**OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
ANALYSIS/MODEL COVER SHEET**

1. QA: QA

Page: 1 of: 55

Complete Only Applicable Items

2. ☒ Analysis ☒ Engineering
☐ Performance Assessment
☐ Scientific

3. ☐ Model ☐ Conceptual Model Documentation
☐ Model Documentation
☐ Model Validation Documentation

4. Title:

REVIEW OF NRC APPROVED DIGITAL CONTROL SYSTEMS ANALYSIS

5. Document Identifier (including Rev. No. and Change No., if applicable):

ANL-OMC-CS-000001 Rev. 00

6. Total Attachments

1

7: Attachment Numbers – No. of Pages in Each:

1 – 27

	Printed Name	Signature	Date
8. Originator	D. W. Markman	<i>D.W. Markman</i>	9/15/99
9. Checker	J. Pullen	<i>J. Pullen</i>	9/15/99
10. Lead/Supervisor	D. McAfee	<i>D. McAfee</i>	9/15/99
11. Responsible Manager	Daniel G. McKenzie III	<i>D.G. McKenzie III</i>	9/15/99

12. Remarks:

D.G. McKenzie III 9/17/99

1. Primary area of responsibility for the originators:

A. Dennis Markman- Coordinated overall preparation of analysis and was the primary author of Sections 6.7.4, 6.8, and 6.9. Revised all sections of analysis to upgrade to revision 1. *DWM* 9/17/99

B. Craig Randle- Primary author for Sections 6.7.5, 6.7.6, 6.7.7.

**OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
ANALYSIS/MODEL REVISION RECORD**

Page: 2 of: 55

Complete Only Applicable Items

2. Analysis or Model Title:

REVIEW OF NRC APPROVED DIGITAL CONTROL SYSTEMS ANALYSIS

3. Document Identifier (including Rev. No. and Change No., if applicable):

ANL-OMC-CS-000001 Rev. 00

4. Revision/Change No.

5. Description of Revision/Change

00

Initial Issue

This analysis supersedes analysis BC0000000-01717-0200-00018 Rev. 00. Change bars in right margin indicate revisions from BC0000000-01717-0200-00018 Rev. 00.

Includes additional case studies of digital control systems. Sections 6.7.4, 6.7.5, 6.7.6 6.8 and 6.9 have been added. Sections 2.0, 4.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.7.1, 6.7.2, 6.7.3, 7.0, 8.0, and 9.0 have been revised . Added additional references, design criteria, and discussion supporting use of and in developing design concepts related to digital control systems.

Analysis to conform to AP-3.10Q Rev.0 requirements.

TABLE OF CONTENTS

1.0	PURPOSE	8
2.0	QUALITY ASSURANCE	9
3.0	COMPUTER SOFTWARE AND MODEL USAGE	9
4.0	INPUTS	9
4.1	PARAMETERS	9
4.2	CRITERIA	10
4.3	CODES AND STANDARDS	10
4.3.1	Institute of Electrical and Electronics Engineers (IEEE)	10
4.3.2	Code of Federal Regulations (CFR)	11
4.3.3	Instrument Society of America	11
4.3.4	International Electrotechnical Commission	11
4.3.5	International Atomic Energy Agency	12
4.3.6	Regulatory Guidance	12
4.3.7	Branch Technical Positions	14
4.3.8	Certification Agencies	14
5.0	ASSUMPTIONS	14
6.0	ANALYSIS	15
6.1	INTRODUCTION	15
6.2	DEVELOPMENT OF NUCLEAR INDUSTRY APPLICATIONS	16
6.3	MGR DIGITAL CONTROLS	17
6.4	REGULATIONS AFFECTING DIGITAL CONTROLS	18
6.5	COMMERCIAL OFF-THE-SHELF APPLICATIONS	19
6.6	COMMON MODE FAILURE	20
6.7	EXAMPLES OF NUCLEAR INDUSTRY APPLICATION OF DIGITAL CONTROLS	21
6.7.1	Entergy Operations, Arkansas Nuclear One, Unit 2	22
6.7.1.1	Project Description	22
6.7.1.2	Instrumentation and Controls Employed	22
6.7.1.3	Instrumentation and Controls Application	22
6.7.2	Indiana/Michigan Power Co., Donald C. Cook Station, Units 1 and 2	23
6.7.2.1	Project Description	23
6.7.2.2	Associated Vendors and Participants	23
6.7.2.3	Instrumentation and Controls Employed	23
6.7.2.4	Instrumentation and Controls Application	24
6.7.2.5	U. S. Nuclear Regulatory Commission Involvement	25
6.7.3	Houston Lighting and Power Company, South Texas, Units 1 and 2	25
6.7.3.1	Project Description	25
6.7.3.2	Associated Vendors and Participants	26
6.7.3.3	Instrumentation and Controls Employed	28
6.7.3.4	Instrumentation and Controls Application	29

6.7.3.5	U. S. Nuclear Regulatory Commission Involvement.....	30
6.7.3.6	In Support of the Yucca Mountain Project	30
6.7.4	Northern States Power Co. Prairie Island Units Nos. 1 and 2	31
6.7.4.1	Prairie Island Diesel Generators Load Sequencers	31
6.7.4.1.1	Associated Vendors and Participants.....	32
6.7.4.1.2	Instrumentation and Controls Employed	32
6.7.4.1.3	Instrumentation and Controls Application.....	32
6.7.4.1.4	U. S. Nuclear Regulatory Commission Involvement.....	32
6.7.4.1.5	In Support of the Yucca Mountain Project	33
6.7.4.2	Prairie Island Emergency Response Computer System.....	34
6.7.4.2.1	Associated Vendors and Participants.....	34
6.7.4.2.2	Instrumentation and Controls Employed	34
6.7.4.2.3	Instrumentation and Controls Applications	35
6.7.4.2.4	In Support of the Yucca Mountain Project	35
6.7.5	Pacific Gas and Electric, Diablo Canyon, Units 1 and 2	36
6.7.5.1	Project Description.....	36
6.7.5.2	Associated Vendors and Participants.....	36
6.7.5.3	Instrumentation and Controls Employed	37
6.7.5.4	Instrumentation and Controls Application.....	37
6.7.5.5	In Support of the Yucca Mountain Project	38
6.7.6	Arizona Public Service Company, Palo Verde Nuclear Generating Station, Units 1, 2, and 3	39
6.7.6.1	Project Description.....	39
6.7.6.2	Associated Vendors and Participants.....	39
6.7.6.3	Instrumentation and Controls Employed	39
6.7.6.4	Instrumentation and Controls Applications	39
6.7.6.5	Support for the Yucca Mountain Project	40
6.7.7	Additional Information on Nuclear Power Plant Use of Digital Controls	40
6.7.7.1	Nuclear Power Plants With Digital Controls	40
6.7.7.2	Case-by-Case Licensing Process	41
6.7.7.3	The Four Party Report	43
6.8	DIGITAL CONTROLS IN SUPPORT OF THE LICENSE APPLICATION	44
7.0	CONCLUSIONS.....	45
7.1	SUMMARY.....	45
7.1.1	Recommendations for Overall Control Strategy.....	45
7.1.1.1	Minimize the Size and Complexity of Safety-Related Systems	46
7.1.1.2	Independence and Physical Separation of Systems Important to Safety	46
7.1.1.3	Design Diversity	46
7.1.1.4	Regulator Partnering	47
7.1.1.5	Additional I&C Design Guidance.....	47
7.1.1.6	Further Analysis of Key Documents Needed	48
7.1.2	Recommendations for Design Criteria.....	49

7.1.2.1	Recommended list of Applicable Codes, Standards and Regulations	49
7.1.2.2	General Design Basis for Repository I&C Systems	50
8.0	REFERENCES	50
9.0	ATTACHMENTS	55

ACRONYMS AND ABBREVIATIONS

ANSI	American National Standards Institute
AMSAC	ATWS (Anticipated Transient Without Scram) Mitigating System Actuation Circuitry
ATWS	Anticipated Transient Without Scram
CDA	Controlled Design Assumptions Document
CFR	Code of Federal Regulations
COTS	Commercial Off-the-Shelf
CRWMS	Civilian Radioactive Waste Management System
DAFAS	Diverse Auxiliary Feedwater Actuation System
DP	Differential Pressure
ECCS	emergency core cooling systems
ERCS	Emergency Response Computer System
e.g.	<i>exempli gratia</i> (for example)
EEPROM	Electrically Erasable Programmable Read Only Memory
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
ERFDS	Emergency Response Facility Data System
ESFAS	engineered safety features actuation system
HFE	Human Factors Engineering
HICB	Instrumentation and Control System Branch
HMI	Human Machine Interface
hp	Horsepower
i.e.	<i>Id est</i> (that is)
in	Inch
I&C	Instrumentation and Controls
I/O	Input/Output
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISA	Instrument Society of America
kW	kilowatt
LADS	License Application Design Selection
LLNL	Lawrence Livermore National Laboratory
M&O	Management and Operating Contractor
MGDS	Mined Geologic Disposal System
MGR	Monitored Geological Repository
MWe	megawatt, electrical
MWt	megawatt, thermal
NFPA	National Fire Protection Association
NMSS	Office of Nuclear Materials Safety and Safeguards
NRC	United States Nuclear Regulatory Commission

NRR	Office of Nuclear Reactor Regulation
NSSS	nuclear steam supply system
PDR	Public Document Room
PLC	programmable logic controller
PPS	Plant Protection System
PROM	programmable read only memory
PWR	pressurized water reactor
RAM	random access memory
RFI	Radio Frequency Interference
RPS	reactor protection system
RTS	reactor trip system
RVLIS	Reactor Vessel Level Instrumentation System
SAR	Safety Analysis Report
SAS	safety assessment system
SDD	System Description Document
SEA	Science and Engineering Associates, Inc.
SER	Safety Evaluation Report
SPDS	safety parameter display system
TMI	Three Mile Island
UL	Underwriters' Laboratory, Inc.
VA	Viability Assessment
V&V	Validation and Verification
W	Watt
YMP	Yucca Mountain Project

1.0 PURPOSE

Preliminary design concepts for the proposed Subsurface Repository at Yucca Mountain indicate extensive reliance on modern, computer-based, digital control technologies. The purpose of this analysis is to investigate the degree to which the U. S. Nuclear Regulatory Commission (NRC) has accepted and approved the use of digital control technology for safety-related applications within the nuclear power industry.

This analysis reviews cases of existing digitally-based control systems that have been approved by the NRC. These cases can serve as precedence for using similar types of digitally-based control technologies within the Subsurface Repository. While it is anticipated that the Yucca Mountain Project (YMP) will not contain control systems as complex as those required for a nuclear power plant, the review of these existing NRC approved applications will provide the YMP with valuable insight into the NRC's review process and design expectations for safety-related digital control systems. According to the YMP Compliance Program Guidance, portions of various NUREGS, Regulatory Guidelines, and nuclear IEEE standards the nuclear power plant safety related concept would be applied to some of the designs on a case-by-case basis.

This analysis will consider key design methods, capabilities, successes, and important limitations or problems of selected control systems that have been approved for use in the Nuclear Power industry.

An additional purpose of this analysis is to provide background information in support of further development of design criteria for the YMP.

The scope and primary objectives of this analysis are to:

- Identify and research the extent and precedence of digital control and remotely operated systems approved by the NRC for the nuclear power industry. Help provide a basis for using and relying on digital technologies for nuclear related safety critical applications.
- Identify the basic control architecture and methods of key digital control systems approved for use in the nuclear power industry by the NRC.
- Identify and discuss key design issues, features, benefits, and limitations of these NRC approved digital control systems that can be applied as design guidance and correlated to the Monitored Geologic Repository (MGR) design requirements.
- Identify codes and standards used in the design of these NRC approved digital control systems and discuss their possible applicability to the design of a subsurface nuclear waste repository.
- Evaluate the NRC approved digital control system's safety, reliability and maintainability features and issues. Apply these to MGR design methodologies and requirements.

- Provide recommendations for use in developing design criteria in the System Description Documents for the digital control systems of the subsurface nuclear waste repository at Yucca Mountain.
- Develop recommendations for applying NRC approval methods for digital control systems for the subsurface nuclear waste repository at Yucca Mountain.

This analysis will focus on the development of the issues, criteria and methods used and required for identifying the appropriate requirements for digital based control systems. Attention will be placed on development of recommended design criteria for digital controls including interpretation of codes, standards and regulations. Attention will also focus on the use of digital controls and COTS (Commercial Off-the-Shelf) technology and equipment in selected NRC approved digital control systems, and as referenced in applicable codes, standards and regulations. The analysis will address design issues related to COTS technology and how they were dealt with in previous NRC approved digital control systems.

2.0 QUALITY ASSURANCE

Control systems, including the Subsurface Operations Monitoring and Control System and the Subsurface Safety & Monitoring System, may have digital based components. These systems have been classified in accordance with QAP-2-3, Classification of Permanent Items and found to be quality affecting (Reference 8.16, Attachment V, page 29). They are also on the Project Q-list (Reference 8.51, Attachment II, pages. 22-23). This design activity has been evaluated in accordance with QAP-2-0, Conduct of Activities. Activity title, *SS Transport & Emplacement-99 Work Package 12012383M1*, Task RPA20794 (Reference 8.8), has been determined to be quality affecting subject to the requirements of the Quality Assurance Requirements and Description (QARD) (Reference 8.2, Rev 8).

3.0 COMPUTER SOFTWARE AND MODEL USAGE

Not applicable.

4.0 INPUTS

The design criteria used in this analysis identifies information and precedence for the use of digital controls in the nuclear industry. Due to the informational nature of this analysis, only applicable system description document data were used as criteria.

4.1 PARAMETERS

Not applicable

4.2 CRITERIA

The following design criteria are obtained from the Subsurface Operations Monitoring and Control System Description Document (Reference 8.37), the Subsurface Safety and Monitoring System Description Document (Reference 8.50), and the Performance Confirmation Data Acquisition/Monitoring System Description Document (TBV-407)(Reference 8.62). The specific criteria listed are normally and technically supported by the use of digital microprocessor based components and control systems.

- 4.2.1** The system shall provide real-time monitoring of all remote control transport and waste emplacement operations. (Reference 8.37 Section 1.2.1.9). (Used in Section 6.7.3.6 & 6.7.5.5).
- 4.2.2** The system shall be designed such that a single failure of the redundant communications between the master control unit and the remote terminal unit (RTU) will not affect monitoring and remote control transport and waste emplacement operations. (Reference 8.37 Section 1.2.1.16). (Used in Section 6.7.4.2.4).
- 4.2.3** The system shall provide the operator with software features to configure the new data displays, re-configure existing displays, and to accommodate future operational requirements the features as a minimum: a. Bar charts, b. Graphical trend representation, c. Alarm limits, and d. Status changes. (Reference 8.37 Section 1.2.1.29). (Used in Sections 6.7.4.2.4 & 6.7.5.5).
- 4.2.4** Communication and data circuits shall be protected or shielded from electromagnetic interference to the extent specified by manufacturers of sensitive data processing, monitoring, and communications equipment used in the system. (TBV-407)(Reference 8.62 Section 1.2.1.387). (Used in Sections 6.7.3.6 & 6.7.4.1.5)
- 4.2.5** The system shall interface with the Site Communication System for voice, data, and video communications related to the subsurface operational functions listed below, as a minimum: a. Alarm annunciation, b. Radiation monitoring, c. Fire monitoring, d. Ground control monitoring, e. Air quality monitoring. (Reference 8.50 Section 1.2.4.4). (Used in Section 6.7.6.5)

4.3 CODES AND STANDARDS

4.3.1 Institute of Electrical and Electronics Engineers (IEEE)

IEEE Std 7-4.3.2 *Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations.* 1993

IEEE Std 279 *Criteria for Protection Systems for Nuclear Power Generating Stations.* 1971

IEEE Std 323	<i>Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.</i> 1983.
IEEE Std 344	<i>Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.</i> August 3, 1987.
IEEE Std C62.41	<i>Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits.</i> 1991.
IEEE Std 1012	Standard for Software Verification and Validation Plans. 1998.
IEEE Std 603	<i>Standard Criteria for Safety Systems for Nuclear Power Generating Stations.</i> 1991

4.3.2 Code of Federal Regulations (CFR)

64 FR 8640	Federal Register. Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Proposed Rule 10 CFR 63. 1999.
10 CFR 60	Energy, Part 60, Disposal of High-Level Radioactive Waste in Geologic Repositories.1998.
10 CFR 50	Energy, Part 50, Domestic Licensing of Production and Utilization Facilities.1998.
10 CFR 50.59	Energy, Part 50, Evaluation Process. 1998.
10 CFR 21	Energy, Part 21, Reporting of Defects and Noncompliance.1998.

4.3.3 Instrument Society of America

ISA S84.01	Functional Safety for Process Systems. 1995
------------	---

4.3.4 International Electrotechnical Commission

IEC 61508	Functional Safety: Safety-Related Systems-Parts 1-7. (Draft). February. 1996. (previously numbered IEC 1508)
IEC 61226	Categorization of Systems Important to Safety. 1993. (previously numbered IEC 1226)
IEC 61131-3	International Standard for Programmable Controllers-Part 3: Programming Languages. March 1993. (previously numbered IEC 1131-3)

4.3.5 International Atomic Energy Agency

IAEA 50-SG-D8 Safety Related Instrumentation and Control Systems for Nuclear Power Plants: A Safety Guide. 1984.

4.3.6 Regulatory Guidance

Refer to Attachments I for inclusion of some of these regulations in this analysis.

NUREG-0700	Human-System Interface Design Review Guideline, Rev. 1. 1996
NUREG-0800	Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, LWR (Light Water Reactor) Edition - Chapter 7, Instrumentation and Controls, Rev. 4. June 1997.
NUREG/CR-6101	Software Reliability and Safety in Nuclear Reactor Protection Systems. November 1993.
NUREG/CR-6463	Review Guidelines for Software Languages for Use in Nuclear Power Plant Safety Systems. October 1997.
NUREG/CR-6263	High Integrity Software for Use in Nuclear Power Plants, Candidate Guidelines, Technical Basis, and Research Needs. June 1995.
NUREG/CR-6294	Design Factors for Safety-Critical Software. December 1994.
NUREG-6278	Survey of Industry Methods for Producing Highly Reliable Software. November 1994.
NUREG/CR-6421	A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications. March 1996.
NUREG/CR-6090	The Programmable Logic Controller and Its Application in Nuclear Reactor Systems, Lawrence Livermore National Laboratory, September 1993. UCRL-ID-112900
NUREG/CR-6479	Technical Basis for Environmental Qualification of Microprocessor-Based Safety-Related Equipment in Nuclear Power Plants. January 1998.
NUREG/CR-6579	Digital I & C Systems in Nuclear Power Plants. Risk-Screening of Environmental Stressors and a Comparison of Hardware Unavailability With an Existing Analog System. January 1998.
NUREG/CR-1401	Estimators for the Binomial Failure Rate Common Cause Model. April 1980.

-
NUREG/CR-4780	Procedures for Treating Common Cause failures in Safety and Reliability Studies. January 1989.
NUREG/CR-5460	A Cause-Defense Approach to Understanding and Analysis of Common Cause Failures. March 1990.
NUREG/CR-5801	Defensive Strategies for Reducing Susceptibility to Common Cause Failures. April 1993.
Reg. Guide 1.53	Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems. June 1973.
Reg. Guide 1.152 Rev. 1	Criteria For Digital Computers in Safety Systems of Nuclear Power Plants. January 1996.
Reg. Guide 1.153 Rev. 1	Criteria for Power, Instrumentation, and Control Portions of Safety Systems. June 1996.
Reg. Guide 1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Formally Draft Reg. Guide DG-1058). September 1997.
Reg. Guide 1.168	Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Formally Draft Reg. Guide DG-1054). September 1997.
Reg. Guide 1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Formally Draft Reg. Guide DG-1056). September 1997.
Reg. Guide 1.171	Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants (Formally Draft Reg. Guide DG-1057). September 1997.
Reg. Guide 1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Formally Draft Reg. Guide DG-1059). September 1997.
Reg. Guide 1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Formally Draft Reg. Guide DG-1055). September 1997.
Reg. Guide 1.118 Rev.3	Periodic Testing of Electric Power and Protection Systems. April 1995.
Reg. Guide 1.22	Periodic Testing of Protection System Actuation Functions (Safety Guide 22). February 1972.

Reg. Guide 1.105 Rev.2 Instrument Setpoints for Safety-Related Systems. February 1986.
(Draft DG-1045, Proposed Revision 3, October 1996).

Reg. Guide 1.62 Manual Initiation of Protective Actions. October 1973.

Reg. Guide 1.75 Physical Independence of Electric Systems. September 1978.

4.3.7 Branch Technical Positions

HICB-10 Guidance on Application of Regulatory Guide 1.97. June 1997 Rev 4.

HICB-14 Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems. June 1997 Rev 4.

HICB-17 Guidance on Self-Test and Surveillance Test Provisions. June 1997 Rev 4.

HICB-18 Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems. June 1997 Rev 4.

HICB-19 Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems. June 1997 Rev 4.

HICB-21 Guidance on Digital Computer Real-Time Performance. June 1997 Rev 4.

4.3.8 Certification Agencies

UL Underwriters' Laboratory, Inc. (UL). Qualification of Computer Based Components. 1998

5.0 ASSUMPTIONS

Not used.

6.0 ANALYSIS

6.1 INTRODUCTION

Safety-related control systems found in most operating nuclear power plants within the United States are based on fairly old and increasingly obsolete analog control technologies. In contrast, the preliminary design concepts for the proposed subsurface repository at Yucca Mountain rely extensively on the use of modern, computer-based, digital control technologies.

While it is not anticipated that any of the control systems being developed for the subsurface repository will need to be as sophisticated as those used at a nuclear power plant, it is important to note that digital control technologies currently have limited precedence within the NRC. Digital based controls have been installed in limited instances in several nuclear power plants since the early 1980's. Digital controls are used extensively in "balance of plant" applications at many nuclear power plants, but in only a few safety related applications. The NRC's regulatory and technical guidance in this area is rapidly developing and evolving. This analysis investigates the degree to which the NRC has approved the use of digitally-based control technologies for safety-related applications within the nuclear power industry.

As mentioned in the purpose section, a strict definition of the expression "NRC approval" with regards to digital control systems is still evolving and somewhat elusive as the NRC continues to formulate its approval processes. Background on the evolution of the case-by-case licensing process for upgrades of control systems is discussed in Section 6.8.2.

An example of this continuing evolution of NRC technical guidance can be seen in Revision 4 of NUREG-0800. NUREG-0800 is the Standard Review Plan (SRP) for the review of Safety Analysis Reports (SARs) for nuclear power plants. Of particular interest are the changes in Chapter 7 of this NUREG which discusses the review of instrumentation and control (I&C) systems for nuclear power plants.

Chapter 7 of NUREG-0800 Rev. 4 contains very significant and substantial changes from its predecessor. New sections have been added that discuss the review process for digital I&C systems, data communication systems, application of IEEE Standard 603, and use of diverse I&C technologies. These changes demonstrate the NRC's current awareness of the need to develop acceptance criteria and regulatory plans for the new digitally-based control technologies. The implications of NUREG-0800 are discussed further in later sections of this analysis.

Additional insight into the current level of acceptance and application of digital control technologies within the nuclear industry can be found by reviewing the National Research Council's recent report entitled: "*Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues*" (Reference 8.4). In analyzing what they termed technical and strategic "key issues," the Council interviewed personnel from the NRC and the nuclear power industry, as well as representatives from other safety-related non-nuclear

industries, such as aerospace, defense, and rail transit industries. The Council's "key issues" and recommendations to the NRC were centered around: (a) the systems aspects of digital instrumentation and control technology, (b) software quality assurance, common-mode software failure potential, (d) safety and reliability assessment methods, (e) human factors and human-machine interfaces, and (f) dedication of commercial off-the-shelf hardware and software. Several of these issues are discussed in more detail in later sections of this analysis.

Also particularly insightful is the NRC's reply to the 39 recommendations outlined in the National Research Council's report (Reference 8.46). In the reply document, the NRC emphasizes its current work and proactive policies to develop regulatory guidance for the application of digital I&C technologies within the commercial nuclear power industry. The new draft of NUREG-0800 Rev. 4 is cited as an example of the NRC's forthcoming technical guidance in this area.

6.2 DEVELOPMENT OF NUCLEAR INDUSTRY APPLICATIONS

Initially economically driven, non-nuclear industries have learned over a considerable period of time that digital application of a control system can provide higher degrees of repeatability, dependability, and event expectance than ever before attainable. It has, however, taken time to develop the standards and guidelines (see Section 4.3.6 for ones used in this analysis) necessary for the NRC to measure and judge the safety and reasonableness of digital systems as applied within the nuclear industry. NUREG-0800 Rev. 4 is a significant milestone in this development because it establishes the future basis against which all such systems are to be measured. Further, it gathers together by reference the documents that form its backbone and of which designers, implementers, and reviewers must be cognizant. (Reference 8.46)

One should never lose sight of the fact that utilities are not in business to provide electrical power gratis or at a loss; they still have to answer to their shareholders. It would be unreasonable to expect any operating utility to invest large sums of money and effort in any transition to newer systems unless those changes could be economically justified. It is clearly not in their best interests to merely promote advancing technology. It is true that many instrumentation and control systems at operating nuclear power plants are in the range of 20 to 40 years old. Refurbishing of existing analog instrumentation would in many instances be much easier and less troublesome to justify to the regulators if spare parts were available. However, modern technology, particularly digital systems, offer better performance, reliability, and accuracy. This, under normal circumstances, should translate to lower generation costs through increased power production, increased plant availability, fewer errors or mistakes and more efficient staffing.

Savings are achievable because of a combination of benefits derived directly from the implementation of digital controls. Not all utilities have the same set of experiences, but typical benefits include:

- Systems become more stable, reliable and cost efficient with the introduction of fault-tolerant controls.
- Digital systems enable self-diagnostics and replacement on-line, decreasing system maintenance.
- Adaptive tuning, drift-free operation, and nonlinear compensation provide improvement in overall control of the plant. Also, with the speed at which data is processed, near real-time control is enhanced.
- The burden of controls on the operator is reduced, as automated systems will take over many previously-manual functions. This feature also eliminates some of those errors caused by such things human panic, response time, skill level, and so on.
- System upgrades are more cost efficient, since some changes are made to the software instead of the hardware. This flexibility is especially attractive when considering the rapid advancement in technological capabilities.
- Automated processing of data with the requisite software frees the plant engineer from time consuming calculations and reduces the risk of misinterpretation.

6.3 MGR DIGITAL CONTROLS

Digital control systems are expected to have a critical role in the development of the Mined Geologic Repository (MGR), both in surface and subsurface operations. Current trends and activities in the NRC and its related support committees and councils (see Section 4.3.6, Reg. Guide 1.172) emphasize acceptable methods and procedures for development, verification, dedication and approval of the use of digital control systems. The Viability Assessment Report (Reference 8.5, pages 4-59 through 4-111) identifies many repository functions and systems that point to the extensive application of digital controls.

Preliminary repository design concepts show a combination of both manual control and remote control design strategies. Design concepts also indicate that a centralized control station or facility will be provided for monitoring and supervisory control of key safety-related repository functions and operations (Reference 8.5, pages, 4-98, 4-99, 4-106, 4-111).

In developing subsurface repository I&C design concepts, the following points were considered:

- Recent studies of enhanced design alternative concepts included criteria to cover personal access provisions for specific conditions that may arise where humans would need to have direct access to emplacement drifts containing Waste Packages. According to the concept, human access to emplacement drifts would be only for responding to operational off normal, upset and/or accident conditions. Some of these conditions include Waste Package handling, support and/or related problems, Waste Package Transporter malfunction, utility (rail, power, lighting) malfunction, minor ground support problems, and backfill and drip shield emplacement systems and equipment

problems (Reference 8.6, Attachment, entitled, Criteria and Guidance for Repository Enhanced Access Design). If such design concepts are pursued it would necessitate the development of several new and specialized types of machines. In fact, the humans access concept would rely heavily on the use of digital instrumentation and remotely operated devices to prepare emplacement drifts and make them suitable for human workers. Special features and controls are needed to provide a safe environment and protection for the human while inside the drift. Some of these controls would be greatly benefited by digital based systems.

- Rail transport will be used for subsurface transport of waste packages. It can be expected that digitally-based controlled interlocking systems will be used for transporting underground supplies and personnel in addition to waste packages (Reference 8.5, page 4-99).
- Waste packages will be placed center in-drift, on pedestals, using gantry emplacement. Being remote from operating personnel, the waste handling equipment and integrated systems will employ digitally-based systems for control and monitoring (Reference 8.5 pages 4-97, 4-100, 4-101, and 4-102). (Discussion of the use of programmable logic controllers and remote control on these pages indicate digital-based control systems).
- Adequate quantities of supply and exhaust air must be provided to and from underground working areas. Further, there will be interrelationships between a minimum of two separate yet mutually-interlocked development and emplacement side ventilation systems. (Reference 8.5, pages 4-84 and 4-96)
- Some of the control systems in the subsurface repository will be determined to be important to safety. These critical control systems must be identified by the Q-levels of the *Classification of the Preliminary MGDS Repository Design* document (Reference 8.16) (Reference is used as a general reference to systems that are being classified as safety-related).
- Other systems such as the performance confirmation monitoring, control and data acquisition system, an emplacement system data communications network, a remote inspection system, emplacement drift isolation doors, and the emplacement drift rail switches are all applications for digital based instrumentation and control systems (Reference 8.5, pages 4-108, 4-110).

6.4 REGULATIONS AFFECTING DIGITAL CONTROLS

The NRC has commissioned, reviewed and published a number of Nuclear Regulations (NUREGs) and Regulatory Guidelines which directly pertain to digital instrumentation and control systems. NRC staff members continue to be involved in nuclear industry working groups and technical committees. The NRC has commissioned the Lawrence Livermore National Laboratory (LLNL) to develop several of the guidelines and NUREGs presently in

use. NUREG-0800, *Standard Review Plan for Nuclear Power Plants, LWR (Light Water Reactor) Edition*, is the prime example of the NUREGs that address digital control. Chapter 7 of NUREG-0800 covers instrumentation and controls. Revision 4 contains the digital controls guidance. This guidance is currently being used in the nuclear industry for new digital control system designs that will require NRC approval. Rev. 4 4.3.6), "Instrumentation and Controls", Any discussion of digital control systems should address the criteria and guidelines of NUREG-0800 Rev. 4. 4.3.6).

In addition, any future designs of digital instrumentation and controls for the Yucca Mountain facilities may have to comply with many of the codes and standards. The Yucca Mountain project under its MGR Compliance Program provides a list of codes, standards, and guidance documents for certain systems and the rationale for applicability of their use on the project.

Although a proposed rule now, (64 FR 8640) 10CFR63, *Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada*, will need to be reviewed for site-specific design criteria and technical requirements when it is issued. This may likely impact the regulations and related guidance.

6.5 COMMERCIAL OFF-THE-SHELF APPLICATIONS

This analysis also indicates that the use of Commercial Off-the-Shelf (COTS) digital controls in nuclear industry applications has gained acceptance within the regulatory community; indeed, it has been reported that the NRC has displayed a strong willingness to deploy such systems because of their operating history (Reference 8.14). Some of this history comes from the military and space programs for example. The use of COTS equipment in nuclear power industry is however an issue that is drawing an increasing level of attention from the regulators and users as is evidenced by development of NUREG/CR-6421, which discusses COTS equipment, and in References 8.7, 8.13, and 8.14. It has been demonstrated that COTS can, in selected applications, be adapted within existing constraints without requiring special procedures or acceptance criteria.

Deployment of commercial off-the-shelf applications is expected to evolve as a more open architecture becomes available from distributors of industrial software-based control systems. This was recognized by the automotive industry, which is pursuing development of an open, modular architecture for controllers. The effort was initiated by General Motors but has found a broad acceptance among all facets of the automotive industry. While they acknowledge that their current use of proprietary technologies has proven to be reliable, the difficulties associated with them needed to be addressed. Many of these difficulties are directly applicable to the nuclear industry and include (a) no common interfaces, (b) higher integration costs, (c) higher costs of extension and enhancement, and (d) the requirement of specific training for operation and troubleshooting. Interestingly, many of these difficulties are similar in some respects to those addressed in European standards. For some time it has been recognized in Europe that, at least insofar as software important to safety is concerned, it is better to use an evolutionary rather than revolutionary approach (Reference 8.32). Their

aim is to produce safer software using current languages and hardware which are already known commodities.

6.6 COMMON MODE FAILURE

A recurring theme throughout the conduct of this study has been a consistently stated concern with common mode failure, and in particular as it applies to software. Common mode failure in software systems may be best defined as the failure of something which is common to more than one application and may cause a fault in more than one application.

This issue was raised repeatedly by operating utilities, regulators, and vendors. The most common reason cited for this concern was the modular development of software; one piece used several times for the same action, or used several times for different actions.

The worry with respect to one piece of software being used in more than one instance for the same action could reasonably be resolved with attention paid to diversity, or a "defense-in-depth" approach which would preclude such design (Reference 8.17). This can be further enhanced for applications where there is an even greater concern with a method of polling redundancy. This is a scheme whereby the same inputs are applied to effectively two different systems, whose outputs are then compared to each other for mutually agreeable, or polled, action.

Of greater concern is the situation where one block, or module, of software is utilized and integrated into the control logic associated with more than one action. In fact, each of the resultant actions could, and would likely, be widely dispersed throughout a facility or application. It has been suggested that some of the early problems encountered at Sizewell B in the United Kingdom were due in part to just such a situation. This is a pressurized water reactor plant in which the Plant Protection System (PPS) is almost wholly software-based, encompassing some 200,000 lines of code (Reference 8.33).

One question which appears to remain unanswered regarding large systems such as Sizewell B is how to adequately conduct and document the necessary software testing. A number of models, schemes, and processes have been advanced which could support validation and verification testing. Three examples are included as References 8.21, 8.25, and 8.27. Some of these methods were not necessarily intended for use in the nuclear industry, but have been suggested for such an application. Of particular interest is a graphical dependability analysis tool requiring less sophisticated data analysis, referred to as MEADEP (MEASURE DEPENDABILITY). The MEADEP technique is an "after-the-fact" look at failures and was applied to a portion of a software-based PPS (most likely Sizewell B) for which there was early field-generated failure data. It is worth noting that the NRCN has been involved and has been a contributor to the development of such analytical tools while encouraging the application of digital computers. Even though the NRC has an interest in data analysis such as the MEADEP technique (Reference 8.28, pages 1 and 4), it does not necessarily reflect the criteria, requirements, and guidelines of the NRC.

There are additional NUREGS that address the common cause or mode failure issue and how it should be considered and analyzed. These can offer additional guidance and information

for the reader and for use during detail design of possible digital based control systems. These documents include NUREG/CR-1401, Estimators for the Binomial Failure Rate Common Cause Model, NUREG/CR-4780, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR-5460, A Cause-Defense Approach to Understanding and Analysis of Common Cause Failures, and NUREG/CR-5801, Defensive Strategies for Reducing Susceptibility to Common Cause Failures. Any future analysis of digital based control system issues and considerations may prove to benefit from more detailed discussion of one or more of these NUREGS.

6.7 EXAMPLES OF NUCLEAR INDUSTRY APPLICATION OF DIGITAL CONTROLS

This analysis presents seven case studies of the application of digital control systems within the nuclear industry. The level and depth of specific analysis of each case varies with the available information, but each project case has undergone some level of NRC scrutiny and acceptance. It is understood that the integration of digital controls within the nuclear industry has been underway for several years. The eighth item is a listing of digital control usage and application of digital control systems within the nuclear industry.

Applications were selected for study and presentation to represent a history of this effort relative to systems important to safety. These included:

- 1) Entergy Operations, Arkansas Nuclear One, Unit 2
- 2) Indiana/Michigan Power Co., Donald C. Cook Station, Units 1 and 2
- 3) Houston Lighting and Power (HL&P) South Texas 1 & 2, with Triconex, and the use of an NRC approved PLC platform generic specification.
- 4) The Safety Evaluation Report (SER) and approval of a PLC at Northern States Power Company's Prairie Island Plant.
- 5) The Safety Analysis Report (SAR) review of Northern States Power Company's Prairie Island Plant, and the use of a Westinghouse PLC and microprocessor based instrumentation system
- 6) The Safety Analysis Report (SAR) review of a Westinghouse Eagle 21 system at Pacific Gas and Electric, Diablo Canyon Units 1 & 2.
- 7) The Safety Analysis Report (SAR) review of a PLC and fiber optic communication links at Arizona Public Service, Palo Verde Generating Station Units 1 & 2.
- 8) Additional sites with digital controls used in safety systems at Nuclear Power Plants are briefly listed.

6.7.1 Entergy Operations, Arkansas Nuclear One, Unit 2

6.7.1.1 Project Description

Unit 2 of the Arkansas Nuclear One Station saw initial commercial operation in March of 1980, and is the first application of a digital computer in concert with a Reactor Protection System (RPS). The unit is a Combustion Engineering PWR, 2-loop nuclear steam supply system (NSSS) located near Russellville, Arkansas. By license it is limited to 2815 MWt, but by design is capable of an ultimate output of 2910 MWt. It is significant for the purposes of this analysis to note that all postulated accidents are capable of increasing the output to 2900 MWt (References 8.35 and 8.36). This narrow margin on core operating limits is due, in part, to this first-use application of software-based digital initiating logic in a portion of the controls associated with the more traditional RPS.

6.7.1.2 Instrumentation and Controls Employed

The original digital hardware deployed was an InterData core-memory device. The application was initially developed on a Data General mini-computer at Combustion Engineering's headquarters in Windsor, Connecticut in the early 1970's. This initial attempt by the NSSS vendor followed, and was encouraged by, its successes in gaining acceptance from the regulators for its solid-state digital rod control systems and control element assembly (CEA) instrumentation systems. Ultimately, nearly identical systems to that for Arkansas were approved for use on Palo Verde (Arizona), Waterford 3 (Louisiana), and Units 2 and 3 at San Onofre (California).

The original InterData machine has long since been replaced by a more state-of-the-art digital computer from Concurrent Computers and takes advantage of newer 32 bit systems. Nonetheless, the original design still stands and is credited by the operator as allowing operations with increased power levels and narrower margins. This comes from the inherent ability of such a system to provide a faster and more accurate response to unusual and upset conditions.

6.7.1.3 Instrumentation and Controls Application

The Arkansas Reactor Protection System itself was nearly identical to other systems of the generation, with the software-based system providing what was then conventional hard-wired inputs to the solid-state safety logic. The application was limited to only two variables; DNBR (Departure from Nucleate Boiling Ratio) and Local Power Density. Both are indicative of high and potentially damaging localized "hot spots" on, or in the vicinity of, the fuel cladding. By providing early, fast, and accurate warning of these two parameters the limits of both could be more closely approached, resulting in higher available power production with resultant increased revenue. While this early application may appear meager in today's technical environment, it was considered to be quite advanced in the late 1970's when it became a licensing issue.

6.7.2 Indiana/Michigan Power Co., Donald C. Cook Station, Units 1 and 2

6.7.2.1 Project Description

Unit 1 of the Donald C. Cook Station saw initial commercial operation in August of 1975. Unit 2 followed in July of 1978. Each is a Westinghouse 4-loop pressurized water reactor (PWR) nuclear steam supply system (NSSS). The 3250 MWt Unit 1 and 3411 MWt Unit 2 are located in Bridgeman, Michigan and use Lake Michigan for both the main condenser Circulating Water System as well as the ultimate heat sink for the Emergency Core Cooling System (ECCS) (References 8.44 and 8.47).

The Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) were initially hard-wired relay systems with analog field devices providing the bistable inputs to the logic. With the development of solid state electronics, both of these systems were eventually combined into one Solid State Logic Protection System (SSLPS). However, the Foxboro Corporation's analog field instrumentation was retained largely intact. The upgraded equipment consists of modules that affect individual channels only. They do not affect the existing SSLPS actuation logic, where the individual channel trips are combined and the seal-in process occurs.

6.7.2.2 Associated Vendors and Participants

The Foxboro Corporation had been associated with the earliest design and construction of the units, supplying its H-Line analog instrumentation for most of the parameters important to safety which provided input to the RPS and the ESFAS. However, it was proving to be increasingly difficult to keep the devices in adequate repair, in part because of a growing scarcity of spare parts.

Because of its history with new-construction and retrofit work and its reputation in the instrumentation industry, Foxboro was approached with the problem. Since 1987, Foxboro has supported forty nuclear plants with over 1,500 nuclear qualified applications. Their experience had already included audited documentation and operating history for the hardware and embedded software.

6.7.2.3 Instrumentation and Controls Employed

The choice of product was the Foxboro SPEC 200 Micro line of microprocessor-based instrumentation. Its use would provide a previously unavailable configurable means of protection and control system input. The SSLPS remained unchanged because the Foxboro instrumentation still supplied a hard-wired relay contact interface between a field parameter and the protection logic. It is important to note that the new devices did, however, condition field signals and provide bistable action to the SSLPS for final logic determination.

The signal conditioning is performed in three steps using three distinct yet compatible types of hardware. The physical measurement (e.g., pressurizer pressure, containment level) are transformed by SPEC 200 transmitters to a recognizable low-level analog electrical value

representative of the measured parameter. This analog value is then input to SPEC 200 MICRO processing equipment for digitizing and modification by a proven algorithm, the output of which is converted back to an analog value for plant-wide use. Where a trip signal was required in support of the SSLPS, this final analog value was provided to a SPEC 200 discrete output device for set point comparison and bistable action. The results of this comparison control an output relay whose associated fail-safe contact, as before, is hard-wired to the combined protection and actuation system.

6.7.2.4 Instrumentation and Controls Application

The application of the Foxboro system to the SSLPS inputs is in two parts; hardware and software. Both parts underwent exhaustive NRC audit and confirmation prior to their implementation. IEEE Standard 279 and IEEE Standard 7-4.3.2 (Section 4.3.1) served for overall guidance, coupled with other applicable NRC and industry standards. IEEE Standard 603 (Section 4.3.1), in part, was used to ascertain whether or not the criteria applicable to safety system performance and equipment had been satisfied. Then, more specifically, the items were tested to and accepted against the requirements of IEEE Standard 344 and portions of IEEE Standard 323 (Section 4.3.1).

1. Hardware - The hardware consists, outside of system support ancillaries like power supplies, entirely of rack-mounted cards installed in existing cabinets. Central to each loop is a microprocessor-based control card which performs signal conditioning, regulatory control and front-end logic functions. These controls' functions are provided by user configuration of up to six control blocks. The control blocks selected for use and validated by the NRC were:
 - CALC: Executes simple arithmetic equations.
 - ALRM: Allows the setting of alarm set points.
 - LLAG: Sets lead-lag compensation parameters.
 - GATE: Provides eight 2-input Boolean logic gates
 - SSEL: Selects max/min variables from 8 possible
 - RAMP: Dual linear ramp generator
2. Software - The above six control blocks, which were used to implement the algorithms, were part of a set of 21 contained in programmable read only memory (PROM) mounted on the control card. Although this project predated NUREG-0800 (Section 4.3.6) and as such was not subject to its review processes, such will not be the case in the future. NUREG-0800 specifically states by definition that even embedded software, or firmware such as a PROM, is to conform to its criteria. In the case of the Foxboro application at Donald C. Cook, the six control blocks are configured by a menu-driven setup process which fills out internal tables that control the operation of the specific control functions and logic.

6.7.2.5 U. S. Nuclear Regulatory Commission Involvement

The NRC was initially notified by letter in late 1992 that the licensee requested amendments to its operating licenses. Specifically, it was proposed to replace portions of its instrumentation systems important to safety that were related to the Reactor Protection System. The system proposed was, in effect, a software-based (firmware) digital control system and the Commission established a program for a Safety Evaluation Report (SER), the objective of which would be to assess the adequacy of the proposed system. The SER was ultimately issued in early 1994 and displays an emphasis on issues such as the specific design basis, potential hardware vulnerabilities and susceptibilities, software development, verification and validation (V&V), configuration management, potential control/protection systems interactions, system failure modes and effects, reliability, and the developmental and operational history of the system equipment.

It was determined that the SER would be organized around five major topics, each of which would be addressed from hardware, software, and systems engineering perspectives. A "thread concept" was employed, whereby a single functional requirement was followed from design through implementation and V&V testing. These major topics for assessment were:

- Functional equivalence of the upgrade relative to the original design basis.
- Vendor's design and V&V processes.
- Licensee and vendor procedures and methodologies for the transformation of functional requirements to the software configuration that implements the requirements.
- Licensee's development of the design modification with respect to the design basis.
- Licensee's configuration management process for the new design.

The reader is directed to Reference 8.39. Study of this document will reveal a picture of NRC concerns and expectations during the review and qualification of a digital control system, such as might be proposed for the Yucca Mountain Project. Clear parallels may be drawn between the SER and NUREG-0800 Rev 4 (Section 4.3.6), as well as between the SER and *Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues* (Reference 8.4). Particular attention should be paid to Quality Assurance and type testing because they included appreciable concern for control room habitability issues.

6.7.3 Houston Lighting and Power Company, South Texas, Units 1 and 2

6.7.3.1 Project Description

Unit 1 at South Texas was first operated commercially after it received its license in August of 1988. Unit 2 followed in June of the next year. Each is a Westinghouse 4-loop pressurized water reactor (PWR) nuclear steam supply system (NSSS). The 3800 MWt

(1250 MWe) units are located near Matagorda, Texas and use a 7,000 acre Main Cooling Reservoir (MCR) for a heat sink (References 8.48 and 8.63).

The two units at South Texas will likely be the first to use a software-based control system in a Class 1E application. (Although Class 1E equipment is discussed in this case, it is important to note that it is unlikely that Class 1E equipment will be used for the Yucca Mountain project). The licensee has gone out to bid for a Programmable Logic Controller (PLC) system replacement for a portion of the controls associated with its Emergency Diesel Generators. The emergency power system at each of the two units is comprised of three 13.8 kV emergency busses designated E1A, E1B, and E1C. Each of these three busses is backed up through a step-down transformer from individual diesel generators rated at 4160 V, 5500 kW.

Each of the emergency diesel generators will employ a PLC for engine control, parameter monitoring, annunciation, trip, and the generator regulator. While of future interest, this first entry in NRC approved digital controls important to safety will retain the present load shedding and sequencing systems as well as engine governor controls. It has been acknowledged that load control (increase and decrease) and even engine speed control are potentially ideal uses for a PLC, but those involved in the project wanted to do everything possible to ensure success the first time out. If this new means of control proves satisfactory, in time load control will probably be added to the in-place PLCs, or separate PLCs will be added for the purpose. A possible replacement of the engine governor may occur later.

A number of operating utilities are watching this application of digital controls for potential use at their facilities. At least one, Virginia Power Company, is considering pursuing replacement of their Reactor Protection System with a similar system for Units 1 and 2 at its Surry station. Much of the industry's interest rests on how successful Houston Lighting and Power is at South Texas.

6.7.3.2 Associated Vendors and Participants

Triconex is a leading contender for the South Texas application, and much of their experience comes from its association with European standards and applications. Triconex, a French company, has been instrumental in the development of common standards for world-wide use of programmable logic controllers. It comes as no surprise that much of their design parallels the requirements of IEC 1131-3. This standard addresses hardware and software, down to the selection of language to be employed (References 8.30, 8.31 and 8.38). (The References are used to show the general relationships, and understandings by Triconex for use of foreign industry standards for PLC hardware and software designs, especially in the area of use in safety-related control systems.) Triconex has been involved for some time in the evolving use and acceptance of software-based controls in nuclear applications, in particular in systems important to safety. It is this background and history that has justified their involvement and contribution in the formulation of NUREG-0800 Rev. 4 (Section 4.3.6) and have been active participants, along with the NRC, in EPRI's preparation of *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*, TR-107330 (Reference 8.24,

pages 179 and 181). The NRC has also been involved before in PLC nuclear reactor systems applications as evidenced in NUREG/CR-6090.

TR-107330 document has now been reviewed by the (NRC). An SER has been written and issued to the Electric Power Research Institute on 7/30/98. The SER's complete title is, *Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute (EPRI) Topical Report, TR-107330, Final Report, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."* (Reference 8.3, mention of title). One of the more interesting features of the specification is that it covers all three major areas of concern of such a system; (a) quality assurance and qualification activities, (b) supporting documentation, and (c) information necessary for qualifying a platform to a specific application.

It should be noted that EPRI TR-107330 provides only generic requirements for pre-qualifying commercial PLCs for use in safety-related applications. This SER addresses the requirements for a PLC system design specification but not the actual use of the PLC in a specific application by the licensee. The SER approves the basis for a design of a PLC system by a PLC manufacturer, thus a basis as only a component for a specific safety-related application. For a plant specific PLC safety-related application, the licensee is responsible for ensuring that the system design incorporating the PLC meets all applicable regulations and associated NRC guidance. By review, the NRC staff will determine if the PLC requirement specification has been followed and that the system design meets all of the applicable regulations and guidance as provided in 10 CFR Part 50 and in the Standard Review Plan (SRP), NUREG-0800, Rev. 4, Chapter 7, for the specific application proposed. This includes a number of plant (or site) specific concerns such as diversity, electromagnetic interference/radio frequency interference (EMI/RFI), separation criteria, and maintenance training that must be satisfied before the PLC system design can be found acceptable in a plant specific safety system design (Reference 8.3, pages 2, 7, 33, and 34).

Regarding quality assurance, the SER applies to PLCs produced under a 10CFR50, Appendix B program or procured as commercial products and dedicated for safety-related applications. Appendix B applies to any activities performed to provide generic qualification of the product, application-specific design and development, including the system integration. The user or licensee will perform audits to verify that the vendor's QA program is equivalent to 10CFR50, Appendix B or compensating tests can provide that verification (Reference 8.3, page 28).

The study of the SER reveals a picture of NRC concerns and expectations during the review and qualification of a PLC digital control system, such as might be proposed for the Yucca Mountain Project. Generic PLC system requirements include criteria for functional, hardware, software/firmware, human/machine interface (HMI), electrical, data communication, software security, maintenance, third party/sub-vendor items, shipping and handling, acceptance testing, qualification testing and analysis, and documentation specifications. The NRC found many of the generic PLC requirements in TR-107330 to be in compliance with the acceptance criteria identified NUREG-0800 Rev. 4, Chapter 7, and therefore acceptable. Where it didn't, specific criteria or requirements are given. Detailed

and clear parallels may also be drawn between the SER and *Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues* (Reference 8.4). This generic specification is particularly significant because it will form the basis under which Triconex will likely supply the first commercially available platform to undergo scrutiny under NUREG-0800 Rev 4 (Section 4.3.6) for use on a Class 1E system. As such, it will be the first "NRC Approved Digital Control System" that has to stand on its own merits. Not only will the I/O be digitally conditioned and internally bussed, but the actual control logic will be software-based and stand-alone, i.e. not undergo oversight by another system. Triconex has already been audited and accepted under 10CFR50 Appendix B (Section 4.3.2) and 10CFR21 (Section 4.3.2)(Reference 8.9). Triconex now plans to have their specification, procedures, and PLC platform sent to an independent lab, Wiley Labs, for testing by June 1999. Results of the tests will be reported, with the reports and a request for approval of the system sent to the NRC. An SER will then be written by the NRC and submitted to Triconex.

It is important to point out that the system selected for certification and hopefully ultimate approval is not Triconex's latest model. The choice was made to pursue acceptance of the system that is one generation older than their current offering. This was done at the suggestion of the NRC in order to show three years worth of operating history. Within a reasonable period of time, it is anticipated that at least three separate manufacturers will have systems available for deployment on systems important to safety within the constraints of the above generic specification.

6.7.3.3 Instrumentation and Controls Employed

The Triconex TRICON Programmable Logic Controller (PLC) is unique in a number of respects, not the least of which is the basis for its inherent configuration. It uses a Triple Modular Redundant (TMR) approach, where virtually everything is done in triplicate (Reference 8.15, page 3). This offers a number of safety and maintenance advantages, such as hot-change out and 2-out-of-3 voting of data and actions. The system is based on three isolated, parallel control systems which are integrated into one set of hardware. The triplication is carried throughout from the inputs, through the processors to the outputs, yet to the user it appears as one system. Overall scan times run in the range of 40 to 150 milliseconds. Extensive diagnostics on each independent leg, each modular component, and each functional circuit, detect and report operational faults. Triconex is also based on Software Implemented Fault Tolerant (SIFT) technology. It has a common software code that has literally millions of hours of use worldwide in many applications (Reference 8.19, page 4).

Field sensors are terminated at field panels where their signals are optically coupled and replicated onto three isolated busses to the input modules. Each leg of the input modules reads the process data and passes that information to its respective main processor via separate communication paths.

Once per scan the three main processors synchronize and communicate with their two neighbors over a separate backplane bus, voting 2-out-of-3 on the inputs. After the control

and interlocking logic has been executed at each of the three processors, the output data undergoes another a 2-out-of-3 comparison. Any patterns of disagreements that develop are flagged and annunciated. The results are sent on three more separate communication paths to triplicated output modules.

At the output modules, redundant installed active and shadow hot-spare units receive the same information, allowing a fail-safe changeover in the event the active unit proves false. In a fashion similar to that at the inputs, the output precedents are presented to a single output for interconnection to a field device.

In addition to its inherent fault tolerance, the TRICON incorporates Sequence of Events (SOE) recording and high speed redundant communication links using a variety of industry accepted protocols for merging with Distributed Control Systems (DCS) including Nodebus (Foxboro), Universal Control Network (Honeywell), and MODBUS (ABB, Bailey, Tayler-Rosemount, and Yokagawa).

6.7.3.4 Instrumentation and Controls Application

Similarly to the Foxboro SPEC 200 system family, the TRICON can best be described as a coordinated application of hardware and software. Both parts have already undergone their initial NRC quality assurance audits for conformance to 10CFR50 and 10CFR21 (Section 4.3.2).

1. Hardware - The processors and I/O can be mounted in a single environmentally controlled cabinet that incorporates three triplicated bus systems at the backplane. Field terminations assemblies, while separate from the electronics, are also included in the rack. The chassis includes two independent power rails, with each module drawing power from both through dual power regulators. A failure on any one rail will not impact the performance of the system. A variety of types of I/O are available, including a unique power-on fail-safe output with active feedback for monitoring of power availability.
2. Software - The TRICON is programmed from a Windows NT workstation using Triconex proprietary software. The workstation allows generation and testing of created and edited programs off-line using one or a combination of three language editors (Reference 8.23).
 - Function Block Diagram (FBD) - A graphical language structured by networks consisting of function block elements interconnected by signal flow lines that communicate boolean, integer, real, and other data types between the FBD elements. In appearance, it resembles the already familiar approach used in most major Distributed Control Systems (DCSs).
 - Ladder Diagram (LD) - A graphical language structured by networks of rungs that are connected on both sides to "power rails." Links transfer binary data from a "power rail" to interconnected LD symbols. LD uses a standard set of

symbols representing relay contacts and coils, as well as function blocks, as instructions. Again, LD resembles something already familiar to controls engineers, namely the very common PLC.

- Structured Text (ST) - A high-level textual language for connective programming similar to PASCAL. ST provides a means to create boolean and arithmetic expressions, as well as structured programming constructs, such as conditional statements. As above, function blocks may be invoked within the use of ST. It affords better self-protection than programming languages C or C++ in part because of its rigid declaration requirements (Reference 8.30).

In support of the above, the language editors are provided with tools including variable declarations, automatic naming, element attribute properties, documentation comment boxes, variable annotation, system or user-modified macros, and user-derived function blocks. An emulator allows testing and debugging of any generated or edited program off-line before downloading to the TRICON.

6.7.3.5 U. S. Nuclear Regulatory Commission Involvement

The cooperation of the (NRC), Houston Lighting and Power, and Triconex began in the early stages of this application. A representative from the licensee provided input and remarks to the NRC during preparation of Chapter 7 to NUREG-0800 Rev 4, *Standard Review Plan for Nuclear Power Plants, LWR (Light Water Reactor) Edition* (Section 4.3.6). (Reference 8.24, pages 179 and 181) discusses that all three organizations aided in the development of the EPRI *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*, with the Commission offering comments throughout in order to provide a useable document that would also be acceptable in the regulatory sense. There is every reason to expect that Houston Lighting and Power, teamed with Triconex, will be successful in this very first true full application of software-based controls on a system important to safety. Although there may be problems and changes, as in all such projects, each approval is approached on a case-by-case basis.

6.7.3.6 In Support of the Yucca Mountain Project

The SER supports the use of PLCs, a digital based control system component, in meeting design criteria and existing design concepts for various subsurface operations. The SER supports the use of digital control technology similar to that being considered in current YMP VA design concepts (Reference 8.5, pages 4-59 to 4-111). One of these design concepts is a very large Performance Confirmation Data Acquisition/Monitoring System. The PLC will be an essential part of this system for the subsurface repository supporting an extensive system of communication and data circuits or highways. System design criteria 4.2.4 indicates the need for these circuits and equipment to be protected from electromagnetic interference (Performance Confirmation Data Acquisition/Monitoring System Description Document, Volume I, page 17)(TBV-407). The PLC and initiating source of these circuits will need to have the appropriate surge withstand, and its I/O

load sequencers utilize Allen-Bradley commercial grade PLCs to execute the control functions and provide continuous monitoring of the load sequencers. The use of commercial grade hardware and the use of software for emergency applications required assurances of qualification, thus the NRC review and subsequent approval through issuance of a Safety Evaluation Report (SER) (Reference 8.34).

6.7.4.1.1 Associated Vendors and Participants

The prime contractor was Fluor Daniel. Spectrum Technologies, Inc., a subcontractor, developed the software for the Unit 2 load sequencer. Allen-Bradley supplied the PLC system.

6.7.4.1.2 Instrumentation and Controls Employed

The purpose of this section is to describe the Allen-Bradley PLC system that was put into operation at Prairie Island. No information was found at the time of this analysis as to the PLC particular equipment or model numbers involved, or how the control system was configured. Because of the common use of the PLC and its typical features, there are adequate references that the reader can explore regarding Allen-Bradley PLC's capabilities, such as reading Allen-Bradley's vendor data and specifications.

6.7.4.1.3 Instrumentation and Controls Application

No data is available to explain or support exactly how the PLC control system was implemented or the benefits it added.

6.7.4.1.4 U. S. Nuclear Regulatory Commission Involvement

This upgrade at Prairie Island is an example of the current use of a commercially available grade PLC for a safety related control system. It represents a case-by-case acceptance by the NRCs Instrumentation and Control Systems Branch (SICB) of a digital based PLC control system. The SER (Reference 8.34) highlights several criteria the NRC based its acceptance on.

The criteria for the NRCs acceptance included several items (Reference 8.34 pages, 1-5) Approved items and requirements included:

- 1) an acceptable dedication process to qualify the PLC as Class 1E for the commercial grade equipment. This is based on previous NRC Generic Letters and other documents including criteria III, IV, and V of Appendix B to 10CFR50 (Sec. 4.3.2).
- 2) a formal verification and validation plan augmented by extensive testing of both hardware and software to satisfactorily follow the guidelines of IEEE Std 1012-1986 (Sec. 4.3.1), and Regulatory Guide 1.152 (Sec. 4.3.3), which indorses ANSI/IEEE-ANS-7.4.3.2-1982 (Sec. 4.3.1).
- 3) PLC on board battery backup capability of retaining all stored (software) program data in the random access memory (RAM) through a continuous power outage of 12 months,

- 4) the use of EEPROM for the PLC's read only memory (software) for download of the PLC operating program to the PLC RAM in the event of PLC loss of power and in the event of failure of the battery backup power to maintain RAM in a power on state,
- 5) an appropriate monthly testing program for the load sequencer control functions,
- 6) an appropriate method of manual control capability for the load and source breakers, as well as methods for providing control room operators with bypass indications and inoperable state indications,
- 7) a qualification program for electromagnetic and radio frequency interference. PLC vendor (Allen Bradley) performs several tests to meet noise, electromagnetic, and surge interference requirements. These tests are based on several different industrial standards for noise, surge transients, and electromagnetic susceptibility, including the National Electrical Manufacturers Association, the Institute of Electrical and Electronics Engineers (IEEE), the Scientific Apparatus Makers Association, and Military Standards. These vendor tests covered the electromagnetic environment at the Prairie Island plant, especially covering radio frequencies for portable two-way radios.

Redundancy was a concern and requirement. The load sequencer for Unit 2 consists of redundant trains of load sequencers, each train dedicated to an Emergency Diesel Generator. A cross-tie connects the emergency power supplies in the two nuclear plants to ensure availability of an emergency diesel generator during a loss of offsite power in one unit. Also mentioned above are the redundant and defense-in-depth features of battery backup capabilities and manual control override capabilities to the load sequencers.

System isolation was also a concern and requirement. Isolation of the load sequencer control system from non-1E systems, or non-safety systems, was provided. Non-1E systems interfacing with the PLC's inputs were isolated from the PLC with coil to contact and contact to contact isolation relays. These forms of isolation were approved by the NRC, and they were verified by the NRC during the site audit of the control system implementation.

6.7.4.1.5 In Support of the Yucca Mountain Project

This SER supports the use of PLCs, a digital based control system component, in meeting design criteria and existing design concepts for various subsurface operations. The SER supports the use of digital control technology similar to that being considered in current YMP VA design concepts (Reference 8.5, pages 4-59 to 4-111). One of these design concepts is a very large Performance Confirmation Data Acquisition/Monitoring System. The PLC will be an essential part of this system for the subsurface repository supporting an extensive system of communication and data circuits or highways. System design criteria 4.2.4 indicates the need for these circuits and equipment to be protected from electromagnetic interference (Performance Confirmation Data Acquisition/Monitoring System Description Document, Volume I, page 17)(TBV-407). The PLC, or the initiating source of these circuits, will have an appropriate qualification and test program for electromagnetic and radio frequency interference all in accordance with several different

industrial standards for noise, surge transients, and electromagnetic susceptibility similar to those described in Reference 8.34.

The SER also supports the statement that "all Monitored Geological Repository (MGR) Systems, Structures and Components (SSCs) shall be designed and fabricated in accordance with applicable industry codes, standards, engineering principles and practices with particular attention to those which incorporate system safety, human factors, reliability, availability, maintainability, and habitability standards" (Reference 8.11, page 3). The SER accepts good engineering principles and practices requiring an acceptable dedication process to qualify the PLC, a formal verification and validation plan, an appropriate monthly testing program, and the qualification and test program for electromagnetic interference (Reference 8.34, page 2-5). These requirements for the PLC help ensure system safety, reliability, and availability.

6.7.4.2 Prairie Island Emergency Response Computer System

The Emergency Response Computer System (ERCS) collects and processes selected field data for display on CRT monitors in the control room. This information, in its multiple forms, is used to assist personnel in the proper implementation of emergency procedures during an accident condition covered by these procedures. The system also provides control room personnel with access to relevant information to assist them during operational transients. During normal operation, the system provides assistance in determining the status and performance of the reactor core and auxiliary process systems. (Reference 8.59, page 7.7-1).

The ATWS (Anticipated Transient Without Scram) Mitigating System Actuation Circuitry, or (AMSAC) system uses microprocessor-based instrumentation to mitigate the effects of a failure to trip the reactor in the event of a loss of normal feedwater. An ATWS is an anticipated operational occurrence that is accompanied by a failure of the reactor protection system to shut down the reactor. The mitigation is accomplished by initiating both a turbine trip and auxiliary feedwater flow after the reactor protection system has been given sufficient time to trip the reactor (Reference 8.59, page 7.11-1).

6.7.4.2.1 Associated Vendors and Participants

The AMSAC design for Prairie Island Units 1 and 2 was developed by the Westinghouse Owners Group to meet the requirements of 10 CFR 50.62 (Reference 8.60, page 8).

6.7.4.2.2 Instrumentation and Controls Employed

The AMSAC system for Prairie Island is built around Westinghouse Automation Division microprocessor-based instrumentation. Furthermore, the feedwater control system at Prairie Island has been upgraded with Westinghouse Distributed Process Family microprocessor-based instrumentation. All feedwater control system inputs pertinent to AMSAC undergo digital to analog conversion and are then transmitted across a redundant data highway to AMSAC, which is implemented in a Westinghouse Numa-Logic programmable logic

controller (PLC). The PLC performs all AMSAC logic function, including providing outputs for the AMSAC actuation relays (Reference 8.61, Attachment I, page I-3).

6.7.4.2.3 Instrumentation and Controls Applications

The ERCS is best discussed in terms of its hardware and software platforms. The hardware configuration consists of two identical fully redundant computer systems with automatic transfer from primary to backup. Analog and digital inputs from field instrumentation and control systems are routed to remote multiplexers where initial signal conditioning is performed. The software is divided into three distinct fully integrated software packages. The plant monitoring system software controls and maintains the ERCS database which consists of all field inputs, constants, setpoints, and outputs calculated by other applications. It provides the standard scan, event logging, alarm, display, archival and periodic reporting functions. The safety assessment system (SAS) software processes all safety parameter display system (SPDS) parameters. It performs all necessary calculations, does limit checking, and assigns SAS quality codes to each parameter. The nuclear steam supply system (NSSS) software provides plant personnel with concise and reliable information to assist in determining the status and performance of the reactor core. It also provides input to the nuclear fuel performance calculations. The NSSS software performs online calculations of data obtained from the reactor control and protection system and the NSSS. It should be emphasized that the NSSS software has no direct protective or safety significance and functions only as an operating aid by enhancing established manual operating procedures. (Reference 8.59, pages 7.7-1 to 7.7.4).

Specifically, the purpose of the AMSAC at Prairie Island is to mitigate the effects of a failure to trip the reactor in the event of a loss of normal feedwater or a loss of load. This AMSAC is based on the Westinghouse Owners Group generic loss of feedwater flow logic, which senses the impending loss of heat sink by monitoring feedwater flow directly. AMSAC initiates a turbine trip and actuates auxiliary feedwater. AMSAC also responds to low feedwater flow. (Reference 8.61, Attachment I, pages I-1 and I-2).

6.7.4.2.4 In Support of the Yucca Mountain Project

This SAR supports the use of several digital based control system components. The NRC's support of digital controls in commercial nuclear power plants provides design and licensing precedence for the application of similar technology to proposed applications within the YMP. The SAR supports the use of digital control technology similar to that being considered in current YMP VA design concepts (Reference 8.5, pages 4-59 to 4-111). Design criteria 4.2.2 can be generally supported by Prairie Island's use of a redundant data highway system linking field data to a safety related PLC and two fully redundant computer systems. The precedence and use of CRT monitors in the control room lends support for their use as operator or human machine interfaces in YMP design concepts (Reference 8.5, pages 4-98, 4-99, 4-106, 4-111), especially as detailed in the Subsurface Repository Integrated Control System Design, and the Subsurface Control System Physical Architecture Drawings (Reference 8.53).

Design criteria 4.2.3 is supported by Prairie Island's use of software to perform on-line calculations for a non-safety significant task. The use of three distinct but fully integrated software packages and CRT monitors to support a field database of setpoints, constants, inputs, limit checking calculations, and to support a safety parameter display system, supports VA concepts that the YMP needs to rely on to integrate its Performance Confirmation, Subsurface Safety and Monitoring System, Subsurface Operations Monitoring and Control System, as well as others.

6.7.5 Pacific Gas and Electric, Diablo Canyon, Units 1 and 2

6.7.5.1 Project Description

Located adjacent to the Pacific Ocean in San Luis Obispo, California, the two installed substantially identical power generating units at the Diablo Canyon plant facility are Westinghouse 4-loop pressurized water reactors. (PWRs). Each unit consists of a nuclear steam supply system (NSSS), turbine-generator, auxiliary equipment, controls, and instrumentation. The 3338 MWt Unit 1 commenced commercial operation in May of 1985, and the 3411 MWt Unit 2 went on line in March of 1986. (Reference 8.57).

The Reactor Trip System (RTS) and the Engineered Safety Features Actuation System (ESFAS) utilize a digital process protection system that takes inputs from various instrument channels and direct inputs corresponding to normal/abnormal status of plant parameters. The system combines these signals in the required logic combination and generates a trip signal to the reactor circuit breakers when the necessary combination of trip signals occurs. (Reference 8.57, page 7.2-15, 7.3-1)

The Reactor Vessel Level Instrumentation System (RVLIS) is a microprocessor-based system that measures level in the reactor vessel or the relative void of the circulating primary coolant system fluid. (Reference 8.57, page 7.5-5)

The Emergency Response Facility Data System (ERFDS) is a microcomputer-based system with distributed processors dedicated to various functions. The system is designed to monitor and display plant parameters used for post-accident monitoring. (Reference 8.57, page 7.5-8)

6.7.5.2 Associated Vendors and Participants

Westinghouse Electric Corporation has had a long history in the design development of reactor protection and engineered safety features actuation systems. Westinghouse process protection systems include three generations of analog electronics: Foxboro H-Line, Westinghouse 7100 Series, and Westinghouse 7300 Series equipment. As a result of technological advances, these systems are rapidly approaching the point of obsolescence. The Westinghouse Eagle-21 Process Protection System is a modular microprocessor-based upgrade system for replacing the older analog process protection equipment. (Reference 8.56, pages 1 and 2).

6.7.5.3 Instrumentation and Controls Employed

The Westinghouse Eagle-21 Process Protection System consists of three subsystems: an Input/Output (I/O) Subsystem, a Loop Processor Subsystem, and a Tester Subsystem. The input portion of the I/O subsystem consists of analog input and contact output signal conditioning modules which satisfy all of the unique signal conditioning, signal conversion, isolation, buffering, termination and testability requirements. Both modules provide signals to the Loop Processor Subsystem which executes all of the algorithms for the protective functions. Typical functions of the loop processor are summation, lead/lag, multiplication, comparing, averaging, and square root conversion. The Tester subsystem is the focal point of human interaction with the protection system. It provides the interface which allows test personnel to adjust setpoints and tuning constants, and to perform surveillance tests on the protection system. (Reference 8.56, pages 11, 12, and 13)

6.7.5.4 Instrumentation and Controls Application

The Westinghouse Eagle-21 Process Protection System is applicable for those instrument systems which are "safety-related" as defined by IEEE Standard 279 (Section 4.3.1). Typical protection channels which may be monitored with the system are as follows (Reference 8.56, page 4):

- ◆ Average Temperature and Delta Temperature
- ◆ Pressurizer Pressure
- ◆ Pressurizer Water Level
- ◆ Steam Flow and Feedwater Flow
- ◆ Reactor Coolant Flow
- ◆ Turbine Impulse Chamber Pressure
- ◆ Steam Pressure
- ◆ Containment Pressure
- ◆ Reactor Coolant Wide Range Temperature
- ◆ Reactor Coolant Wide Range Pressure
- ◆ Boric Acid Tank Level
- ◆ Pressurizer Liquid and Vapor Temperatures
- ◆ Steam Generator Narrow Range and Wide Range Water Level

The microprocessor for the RVLIS accepts inputs from differential pressure (DP) transmitters, compensating inputs from the temperature measurements of the DP cell impulse lines, compensating temperature and pressure measurements from the reactor coolant system, and status inputs from the reactor coolant pumps. The system consists of two independent channels. Each channel utilizes three DP cells, where each cell measures a different pressure range. These different ranges are necessary in order to cover different flow behaviors of the core coolant, depending on whether the reactor coolant pumps are operating. (Reference 8.57, page 7.5-5 and 7.5-6).

The computerized ERFDS is divided into three subsystems. The high-speed data acquisition subsystem is a remote multiplexing system that interfaces with the plant instrumentation, converts the data to a digital form through 12-bit A/D converters, and then transmits the data to master control units that interface with the safety parameter display system (SPDS) server. The SPDS server subsystem is a dedicated server computer that controls data transfer between the data acquisition subsystem and the different processors making up the data display subsystem. Display data is updated at one-second intervals. The data display subsystem provides the system interface for the operators and emergency personnel. (Reference 8.57, pages 7.5-8 and 7.5-9).

The SPDS is the display subsystem of the ERFDS. The SPDS provides a display of plant parameters pertaining to the safety status of operations. The primary function of the SPDS is to help operating personnel in the control room to make quick assessments of plant safety status. The SPDS equipment includes personal computers with color display monitors, each of which communicates with the SPDS server computer through an Ethernet network. Each power plant unit has its own SPDS server computer. The primary display of the SPDS corresponds to important plant functions such as reactivity and radioactivity control, core cooling and heat removal, core coolant system integrity, and containment integrity. (Reference 8.57, pages 7.5-9, 7.5-10, and 7.5-11).

6.7.5.5 In Support of the Yucca Mountain Project

This SAR supports the use of many digital based control system components, instruments, and computers in both safety and non-safety-related processes. The NRC's support of digital controls in commercial nuclear power plants provides design and licensing precedence for the application of similar technology to proposed applications within the YMP. The SAR supports the use of digital control technology similar to that being considered in current YMP VA design concepts (Reference 8.5, pages 4-59 to 4-111). Design criteria 4.2.3 for operator access via software an operating system to affect process monitoring changes or how process information is displayed is generally supported by the Process Protection System's Tester subsystem interface which allows adjustments of setpoints and tuning constants.

The use of color display monitors, and personal computers communicating to a larger server computer over an ethernet network is a clear precedence for support of YMP design concepts (Reference 8.5, pages 4-98, 4-99, 4-106, 4-111), especially as detailed in the

Subsurface Repository Integrated Control System Design, and shown on the Subsurface Control System Physical Architecture figures (Reference 8.53, pages 46 to 57).

Design criteria 4.2.1 for real-time monitoring is supported by the computerized Emergency Response Facility Data System's data display system of one-second intervals. This frequency of data monitoring is accomplished by a high-speed data acquisition subsystem and its data transfer (server) computer.

6.7.6 Arizona Public Service Company, Palo Verde Nuclear Generating Station, Units 1, 2, and 3

6.7.6.1 Project Description

Unit 1 at Palo Verde first became operational in January of 1986 and was followed by Unit 2 in September of the same year. Unit 3 began operations in January of 1988. Each is a 2-loop pressurized water reactor (PWR) consisting of a Combustion Engineering System 80 nuclear steam supply system (NSSS) and a General Electric turbine-generator. The three 3800 MWt units are located thirty-four miles west of the city of Phoenix in Maricopa County, Arizona.

The Diverse Auxiliary Feedwater Actuation System (DAFAS) is a computer-based system that initiates auxiliary feedwater flow upon conditions indicative of an ATWS (anticipated transient without scram) event combined with selective low steam generator level signals. (Reference 8.58, page 7.3-72).

6.7.6.2 Associated Vendors and Participants

In 1984 the Code of Federal Regulations (CFR) was amended to include Section 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants", known as the "ATWS Rule". The ATWS rule requires specific improvements in the design and operation of commercial nuclear power facilities to reduce the likelihood of failure to trip a reactor following an ATWS event, and to mitigate the consequences of an ATWS event.

6.7.6.3 Instrumentation and Controls Employed

The DAFAS uses programmable logic controllers (PLCs) with solid state I/O modules and fiber optic communication links to receive and transmit signals to and from its various subsystems. (Reference 8.58, page 7.3-79).

6.7.6.4 Instrumentation and Controls Applications

The Palo Verde DAFAS is designed to initiate auxiliary feedwater flow upon conditions indicative of an ATWS combined with selective low steam generator level signals. The DAFAS will stop auxiliary feedwater flow to the affected steam generator after reaching a predetermined level setpoint, at which time manual operator intervention is required to control the system. (Reference 8.58, page 7.3-73).

6.7.6.5 Support for the Yucca Mountain Project

This SAR supports the use of digital based PLCs with I/O modules and computers in both safety and non-safety related processes. The NRC's support of digital controls in commercial nuclear power plants provides design and licensing precedence for the application of similar technology to proposed applications within the YMP. The SAR supports the use of digital control technology similar to that being considered in current YMP VA design concepts (Reference 8.5, pages 4-59 to 4-111).

Part of design criteria 4.2.5 for an integrated data communications system(s) between various subsystems is supported by the SAR. The use of fiber optic communication links for plant wide data transmission is a clear precedence for support of YMP design concepts (Reference 8.5, page 4-106 and 4-108), especially as detailed in the Subsurface Repository Integrated Control System Design, and shown on the Subsurface Control System Physical Architecture figures (Reference 8.53, pages 46 to 57).

6.7.7 Additional Information on Nuclear Power Plant Use of Digital Controls

Other documentation from the NRC reveals many other examples of the use of digital based controls in many Nuclear Power Plants. It becomes clearer that there is significant working precedence of digital control devices and digital control systems in nuclear power plants throughout the United States and the world today. The extensive NRC involvement in the acceptance and performance criteria issues for the use of digital controls has been a positive factor.

Also, available in the NRC Public Document Reading Room (PDR) are numerous Safety Evaluation Reports written by the NRC as well as Safety Analysis Reports from many nuclear power plants. Many of these SARs and SERs were reviewed for this analysis and provided general support for the information presented. Only a few specific cases were summarized. Should the reader find an interest, contact can be made with the NRC PDR to explore some of the many additional SERs and SARs.

6.7.7.1 Nuclear Power Plants With Digital Controls

In the NRC quarterly report, *Computer-Based Digital Systems Failures: December 1996-March 1997*, an NRC quarterly report, a summary of the results search and review of digital system problems and failures is presented. Many of these digital systems are safety related and some are not. The report gives the date of the digital control system problem or failure, the cause and symptoms observed, and related references, such as inspection reports, morning reports, and event notifications. The report is broken down into categories of software, hardware, electromagnetic interference, and man-machine interface problems. The Instrumentation and Controls Branch (HICB) of the NRC tracks these problems by interfacing with designated instrumentation and controls contacts in each region of the country and reviewing the Nuclear Plant Reliability Data System data. It also reviews License Event Reports, event notifications, morning reports, and Nuclear Utilities Software

Management Group news bulletins for information concerning digital system problems. The report is not a comprehensive list (Reference 8.55).

The information gathered for the report is continually referred to by the NRC when performing reviews and inspections of new and future digital system retrofits or when considering new industry standards and NRC guidelines. What's interesting about some of these digital control's problems is that they serve as a confirmation or justification for a significant portion of the NRC's developed guidance issues or design and performance criteria for the use of digital control systems. They give substantiation to the guidance and direction found in NUREG-0800 Rev 4 and in their published SERs. One other thing to note is that these problems or failures are used in a positive learning way by the NRC, because the NRC continues to give approvals and improve the acceptance criteria for digital based control systems.

The quarterly report lists as many as 40 nuclear power plants with digital controls or digital based instrument or components. Some of these include digital systems or components at Southern California Edison & San Diego Gas & Electric Co. San Onofre, at Florida Power & Light Turkey Point 3 & 4, at Arizona Public Service Company Palo Verde 1, 2, 3, and at Pennsylvania Power & Light Co. Susquehanna 1. These specific sites mentioned have digital based control systems in safety-related systems.

Some worthy comparisons to YMP systems would include Susquehanna 1 which has a plant processor computer interface with the ventilation monitoring system control terminal, and Turkey Point 3 & 4 which has a digital microprocessor based radiation monitoring system and an Allen-Bradley PLC based emergency diesel generator load sequencer. The subsurface repository of Yucca Mountain will have significant radiation monitoring and ventilation monitoring and control systems. (Reference 8.5, page 4-84 to 4-90, 4-101, 4-106, 4-109 and 4-110).

6.7.7.2 Case-by-Case Licensing Process

In the National Research Council's report, *Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues* (Reference 8.4), the case-by-case licensing process of digital instrumentation and control technology applications in the nuclear industry is discussed. It's recommendation for use of digital controls is the extensive and largely successful use of digital controls in other safety-related industries. This significant precedence of digital controls serves as a strong beginning basis for their use in the nuclear industry. The analysis, *Digital Controls for Safety Related Systems* (Reference 8.52), provides extensive and comprehensive examples of safety-related applications of digital controls in the various industries that were exemplified in the National Research Council's report.

The major elements of the evolution of the acceptance of digital controls are the procedural process for achieving approvals, implementing digital systems with or without NRC approval, and the available substantive regulatory standards that apply to digital controls.

Individual nuclear power plants make decisions regarding their upgrades according to 10 CFR 50.59 to determine whether or not prior regulatory approval is required. This is based on whether a proposed upgrade introduces an unreviewed safety question not previously covered in a plant's Safety Analysis Report and license application. If approval is required the NRC undertakes a formal review of the proposed change(s) before the change can be implemented. This results in the issuance of a Safety Evaluation Report and reviews and inspections prior to commissioning and startup to ensure the SER conditions have been met. Typically the general design criteria in 10 CFR 50, for I&C systems provides a high level guidance, and considerable latitude is given in the interpretation and application of the criteria. Because of this and the NRC's recent past (prior to NUREG 0800 Rev. 4) of having no standards and criteria explicitly developed for digital systems, the reviews and approvals were conducted on what was termed the "case-by-case" basis (Reference 8.4, page 79).

Particular concern for achieving consistent interpretation and uniform application by the industry of 10 CFR 50.59 resulted in the development of an industry guidance document by EPRI and the Nuclear Management and Resources Council. The NRC does not endorse the document but accepts it as useful in the evaluation of proposed facility design changes in light of the logic used in making a 10 CFR 50.59 interpretation. Subsequently, after disagreement with a Haddam Neck power plant interpretation of 10 CFR 50.59 over a replacement-in-function-kind of reactor protection control system analog modules with microprocessor-based modules, the NRC issued a draft letter that addressed the application of 10 CFR 50.59 digital upgrades. The NRC believed this to be a safety-significant upgrade. The letter explicitly required that all safety-related digital upgrades be approved in advance by the NRC staff, irrespective of the results of a utility's evaluation under 10 CFR 50.59. In effect, digital upgrades became an exception to 10 CFR 50.59. The reader may refer to Reference 8.4, pages 79 to 81, for a detailed discussion and the titles of the document and letter involved.

With uncertainty among the utilities planning digital upgrades and with many canceling their plans, the industry sought to develop more specific guidance addressing the applicability of 10 CFR 50.59 to digital upgrades, especially in safety-related systems. Upon this effort, the NRC withdrew its generic letter. A more specific industry guidance document was published in December of 1993, with a workshop held on its implementation in June 1994. The outcome of this was an NRC Generic Letter which generally endorsed the specific guidance document. The reader may refer to reference 8.4, page 81, for a detailed discussion and the titles of the document and letter involved.

A significant result of the events described above helped lead to the development of NUREG 0800 Rev 4, Standard Review Plan for digital upgrades to safety-related systems.

In general, the National Research Council committee in their report (Reference 8.4, pages 81 and 82) agrees with the fundamentally sound framework of 10 CFR 50.59. However, it didn't agree with all digital upgrades as an exception to 10 CFR 50.59. It feels that to consider all safety-related digital upgrades the same without their safety significance weighed is not a wise approach, and that it endorses maintaining and formalizing the distinction between major and minor systems upgrades containing digital technology.

(Reference 8.4, page 82). Finally, it is believed that it would be useful for the NRC to establish a process for cataloging its 10 CFR 50.59 determinations and where no prior NRC review is required (Reference 8.4, page 82). (These statements above are very close to being the exact wording in Reference 8.4).

Impact on the Yucca Mountain Project

The regulatory and guidance path that the NRC has developed, emphasizes the acceptable methods for implementing and accepting digital based control systems. NUREG-0800 Rev 4, the "key issues" analyzed and recommended in the National Research Council's report, *Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues, Final Report* (Reference 8.4) (see Section 6.1), and the Four Party Report in Section 6.7.7.3 below, all show evidence, guidance, and recommendation of this path regarding the application of digital controls.

Finally, this groundwork for the path of NRC guidance and procedure has been firmly laid and should be strongly considered by the Yucca Mountain project when implementing and recommending digital control system designs for its various facilities and processes. The project's analyses and reports relating to the repository subsurface instrumentation and controls design concepts in References 8.5, 8.52, 8.53, and 8.54, and the project's Engineering Compliance Packages support this path for the Yucca Mountain project. Several YMP analyses describing digital control system design concepts and recommendations for various operations and processes should include reference to this analysis in their future revisions and their engineering designs.

6.7.7.3 The Four Party Report

Another interesting NRC PDR document is entitled, *Four Party Regulatory Consensus Report on the Safety Case for Computer-Based Systems in Nuclear Power Plants*, (Reference 8.33). This document discusses the consensus on the elements of a safety case for acceptance of computer-based instrumentation and control (I&C) systems. It is the culmination of several years of discussions and interactions between the regulatory authorities of the United Kingdom, Canada, France, and the United States.

The NRC's Safety Case for Computer-Based Systems (Reference 8.33) establishes high level regulatory requirements common to those four nations. The Safety Case for Computer-Based Systems as applied to a safety-related system requires the licensee's documented demonstration that, 1) the correctness and completeness of the overall requirements specification has been justified in relation to the intended system function, 2) the system design has been developed to standards compatible with the safety importance of the application, 3) the delivered system satisfies all aspects of its requirements specification, and 4) adequate means and arrangements are specified which will ensure the required performance of the system throughout its operational life. The report goes on to say issues such as safety importance, defense-in-depth, system boundaries, novelty, basis of safety case, license/regulatory interface arrangements, and the need for independent assessment are very important aspects requiring consideration at the earliest stage of a project (Reference 8.33,

Section 4, pages 4 to 7). Again several of these same issues discussed throughout Reference 8.4 are a recurring theme throughout the documentation of the NRC.

For safety systems, particular emphasis is placed on the digital software aspects of the control systems. Additional detailed requirements are for high integrity regarding single failure criterion and common cause failures, a structured software development process, system design principles, complete verification and validation using both testing and static analysis, and the use of valid and controlled tools. Again, these issue are described in much greater detail in NUREG-0800 Rev 4.

Impact on the Yucca Mountain Project

The above Safety Case for Computer-Based Systems demonstration criteria discussed in detail in the Four Party Report supports the general theme presented in this analysis, that the NRC is in the process of developing regulatory guidance that support the use of digital control systems in nuclear applications. These design criteria and overall control strategies found in the Four Party Report (Reference 8.33) add additional backing to the conclusions in Section 7 of this analysis. Its presentation is easy to follow and would provides guidance that may be useful in presenting control system requirement descriptions in the YMP license application.

6.8 DIGITAL CONTROLS IN SUPPORT OF THE LICENSE APPLICATION

When discussing digital control systems in the license application, consideration of the design path to follow when digital controls are considered and implemented should be given (see Section 6.7.7.2). The LA should make it clear to the reader and approving agency, that NRC guidance has been applied correctly and thoroughly. Appropriate discussions need to show that the licensee is clearly aware of, recognizes, and understands NRC's guidance regarding the use of digital controls. License application discussions informing the NRC of the issues that are considered when determining or justifying the use of digital controls need to: 1) make clear statements that digital control system(s) should be based on "acceptance and performance criteria issues and guidelines," 2) make clear statements that a "decision or approval procedural method(s) and dedication process" needs to be considered for each control system, and 3) include reference to this and other analyses supporting repository control systems. List criteria that apply to each control system, such as defense-in-depth, common mode failure, verification and validation process, and others as presented in Sections 6.1, Section 6.7.7, and the SERs (Reference 8.3, 8.34, and 8.39).

Discussions of exact or detailed criteria, guidelines, and approval processes should not be required in the license application at this time because detail designs are not available. Discussions would also be benefited by inclusions from the SDDs descriptions, functional requirements, and design criteria as guidance to the input on the control systems. For safety-related systems, the depth of the particular discussions should be commensurate with the level of safety significance and quality affecting criteria as presented in *The Classification of the Preliminary MGDS Repository Design* (Reference 8.16).

Additional resources, expertise, and involvement by the instrument and controls discipline would benefit the license application design and the Safety Analysis Report for the YMP.

7.0 CONCLUSIONS

7.1 SUMMARY

Over the course of researching, locating and obtaining pertinent documentation for this study, three recurring themes were encountered. As if to provide additional emphasis, the same three things surfaced repeatedly in telephone conversations with a variety of individuals in the nuclear industry, ranging from instrument technicians through upper level engineering management. Of perhaps equal importance was the discovery that every one of the vendors contacted, without exception, was well aware of these three concerns and was already taking active steps to accommodate them. The three concerns, all relative to applications important to safety with ties to common mode failure, are (1) small systems will be favored by the NRC over large systems, (2) the NRC will look for specific identifiable "defense-in-depth" diversity, and (3) work should begin with the Commission as early as possible and they should be kept apprised of your activities. Each of these three items should be seriously considered during any design activities on the Yucca Mountain Project, and are addressed in more detail below.

It was interesting to note that all three of the above were presented to the Yucca Mountain Project staff in January 1998 (Attachment I). In fact, the information presented was important enough to the success of this project that specific concepts from it will be cited in the discussions that follow. It is further suggested that the reader consider the parallels that appear between the above reference and *Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues* (Reference 8.4), including the subsequent response from the NRC in *Staff Disposition of Recommendations in the National Research Council, NAS, Study on Digital I&C Systems in NPPs* (Reference 8.46).

The following recommendations are broken down into the two areas, overall control strategy and design criteria.

7.1.1 Recommendations for Overall Control Strategy

While considering the following, it is suggested that a comparison be made of the content and recommendations of Attachment I, Reference 8.3, Reference 8.39, as well as Reference 8.4. Study of these four documents has revealed a number of clear parallels, all of which provide a picture of NRC concerns and expectations during the review and qualification process of digital control technologies for use within the Yucca Mountain Project.

7.1.1.1 Minimize the Size and Complexity of Safety-Related Systems

It is recommended that the design of safety-related systems within the repository be kept as small and as simple as possible. Higher system complexity typically equates to less reliability.

The concern regarding large versus small systems also includes the risks of common mode failures. As discussed previously in Section 7, a common reason cited for this concern was the control system design practice of modular development of software, but there are other factors that also need to be considered.

During the development of software-based systems, the designer and implementor have a very valid concern regarding consistency of data. For this reason, most industrial applications prefer to rely on a limited number of large data bases which can be accessed by any number of distributed control systems. In this way, erroneous data may then be provided to several different systems, important to safety or not, that access the corrupted database.

For the system designer, the design philosophy is focused on the maximum possible avoidance of common mode errors. Recurrent comments throughout recognized information sources indicate that currently the most acceptable methods for avoiding common mode errors are: (a) redundant supervised I/O dedicated only to systems important to safety, (b) strict separation of systems important to safety and those that are not, and (c) minimize the size and complexity of each system important to safety (Attachment I; plates 8, 11, 25, 27, and 40).

7.1.1.2 Independence and Physical Separation of Systems Important to Safety

It is recommended that design of control systems apply the design strategies of system independence and physical separation of systems important to safety. The performance of safety-related functions can be protected by the physical separation between the safety system equipment and the effects of a design basis event.

7.1.1.3 Design Diversity

In order to minimize or eliminate the risks associated with single point failures and common mode failures, it is recommended that multiple levels of design diversity be provided for safety-critical digital control systems. As exemplified in many of the references, developing systems with multiple levels of diversity is a "defense-in-depth" approach that results in highly reliable systems.

Conducting the same activity three times does not constitute design diversity. Rather, there must be a genuine uniqueness among the various design elements, be it software or hardware. Design diversity leads towards more fail-safe systems.

In the case of software, design diversity could be accomplished by the use of two different software languages, or use of both ladder diagrams and structured text during the development process. In the case of hardware, design diversity is commonly achieved by

utilizing two different physical phenomena such as a motor operated valve together with an air operated pilot solenoid actuated valve. A third level of diversity, and typically that of last resort, are manual backup or bypass systems. These systems typically provide a hard-wired emergency stop push button to halt a process or activity. Acceptance and final success will be difficult to obtain unless one of the levels of design diversity provides a means for manual operation (Attachment I; plates 14, 15, 23, and 25). In the SER on Prairie Island's Station Blackout/Electrical Safeguards Upgrade Project (Reference 8.34), design diversity, redundancy, and manual backup systems were required to be implemented as a method for defense-in-depth strategy.

7.1.1.4 Regulator Partnering

It is recommended that "Regulator Partnering" with the NRC be initiated as soon as possible. The nuclear industry is no different than others in this respect. It is in the project's best interest to develop peer-to-peer contacts between the YMP's design organizations and the organization that will ultimately make the decision regarding licensing of the repository. These contacts must be made in a consistent way and should follow YMP procedures and protocol. Experience in many industries, from coal mining to operation of nuclear power plants, has been positive when the regulatory authorities were involved in selected areas of decision-making. It is in their best interest to find ways to encourage an operation to succeed, not fail. The regulators are, after all, the interpreters of "the letter versus the intent of the law." This project is especially unique because none of the participants, including the NRC, have amassed any experience in the licensing of this type of facility and everyone needs to join in the learning process.

A recent example of regulator partnering is Houston Lighting and Power's experience at South Texas, as outlined in previous Section 6.7.3. The NRC was involved in preparation of the parent national consensus standards, participated in developing the generic PLC specification, and issued the Safety Evaluation Report. The licensee has every reason to expect that the NRC's review of its own work will be favorable, subject to only the vagaries of the specific case (Attachment I; plates 5, 16, 45, and 46)

7.1.1.5 Additional I&C Design Guidance

Based on the documentation examined as part of this analysis, the following points of general design guidance can be recommended.

Where applicable, the YMP Repository I&C systems shall be based on best available digital control technologies. There is overwhelming evidence and precedence provided in this analysis and others of digital control's use in safety-related and non-safety applications in the nuclear industry, as well as safety-related applications in many other industries with extensive safety requirements (References 8.4, 8.5, 8.52, 8.53, 8.54, 8.55, 8.57, 8.58, and 8.59). There is system design criteria found in the SDDs that provide insight into the equipment requirements that may apply to the YMP design concepts and the essential use of digital based components. (References 8.37 and 8.50, and TBV-407). The long pre-closure life for the repository of many decades demands systems that will have normal characteristics

of flexibility, maintainability, and control and communication integration and multiplexing capabilities. These systems will need to be upgraded or replaced perhaps (with minimum or no disrupting impacts on existing hardware and software capabilities) several times during the project's lifetime (Reference 8.37 and 8.50). The evolution of control systems and their components is toward digital based with these characteristics. Analog controls will no longer be able to be maintained or replaced simply because of their unavailability and lack of vendor and manufacturer support, and spare parts and components will simply be no longer available.

This analysis provides, in part, a basis for concluding that digital based control technologies are and will be acceptable to the NRC for use in the proposed nuclear waste repository. The license application should make it clear to the reader and approving agency, that NRC guidance has been applied correctly and thoroughly. Appropriate discussions need to show that the licensee is clearly aware of, recognizes, and understands NRC's guidance regarding the use of digital controls. These measures will help assure the acceptance of the YMP license application (see Section 6.8).

To the extent feasible, commercial off-the-shelf (COTS) hardware and software will be used for Repository I&C systems. (See Sections 6.5 and 6.7). The Houston Lighting and Power, EPRI, and Triconex experience can be seen as a general acceptance of existing and commercially available hardware and software components. Particular attention can also be given to the SER for Prairie Island (Reference 8.34). It provides specific evidence of the use of COTS equipment, manufacturers, and consulting engineering companies. The SERs referenced in this analysis provide a valuable tool of precedence and probable basis for some of the YMP control systems design criteria and implementation requirements. They tie together the various design criteria and guidance documents listed in Section 4 of this analysis.

The control system cases studied for this analysis came from Safety Analysis Reports and Safety Evaluation Reports. They presented digital based control system descriptions and recommended or approved specific requirements. The NRC is very familiar with the subject of digital control systems. The NRC's technical acceptance and performance criteria requirements are consistent throughout the documentation presented in this analysis on the digital control system subject. To support the License Application (LA) and the Safety Analysis Report, written descriptions of these digital based control systems for operating and monitoring the repository facilities will be needed.

7.1.1.6 Further Analysis of Key Documents Needed

It is suggested that NUREG-0800 Rev 4, Chapter 7, References 8.3 and 8.39, and the document contained in Attachments I of this analysis, be analyzed further and reviewed frequently during the development of digital control systems for the repository. These documents should also provide guidance and support to the *Repository Subsurface Control Integration Plan* (Reference 8.54).

NUREG-0800 Rev. 4, Chapter 7, provides valuable insight into the NRC's regulatory processes and acceptance criteria for digital control systems. Reference 8.39 complements NUREG-0800 with descriptive examples of what is required to satisfy the approval process for both software and hardware. Attachment I offers concise advice and cautions for obtaining NRC approval for safety-related digital I&C systems. Reference 8.3 approves the basis for a design of a PLC system, thus the basis as a component for a specific safety-related application.

As indicated by the list of documents in Section 4.3 of this analysis, other NRC documents can provide additional insight and guidance into what may be expected of digitally-based control systems. Evaluation of the applicability of the documents listed in Section 4.3 should be continued.

For guidance on control system software development and application the following documents should be evaluated further: Reference 8.7, "Using Commercial Off-the-Shelf (COTS) Software in High-Consequence Safety Systems," NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems", NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems", NUREG/CR-6263, "High Integrity Software for Use in Nuclear Power Plants, Candidate Guidelines, Technical Basis, and Research Needs", NUREG/CR-6294, "Design Factors for Safety-Critical Software," NUREG-6278, "Survey of Industry Methods for Producing Highly Reliable Software," NUREG/CR-6479, "Technical Basis for Environmental Qualification of Microprocessor Based Safety-Related Equipment in Nuclear Power Plants. Risk-Screening of Environmental Stressors and a Comparison of Hardware Unavailability With an Existing Analog System," and NUREG/CR-6579, "Digital I&C Systems in Nuclear Power Plants. Risk-Screening of Environmental Stressors and a Comparison of Hardware Unavailability With an Existing Analog System."

7.1.2 Recommendations for Design Criteria

One of the purposes of this analysis is to provide background information to support the development of design concepts and recommendations for consideration for the project's System Description Documents. As such, the following sections provide recommendations to be considered in developing design concepts using digital instrumentation and control system components.

7.1.2.1 Recommended list of Applicable Codes, Standards and Regulations

Based on this analysis, the codes, standards and regulations listed in Section 4.3, Attachment I and References 8.3 and 8.39, have been identified as being potentially useful in the development of technical design guidance and design concepts for the repository. The list is not intended to be comprehensive. Further analysis will be necessary in order to determine the extent of applicability. For further listings and justification of the applicability of codes, standards, and regulations the reader should refer to the YMP MGR *Compliance Program Guidance Packages*.

Many of these Compliance Program Guidance Package documents listed in the Compliance Program Guidance Packages were developed specifically in support of commercial nuclear power plant design and regulation, and therefore, cannot be directly applied to the development of the nuclear waste repository. However, these documents also contain fundamental design criteria and practices that should be considered in the development of any highly reliable I&C systems to be used within a nuclear environment. As such, the design criteria contained within the listed codes, standards, and regulations can be evaluated, modified and adapted for use within the YMP.

7.1.2.2 General Design Basis for Repository I&C Systems

It is intended that these design basis will be supportive of the project's on-going SDD work of design concept development. The precedence of digital instrumentation and control systems in the nuclear industry as presented in this analysis should be considered when developing design concepts as applicable to repository I&C systems. The following are not intended to be inclusive of all design basis requirements.

- Safety-related I&C systems shall be fault tolerant and not subject to single-point failures. [Based on this analysis, recommendations in Attachment I, and adaptation of guidance in Reg. Guide 1.53, IEEE Std 603, IEEE Std 7-4.3.2, NUREG 0800]
- The design of safety-related I&C systems shall utilize redundant and diverse technologies to achieve system reliability requirements. [Based on this analysis, recommendations in Attachments I, Reference 8.39, and adaptation of guidance in IEEE Std 603, IEEE Std 7-4.3.2, NUREG 0800]
- Safety-related I&C systems shall be fail-safe, i.e., fail in a safe mode or state. [Based on this analysis, recommendations in Attachments I, NUREG 0800, IEEE Std 603, IEEE Std 7-4.3.2]
- To the extent feasible, safety-related I&C systems shall be independent from non-safety systems. [Based on this analysis, recommendations in Attachments I, Reference 8.39, and adaptation of guidance in IEEE Std 603, IEEE Std 7-4.3.2, NUREG 0800]

8.0 REFERENCES

- 8.1** Not Used
- 8.2** DOE (U.S. Department of Energy). 1998. *Quality Assurance Requirements and Description*. DOE/RW/-0333P, REV. 8. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management System. ACC: MOL. 19980601.0022.
- 8.3** NRC. 1998. Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute Topical Report, TR-107330. "*Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants.*" Washington, D.C.: U. S. Nuclear Regulatory Commission. TIC: 243668.

- 8.4 National Research Council 1997. *Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues*. Washington, D.C.: National Academy Press. TIC: 235537
- 8.5 DOE (U. S. Department of Energy). December 1998. *Viability Assessment of a Repository at Yucca Mountain: Preliminary Design Concept for the Repository and Waste Package*. DOE/RW-0508. Volume 2 of 5: Washington, D. C.: U. S. Department of Energy, Office of Civilian Radioactive Waste Management. Preliminary Design Concept for the Repository and Waste Package. DOE/RW-0508/V2. ACC: MOL. 19981007.0029.
- 8.6 CRWMS M&O. 1999. *Design Input Request-LADS Phase II EDA Evaluations*. LAD-SSR-99112.R. Las Vegas, Nevada: ACC: MOL. 19990209.0147.
- 8.7 LLNL (Lawrence Livermore National Laboratory) 1995. *Using Commercial-Off-the-Shelf (COTS) Software in High-Consequence Safety Systems*. UCRL-JC-122246. Livermore, California: Lawrence Livermore National Laboratory. ACC: MOL. 19980602.0042.
- 8.8 CRWMS M&O. QAP-2-0, 1999. *SS Transport & Emplacement-99 Work Package 12012383M1*, Task RPA20794. Conduct of Activitiesy Evaluation. Las Vegas, Nevada:. Activity title, *SS Transport & Emplacement-99 Work Package 12012383M1*, Task RPA20794. ACC: MOL. 19990714.0231
- 8.9 Martel, J. T. 1997. Memorandum from J. Troy Martel to Larry Lambert describing the Triconex Corporation, La Marque, Texas: Triconex Corporation. TIC: 244163.
- 8.10 Not Used.
- 8.11 CRWMS M&O. 1998. *Mined Geologic Disposal System Requirements Document*. YMP/CM-0025, Rev. 3. Las Vegas, Nevada:. CRWMS M&O. ACC: MOL. 19980520.1022.
- 8.12 Not Used.
- 8.13 (ANS) Editorial Staff. 1997. *Nuclear Power's Move to Digital I&C*. Nuclear News, 40, /3, Pages 31-32, La Grange, Illinois: American Nuclear Society. TIC: 243723
- 8.14 American Nuclear Society (ANS) Editorial Staff. Stewart, J. C. 1997. *An NRC Perspective on the Use of Commercial Off-the-shelf Software*, Nuclear News, 40/, 10, Page 43-46, La Grange, Illinois: American Nuclear Society. TIC: 243722.
- 8.15 Triconex Corporation 1997. *TRICON: Technical Product Guide, Version 9.2 Systems, Part No. 9791007-004*. Irvine, California.: Triconex. TIC: 243804
- 8.16 CRWMS M&O 1998. *Classification of the Preliminary MGDS Repository Design*. B00000000-01717-0200-00134 REV 01. Las Vegas, Nevada: CRWMS M&O. ACC: MOL. 19981103.0546.

- 8.17** Lawrence Livermore National Laboratory 1997. *Defense Against Common-Mode Failures in Protection System Design*. UCRL-JC-128414 (Preprint). Livermore, California: Lawrence Livermore National Laboratory. ACC: MOL. 19980602.0045.
- 8.18** Not Used.
- 8.19** Geddes, Bruce (ed.) 1998. *Playing it Safe*. Control Magazine., Itasca, Illinois: Putnam Publishing. <http://www.controlmagazine.com/0497/c0320497.html>. TIC: 243822.
- 8.20** Not Used.
- 8.21** Hecht, Herbert. and Wallace, D. 1996. "Project Data to Support High Integrity Software Methods," Proceedings of 1996 ANS International Topical Meeting., 1047-1051. La Grange Park, Illinois,: American Nuclear Society. TIC: 244022.
- 8.22** Not Used.
- 8.23** Triconex Corporation 1996. *TriStation 1131 Programming Software*. Irvine, California: TIC: 244291.
- 8.24** Naser, J. 1997. "Generic Qualification of Commercially Available Programmable Logic Controllers for Safety Grade Systems in Nuclear Power Plants." *ISA Proceedings, Instrumentation, Controls and Automation in the Power Industry*, pp.179-186. Research Triangle Park, North Carolina: Instrument Society of America. TIC: 243813
- 8.25** Tso, K. and Shokri, E. July, 1996. "An Integrated Environment for Development and Testing of Software Fault Tolerance Systems." *International Workshop on Computer-Aided Design, Test, and Evaluation for Dependability*, Beijing, China, China: International Academic Publishers. TIC: 243972.
- 8.26** Not Used.
- 8.27** Hecht, H. and Hecht, M. 1995. "Dependability Assessment for Decentralized Systems." *Proceedings, Second International Symposium on Autonomous Decentralized Systems*, pp.281-286, Piscataway, New Jersey: IEEE. TIC: 243799.
- 8.28** Tang, D.; Hecht, M.; An, X.; and Brill, R. 1998. "MEADep and its Application in Dependability Analysis for a Nuclear Power Plant Safety System.", *IEEE Transactions on Nuclear Science*, 45, 3: 1014-1021. New York, New York: IEEE.Symposium on Nuclear Power Systems. TIC: 244134
- 8.29** Not Used.
- 8.30** PLCOpen. 1996. *Second International Symposium, PLCs in Safety Related Applications. Cologne, Germany*. Netherlands: <http://www.plcopen.org:81/safety.htm>. TIC: 244126.

- 8.31 Moore Products. 1998. *IEC (6)1131-3 International Standard for Programmable Controllers*. Moore Process Automation Solutions. <http://www.mooreproducts.com/thismonthsfeatures/marchstopic.htm>. Moore Process Automation Solutions. TIC: 243871.
- 8.32 PLCOpen. 1998. *PLC Software Safety*. Netherlands: PLCOpen. <http://www.plcopen.org:81/safesys.htm>. TIC: 243809.
- 8.33 NRC. 1997. *Four Party Regulatory Consensus Report on the Safety Case for Computer-Based Systems in Nuclear Power Plants*. Washington, D.C.: U. S. Nuclear Regulatory Commission. TIC: 243669.
- 8.34 NRC. 1993. Safety Evaluation by the Office of Nuclear Reactor Regulation. *Review of the Load Sequencers Safeguards and Voltage Regulators in the Station Blackout/Electrical Safeguards Upgrade Project Prairie Island Nuclear Generating Plant, Unit Nos. 1 and 2 Facility Operating License Nos. DPR-42 and DPR-60 Northern States Power Company Dockets Nos. 50-282 and 50-306*. Washington, D.C.: U. S. Nuclear Regulatory Commission. TIC: 243667
- 8.35 NRC, 1999. *Facility Statistics. Arkansas Nuclear One, Unit 1*. <http://www.nrc.gov/AEOD/pib/reactors/313/a/313atxt.html>. TIC: 243795.
- 8.36 NRC 1999. *Facility Statistics. Arkansas Nuclear One, Unit 2*. <http://www.nrc.gov/AEOD/pib/reactors/368/a/368atxt.html>. TIC: 243794
- 8.37 CRWMS M&O. 1998. *Subsurface Operations Monitoring and Control System Description Document*. BCA000000-01717-1705-00001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL. 19980918.0006.
- 8.38 PLCOpen, 1998. *The IEC 1131-3 Standard.*, Netherlands: PLCOpen. <http://www.plcopen.org:81/stddscr.htm>. TIC: 243810
- 8.39 NRC. 1994. Safety Evaluation by the Office of Nuclear Reactor Regulation. *Safety Evaluation by the Office of Nuclear Reactor Regulation Related to Amendment No. 175 to Facility Operating License No. DPR-58 and Amendment No. 160 to Facility Operating License No. DPR-74*, Indiana Michigan Power Company, Donald C. Cook Nuclear Plant, Unit Nos. 1 and 2, Docket Nos. 50-315 and 50-316, January 7, 1994. Washington, D.C. U. S. Nuclear Regulatory Commission. TIC: 244379
- 8.40 Not Used.
- 8.41 Not Used.
- 8.42 Not Used.
- 8.43 Not Used.

- 8.44 NRC, 1999. *Facility Statistics: Cook-Unit 1*. Washington, D.C., NRC. <http://www.nrc.gov/AEOD/pib/reactors/315/a/315atxt.html>. TIC: 243796
- 8.45 Not Used.
- 8.46 Morrison, D. 1998. *Staff Disposition of Recommendations in NAS Study on Digital Instructionmentation and Control*. Letter from David L. MorrisonMorrison, D.L. (NRC) to L. Joseph Callan, L.J. (NRC). CRWMS M&O. ACC: MOL. 19980602.0066
- 8.47 NRC 1999. *Facility Statistics: Cook,-Unit 2*. Washington, D.C., NRC. <http://www.nrc.gov/AEOD/pib/reactors/316/a/316atxt.html>. TIC: 243797.
- 8.48 NRC, 1999. *Facility Statistics: South Texas Unit 1*. Washington, D.C., NRC. <http://www.nrc.gov/AEOD/pib/reactors/498/a/498atxt.html>. TIC: 243793.
- 8.49 Not Used.
- 8.50 CRWMS M&O. 1998. *Subsurface Safety and Monitoring System Description Document*. BCA000000-01717-1705-00015 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL. 19981111.0029
- 8.51 CRWMS M&O 1998. Q-List. YMP/90-55Q, Rev. 05, Las Vegas, Nevada: Yucca Mountain Site Characterization Project. ACC: MOL. 19980513.0132.
- 8.52 CRWMS M&O. 1998. *Digital Controls for Safety Related Systems*. BC0000000-01717-0200-00017 REV. 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL. 19980803.0619.
- 8.53 CRWMS M&O. 1998. *Subsurface Repository Integrated Control System Design*. BCAC00000-01717-0200-00003 REV. 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990104.0179.
- 8.54 CRWMS M&O. 1998. *Repository Subsurface Control Integration Plan*. BCAC00000-01717-4600-00001 REV. 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL. 19990223.0154.
- 8.55 NRC 1999. *Computer-Based Digital System Failures: December1996-March 1997*. <http://www.nrc.gov/NRC/REACTOR/DIGITAL/failure9.html>. Washington, D.C.: U. S. Nuclear Regulatory Commission. TIC: 243666.
- 8.56 Erin, L.E. 1989. *Topical Report-Eagle-21Microprocessor-BasedProcess Protection System*, WCAP-12374. Pittsburgh, Pennsylvania: Westinghouse Electric Corporation. TIC: 243805.
- 8.57 Pacific Gas and Electric Co. 1984. *Updated Final Safety Analysis Report for Diablo Canyon Units 1 & 2. Chapter 7, Instrumentation and Controls*. San Francisco, California: Pacific Gas and Electric. TIC: 243973

- 8.58** Arizona Public Service Co. 1999. *Palo Verde Nuclear Generating Station Updated Final Safety Analysis Report* for Palo Verde Nuclear Generating Station,. Vols. 1-19, Chapter 7. Phoenix, Arizona: Arizona Public Service Company. Applied For Number.TIC: 243852.
- 8.59** Northern States Power Co. 1981. *Updated Final Safety Analysis Report for Prairie Island Units 1 and 2.* Chapter 7. Minneapolis, Minnesota: Northern States Power Company. TIC: 244127.
- 8.60** Dilanni, D.C., 1986. *Letter from, D. C. Dilanni (NRC) to D. M. Musolf, concerning "Anticipated Transients Without Scram – Prairie Island Nuclear Generating Plant Unit Nos. 1 and 2"*. Washington D.C.: U. S. Nuclear Regulatory Commission. TIC: 243807.
- 8.61** Musolf, D.M., 1988. *Letter from, David Musolf to Director of Nuclear Reactor Regulation (NRC), "Description of Final AMSAC Design."* Minneapolis, Minnesota: Northern States Power Company. TIC: 243806.
- 8.62** CRWMS M&O. March 3, 1999. Input Transmittal, *Performance Confirmation Input Criteria*. Input Tracking No. EBS-SEI-99255.T. Las Vegas, Nevada.: CRWMS M&O. ACC: MOL. 19990826.0071. (This reference is in support of TBV-407 for the Performance Confirmation Data Acquisition/Monitoring System Description Document that is not baselined).
- 8.63** NRC 1999. *Facility Statistics: South Texas Unit 2.* Washington, D.C., NRC <http://www.nrc.gov/AEOD/pib/reactors/499/a/499atxt.html>. TIC: 243798.

9.0 ATTACHMENTS

- I** *Licensing of Digital Instrumentation and Control Systems*, presented to the Yucca Mountain Project by G. Johnson of Lawrence Livermore National Laboratory on January 22, 1998

ATTACHMENT I

Licensing of Digital Instrumentation and Control Systems, presented to the Yucca Mountain Project by G. Johnson of Lawrence Livermore National Laboratory on January 22, 1998

FESSP

Fission Energy and Systems Safety Program

Lawrence Livermore National Laboratory

Licensing of Digital Instrumentation and Control Systems

Presented to:
Yucca Mountain Project

Gary L. Johnson
Manager
Computer Safety and Reliability Center
January 22, 1998

Outline

- ➔ • Who we are
- How NRC makes decisions about Instrumentation & Control (I&C)
 - What strategy works
 - What technical issues NRC will focus on
 - What are the uncertainties
 - What are the important documents
 - How we could help

We have supported NRC in licensing of I&C systems for over 15 years

- Advanced light water reactor I&C review
- Standard Tech Specs for reactor I&C
- Human factors processes and design criteria
- Control room design review
- Safety parameter display systems
- Post TMI changes
- Field inspections
- Allegation resolution

9801/317 gñ

3

We developed NRC's current guidance on review of reactor I&C systems

- Major update of Standard Review Plan to address
 - Computer-based systems
 - Operational experience
 - TMI rulemaking
 - One-step licensing
- Six new Reg Guides on software engineering
- More than 30 detailed technical reports that support the guidance or evaluate specific designs
- Human factors criteria for digital control room (SEA)
 - Also participating in development of military robotics and autonomous systems
 - Virtual reality technology for safety analysis, design review, and training

9801/317 gñ

4

All of this experience and guidance is relevant to YMP licensing

- Guidance specific to YMP I&C does not exist
- NMSS does not have I&C staff
- NMSS review will almost certainly use NRR staff
- NRR staff will use reactor guidance as a starting point

9801/317 g§

5

Outline

- Who we are
- ➔ • How NRC makes decisions about I&C
- What strategy works
- What technical issues NRC will focus on
- What are the uncertainties
- What are the important documents
- How we could help

9801/317 g§

6

NRC's review is directed at making a safety judgment

- There is reasonable assurance that material can be processed and disposed of without unreasonable risk to the health and safety of the public. (10 CFR 60.31(a))
- In reaching this decision they will consider:
 - Principle design criteria for operations area (a)(1)(iii)
 - Features or components incorporated into the design for protection of the health and safety of the public (a)(1)(v)
 - Compliance with regulatory performance objectives(a)(2)
 - Compliance of quality assurance program with criteria (a)(3)

9801/317 gij

7

NRC will focus on systems important to safety

- Systems essential to preventing or mitigating accidents that could cause exposure ≥ 0.5 rem at restricted area boundary
- Review of other systems will be limited
 - Confirm safety challenges are infrequent
 - Confirm failure modes are tolerable
 - Appropriate radiation protection instrumentation
 - Appropriate performance monitoring

9801/317 gij

8

NRC will review a sample of design and implementation activities

9801/317 gij

9

Outline

- Who we are
- How NRC makes decisions about I&C
- ➔ • What strategy works
- What technical issues NRC will focus on
- What are the uncertainties
- What are the important documents
- How we could help

9801/317 gij

10

Limit what NRC must examine to reach a safety conclusion

- Minimize the number of systems important to safety
- Minimize the complexity of systems important to safety
- Minimize the integrity needed of systems important to safety
 - Higher integrity → higher confidence in performance
- Minimize potential for NRC expanding review scope

980V317 g4

11

Select safety strategy to minimize the number of systems important to safety

- Avoid depending on active systems for safety
- Reliable normal control to avoid accidents
- Systems important to safety detect abnormal conditions and prevent or limit accidents
 - Enforce safety analysis assumption
 - Detect and act upon anticipated occurrences
- Systems important to safety to confine releases from accidents

980V317 g4

12

Simple safety functions minimize complexity

- Safety should be the primary mission of systems important to safety
- Other systems can optimize performance within the safe envelope

Good implementation strategy minimizes complexity

- Systems important to safety should be as simple as possible, but no simpler
 - Simple technology
 - Simple design
 - Error tolerant
 - Fail safe
- Be careful when trading off complexity and performance
- Be careful when trading off complexity and integrity requirements
 - Redundancy
 - Testing
 - Failure tolerance

Minimize the level of integrity needed by limiting challenges

- Normal systems that:
 - Are reliable, thus minimizing the frequency of challenges
 - Have benign failure modes, thus minimizing the severity of challenges
- Systems important to safety that:
 - Minimize the challenge of failure by providing defense-in-depth
 - Minimize need for protection against natural phenomena, environmental conditions, dynamic effects of failures, fires, and explosion by careful layout and independence

Minimize review scope by working with NRC prior to submittal

- Identify reviewers
- Request review plan
- Request review criteria
- Work with them to ensure plan and criteria are reasonable

Outline

- Who we are
- How NRC makes decisions about I&C
- What strategy works
- ➔ • What technical issues NRC will focus on
- What are the uncertainties
- What are the important documents
- How we could help

NRC will focus on safety

- Are systems important to safety performing the necessary functions?
- Will systems important to safety have the necessary integrity?
- Operational reliability and performance is generally left to the licensee
 - Unless there is some safety impact
 - Unless it shakes confidence in the licensee

NRC will expect good design basis requirements

- **Functional requirements consistent with and traceable to:**
 - safety analysis
 - regulatory requirements
 - licensing commitments
 - design of interfacing systems
- **Integrity requirements consistent with importance to safety**
- **Environmental requirements consistent with safety analysis**
- **The design basis statement should be:**
 - unambiguous
 - verifiable
 - internally consistent
 - complete to support detailed design

9801/317 gij

19

Most of the review and debate usually revolves around integrity requirements

- **NRC will expect commitments to**
 - Quality hardware and software
 - Performance consistent with functional requirements
 - Reliability commensurate with importance to safety
 - Environmental qualification
 - Human factors
 - Derivation of inputs based upon direct measurements
 - Control of interaction between systems
 - Formally derived setpoints
- **NRC will expect design information that explains how commitments will be met**

The next twenty slides describe the commitments expected.
 You will need to understand the detailed criteria
 and many nuances when making and implementing commitments.

9801/317 gij

20

Effective quality assurance will be implemented

- Well defined methodical processes
 - Conformance with 10 CFR 60.152 (10 CFR 50 Appendix B) for systems important to safety
 - Qualification of commercial components for functions important to safety
- Faithful implementation of the process
- Production of quality products
- Documentation that allows independent confirmation of quality

9801/317 gij

21

Effective software engineering processes will be established

Life Cycle Activity Groups	Planning Activities	Requirements Activities	Design Activities	Implementation Activities	Integration Activities	Validation Activities	Installation Activities	Operation & Maintenance Activities
Software Management Plan Software Development Plan Software QA Plan Integration Plan Installation Plan Maintenance Plan Training Plan Operations Plan Software Safety Plan Software V&V Plan Software CM Plan	Requirements Specification <							

Process requirements

Design outputs
Process documents

Generally expected of both purpose-built and off-the-shelf software

9801/317 gij

22

System performance will be consistent with functional requirements

- **System will perform functions under full range of design basis conditions**
 - Performance will be demonstrated
 - » Validation testing
 - Success won't depend upon failure
 - Timing performance will be demonstrated
 - Systems will be "fail-safe" where practicable
- **Detected failures will actuate the protective functions**
- **Failures will not inhibit manual actuation**
- **Systems reset to a "safe" state**

Several reliability topics need to be addressed

- **Single failure criterion**
- **Completion of protective action**
- **Independence**
- **Capability for test and calibration**
- **Control of access**
- **Maintainability**
- **Identification**
- **Bypasses**
- **Reliability analysis**

No single failure will prevent safety action

- **Assuming:**
 - All undetectable failures
 - All consequential failures
 - Worst action of non-safety systems
 - » failure or designed operation
 - Quality processes prevent hardware common-mode failures
 - » diversity is encouraged nevertheless
 - Software common-mode failures will occur
 - » diversity may be required

Protective actions will go to completion without operator intervention (seal-in)

- Seal-in may incorporate some time delay provided response time requirements are met
- Time delay may be allowed to confirm validity of protective command
- Actions that don't seal-in will be justified

Independence will be ensured:

- **Between redundant parts of systems important to safety**
- **Between systems important to safety and effects of design basis events**
 - Typically addressed by equipment qualification
- **Between systems important to safety and other systems**

Three types of independence will be addressed

- **Physical**
 - Typically achieved by barriers and/or distance
- **Electrical**
 - Typically achieved by use of qualified electrical isolation devices
 - » Isolation device qualification will be established by test
- **Communications**
 - Typically achieved by selection of communications protocols

The capability to test will be provided

- Testing will be possible during operation
 - Exceptions will be justified
- Safety function (including single-failure criterion) will be retained during testing
- Test capability will be consistent with commitments made with respect to 10 CFR 60.131(a)(6)

98012317 g1

29

Design will allow control of access to I&C important to safety

- Typically provided by physical barriers
 - Locked cabinet doors
 - Cabinet door alarms
- Digital systems will consider barriers to electronic access
 - Network connections
 - Maintenance terminals

98012317 g1

30

Equipment and systems important to safety will be readily repairable

- Systems design will facilitate trouble-shooting and repair
- Digital system self-diagnostics
- Thorough procedures and training

Equipment and systems important to safety will be clearly identifiable

- By identification on drawings
- By clear marking of equipment

Operating bypasses will be automatically removed

- When bypass permissive conditions are not met, this may involve:
 - Removing bypass
 - Changing plant state to within permissive conditions
 - Initiating protective actions
- Operators will have no role in removing operational bypasses

Maintenance bypasses will not defeat safety functions

- Single-failure criterion met during bypass
- Control protective interaction still addressed during bypass
- Exceptions will be justified

Conformance with reliability goals will be demonstrated

- Both hardware and software reliability will be considered
- Note: quantitative reliability analysis by itself will not convince NRC of system reliability
 - Deterministic criteria must also be established and met

Equipment will be qualified for the design basis environments

- Normal and abnormal environments
 - Sound engineering practice and manufacturer's recommendations
- Electromagnetic environments
 - Qualification testing
- Accident and natural phenomena environments
 - Qualification testing

Human factors will be thoroughly considered

- An effective human factors engineering (HFE) program will be established
- Lessons from operation of similar systems will be investigated and considered
- Human – machine allocation will take advantage of human strengths and avoid human weaknesses
- Task analyses will be used to identify human-machine interface (HMI) characteristics
- HFE principles will be systematically applied in translating HMI requirements to detailed design
- Human error and recovery mechanisms will be identified
- Remote systems issues will be addressed
- The HMI design will be verified and validated

9801/317 g1

37

Human-machine allocation of safety functions might be a key issue

- Manual vs. automatic safety control devices
- Manual vs. automatic monitoring devices
- Manual vs. alarm devices

9801/317 g1

38

Functions important to safety act on parameters of direct interest

- Measurement characteristics will be consistent with accident analysis assumptions
- Direct measure not always possible
 - Indirect measurements will be verified to validly represent the parameter of interest

Events requiring action by systems important to safety will not prevent that action

- This is a concern when the same sensor provides information for both normal control and protection
- Sense channel failures that raise this concern may be addressed by
 - Isolation and additional redundancy
 - Data validation in the control function
 - » e.g., control on the high, low, or median sense channel

Setpoints will be established through analysis

- Adequate margin will exist between setpoints and
 - Analytical limits
 - Operating limits
- If multiple setpoints are provided for a function, the design will automatically ensure the most restrictive setpoint is always used

9801/317 gq

41

Commitments will also be expected for systems not important to safety

- Will keep operations within normal limits
 - Design basis
 - Appropriate QA and HFE programs
- Failures will be tolerable
 - Effects of action or inaction during accidents are considered
 - Effects of failures considered
 - Failures caused by actions considered
- Challenges to safety systems will be limited
 - Appropriate quality and reliability

9801/317 gq

42

You will want robust normal systems for reasons other than licensing

- Operational reliability
- Public and regulator confidence
- Many of the integrity strategies for systems important to safety can be adapted

Outline

- Who we are
- How NRC makes decisions about I&C
- What strategy works
- What technical issues NRC will focus on
- ➔ • What are the uncertainties
- What are the important documents
- How we could help

The technical issues for YMP I&C will be different

- But probably not substantially so, if a good strategy is selected
- Some of the traditional issues may be less important
- Some additional issues may arise

9801/317 gij

45

You are not required to do what NRC expects

- Whatever you do, you must provide good technical justification
- Expect NRC to carefully consider bases
- There is ongoing NRC work that may help
 - Risk-based regulation
 - Graded quality assurance requirements
 - Still in progress
 - Controversial
- The best approach is to negotiate criteria with the staff as early as possible
 - Having a good NRC reviewer is an advantage!

9801/317 gij

46

Certain non-reactor standards might offer alternative guidance

- IEC 1508, Functional safety for any I&C system
- IEC 1226, Categorization of systems important to safety
- ISA S84.01, Functional safety for process systems
- UL 1998, Qualification of computer based components
- IAEA 50-SG-D8, I&C systems important to safety
- Emerging IEC standards on centralized radiation monitoring

9801/317 gij

47

NRC has not thought much about remote systems

- They are likely to develop an interest in the human factors aspects
- Careful selection of safety strategy and system architecture may limit their interest in other design aspects
- Otherwise, expect them to independently develop acceptance and evaluation criteria

9801/317 gij

48

Outline

- Who we are
- How NRC makes decisions about I&C
- What strategy works
- What technical issues NRC will focus on
- What are the uncertainties
- ➔ • What are the important documents
- How we could help

9801/317 gij

49

A NRC review is likely to start with the Standard Review Plan for reactors

- The staff will refer to what is useful for a YMP review
- The following SRP sections are likely to be relevant
 - 7.0 & 7.0-A: Review process
 - 7.1-C: Review of safety systems
 - 7.7: Review of control systems
 - 7.9: Review of data communications
 - Branch Technical Positions 14, 17, 18, 19, & 21: Digital systems
 - Branch Technical Position 10: Electrical isolators
 - 18: Human Factors
 - 3: Environmental and natural phenomena qualification

Chapter 7 of the SRP is available at www.nrc.gov

9801/317 gij

50

The staff will also refer to Regulatory Guides that can be applied or adapted

- 1.22, 1.118 — Testing
- 1.53 — Single failure criterion
- 1.62 — Manual initiation
- 1.75 — Physical independence
- 1.105 — Setpoints
- 1.153 — Safety systems
- 1.152, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173 — Computer-based systems
- NUREG 0700 — Human factors

A bibliography of other useful references is provided
LLNL documents are available at nssc.llnl.gov/FESSP/CSRC/refs.html

9801/317 g4

51

Outline

- Who we are
- How NRC makes decisions about I&C
- What strategy works
- What technical issues NRC will focus on
- What are the uncertainties
- What are the important documents
- ➔ • How we could help

9801/317 g4

52