.6.2-7	In situations where mistaken or unwanted data changes may be possible, users (or a system administrator) should be able to request a record of data entry/change transactions.				
			=>	4.2.5.6.2-8	When a control entry will cause any extensive change in stored information, particularly if that change cannot be easily reversed, the user should be notified and confirmation of the action should be required before implementing it.				
			=>	4.2.5.6.2-9	For conditions that may require special user attention to protect against information loss, an explicit alert and/or advisory message should be provided to prompt appropriate user action.				
			=>	4.2.5.6.2-10	When a user requests logoff, pending transactions should be checked and if any pending transaction will not be completed, or if data will be lost, an advisory message requesting user confirmation should be displayed.				
			=>	4.2.5.6.2-11	If a user requests change (or deletion) of a stored data item that is not currently being displayed, both the old and new values should be displayed so that the user can confirm or nullify the change before the transaction is completed.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.6.2-12	When records of data access are necessary, the records should be maintained automatically.				
	4.2.5.7		Managing Information						
		4.2.5.7.1		Editing Documents					
			=>	4.2.5.7.1-1	Users should be allowed to specify segments of text in whatever units are natural for entry/editing.				
			=>	4.2.5.7.1-2	Users should be allowed to display text exactly as it will be printed.				
			=>	4.2.5.7.1-3	Easy means should be provided for users to specify required format control features (e.g., margin and tab settings) during text entry/editing.				
			=>	4.2.5.7.1-4	Text entered by users should be formatted automatically.				
			=>	4.2.5.7.1-5	Users should be able to modify the formatting of text as needed.				
			=>	4.2.5.7.1-6	A tab function should be available for paragraph indentation and for moving the cursor to a preselected location.				
			=>	4.2.5.7.1-7	For editing programs or tabular data, cursor tab controls or other provisions for establishing and moving readily from field to field should be provided.				
			=>	4.2.5.7.1-8	The means should be provided to readily move the cursor to the head (beginning) or the foot (end) of the file.				
			=>	4.2.5.7.1-9	When inserting words or phrases, items to be inserted should be displayed as the final copy will appear.				
			=>	4.2.5.7.1-10	Users should be allowed to specify a string of text and request the computer to advance (or back up) the cursor automatically to the next (or last previous) occurrence of that string.				
			=>	4.2.5.7.1-11	When systematic editing changes will be made throughout a long document, a “global search and replace” capability should be provided.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.7.1-12	Users should be allowed to select and move text segments from one place to another within a document.				
			=>	4.2.5.7.1-13	Users should be allowed to label and store frequently used text segments, and to later recall (copy into current text) stored segments identified by their assigned labels.				
			=>	4.2.5.7.1-14	If the selected text, table, or graphics area extends beyond the bottom of the displayed page, the screen should automatically scroll until the user stops selecting or when the end of the display page is reached.				
			=>	4.2.5.7.1-15	Users should not be able to select non-contiguous blocks of text when copying, cutting, or pasting.				
		4.2.5.7.2		Saving Files					
			=>	4.2.5.7.2-1	The user should be able to save the information entered into a file by a single action that will permit the user to continue interacting with that file.				
			=>	4.2.5.7.2-2	After finishing the interaction with any type of file, the user should be able to save the information and stop interacting with the file by a single action.				
			=>	4.2.5.7.2-3	After finishing the interaction with any type of file, the user should be able to stop interacting with the file by a single action (e.g., selecting a menu item) without saving the changes to the file.				
			=>	4.2.5.7.2-4	The command used to “exit with save” should differ from the commands for “save” (without exit) and for “exit without save.”				
			=>	4.2.5.7.2-5	Processing of files should be designed to prevent the lost of input or changes.				
		4.2.5.7.3		Temporary Editing Buffer					
			=>	4.2.5.7.3-1	When selected data is cut or copied from a text file, tabular file, and/or graphics file and placed in a temporary editing buffer, the data should be placed in the buffer automatically, with the only specific action required by the user being the cut or copy action.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.5.7.3-2	The contents of the temporary editing buffer should remain intact after the application from which the contents were taken is closed.				
			=>	4.2.5.7.3-3	The default condition should be that additions to the temporary editing buffer are not cumulative.				
			=>	4.2.5.7.3-4	The user should be able to access the contents of the temporary editing buffer in a window with a single action.				
		4.2.5.7.4		Excerpt File					
			=>	4.2.5.7.4-1	The capability to accept and maintain information, independent of application, should be provided for holding relevant information across displays or applications.				
			=>	4.2.5.7.4-2	Users should have the capability to create multiple excerpt files.				
			=>	4.2.5.7.4-3	The user should have the capability to integrate new data with data already in the excerpt file.				
			=>	4.2.5.7.4-4	The user should be able to cut or copy data from the excerpt file and paste it to any other file.				
			=>	4.2.5.7.4-5	The user should be able to save the excerpt file.				
4.2.6		Interacting with Interface Components							
	4.2.6.1		Windows						
		4.2.6.1.1		General					
			=>	4.2.6.1.1-1	As appropriate to the user task, windows should be capable of the following operations: scrolling/panning, resizing, moving, hiding, activating, deactivating, copying to/from, zooming in/out, tabbing, and undo-last.				
			=>	4.2.6.1.1-2	User control of windows should operate consistently from one display to another for each type of window.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.1.1-3	When control actions such as command entry may be taken by a user working within a window, those control actions should be consistent from one window to another.				
		4.2.6.1.2		Labeling and Appearance					
			=>	4.2.6.1.2-1	Windows should be identified by a label consistently located at the top of the window's border.				
			=>	4.2.6.1.2-2	Window objects, dialog boxes, and subordinate windows should be labeled.				
			=>	4.2.6.1.2-3	The titles of subordinate windows should match the menu selection items of the menus from which they are selected.				
			=>	4.2.6.1.2-4	Windows should be visually separated from each other and from their background, preferably by borders or similar demarcation.				
			=>	4.2.6.1.2-5	Window types should be perceptually distinct (see Figure 4.26).				
		4.2.6.1.3		Multiple Windows					
			=>	4.2.6.1.3-1	If separate display pages contain information that the user must compare, combine, or otherwise mentally process, then they should be presented simultaneously.				
			=>	4.2.6.1.3-2	Users should be able to select separate data windows that will share a single display screen.				
			=>	4.2.6.1.3-3	When multiple windows are open simultaneously, the user should have the capability to easily tile, layer, or sequentially view the windows (see Figure 4.26).				
			=>	4.2.6.1.3-4	The system should keep track of the windows that are open (but not necessarily active or displayed), and provide a means of displaying the list of open windows to the user.				
			=>	4.2.6.1.3-5	An upper limit on the number of windows allowed to be open at one time should be defined to ensure that system response time is not compromised.				
			=>	4.2.6.1.3-6	If several windows are displayed at once, the window(s) in which action can be taken should be indicated.				

					Guidelines	**Complies**	**Does not Comply, but with Justification**	**Does not Comply, but without Justification**	**Not Applicable**
			=>	4.2.6.1.3-7	A separate menu bar should be provided for each application window, where different applications are operating concurrently in open windows (e.g., multi-tasking).				
		4.2.6.1.4		Active and Inactive Windows					
			=>	4.2.6.1.4-1	The user should be able to activate a window by performing any of a set of simple actions in that window or related to that window.				
			=>	4.2.6.1.4-2	The action that activates a window should automatically position the place-holding cursor in that window so that the user can provide inputs through that window.				
			=>	4.2.6.1.4-3	If windows are capable of different modes, the system should provide immediate and unambiguous feedback concerning which mode is in effect.				
			=>	4.2.6.1.4-4	A window that is not displayed should be capable of receiving information from the system.				
			=>	4.2.6.1.4-5	The system should alert the user to critical information that becomes available in an inactive or non-displayed window.				
			=>	4.2.6.1.4-6	Under normal operating conditions, active windows should be frontmost on the display.				
			=>	4.2.6.1.4-7	Caution and warning windows should be frontmost on the display.				
		4.2.6.1.5		Size and Location of Windows: Defaults					
			=>	4.2.6.1.5-1	The size and shape of the initial presentation of a window should be consistent with its contents (amount of information, number of menus, and data fields).				
			=>	4.2.6.1.5-2	The default dimensions of text windows should be large enough so that the readability of the information is not impaired.				
			=>	4.2.6.1.5-3	The amount of resizing, placement, and manipulation of windows required for using the HSI should be minimized.				
			=>	4.2.6.1.5-4	The system should not allow the user to move or resize a window containing non-critical information such that it obscures critical information.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.1.5-5	A temporary window object should not obscure critical control information and command entry interfaces of the active window.				
			=>	4.2.6.1.5-6	The system should not allow the user to move a window containing critical information off the display screen.				
			=>	4.2.6.1.5-7	Windows should have a default location on the display screen.				
			=>	4.2.6.1.5-8	Display data that is temporarily obscured by a window object should reappear when the object is removed.				
		4.2.6.1.6		Size and Location of Windows: Adjusting					
			=>	4.2.6.1.6-1	Window movement capability should be provided such that the user can move windows to different areas of the display.				
			=>	4.2.6.1.6-2	It should not be possible to position windows in such a way that menu bars, access to the command area, or caution and warning messages are obscured.				
			=>	4.2.6.1.6-3	Movement of a window should appear to be smooth and continuous to the user.				
			=>	4.2.6.1.6-4	Windows partially moved off the display should be made readily accessible with a single action.				
			=>	4.2.6.1.6-5	Users should be able to change the horizontal and vertical dimensions of a window independently or together.				
		4.2.6.1.7		Opening and Closing Windows					
			=>	4.2.6.1.7-1	The user should be able to open a window by performing any of a set of simple actions.				
			=>	4.2.6.1.7-2	Users should be able to close a window with a single action.				
			=>	4.2.6.1.7-3	If several windows are open, several easy means should be provided for a user to shift among them.				
			=>	4.2.6.1.7-4	The action that opens a window should automatically make that window active.				
			=>	4.2.6.1.7-5	An easy means for the user to suppress the display of windows should be provided.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.1.7-6	The window system should convey to the user the relationship between the window, the icon, and the action when a window is opened or closed.				
			=>	4.2.6.1.7-7	When a main application window is closed by the user, all associated subordinate windows and dialog boxes should also close.				
			=>	4.2.6.1.7-8	When a windows are being closed (either by the user or as the result of some other action), the user should be made aware of any pending changes or incomplete interactions.				
	4.2.6.2		Cursors						
		4.2.6.2.1		Appearance					
			=>	4.2.6.2.1-1	Cursors should have distinctive visual features (shape, blink, or other means of highlighting).				
			=>	4.2.6.2.1-2	The cursor should not move beyond the display boundaries or disappear from sight.				
			=>	4.2.6.2.1-3	The cursor should not be so distracting as to impair the searching of the display for information unrelated to the cursor.				
			=>	4.2.6.2.1-4	The displayed cursor should be stable.				
			=>	4.2.6.2.1-5	On the initial appearance of a data entry display, the cursor should appear automatically at some consistent and useful location.				
			=>	4.2.6.2.1-6	When there is a predefined HOME position for the cursor, that position should be consistently defined on all displays of a given type.				
			=>	4.2.6.2.1-7	When the user must repeatedly return the cursor to the origin or other specific screen location, automatic return or repositioning of the cursor should be provided.				
		4.2.6.2.2		Controls					
			=>	4.2.6.2.2-1	The user should be able to adjust the sensitivity of the cursor movement to be compatible with the required task and user skills.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.2.2-2	Control actions for cursor positioning should be compatible with movements of the displayed cursor, in terms of control function and labeling.				
			=>	4.2.6.2.2-3	Users should be provided with an easy, accurate means of positioning a displayed cursor to point at different display elements and/or display locations.				
			=>	4.2.6.2.2-4	Where cursor positioning is incremental by discrete steps, the step size of cursor movement should be consistent horizontally (i.e., in both right and left directions), and vertically (in both up and down directions).				
			=>	4.2.6.2.2-5	At the minimum, keys for cursor control should allow horizontal and vertical cursor movement.				
			=>	4.2.6.2.2-6	When position designation is required in a task emphasizing keyed data entry, cursor control should be provided by some device integral to the keyboard (function keys, joystick, and trackball).				
			=>	4.2.6.2.2-7	If cursor movement is accomplished by depressing keys, the keys should be located on the main keyboard.				
		4.2.6.2.3		Movement					
			=>	4.2.6.2.3-1	If the cursor is moved by depressing a key, releasing the key should cause the cursor to stop moving.				
			=>	4.2.6.2.3-2	The cursor control should permit both fast movement and accurate placement.				
			=>	4.2.6.2.3-3	When fine accuracy of positioning is required, as in some forms of graphic interaction, the displayed cursor should include a point designation feature.				
			=>	4.2.6.2.3-4	The user should be able to turn rate aiding of the cursor movement on or off.				
			=>	4.2.6.2.3-5	Users should be able to select at least two speeds (normal and fast) for the movement of the cursor when the keys for cursor control are held down.				

					Guidelines	Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.2.3-6	When character size is variable, the incremental cursor positioning should vary correspondingly, with a step size matching the size of currently selected characters.				
			=>	4.2.6.2.3-7	If a cursor must be positioned sequentially in predefined areas, such as displayed data entry fields, this should be accomplished by simple user action.				
			=>	4.2.6.2.3-8	Users should be required to take a separate, explicit action, distinct from cursor positioning, for the actual entry (enabling, activation) of a designated function.				
			=>	4.2.6.2.3-9	When there are areas of a display in which data entries cannot be made (such as in field labels or in blank spaces that are part of data formatting), the cursor should 'step over' those areas, and they should be insensitive to pointing actions.				
			=>	4.2.6.2.3-10	For text editing, users should be allowed to move the cursor freely over a displayed page of text to specify items for change, and to make changes directly to the text.				
			=>	4.2.6.2.3-11	If proportional spacing is used for displayed text, computer logic should make necessary adjustments automatically when the cursor is being positioned for data entry or data change.				
			=>	4.2.6.2.3-12	Users should be able to move the cursor by specific units of text, as well as one character at a time.				
			=>	4.2.6.2.3-13	An ENTER action for multiple data items should result in entry of all items, regardless of where the cursor is placed on the display.				
		4.2.6.2.4		Multiple Cursors					
			=>	4.2.6.2.4-1	Multiple cursors on a single display should be used only when it can be demonstrated that they are required by the task.				
			=>	4.2.6.2.4-2	In a multitasking environment with multiple monitors, controllers, or cursors, the location of the active cursor should be obvious to the user.				
			=>	4.2.6.2.4-3	If multiple cursors are used, they should be visually distinctive from one another.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.2.4-4	If multiple cursors are controlled by different devices, their separate controls should be compatible in operation.				
			=>	4.2.6.2.4-5	When multiple cursors are controlled by a single device, the cursor currently being controlled should be clearly indicated.				
			=>	4.2.6.2.4-6	When there are multiple cursor control/pointing devices, a unique pointing cursor shape should be associated with each device.				
			=>	4.2.6.2.4-7	Cursors of different shapes should be used for different purposes.				
		4.2.6.2.5		Pointing Cursors					
			=>	4.2.6.2.5-1	The pointing cursor should be visible to the user at all times and may obscure characters unless it interferes with performance within an application.				
			=>	4.2.6.2.5-2	The pointing cursor should not blink.				
			=>	4.2.6.2.5-3	Pointing cursors should maintain image quality throughout an entire range of motion within the display. The position of the pointing cursor should be clearly visible during movement from one screen position to another. Flicker should be minimized.				
			=>	4.2.6.2.5-4	To the greatest degree possible, pointing cursors should be completely graphic and should not contain a label.				
			=>	4.2.6.2.5-5	The pointing cursor should maintain its size across all screen and display locations.				
			=>	4.2.6.2.5-6	The movement of the pointing cursor should appear to the user to be smooth and continuous, with smooth and continuous movement of the cursor control device. The pointing cursor should not move in the absence of any input from the user.				
		4.2.6.2.6		Text Entry Cursors					
			=>	4.2.6.2.6-1	The text entry cursor should only be visible when text entry is possible.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.2.6.2.6-2	At the initiation of a task, an application, or a new display, the user should be able to immediately determine the location of the text entry cursor. Following the initial placement of the text entry cursor, the position of the cursor should be under the user's control.				
			=>	4.2.6.2.6-3	If text entry cursor blinking is to be used to direct the user's attention, the default blink rate should be 3 Hz.				
			=>	4.2.6.2.6-4	The place-holding cursor should not obscure any other character displayed in the position designated by the cursor.				
			=>	4.2.6.2.6-5	There should be only one text entry cursor per window.				
			=>	4.2.6.2.6-6	The text entry cursor should assume the height and/or width of the text characters adjacent to it.				
		4.2.6.2.7		Multiple Display Devices					
			=>	4.2.6.2.7-1	When displays are the same size and are located adjacent to each other, the cursor should appear to move in a smooth, continuous motion from one display device to the next.				
			=>	4.2.6.2.7-2	When display devices are physically separated, have different orientations, or different sizes, techniques should be employed to help the user keep track of the cursor's position.				

D.3 Soft Controls

D.3.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.3.3	Deciding Whether to Use Hard or Soft Controls							
	=>	4.3.3-1	Identify hardwired controls that are required by regulation or needed for diversity from the computer system.					
	=>	4.3.3-2	Determine the need for spatial dedication and continuous availability. Consider using spatially dedicated, continuously available controls (hard or soft) when the user's tasks require rapid action, highly-reliable response, or frequent access to controls.					
	=>	4.3.3-3	Determine whether tradeoffs favor a hard or soft control implementation.					
4.3.4	Selection Displays							
	=>	4.3.4-1	Provide flexible approaches to soft control selection.					
	=>	4.3.4-2	The design of the HSI should clearly distinguish between control actions and interface management actions.					
	=>	4.3.4-3	The selection display should be clearly and prominently labeled to identify the set of items being presented.					
	=>	4.3.4-4	The display should clearly indicate what items can be selected for control and the items themselves should be visually distinct.					
	=>	4.3.4-5	The selection display should support the identification of items based on recognition rather than recall.					
	=>	4.3.4-6	Selection of an item from a display should require simple input actions.					
	=>	4.3.4-7	The selection display should provide feedback to the user of the items that have been selected.					
4.3.5	Control Displays							
	4.3.5.1	Identification and Management of Control Displays						
		=>	4.3.5.1-1	A clear link should be provided between the selection display and the control display.				
		=>	4.3.5.1-2	The item to be controlled should be clearly and prominently identified in the control display.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.3.5.1-3	The control display should not obscure associated information. If this is not possible, a means should be provided for viewing information that may be concealed by the control display.				
	=>	4.3.5.1-4	When multiple control displays are opened at the same location, their unique identification should be visible.				
4.3.5.2		Display of Control Modes, Logic, and Constraints					
	=>	4.3.5.2-1	When the soft control can be operated in more than one mode, the current mode should be clearly and prominently identified and the other mode options should be available.				
	=>	4.3.5.2-2	Higher-level controls should be considered for common operational situations.				
	=>	4.3.5.2-3	Information defining the control logic should be available to help personnel properly perform control functions.				
	=>	4.3.5.2-4	Timing requirements should be considered in the design of soft controls				
	=>	4.3.5.2-5	Deadband should be displayed where appropriate and important for the operators' understanding of the control response.				
	=>	4.3.5.2-6	Error signals for control systems should be supplied for selected controls				
	=>	4.3.5.2-7	A soft control display should allow users to quickly assess the status of individual components affected by the control.				
	=>	4.3.5.2-8	Information concerning interlocks, lockouts, and lockins related to the control action should be available to help personnel properly perform control functions. The user should be notified when interlocks, lockouts, and lockins are in effect and which actions are being blocked and what conditions activated the block.				
	=>	4.3.5.2-9	An interlock, lockout, or lockin should not initiate an action that was previously blocked merely because the status of the triggering condition has changed.				
4.3.5.3		Control Input and Commands					
	4.3.5.3.1	General Control Input Guidance					

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.3.5.3.1-1	The control display should be labeled and contain clear information to identify the item being controlled.				
			=>	4.3.5.3.1-2	The control input field should clearly and predominantly identify the aspect of the item that is being controlled				
			=>	4.3.5.3.1-3	The control options should be clearly presented and easily distinguished from each other.				
			=>	4.3.5.3.1-4	The user interaction with the control display should minimize the possibility of initiating a control action if the visual display is not working properly.				
			=>	4.3.5.3.1-5	If an input device controls more than one variable, the user should not have to reset the device to match the value of the new variable before executing a control action.				
			=>	4.3.5.3.1-6	If multiple soft controls are needed for a particular task, they should be retrievable as a predefined group.				
			=>	4.3.5.3.1-7	If keyboard input is used for a soft control, the input should be displayed in an input field on the control display and the control should not be acted on until a confirming response is made, such as hitting the return or enter key.				
		4.3.5.3.2		Discrete-Adjustment Controls					
			=>	4.3.5.3.2-1	Discrete-adjustment controls should be used for selecting among a set of individual settings or values.				
			=>	4.3.5.3.2-2	Discrete-adjustment controls should indicate which setting was selected				
			=>	4.3.5.3.2-3	If a discrete-adjustment control initiates continuous operation, it should provide continuous indication on the current state.				
		4.3.5.3.3		Continuous-Adjustment Controls					
			=>	4.3.5.3.3-1	Continuous-adjustment controls should be used when precise adjustments along a continuum are needed or when many discrete settings are present.				
			=>	4.3.5.3.3-2	Reference values should be provided to help users judge the appropriateness of values when entering continuous variable inputs.				
			=>	4.3.5.3.3-3	When part of the range of values depicted by a continuous-adjustment control represents critical information, such as alarm limits, those values should be coded to facilitate recognition.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.3.5.3.3-4	The value to which a continuous-adjustment control is set should be digitally displayed.				
			=>	4.3.5.3.3-5	The physical size of the continuous-adjustment control should allow the user to read the current and target values with the required precision and accuracy.				
			=>	4.3.5.3.3-6	A means of providing incremental increases or decreases in demanded values should be provided when precise inputs are needed. Each press of an arrow button should change the current value uniformly.				
			=>	4.3.5.3.3-7	Incremental input devices should provide salient feedback when they are actuated.				
		4.3.5.3.4	Error Tolerance and Correction						
			=>	4.3.5.3.4-1	Where possible, a command entry field should show valid value range and the expected number entry format, e.g. 0XX or XXXXX as well as a default value.				
			=>	4.3.5.3.4-2	Confirmation steps should be considered and, where used, implemented as a separate user input from control actions.				
			=>	4.3.5.3.4-3	User control input verification should be considered.				
			=>	4.3.5.3.4-4	A specific command that produces one action in one mode should not cause a different action in another mode.				
			=>	4.3.5.3.4-5	Unique commands associated with actions that have important consequences should not be easily confused with other commands used in the same or different modes.				
4.3.6		Feedback and Monitoring							
	=>	4.3.6-1	The soft control should display the user's input in a way that allows the user to review it and determine whether it is correct.						
	=>	4.3.6-2	Immediate feedback should be provided that a command was received. Additional feedback should indicate whether the user's command is being acted upon and the current status of the item being controlled relative to the demanded status.						
	=>	4.3.6-3	Feedback should indicate the status of sequential actions that are in progress.						

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.3.6-4	Systems that can change mode automatically should provide feedback to make the user aware of the current mode.				
	=>	4.3.6-5	Feedback should indicate when the demanded status is achieved.				

D.4 Alarms

D.4.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.4.3	General Considerations for Alarm Modifications						
	=>	4.4.3-1	The utility should ensure that the characteristics and features of existing alarms are defined, i.e., how the current alarms are used and how the users interact with them. This should include all uses of the alarms, even those that may be beyond the primary detection of abnormal conditions.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.4.3-2	The utility should define the impact of the current I&C modernization program on the plant's alarms. The utility should define: • What existing alarms are no longer needed • What existing alarms now have changed meaning • What additional alarms need to be incorporated, including those alarms associated with the digital system itself • The impact of alarm changes on overall control room changes				
	=>	4.4.3-3	The utility should identify any improvements they would like to make during the modernization program to the way in which alarms are used.				
	=>	4.4.3-4	The utility should consider all sources of alarm information that the users will use, consider the potential to integrate alarm information, and take advantage of the strengths of each approach presenting alarms.				
	=>	4.4.3-5	The utility should consider the effects of failures of portions or all of the equipment that generates or presents alarms, i.e., how failures are handled currently, and how they will be handled after the changes are made and during the process of effecting the changes.				
4.4.4		Alarm Definitions					
	=>	4.4.4-1	Only conditions that require the users' near-term attention or action should be defined as alarms.				
	=>	4.4.4-2	The following criteria should be included in the basis for selecting alarm conditions: • monitoring important plant functions, systems, components, and key parameters • preventing personnel hazards • monitoring the functioning of automatic systems • avoiding significant damage to equipment • assuring that technical specifications are met • monitoring emergency procedure decision points • monitoring plant conditions appropriate to plant modes ranging from full power to shutdown.				
	=>	4.4.4-3	Conditions that result in nuisance alarms should not be defined as alarms.				
	=>	4.4.4-4	Alarm set points should be established so that the operating crew is given timely warnings of accident or abnormal conditions, without establishing thresholds so close to the 'normal' operating values that false alarms are likely.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.4.4-5	The loss of alarm functions (e.g., ‘loss of annunciation’) should be indicated in the control room.				
4.4.5		Alarm Prioritization and Processing					
	=>	4.4.5-1	Alarms should be prioritized so that users can quickly distinguish which alarms are more important. The criteria used to establish the priority of an alarm condition should include the required immediacy of user action and the threat posed by the condition to safe plant operation.				
	=>	4.4.5-2	If alarms are prioritized into absolute categories, then no more than four alarm priorities should be used.				
	=>	4.4.5-3	Processing should prevent spurious alarms (i.e., alarms that are the result of faulty sensor input).				
	=>	4.4.5-4	Processing should prevent nuisance alarms (i.e., alarm signals for conditions that are not abnormal in the current operating mode or system configuration).				
	=>	4.4.5-5	Processing should identify alarms that are less important because they are redundant with or implied by other alarms (i.e., alarms that necessarily follow from other alarms owing to logical or physical principles or relationships).				
	=>	4.4.5-6	Processing should identify deviations from expected patterns or sequences of events.				
	=>	4.4.5-7	Processing should identify the first-out alarm, the initiating event associated with plant trips.				
	=>	4.4.5-8	Alarm processing should be used to reduce the number of alarms to a manageable level, to support the users’ ability to rapidly determine the state of the process.				
	=>	4.4.5-9	Alarm processing should not be so complex that users cannot determine how the current alarms were processed.				
4.4.6		Alarm Display					
	4.4.6.1	General Alarm Display Considerations					
		4.4.6.1.1	SDCV Alarm Displays				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.4.6.1.1-1	Spatially dedicated, continuously visible (SDCV) alarm displays should be considered for: • Alarms that require short-term response • The most important alarms used in diagnosing and responding to transients • The most important alarms used to maintain an overview of plant and system status Regulatory Guide 1.97 Type A parameters				
			=>	4.4.6.1.1-2	The format of messages on alarm tiles or tile-like displays should be consistent for all alarms.				
			=>	4.4.6.1.1-3	Detailed alarm information should be immediately available by other means.				
			=>	4.4.6.1.1-4	Alarm elements within a display should be grouped and ordered according to logical principles and/or natural relationships; the same principles and relationships should be used to organize displays throughout the control room.				
			=>	4.4.6.1.1-5	Groups of visual elements in alarm displays should be visually distinctive and arranged to be readily accessible and useable by users.				
		4.4.6.1.2		Alarm Message Lists					
			=>	4.4.6.1.2-1	Alarm messages should contain all the information the users need to respond to them effectively.				
			=>	4.4.6.1.2-2	Lists of alarm messages should typically be segregated by alarm priority with highest priority alarms being listed first, but users should have the capability to group alarm messages according to operationally relevant categories, such as function, chronological order, and status (unacknowledged, acknowledged/active, cleared).				
			=>	4.4.6.1.2-3	The presentation of alarm lists should be designed to enhance the readability of the information.				
			=>	4.4.6.1.2-4	Terminology in alarm message lists should be consistent with that used in other contexts.				
			=>	4.4.6.1.2-5	Printed copies of alarm message lists should convey all the information available in the VDU-displayed lists.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.4.6.1.3	Alarms Integrated into Other Displays						
	=>	4.4.6.1.3-1	Alarms that are important to plant monitoring and user action should be integrated into the associated displays.				
	=>	4.4.6.1.3-2	Alarms should be easily distinguishable, salient features in the display. Alarms should be displayed in a consistent way across all displays of a particular type.				
	=>	4.4.6.1.3-3	Since alarms embedded in displays may not provide messages, this information should be easily retrievable.				
4.4.6.2	Display of Alarm Priority						
	=>	4.4.6.2-1	The highest-priority alarms should be presented in SDCV displays.				
	=>	4.4.6.2-2	Spurious and nuisance alarms should be filtered.				
	=>	4.4.6.2-3	Redundant and lower-priority alarms should be coded to indicate their lower priority or suppressed. If suppressed, users should be able to access them easily.				
	=>	4.4.6.2-4	When coding priority levels, the highest-priority alarms should have the codes with greatest salience.				
4.4.6.3	Display of Alarm Status						
	=>	4.4.6.3-1	Visual and auditory signals should be used to convey the status of alarms and these signals should be readily distinguishable.				
	=>	4.4.6.3-2	Visual and auditory signals should direct users' attention so that they are aware of the status of all current alarms.				
4.4.6.4	Display of Shared Alarms						
	=>	4.4.6.4-1	The use of alarms that are triggered by any one of an aggregate of individual alarms and which require the users to perform additional actions to determine the cause should be limited.				
	=>	4.4.6.4-2	Accessing the individual alarm information represented by a shared alarm should require little effort.				
4.4.6.5	Coding of Alarms						

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.4.6.5-1	A systematic approach to coding should be developed across the various alarm displays.				
		=>	4.4.6.5-2	Signals used as codes should be readily detectable in any anticipated control room environment.				
		=>	4.4.6.5-3	Signals used as codes should not startle or annoy users.				
		=>	4.4.6.5-4	Levels of a code should be readily distinguishable from one another.				
		=>	4.4.6.5-5	The coding scheme applied to alarms should be simple and easily understood.				
	4.4.6.6		Auditory Characteristics					
		=>	4.4.6.6-1	The auditory characteristics of an alarm should not startle or annoy users.				
		=>	4.4.6.6-2	Redundant coding should be considered if the source of an audio signal is to be used to indicate where to direct attention.				
		=>	4.4.6.6-3	If audio patterns are used to represent information about alarms (as opposed to just the presence of an alarm), the patterns should be easily recognizable.				
		=>	4.4.6.6-4	When multiple audio signals are used to represent alarm information, interference among them should be avoided.				
	4.4.6.7		Alarm Location					
		=>	4.4.6.7-1	Important SDCV alarms should be located where everyone in the control room can see them.				
		=>	4.4.6.7-2	Lower-priority alarms can be presented at individual workstations or at displays on individual panels.				
4.4.7	Alarm Control and Management							
	4.4.7.1		Alarm Controls					
		=>	4.4.7.1-1	The methods by which alarms are silenced, acknowledged, and reset should be designed to support users' awareness of plant conditions without unnecessarily demanding users' time and attention.				

				Guidelines	Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.4.7.1-2	Separate controls should be provided for silence, acknowledgment, reset (acknowledging an alarm that has cleared and returning it to normal), and testing; the controls should be distinctively coded for easy recognition and should have the functions in the same relative locations.				
		=>	4.4.7.1-3	If the alarm presentation includes both alarm tiles and VDU alarm displays, each should have its own set of controls.				
		=>	4.4.7.1-4	Alarm controls should be designed so that they cannot be altered or defeated.				
	4.4.7.2	Alarm Management						
		=>	4.4.7.2-1	Facilities should be provided for selecting, sorting, grouping, searching, and printing the recorded alarm information.				
		=>	4.4.7.2-2	Separate controls should be provided for silence, acknowledgment, reset (acknowledging an alarm that has cleared and returning it to normal), and testing; the controls should be distinctively coded for easy recognition and should have the functions in the same relative locations.				
		=>	4.4.7.2-3	It should be possible to establish temporary, user-defined alarms and user-defined setpoints for specific conditions where such alarms are determined to be of assistance.				
		=>	4.4.7.2-4	When users are able to change the user-defined characteristics of alarms, the existence of such changes should be unambiguously indicated to all users, and should not interfere with normal alarm functioning.				
		=>	4.4.7.2-5	When characteristics of alarms can be modified automatically, the change should be unambiguously signaled to all users; an indication of the current configuration should be prominently displayed.				
		=>	4.4.7.2-6	If a change is automatically made to alarms, users should confirm the change.				
		=>	4.4.7.2-7	An alarm log should be maintained to support analysis of events.				
4.4.8	Alarm Response Procedures							
	=>	4.4.8-1		Alarm response procedures should be available for all alarms requiring users to take an overt action affecting plant process controls or plant equipment.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.4.8-2	Alarm response procedures should be immediately accessible to users.				
	=>	4.4.8-3	Alarm response procedures should contain all the information the users need and should be designed so that users can use them effectively.				
	=>	4.4.8-4	Information and terminology in alarm response procedures should be consistent with that used in other contexts.				

D.5 Computer-Based Procedures

D.5.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.5.3	Scope and Functionality of the CBP System						
	=>	4.5.3-1	Determine the scope of the computer-based procedure system; i.e., identify the procedures or types of procedures that will be computerized.				
	=>	4.5.3-2	Determine the functionality of the computer-based procedure system.				
4.5.4	Display of Procedures						
	4.5.4.1	General Alarm Display Considerations					

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.5.4.1-1	The detailed CBP design should be fully consistent with the rest of the HSI.				
		=>	4.5.4.1-2	CBP material should be legible and easy to read on any device at which it might be displayed.				
		=>	4.5.4.1-3	The display area dedicated to procedure-related information should be sufficient to show all the material that the user must view in parallel to execute a procedure step, including cautions and reference material.				
	4.5.4.2		Format and Screen Layout					
		=>	4.5.4.2-1	The procedure’s title and identification should be continuously presented.				
		=>	4.5.4.2-2	The status of high-level procedure goals should be continuously presented.				
		=>	4.5.4.2-3	The procedure’s format should reflect its organization.				
		=>	4.5.4.2-4	A consistent format should be used to display procedures.				
		=>	4.5.4.2-5	A consistent approach to partitioning procedures should be used.				
		=>	4.5.4.2-6	Each display screen should locate information and HSI features consistently.				
	4.5.4.3		Procedure Steps					
		=>	4.5.4.3-1	Procedure steps should be clear and unambiguous.				
		=>	4.5.4.3-2	Numerical information in procedure steps should be immediately understandable and useable.				
		=>	4.5.4.3-3	Procedure steps should be coded to indicate importance.				
		=>	4.5.4.3-4	Procedure steps should be coded to indicate when communication between the procedure user and other crew members in necessary or desirable.				
	4.5.4.4		Warnings, Cautions, Notes, and Supplementary Information					
		=>	4.5.4.4-1	The warnings and cautions applicable to a single step (or to a series of steps) should be displayed when the step(s) is on the screen.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.5.4.4-2	Warnings, cautions, and notes should be presented so that they will be read before the applicable action steps.				
		=>	4.5.4.4-3	Warnings, cautions, and notes should not include implied or actual action steps.				
		=>	4.5.4.4-4	Warnings, cautions, and notes should be uniquely presented, so that they are easily distinguished from each other and from other display elements.				
		=>	4.5.4.4-5	All supplementary information (such as tables and figures) associated with a procedure step and available to the CBP should be available on the screen concurrently with the step, or on another easily viewed display.				
	4.5.4.5		Lists					
		=>	4.5.4.5-1	Groups of related items (e.g., actions, conditions, components, criteria, systems) should be presented as a list.				
		=>	4.5.4.5-2	Formatting should be used to differentiate items in a list from other procedure elements.				
		=>	4.5.4.5-3	The presence or absence of precedence among items in lists should be indicated.				
		=>	4.5.4.5-4	Overviews should introduce each list.				
		=>	4.5.4.5-5	The method for assuring that each item in a list has received the users' attention should be consistent.				
4.5.5	Interaction with CBPs							
	4.5.5.1		Users' Control of Procedure Execution					
		=>	4.5.5.1-1	Users should control the execution of computer-based procedures.				
		=>	4.5.5.1-2	Users should be able to evaluate the acceptability of the CBP's assessments, calculations, or recommendations and, if needed, override them.				
	4.5.5.2		Indicating the Status of Procedure Execution					

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.5.5.2-1	There should be an indication of whether or not a step was completed.				
		=>	4.5.5.2-2	Users should be alerted to incomplete procedure steps.				
		=>	4.5.5.2-3	The current procedure step(s) should be indicated.				
		=>	4.5.5.2-4	The pathway taken through procedures should be stored and made available to users.				
		=>	4.5.5.2-5	The user should be informed when multiple procedures or multiple procedure steps are to be followed concurrently. A list of all currently active procedures should be available.				
	4.5.5.3		Navigation					
		=>	4.5.5.3-1	Navigation support should allow users to freely and easily move between procedure steps, to other parts of the same procedure, and to other procedures.				
		=>	4.5.5.3-2	Users should be able to easily access cross-referenced information, notes, cautions, warnings, and reference material.				
		=>	4.5.5.3-3	Users should be able to easily access appropriate contingency actions.				
	4.5.5.4		Explanation and Help					
		=>	4.5.5.4-1	CBPs should have facilities to enable the user to determine how CBP functions are performed.				
		=>	4.5.5.4-2	Help for performing procedure specified activities should be provided.				
		=>	4.5.5.4-3	There should be a way for users to record their notes and comments in the CBP.				
4.5.6		CBP Functions						
	4.5.6.1		Sensing of Plant Conditions					

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.5.6.1-1	The CBP should automatically identify when the entry conditions for a procedure exist.				
		=>	4.5.6.1-2	The CBP should monitor conditions for transitioning or exiting from a procedure (or for jumping to different non-sequential steps within the procedure) and indicate when those conditions exist.				
		=>	4.5.6.1-3	The link from an existing procedure and the related entry to another procedure should be clearly displayed and saved.				
		=>	4.5.6.1-4	The CBP should continuously assess and present the status of higher-level safety goals, such as critical safety functions, and alert the user to any challenges.				
	4.5.6.2		Providing Relevant Parameter Values and Equipment Status					
		=>	4.5.6.2-1	The CBP should automatically provide accurate and valid information on the values of parameters and status of equipment, when they are available to the system.				
		=>	4.5.6.2-2	Parameters that are displayed or used by the CBP system should be updated with a frequency that is appropriate given the purpose for which they are used, but no more frequently than the response of the underlying sensor will support.				
		=>	4.5.6.2-3	If values required when using procedures (e.g., subcooling margin) are not available from the general plant information system, the CBP system should perform those calculations.				
		=>	4.5.6.2-4	Procedure guidance should be context sensitive where possible.				
		=>	4.5.6.2-5	The CBP should provide users with clear, timely prompts when users need to input information not available to the CBP.				
		=>	4.5.6.2-6	This CBP should clearly indicate the required immediate operator actions after a reactor trip.				
	4.5.6.3		Resolving Step Logic					
		=>	4.5.6.3-1	The CBP should evaluate the logic of each procedure step and provide the result to the user. The CBP should make available the inputs, logic, and results, along with any associated limitations or assumptions.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	4.5.6.3-2	The results of the step analysis should be coded to make it salient to users.				
		=>	4.5.6.3-3	Steps of continuous applicability, time-dependent steps, and process-dependent steps should be monitored by the CBP and the user should be alerted when conditions in those steps become effective.				
	4.5.6.4	Monitoring User Actions						
		=>	4.5.6.4-1	Users should be alerted when their inputs and actions are not consistent with CBP evaluations.				
4.5.7	Degraded Conditions and CBP Failure							
	=>	4.5.7-1	The CBP system should clearly indicate when data are degraded or unavailable.					
	=>	4.5.7-2	An alarm should be presented for loss of the CBP.					
	=>	4.5.7-3	A procedure should be available for managing operations with a degraded CBP.					
	=>	4.5.7-4	PBPs should be available for selected procedures in the event of complete CBP failure.					
	=>	4.5.7-5	Upon transfer to PBPs, a means should be provided to support the user’s determination of currently open procedures, location in the procedures, completed and not completed steps, and currently monitored steps.					

D.6 Computerized Operator Support Systems (COSS)

D.6.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.6.3		Deciding if COSS is Needed					
4.6.4		General Design Considerations					
	=>	4.6.4-1	Where practical, the COSS should be fully integrated with and consistent with the rest of the HSIs. The operator should be able to use the COSS as a natural element of the tasks being performed.				
	=>	4.6.4-2	The appearance and functionality of the COSS should follow the same design conventions as other HSI resources, e.g., use the same nomenclature, abbreviations, acronyms, symbology, iconic representations, and coding techniques as the general information display system.				
	=>	4.6.4-3	The COSS should be able to access needed plant information already available in other information and other HSI systems, thus minimizing the need for the operator to manually input information.				
	=>	4.6.4-4	If necessary, different user groups should have different access levels to COSS functions.				
4.6.5		Modes of Operation					
	=>	4.6.5-1	For COSSs capable of different modes of operations, the current mode should be clearly indicated.				
	=>	4.6.5-2	Mode switching should require an explicit command.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.6.5-3	The COSS should provide an overview of which data are included in each analysis mode.				
	=>	4.6.5-4	If the COSS performs any sort of filtering or selective use of data, the current filter that is active should be identified. It should also be possible for the operator to access the unfiltered data.				
4.6.6		User Control of Interaction					
	=>	4.6.6-1	If the COSS is designed to support problem solving, it should provide the capability to plan a strategy for addressing problems.				
	=>	4.6.6-2	When the COSS is capable of a range of problem solving strategies, it should be capable of accepting direction from the user regarding which strategy to employ.				
	=>	4.6.6-3	The COSS should automatically record all rules invoked during an analysis.				
	=>	4.6.6-4	Query and explanation facilities should be provided so that users can determine the basis of COSS analyses and recommendations. User should be able to recall each invoked rule and relate it with a specific event (i.e., question or conclusion) to explain the rationale for the event.				
	=>	4.6.6-5	The system should permit rapid retrieval of previous exchanges between the user and the COSS.				
	=>	4.6.6-6	The user should be capable of requesting a hardcopy of data including screen displays (text and graphics), data employed during a consultation, summaries of consultations, lists of rules/facts invoked during a consultation, and summaries of hypotheses tested.				

D.7 Communication Systems

D.7.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.7.3	Main Aspects of Communication System Design							
	=>	4.7.3-1	Identify the implications to communications and communication systems as part of defining the endpoint vision and developing the migration strategy.					
	=>	4.7.3-2	Identify the changes that need to be made to the communication system due to modification impacts.					
	=>	4.7.3-3	Identify the changes to the communication system required by the new I&C and HSI systems. The functions and features of any aspects of the existing communication system that will be affected by the plant modifications should be identified.					
	=>	4.7.3-4	Identify the changes desired to correct existing communication problems.					
4.7.4	Communication System Design							
	4.7.4.1	General Considerations						
		=>	4.7.4.1-1	Location of workstations should facilitate communication and interaction among operators.				
		=>	4.7.4.1-2	HSIs should provide information quickly and comprehensively to facilitate communication among operators without creating additional workload burden.				
		=>	4.7.4.1-3	Communication among personnel should remain effective under any foreseeable operational conditions and at any stage of the upgrade.				
		=>	4.7.4.1-4	Changes in task allocation and workload should not adversely affect the way people communicate.				
		=>	4.7.4.1-5	Training on communication system should be performed to ensure adequate use.				
		=>	4.7.4.1-6	Evaluation of communications and identification of any problem areas should be part of in-service monitoring.				
	4.7.4.2	Speech-Based Communication						
		=>	4.7.4.2-1	Communication devices (e.g. telephones, radios, etc.) should be reliable and reasonably located within the workplace for ease of operators use.				

			Guidelines	Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.7.4.2-2	Visual aids (e.g. overview displays) may be used to reinforce communication among operators or to call attention to various operational conditions, such as abnormal conditions.				
	=>	4.7.4.2-3	Auxiliary, backup and/or emergency communication devices should be available at local control stations, especially where communications are critical.				
	=>	4.7.4.2-4	If the communication system requires entry of device addresses or numbers, these should be posted in open view close to the communication devices (e.g., telephones).				
	=>	4.7.4.2-5	When telephone systems are used as part of the announcing system (e.g. loudspeakers), the systems should be provided with multiple channels.				
	=>	4.7.4.2-6	Communication devices (e.g. intercoms) should be easily accessible to personnel at local control stations.				
	=>	4.7.4.2-7	Communication devices should have special administrative controls that regulate their use.				
	=>	4.7.4.2-8	The communication media should remain effective under any foreseeable conditions.				
	=>	4.7.4.2-9	In areas with high noise levels, visual annunciation (e.g. indicators) may be installed to emphasize alert conditions and/or receiving information through the communication device.				
	=>	4.7.4.2-10	The communication system in local control stations should be subjected to periodic surveillance.				
4.7.4.3		Computer-Based Communication					
	=>	4.7.4.3-1	Procedures for preparing, sending, and receiving messages should be designed and incorporated as part of the operating philosophy so consistency is promoted when handling information and critical tasks requiring communication between personnel.				
	=>	4.7.4.3-2	Both sending and receiving messages should be accomplished by an unambiguous user action.				
	=>	4.7.4.3-3	Personnel should have full control of what, when, and where the data are transmitted.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.7.4.3-4	Personnel should be able to interrupt message preparation, review, or disposition. Resumption should be from the point of interruption.				
	=>	4.7.4.3-5	When important or critical data is transmitted, the message should be annotated with any alarm or alert conditions, priority indicators, and other significant information that exists.				
	=>	4.7.4.3-6	The computer-based communication system should be independent and part of a secure network and therefore, should have filter capabilities to block messages, such as commercial advertising, deceptive, quasi-legal services, and partly or entirely fraudulent messages.				
	=>	4.7.4.3-7	Notification of new messages can be enhanced by sound annunciation.				
	=>	4.7.4.3-8	The arrival of a message in a format incompatible with that of the system receiving the message should not result in the loss of the message or of any ongoing operation.				
	=>	4.7.4.3-9	Computer-based communication systems in local control stations should be capable of exchanging the information with other locations including the Main Control Room.				
	=>	4.7.4.3-10	The throughput time of communication data should be adequate for the message being sent or received.				
	=>	4.7.4.3-11	If possible, adequate indications should be provided at the local control station to show the communication network status.				
4.7.5	Control Room Design and Communication System						
	=>	4.7.5-1	Enhance communication in the control room by identifying the different ways that the operators interact with each other and by incorporating the solutions that meet the operator needs at the design level.				
	=>	4.7.5-2	The types and locations of communication devices, such as telephones and radios, should not interfere or disturb other operators.				
	=>	4.7.5-3	Communication between the members of operational teams should be considered when modifying the control room so that communication among the team members and other personnel is enhanced.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	4.7.5-4	The location of the supervisor's workstation should be chosen considering the communication and observation needs between him/her and other personnel.				
	=>	4.7.5-5	Provide means to improve inter-shift communication without disrupting operations.				
	=>	4.7.5-6	The communication capabilities should be usable in the expected acoustical environment.				
	=>	4.7.5-7	Non-operating personnel in the control room should not be a source of distraction for control operators.				

D.8 Workstations and Workplaces

D.8.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
4.8.3		Overview					
	=>	4.8.3-1	W&W implications of the endpoint vision should be identified.				
	=>	4.8.3-2	W&W changes necessitated by any new systems or equipment that will be added to the plant should be identified.				

Guidelines					**Complies**	**Does not Comply, but with Justification**	**Does not Comply, but without Justification**	**Not Applicable**
	=>	4.8.3-3	Control room improvements based on operating experience should be identified.					
	=>	4.8.3-4	The functions and features of any aspects of the existing workplaces that will be affected by the plant modifications should be identified.					
4.8.4		Workstation Design						
	4.8.4.1		Configuration					
		=>	4.8.4.1-1	In choosing the workstation modifications or additional workstations to be introduced into the control room, consider the tasks to be carried out and the users' needs to access other control room resources or interfaces while performing the tasks.				
		=>	4.8.4.1-2	The number and kind of display devices (i.e., amount of display area) provided at a workstation should reflect a comprehensive consideration of what information is needed, where it is available, how it is organized, and what must be done to obtain it.				
		=>	4.8.4.1-3	The number and location of display devices should take into account the need for coordination of activities across crewmembers.				
		=>	4.8.4.1-4	For seated workstations, rolling chairs should be considered for flexibility and comfort.				
		=>	4.8.4.1-5	Workstation designs should be flexible, so that they can accommodate infrequent or unusual user activity, or simply provide an opportunity for users to alleviate fatigue.				
		=>	4.8.4.1-6	When conventional instrumentation is physically replaced in an existing console or panel by computer-driven equipment, it should be verified that the new equipment is visible and readable from the work positions.				
		=>	4.8.4.1-7	Changes to workstations or interfaces should not force users to have to unlearn existing skills.				
		=>	4.8.4.1-8	Changes to the workstations or interfaces should be conspicuous.				
		=>	4.8.4.1-9	Non-functional interfaces in the control room should be eliminated or minimized.				

Guidelines			Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	4.8.4.2	Control and Display Device Layout				
	4.8.4.3	Labeling and Demarcations				
	4.8.5	Workplace Design				
	4.8.5.1	Control Room Layout and Configuration				
=>	4.8.5.1-1	Workplace elements, such as panels, workstations, large displays, etc., should be laid out to support smooth movement of people to and from their work areas and allow easy access to needed interfaces and support equipment with minimal disruption of others.				
=>	4.8.5.1-2	Workplace components that must be viewed from a primary work location should be located to provide the required visibility.				
=>	4.8.5.1-3	Workstations should be located so that crewmembers can easily communicate and observe each other's actions.				
=>	4.8.5.1-4	The workplace should be large enough to allow the operating crew to interact with others (auxiliary personnel, crews coming on shift) comfortably without crowding or interference.				
=>	4.8.5.1-5	When workstations are added to the workplace, they should be located so that personnel at those stations (and at other stations) remain able to see displays elsewhere in the room, and their presence doesn't interfere with operations (e.g., operator movements from one station to another).				
	4.8.5.2	Control Room Environment				
	4.8.5.2.1	Illumination				
=>	4.8.5.2.1-1	Illumination should be suitable for the tasks performed at all work locations.				
=>	4.8.5.2.1-2	To meet varying lighting requirements, adjustable task lighting should be considered.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.8.5.2.1-3	Workstation VDUs should be positioned to minimize variations in brightness in the user's field of view.				
			=>	4.8.5.2.1-4	Workstation VDUs should be positioned to minimize glare on the display surfaces.				
			=>	4.8.5.2.1-5	VDUs, workstation surfaces, and lighting fixtures should be designed to minimize reflections and glare.				
		4.8.5.2.2		Sound					
			=>	4.8.5.2.2-1	Equipment or cabinets that make noise (e.g., those containing ventilating fans) should be located away from operators whenever possible.				
			=>	4.8.5.2.2-2	Sounds produced by computerized interfaces introduced into the control room should not interfere with existing control room audio codes, especially those that signal important information.				
			=>	4.8.5.2.2-3	Audio signals associated with different computer-driven HSIs in the control room should not interfere with each other.				
			=>	4.8.5.2.2-4	If operators use similar interfaces in proximity to one another (e.g., operators at a bench consisting of a row of displays and pointing devices), measures should be taken to prevent an operator at one workstation from mistakenly attending to auditory feedback from neighboring workstations.				
			=>	4.8.5.2.2-5	Sound levels at the workstation should be such that the workstation operators may still hear any workplace alarms or announcements and so that general conversation and communication between operators or between any personnel in the workroom is convenient.				
			=>	4.8.5.2.2-6	After modifications are implemented, the workplace should still conform to human factors guidance on the effectiveness of auditory signals (alarms in particular) and the intelligibility of speech.				
		4.8.5.2.3		Temperature					
			=>	4.8.5.2.3-1	Verify either by analyses or testing or both that the control room HVAC system can keep the area within the established comfort limits.				

Guidelines						Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
			=>	4.8.5.2.3-2	Ensure that the airflow produced by the equipment itself or that is required to keep it within temperature limits does not result in areas in the control room where air velocity is too high.				
	4.8.5.3		Local Control Stations						
4.8.6		Managing the Impact of Modifications							
	=>	4.8.6-1		For each stage of the migration, possible changes to the workplaces and workstations should be considered that are ancillary to the planned modifications of the interface per se.					
	=>	4.8.6-2		Activities associated with the implementation of modifications should not result in obstruction of users' view of or physical access to controls and displays.					
	=>	4.8.6-3		Implementation activities should be planned so that the ability of operating personnel to access needed HSIs and support material in the control room is not restricted.					
	=>	4.8.6-4		Errors or misinterpretations as a result of a phased introduction of digital upgrades should be minimized.					
	=>	4.8.6-5		Measures should be taken to minimize the distraction or interference associated with the activities of personnel involved in implementing modifications.					
	=>	4.8.6-6		Provisions should be made so that workplace hazards are not created during any work in the control room.					

D.9 Human Factors Engineering for the Maintenance of Digital Systems

D.9.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
6.1.3	General Design for Maintainability							
	6.1.3.1	Maintenance-Related Tasks						
		=>	6.1.3.1-1	Human factors analyses that are used to support the design of the human-system interface used for the upgraded system should include maintenance-related tasks as well as tasks needed to operate the modified systems.				
	6.1.3.2	Redundant Components and Hot Spares						
		=>	6.1.3.2-1	For redundant components in hot standby configurations, there should be unambiguous indication of which component is operating and which is in standby.				
		=>	6.1.3.2-2	Testing of redundant equipment should include testing to confirm all potential fail-over and recovery situations.				
		=>	6.1.3.2-3	Alarms should be provided for any processor failure, prioritized based on consistent criteria, and clearly presented to the operators or maintenance technicians who have to take action.				
		=>	6.1.3.2-4	Where modules are installed in the system as “hot spares,” the maintenance procedures and labeling should distinguish the installed hot spares from the primary operating modules.				
6.1.4	Detailed Design Features for Maintainability							
	=>	6.1.4-1		The system, module or equipment should provide indication to technicians and operators that modules have been inserted into the correct slot or rack location.				
	=>	6.1.4-2		Modules should not normally have configuration jumpers, switch settings or uniquely embedded software that must be configured prior to putting that module into operation. Where that cannot be avoided, the operating system software should confirm that these settings are correct.				
	=>	6.1.4-3		Different interfaces (e.g. connectors, fittings, etc.) should be provided for each type of test or service equipment to minimize the likelihood of error.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	6.1.4-4	The I/O module terminations should accommodate the testing tasks, and the field connections should not introduce unreliability or trouble shooting complexity.				
	=>	6.1.4-5	Blown fuses, or open circuits of any kind, should be automatically detected and reported by the system diagnostics. The system's HSI should direct maintenance personnel to the specific point affected.				
	=>	6.1.4-6	All modules should have readily observable indications to show that the module is operational.				
	=>	6.1.4-7	For I/O modules, front panel indicators should distinguish unused points. They should not be displayed with a particular status or error state. Where this is not possible, other labeling means should be used to clearly indicate that these points are not in use.				
	=>	6.1.4-8	When output modules are configured to go to a predetermined state or to freeze as-is on failures of the controlling CPU or failure of the communication to the controlling CPU, appropriate information on failure state should be displayed to maintainers and operators in addition to information that there has been a failure.				
	=>	6.1.4-9	All modules should have labels that are keyed to system documentation.				
	=>	6.1.4-10	Module labels or cabinet maps should be such that they can be correctly updated as an integral part of any system design change.				
	=>	6.1.4-11	If geographically distributed components are used, the digital platform and system should provide communication and operation diagnostics, automatic fault detection, isolation capability, and appropriate indication to maintenance technicians and operators. The system's centrally located HSI should clearly diagnose failures to the replaceable module level.				
	=>	6.1.4-12	Displays should be configured to show system errors in graphic format. The self-diagnostic features of the platform should isolate a problem down to the component level (e.g. specific module I/O point).				
	=>	6.1.4-13	Local controls should be provided to permit component maintenance operations without the coordination between remote and local personnel.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	6.1.4-14	Local controls should include switches to disconnect all remote control actuation symbols. Adequate indications of alarms should be provided in the main control room to ensure operators are aware that they have lost control of that component.					
	=>	6.1.4-15	If remote switches are located in the main control room, additional isolation and transfer/disconnect capability for these control interfaces should be provided.					
	=>	6.1.4-16	Failed sensors in safety monitoring systems should be alarmed and logged and the out-of-service times monitored for technical specification compliance.					
	=>	6.1.4-17	Protection system bypasses should have controls to ensure they are not implemented in a way that can totally bypass all trip and actuation functionality.					
	=>	6.1.4-18	Administrative controls and security access restrictions such as passwords or key locks should be built into the system to control the use of bypasses.					
	=>	6.1.4-19	Bypasses should be clearly indicated and alarmed.					
	=>	6.1.4-20	Where plants are vulnerable to spurious trips and actuations until a bypass is manually activated, the HSI associated with activating and displaying bypasses should be easily and quickly accessible by plant operators.					
	=>	6.1.4-21	If a value is substituted in a calculation, then the calculated result should have a clearly distinguishable quality flag. Such a substitution should be treated as a bypass and the previous guidelines should be applied.					
6.1.5	Diagnosis and Testing							
	6.1.5.1	Self-Diagnosis						
		=>	6.1.5.1-1	Malfunction messages should be displayed at the HSIs and archived.				
	6.1.5.2	Error Detection and Indication						
		=>	6.1.5.2-1	The digital platform should provide the capability to automatically detect and indicate the following out-of-service conditions. However, since the functional impairment is different for each of these conditions, distinct indication should be provided.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	6.1.5.2-2	For important control or protection applications, out-of-range detection should be provided.				
		=>	6.1.5.2-3	In digital platforms, CPU and communication should incorporate error detection methods at power up and at the request of the operator.				
		=>	6.1.5.2-4	Where communication redundancy is employed, the method and coverage of automatic error detection and self-testing of these peripheral devices should be carefully reviewed; manual testing is sometimes required.				
		=>	6.1.5.2-5	The determination of the significance of errors and how they are alarmed or presented should be consistent across the various digital platforms.				
		=>	6.1.5.2-6	In redundant systems, sustained faults should be alarmed. Operators should be able to acknowledge the alarm, but the alarm should remain activated until the system becomes operable again.				
		=>	6.1.5.2-7	If the plant general alarm system employs multiple levels of alarm prioritization, the process effect of each error should be consistent with the plant's general alarm prioritization criteria.				
		=>	6.1.5.2-8	Out-of-service indications should be provided at the normal control location as an integral part of the component status display in all formats for which that status is displayed.				
		=>	6.1.5.2-9	Out-of-service conditions should be alarmed at the normal control location to ensure operators are aware of the abnormal event and the conditions should be logged in the plants historical recording system.				
		=>	6.1.5.2-10	The capability to manually identify an out-of-service condition for any plant component should be provided.				
		=>	6.1.5.2-11	The capability for operators and maintenance personnel to manually enter notes regarding the out-of-service conditions should be provided.				
		=>	6.1.5.2-12	In addition to the out-of-service condition, component position status should always be displayed.				
		=>	6.1.5.2-13	The human system interfaces should not combine detailed information needed by diagnostic technicians into the same set of displays as are used by the end-users.				

Guidelines					Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
		=>	6.1.5.2-14	Replacement modules should require a minimum of special handling precautions.				
		=>	6.1.5.2-15	Replacing equipment should not create a hazardous condition for technicians or equipment.				
	6.1.5.3		Application Level Testing					
		=>	6.1.5.3-1	Where customized application level testing is required, test features should be built into the system so that all tests can be conducted without the addition of temporary modifications, such as shorting contacts or opening circuit loops.				
		=>	6.1.5.3-2	Procedures and interlocks should be provided to ensure the system is in an acceptable bypassed mode before allowing manual tests to be initiated. Operations personnel should be provided with indications that the bypasses have been instituted.				
		=>	6.1.5.3-3	Tests of output devices should normally be manually initiated. The HSI should be specifically designed for the testing to be conducted and should not contain other unrelated information that can cause confusion and errors.				
		=>	6.1.5.3-4	For output interface tests, adequate indication and interlocks to avoid spurious plant disturbances should be provided.				
		=>	6.1.5.3-5	Digital platforms should provide the capability of taking inputs and outputs out-of-scan, and the ability to manually insert values for testing. When points are out-of-scan there must be clear indication that a value has been manually inserted.				
		=>	6.1.5.3-6	To ensure points are not unintentionally left in an out-of-scan condition summary displays should provide a listing of all points utilizing substituted values. If a value is manually substituted for a true process input, then calculated results should have a clearly distinguishable quality flag.				
		=>	6.1.5.3-7	System security features, such as passwords or keylocks, should ensure forced value functionality, e.g., taking a point out-of-scan, is only available to authorized users.				
6.1.6		Maintenance Performance						

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
6.1.6.1		Maintenance Tools					
	=>	6.1.6.1-1	Digital platform maintenance tools should be available only at designated workstations.				
	=>	6.1.6.1-2	Digital platform maintenance tools should allow plant personnel to monitor system performance and maintain the system software without software programming expertise.				
	=>	6.1.6.1-3	System security features, such as passwords, should ensure that maintenance tools are only available to authorized users.				
	=>	6.1.6.1-4	The user should be able to specify the extent of testing to be performed (i.e., all or any combination of the included tests) and the number of times the test(s) should be repeated.				
	=>	6.1.6.1-5	Both the status and result of off-line diagnostics test should be indicated at the maintenance workstation and, if requested by the user, to a printer or file.				
6.1.6.2		Security					
	=>	6.1.6.2-1	Any user action which might result in permanent changes to existing data or yield significant consequences to the computer or controlled system should be executed only after explicit user confirmation. The confirmation should not be a component of a routine command sequence and should present a sufficient safeguard against inadvertent actions.				
6.1.6.3		Maintenance Personnel Responsibility					
	=>	6.1.6.3-1	The existing practices for repair and troubleshooting and the existing assignments and responsibilities of personnel for maintenance-related tasks should be re-evaluated for the modified digital equipment.				
6.1.7	Maintainability in Procurement and Plant Changes						
=>	6.1.7-1	Specifications and other procurement documents should include or specifically cite maintainability-related human engineering requirements of the modification.					

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	6.1.7-2	Where a maintenance human-system interface will be provided by a vendor as part of an entire component package, human factors requirements should be included in the procurement specification or these interfaces should be required to be completely described by the vendor’s proposal.				
	=>	6.1.7-3	The planning for the modification should explicitly identify and include the completion of the maintenance-related tasks needed to close the related change package.				
	=>	6.1.7-4	Where maintenance tasks are implicitly or explicitly considered in a risk assessment, changes in the maintenance involved should have a human factors evaluation and this should be reflected in the change package.				
	=>	6.1.7-5	Instructions for preventive maintenance, testing and trouble-shooting tasks should be provided by the suppliers. The procedures should cover each step in sequence with an explanation of how each step is performed, which parameters can be adjusted, and the effects obtained by varying each parameter.				

D.10 Human Factors Engineering for Configuration Management

D.10.1 Display Guidelines Checklist

This checklist summarizes the detailed guidelines contained in the remaining display sections. For additional information, please consult the sections and guidelines referenced.

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
6.2.3		General Configuration Control Guidance					
	=>	6.2.3-1	Where operation or servicing of the digital upgrade modification results in human tasks that require information from the configuration management system and similar data sources, those tasks should be identified in the design process and appropriate human factors review provided.				
	=>	6.2.3-2	Where human tasks involve consulting configuration information, some way to confirm expeditiously that the version of the requested information is up-to-date should be provided.				
6.2.4		Configuration Change Control Guidance					
	=>	6.2.4-1	If the human-system interfaces involved in the upgrade modification provide means by which information in the configuration management or similar data bases can be directly changed, control methods comparable to that for other similar configuration information should be provided.				
	=>	6.2.4-2	Procedures should be established that ensure that human factors engineering review of HSI and plant configuration changes that affect the tasks performed at the modified human-system interfaces is done when necessary.				
	=>	6.2.4-3	Where the human tasks require operators or technicians to access configuration information, practical methods for temporary changes and corrections should be provided.				
	=>	6.2.4-4	Generating a temporary change or correction and incorporating it in the currently used information should comply with existing administrative procedures. Where the technology has changed how this is accomplished, the intent of the previously used controls should be maintained.				
	=>	6.2.4-5	The human system interfaces in the digital upgrade modification should incorporate limitations on making temporary changes or corrections equivalent to those required by plant administrative change control procedures.				
	=>	6.2.4-6	A temporary change or correction to an item of configuration information should be available to all users of the information.				

Guidelines				Complies	Does not Comply, but with Justification	Does not Comply, but without Justification	Not Applicable
	=>	6.2.4-7	Means should be provided to identify all outstanding temporary changes or corrections. Temporary changes should have a limited life. A temporary change or correction should not be allowed to become a de facto permanent feature of the HSI.				
6.2.5		Control of User-Defined Interface Features					
	=>	6.2.5-1	Methods to provide for the management of user-defined features of the human-system interface that are provided as part of the upgrade modification should be established and the interface designed to support that management.				
	=>	6.2.5-2	Protocols should be established as to what will be done with special displays of information when shifts change or operators are relieved.				
	=>	6.2.5-3	Means should be provided so that supervisors can know what special displays are being used by the persons that they supervise. Furthermore, the supervisors should have easy access to the identical display.				
	=>	6.2.5-4	Methods should be provided to monitor and record the use of special displays. These records should provide information on who created the special display and when it was in use. The records should also provide the ability to reconstruct the display itself. (Additional guidelines related to the use of these records are provided below.)				
	=>	6.2.5-5	The records should be configured so that they could be used as indications of the need for changes in the plant or the human-system interface.				
	=>	6.2.5-6	Enough information should be recorded so that all special displays that were used by the operators in the course of an event can be reconstructed and properly placed in time.				
	=>	6.2.5-7	Information should be recorded in a form that training personnel can evaluate the displays that were used for possible incorporation in the standard training program.				