ornl

**OAK
RIDGE
NATIONAL
LABORATORY**

**UNION
CARBIDE**

**OPERATED BY
UNION CARBIDE CORPORATION
FOR THE UNITED STATES
DEPARTMENT OF ENERGY**

NUREG/CR-1761
NUREG/CR-1760
ORNL/NUREG/TM-396

**A Survey of Proposed
Functional Requirements for a
Disturbance Analysis and
Surveillance System**

W. H. Sides, Jr.
C. B. Oh
P. F. Knight

**DO NOT MICROFILM
COVER**

Prepared for the
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Under Interagency Agreement DOE 40-550-75

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Printed in the United States of America. Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road, Springfield, Virginia 22161

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

**DO NOT MICROFILM
COVER**

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

NUREG/CR-1760
ORNL/NUREG/TM-396
Dist. Category R1

NUREG/CR--1760

TI86 002667

INSTRUMENTATION AND CONTROLS DIVISION

A Survey of Proposed Functional Requirements For a Disturbance Analysis and Surveillance System

W. H. Sides, Jr. C. B. Oh* P. F. Knight*

*Consultant from Technology for Energy Corp., Knoxville, TN 37922.

Manuscript Completed - June 11, 1980

Date Published - October 1980

NOTICE: This document contains information of a preliminary nature. It is subject to revision or correction and therefore does not represent a final report.

Prepared for the
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, D. C. 20555
Under Interagency Agreement DOE 40-550-75

NRC FIN No. (B0438)

Prepared by the
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830
operated by
UNION CARBIDE CORPORATION
for the
DEPARTMENT OF ENERGY

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

THIS PAGE
WAS INTENTIONALLY
LEFT BLANK

HIGHLIGHTS

A program to enhance the capabilities of operators of nuclear power plants is being pursued by the U.S. Nuclear Regulatory Commission (NRC). The program includes improvements in plant monitoring, diagnostic and corrective action aids, operator-process communication, and operator training. Concerning diagnostic aids, a disturbance analysis and surveillance system (DASS) was considered which would monitor the plant for the approach or occurrence of disturbance conditions and would assist the operator in returning the plant to normal operation or to help mitigate the consequences of a failure condition or misoperation. (A disturbance condition is defined as a condition in which a physical parameter, component, system, or some other element of the plant is outside of or approaching the tolerance limits for a particular mode of operation.)

The NRC had requested Oak Ridge National Laboratory to survey the functional requirements being proposed for a DASS. In fulfilling this task, the proposed requirements were categorized according to whether they could be realized in the short term and backfitted to existing plants or whether they could be realized only in the long term by incorporation into new plant designs. In addition, several recommendations concerning DASS development were made for consideration by the NRC. Finally, the effects of human factors on a DASS were evaluated, and the results are discussed in this report.

The result of the survey indicates that the scope envisioned for a DASS ranges from the display of a few critical plant parameters to the inclusion of extensive cause-consequence analyses and comprehensive plant dynamic models to predict behavior during upset conditions. A principal recommendation from the task is that fundamental decisions be made concerning the role and responsibilities of the operator during plant disturbance conditions, particularly in rapidly developing situations, taking into account the limitations of humans under stress to handle large quantities of information. A licensing question to be answered in the application of a DASS is whether the DASS will be allowed to advise the operator to alter the function or sequence of any safety system or engineered safety feature in the course of a disturbance condition on a time scale which does not allow adequate assessment of the correctness of DASS information. The essential impact on safety is the consequence of DASS failure or misinformation.

* Consultant from Technology for Energy Corp., Knoxville, TN.

CONTENTS

	<u>Page</u>
1. INTRODUCTION	1
2. DASS FUNCTIONAL REQUIREMENTS	2
2.1 General Requirements	2
2.2 Short Term Requirements	3
2.3 Long Term Requirements	4
3. DASS HUMAN FACTORS CONSIDERATIONS	5
4. RECOMMENDATIONS	6
APPENDIX	7

1. INTRODUCTION

A program to enhance the capabilities of operators of nuclear power plants is being pursued by the U.S. Nuclear Regulatory Commission (NRC). The program includes improvements in plant monitoring, diagnostic and corrective action aids, operator-process communication, and operator training. Concerning diagnostic aids, a system to provide surveillance and diagnosis of plant disturbances is being considered. (A disturbance is a condition in which a physical parameter, component, system, or some other element of the plant is outside of or approaching tolerance limits for the particular mode of operation.) The goal of a DASS is to monitor the plant for the approach or occurrence of such conditions and to assist the operator in returning the plant to normal operation or in mitigating the consequences of a failure condition or misoperation.

This report is the result of a survey of functional requirements currently proposed for a DASS. Suggestions for the scope of a DASS range from the relatively simple and straightforward to the far-reaching and complex. No judgment as to adequacy or necessity of any requirement is made by the authors; inclusion of a requirement in this report does not imply concurrence that the requirement should be pursued in the development of a DASS. While not exhaustive, the survey is intended to indicate the scope and breadth of existing suggestions regarding DASS functions.

Some of the proposed requirements of a DASS could be realized in the short term and applied to existing plants; others may require development and be realized only by incorporation into new plant designs. In forming the composite list of suggested requirements, a principal objective of this report is to distinguish between those considered short term and those considered long term. Before specific functional requirements can be formed, however, fundamental decisions must be made concerning the operator's role and responsibility in plant operation. This point is discussed further in Sect. 4.

The design of a DASS addresses (1) the hardware and software network required for gathering extensive data from the plant and the techniques of data manipulation, and (2) the form and techniques for exchanging the information with the operator (human factors). These areas are not entirely separable; decisions concerning one affect the design of the other. To some degree, however, they may be treated separately, and are presented separately as Sects. 2 and 3 in this report.

In Sect. 4, several recommendations are made which should be considered by the NRC when reviewing and evaluating proposed DASS applications. A conceptual scheme to evaluate human factors within the context of DASS is discussed in the Appendix.

2. DASS FUNCTIONAL REQUIREMENTS

The scope envisioned for a DASS ranges from the display of a few critical plant parameters to the inclusion of extensive cause-consequence analyses and comprehensive plant dynamic models to predict behavior during upset conditions. The following criteria were used in categorizing the proposed requirements as either short term or long term. The short term requirements could be realized by the relatively simple DASS applications in existing plants. The long-term requirements may involve more extensive plant modifications (e.g., addition of sensors, design of control and safety systems, and design of control room changes) and development and verification of advanced techniques (e.g., comprehensive predictive modeling) which may limit the capability or timeliness of backfit. The division of requirements between short term and long term is subjective and, in some cases, arbitrary; a useful degree of application of some long-term requirements could be realized in the short term. Safety implications not yet identified or cost/benefit decisions may alter the placement of requirements in these lists.

The proposed requirements are presented in three lists: first, the general requirements that apply both to short-term and to long-term applications; second, the short-term requirements; and third, the long-term requirements.

2.1 General Requirements

The general requirements for a DASS, which apply both to short-term and to long-term applications, are as follows:

1. Assist the operator in diagnosing the primary cause of a disturbance and/or direct his attention to the area of the disturbance.
2. Provide timely disturbance recognition and provide information in time for corrective action to be taken.
3. Perform signal verification and data validation (e.g., by observing functionally redundant sensors, comparing interrelated parameters, and making instrument current/voltage checks).
4. Assign a priority to the information output to the operator according to its significance and the speed of response required.
5. Provide information during normal as well as off-normal plant conditions, including accidents.
6. Interact with the operator, produce information on request, and automatically produce unrequested information.
7. Adapt to a changed plant configuration when various plant equipment is out of service.

8. Be generic, modular, and expandable, as far as practicable; adapt to different types of plants.
9. Have a reliability commensurate with the safety implication of its application.

2.2 Short-Term Requirements

The list of short-term requirements is based primarily on the use of existing plant sensors and instrumentation and the plant process computer for input to DASS, although some additional instrumentation may be required. A means of display should not require a major redesign of existing control rooms, but some rearrangement or additions may be required. In addition, a short-term DASS could be applied to subsystems (e.g., feedwater) rather than plant-wide; that is, to subsystems that are statistically most troublesome or would produce the most serious consequence if misoperated.

In backfitting a DASS to an existing plant, an important consideration for its success would be operator training, understanding, and acceptance. Designing the DASS as an interactive system, which provides verified information during normal as well as off-normal conditions, would aid in achieving these goals.

The suggested short-term requirements are as follows:

1. Determine and display whether the plant (or a subsystem) is in a selected, predetermined mode of operation (e.g., run, hot standby, hot shutdown, cold shutdown). A plant mode of operation, or system state, defines the proper mode of operation of each major piece of equipment. Information to make the determination is derived from valve line-ups, flow paths, equipment status (e.g., pumps running), etc.
2. Monitor for deviations from the selected operating state.
3. Provide surveillance of subsystem configuration.
4. Assist the operator by monitoring the operating procedures when the plant is changing state (e.g., sequence of control actions).
5. Monitor the operating state with respect to the technical specifications and limiting conditions for operation (LCO), and provide the margin to the limits. Conditional alarms or warnings may also be provided on approach to limits.
6. Provide information to the operator; it should not perform any control task directly or initiate any control or safety action (some long term goals consider this as an option).
7. Analyze and filter alarms; suppress extraneous alarms (e.g., on the basis of plant mode of operation, heat and mass balances, margin to saturation).

8. Provide event sequence recording and recall.
9. Be compatible with (able to obtain information from) existing plant process computers and data acquisition systems.
10. Have some degree of self-testing capability.
11. Provide suggested corrective actions for a plant malfunction if it can be unambiguously diagnosed by the DASS.

2.3 Long-Term Requirements

The long-term requirements of a DASS could be incorporated in new plant designs. These requirements may require a greater number of sensors and a larger capability for data processing and modeling. also, they may call for a more comprehensive involvement of the DASS in routine monitoring functions, and they may have greater impact on the basic control room design. For example, such a system may be integrated into an advanced control system which utilizes disturbance analysis. Some of the long-term requirements are extensions of the short-term requirements, encompassing a larger part of the plant systems or providing analysis in greater depth. Most of the more extensive predictive model capabilities (e.g., predicting the results of intended operator actions) are included in this category. The greater the complexity of DASS analyses, the more difficult it will be for an operator to assess the correctness of the DASS analysis. For this reason, the safety implication of the use of DASS output by the operator in actions intended to mitigate the consequences of disturbance conditions may be increased. Evaluating the reliability of such systems should receive high priority.

The long-term DASS requirements are as follows:

1. Track the values and trends of operating parameters and measure their margins to limits vs the margins which should exist under the current plant operating conditions.
2. Provide an early warning of disturbances.
3. Predict the consequences of possible operator actions prior to initiation.
4. Accommodate incorrect operator actions as well as equipment malfunctions.
5. Provide the operator with appropriate corrective response action to safety related problems, and produce an alarm if the action is not accomplished.
6. Initiate corrective action if none had been initiated by the operator, or override an incorrect operator action and advise him of his error.

7. Identify suggested vs required operator responses.
8. Predict the consequences of suggested actions vs the consequences of inaction.
9. On request, justify recommended actions, i.e., provide the basis for DASS conclusions.
10. Provide disturbance cause and consequence analysis.
11. Predict the propagation of events in a sequence.
12. Provide the status of each component and subsystem on request.
13. Monitor the status of valve, control switch, and breaker positions.
14. Monitor for potential equipment problems and extrapolate interrelated problems for their effect on safety and availability.
15. Automatically account for testing and maintenance activities on equipment under surveillance.
16. Perform tests and inspections of the systems under surveillance.
17. Predict the impact of testing and maintenance on plant system operability.
18. Analyze disturbances on a plant-wide basis.
19. Incorporate detailed modeling of the plant for various off-normal situations.
20. Analyze disturbances based on a preestablished model to determine the cause, nature, consequences, and corrective action required.
21. Track the system with dynamic models during transient conditions.
22. Be integrated into the control room design.
23. Incorporate adjustment of control system setpoints into the DASS.
(In this case, the DASS would exercise a direct control function.)

3. DASS HUMAN FACTORS CONSIDERATIONS

Human engineering principles used in other technologies have not been applied effectively by the nuclear industry. Such principles apply to the interface between the operator and DASS, and between the operator and the plant controls. These principles have been developed from a large body of industrial, space, and military experience,¹⁻⁶ and they are best applied during design of a DASS.

That human engineering standards used in other industries have not been applied by the nuclear industry is verified by studies conducted by the Electric Power Research Institute (EPRI), the Nuclear Regulatory Commission (NRC), Sandia Laboratories, and other research organizations.⁷⁻¹⁰ Deficiencies in operator training, control room design, operating procedures, and improper use of instruments are cited and evaluated in these studies.

These studies note that serious accidents could result from inadequate human engineering. Nuclear safety has emphasized hardware engineering, and generally the human-machine interface and human performance have not been adequately appreciated. Human requirements should be considered early in the design process and integrated into the DASS hardware functional requirements. Such integration is necessary to fully realize the intent of the DASS in enhancing operator capability. Since the accident at Three Mile Island (TMI), industry and the NRC have responded by initiating short- and long-term solutions, including considerations of human-machine interactions as they affect reactor safety issues.

Human factors are discussed in the Appendix. A conceptual scheme and examples for establishing and evaluating human factors relative to a DASS are presented. The scheme characterizes the operator as a part of the DASS and of the DASS-assisted controls. It provides a systems perspective of DASS which integrates human requirements with machine functional requirements.

4. RECOMMENDATIONS

As a result of compiling the composite list of proposed functional requirements for a DASS and categorizing them according to short-term and long-term applications, the following recommendations are made to the NRC in considering industry's DASS activity.

1. Before designing a DASS, it is recommended that fundamental decisions be made concerning the role and responsibilities of the operator during plant disturbance conditions, particularly in rapidly developing situations, taking into account the limitations of humans in handling large quantities of information under stress conditions. Such roles may be specific to a particular plant or plant design. A general design principle which has been used in Canadian plants, for example, states that the operator should not be required to take any action during the first 15 min following the onset of a disturbance (e.g., reactor or turbine trip). In the United States, similar efforts to define the operators role are underway,^{11,12} but they are not complete.

Decisions must also be made concerning the operator's response to information made available by the DASS. The use of the information

produced by the DASS may have fundamental safety implications. The DASS (or any such analysis system) cannot analyze and predict the course of a situation which cannot be analyzed--given time--by the operators, designers, and analysts of plant systems. The DASS may, however, perform a known analysis of a disturbance more rapidly than the operators. It is the speed of the DASS in analyzing and handling complex or rapidly developing situations that potentially may benefit the operator. This implied reliance by the operator on the DASS gives the DASS its safety implication because of the difficulty of assessing the correctness of complex DASS analyses. A licensing question to be addressed in the application of a DASS, at almost any level of complexity, is whether the DASS will be allowed to advise the operator to alter the function or sequence of any safety system or engineered safety feature in the course of a disturbance condition on a time scale which would not allow adequate assessment of the correctness of DASS information. The essential impact on safety is the consequence of DASS failure or misinformation.

2. Interest has existed for some time in a system to enhance the operator's capability to keep informed in a timely manner of the conditions in a power plant and to handle off-normal (disturbance) conditions. Interest in such systems predates the events at TMI.

While these events point to the need for improvement in human-machine interactions, they should not be allowed to dominate the formulation of the scope and functions of a DASS. This activity should not be limited to one of producing a short-term remedy for shortcomings revealed at TMI. Rather, it should continue to be a comprehensive review of the interface between the operator and the plant, resulting in a phased approach to improvements in this area.

3. Prior to the events at TMI, the primary goal of a DASS was viewed as improvement of plant availability. More recently, the goal has been expanded to include improvement of plant safety. Although suggested requirements of a DASS have sometimes been categorized according to whether they address the safety goal or the availability goal, such categorization is difficult, even somewhat artificial. It is recommended that this distinction not be emphasized.

APPENDIX

HUMAN FACTORS PRINCIPLES AND APPLICATIONS

C. B. Oh

A conceptual scheme and examples for establishing and evaluating human factors relative to DASS are presented. The scheme characterizes the operator as a part of the DASS and of the DASS-assisted controls. It provides a system perspective of DASS which integrates human requirements

with machine functional requirements. Such integration is necessary to fully realize the intent of the machine functional requirements. However, many of the examples of human requirements listed here are general because the integration of the human and functional requirements generally occurs in the design stage. This integration has not been written about in DASS proposals. Nevertheless, the conceptual scheme, coupled with the examples, may be useful when human factors are considered in connection with DASS and may aid a regulatory evaluation of the effectiveness of DASS.

This analysis assumes that DASS is not directly involved with process control; it assumes that the operator carries out process control functions suggested by DASS.

Definitions

Human requirements are those placed on the interface between the operator and the DASS and between the operator and the DASS-assisted controls. Specifically, the interface may be classified in three groups useful for analysis with respect to the operator: inputs, processing, and outputs. In general, inputs consist of information received through the operator's channels (receptors). Processing involves cognitive activities, including the ability to discriminate signals, judgment, reasoning, decision making, and memory functions. Outputs are the operator's physical responses to the input information, as well as his physical responses originating independently of inputs. Inputs, processing, and outputs are defined in the following paragraphs.

Human input requirements

These are desirable characteristics which should exist at the DASS-operator and the operator-control interfaces as determined by the output mode and the signals transmitted therefrom. "Output modes" include hardware for conveying information to the operator. "Output signals" are the characteristics, e.g., content, quality, and quantity of information, transmitted via the output mode.

Human output requirements

These are desirable characteristics which enable the operator to physically respond to information (inputs). "Respond" means to manipulate both DASS controls and DASS-facilitated plant controls actuated in connection with DASS input signals.

Human processing requirements

These include desirable characteristics relating to the operator's cognitive processes and physical characteristics which enable him/her to perceive inputs, mentally process information, and physically act upon DASS or plant controls.

Human requirements are otherwise known as *human factor principles* or simply *human factors*.

In summary, three functional categories of human requirements have been defined: input, processing, and output with respect to the operator. Input and output attributes exist at the DASS-operator interface and at the operator-control interface. Processing is not involved with the interfaces, although it affects the perception of the input signals and the quality and timeliness of the responses.

Interfaces

These are locations of machine output and human input links, such as a CRT-visual link, an audio annunciator-auditory link, or an arm-control link.

Interaction

This is feedback which is the modification of an input signal caused by an output signal derived from another part of the DASS-human-control (DHC) system. Interaction will be discussed below.

Role of Human Requirements in DASS

Human requirements should be included in the stage at which specific functional design requirements are completed. They should be considered in the development of functional requirements which qualitatively describe how the DASS interacts with the operator, and the operator with the DASS-facilitated controls. For example, a possible system functional requirement may be to provide timely recognition of disturbances and their causes. In addition to a description of how disturbances and causes are to be recognized in a timely manner, there should be an explanation of how the information should be used by the operator. The desired responses (outputs) based on human factor considerations should also be described.

Functional requirements are necessary, but not sufficient, for defining a system to analyze plant disturbances. They do not describe how the operator will recognize and respond to the machine-recognized disturbances and causes. The design requirement stage must include human factor principles. Such principles are used in the selection and design of hardware and computer programs which control various machine output functions. Operating procedures may also describe both ideal and expected responses that might occur under a specified set of operating conditions.

Design criteria follow the determination of design requirements. Hardware (design, control configuration, output modes, etc.) is specified which relates to input and output. Human factor principles considered in the design requirement stage are quantified, if possible, and included in design criteria. Figure 1 illustrates the integration of human factors into the system building process.

General Conceptual Scheme

A conceptual scheme is presented to show how an operator would interface with the DASS and DASS-facilitated controls. The conceptual scheme first characterizes the DASS-human-control interface (DHC) as a one-direction flow of information (Fig. 2) that originates from the plant and terminates with an operator response:

1. Signals originate from the plant.
2. DASS detects the signals.
3. DASS processes the signals.
4. DASS communicates the information to an operator.
5. Operator detects the information via an input mode (e.g., sight, hearing, touch).
6. Operator processes the information and determines what to do.
7. Operator responds to the perceived information. In this step the operator may:
 - a. respond by actuating DASS controls,
 - b. respond by actuating plant controls,
 - c. respond to a noncontrol function,
 - d. not respond.

The entire DHC flow has been divided into groups of inputs, processes, and output functions. This division is useful in analyzing the human interfaces in greater detail than that presented in the conceptual scheme. Therefore, the divisions are made explicit for each step of the flow:

1. Output by the plant,
2. Input to DASS,
3. Processes by DASS,

Fig. 1. Role of human factors.

Fig. 2. DHC process flow.

4. Output by DASS,
5. Input by the operator,
6. Process by the operator,
7. Output by the operator.

Feedback

Simple and complex feedback exists between the modules in the DHC scheme which permits a control function on one or more of the components. Feedback is the initiation of a signal which alters or maintains an output (displayed in terms of output information) from another module in the flow. Specifically, the feedback signals which exist in DHC are identified below:

Plant-DASS

Plant sends signals to DASS, and DASS verifies and/or seeks additional information from the plant.

DASS-Human

DASS sends information to the operator. The operator verifies, seeks additional information, or terminates information being sent.

Human-Controls

In response to DASS, the operator manipulates controls where movement is verified through tactile, audio, or visual indicators on the control or on instrumentation associated with a control.

Controls-Plant

Operator-actuated control systems cause a change in plant parameter values which are observed by the operator via control instrumentation, DASS output mode, or other mode. The operator manipulates the controls until a desired variable level is achieved. In other words, the operator processes input information and provides a control response.

Control-DASS-Human (Example of a complex feedback loop)

Control movement may be detected by DASS and processed in accordance with functional requirements, and information may be transmitted to the operator. A behavior-terminating or -reinforcing signal may be presented by DASS. For example, improper movement of controls as programmed into DASS may result in a warning signal to the operator. Alternatively, proper control movement (e.g., correct sequence in control movement) may

also be detected by DASS, and a behavior reinforcing signal (e.g., green light, if indicated in human factors analysis) will be presented to the operator. The operator would respond to the signals in accordance with predefined operating procedures or discretion, if appropriate.

The diagram of the DHC feedback scheme (Fig. 3) may be useful to visualize all of the interactions involving the human in DASS.

In summary, the operator is characterized as a component in an information and process control system where he acts as a receiver, processor, and controller in flow 2 and flow 3 (F2, F3). In addition, the operator is the processor in feedback loops FB2, FB3, FB4, and FB5. Although operator processing frequently occurs in the feedback loops, it is not addressed in this operational analysis. Operator processing involves many factors which do not relate directly to DASS hardware/software functional requirements. The following partial list indicates some factors which may affect processing: training, cognitive capabilities, physical capabilities, motivation, motor skills, social-psychological skills, physical environment, perception, fatigue, quality of written procedures, and stress.

Fig. 3. DHC feedback loops.

Detailed Conceptual Scheme

Each interface may be visualized as a junction through which a physical and measurable entity traverses and causes a desired observable human response. To exemplify this concept, the single-direction flow paths are analyzed at the DASS-Human and Human-Control interfaces (i.e., F2, F3). Each interface, including the feedback processes, is considered in a complete analysis.

DASS-Human Interface (F2)

DASS processes signals received from the plant and determines the form, rate, and mode in which the information will be transmitted (Fig. 4). Since particular types of information are best suited for specific receptors (senses), a predetermined transmission mode is identified to transfer the information across the interface junction to the specific receptor. While crossing the junction, information may be lost in noise, altered because of external conditions, or lost because of the distance between the receptor and the transmission. However, if there is a clear transmission and receipt via the specific receptor, the information is processed by the operator in time t . If inputs are sufficiently diverse or occur at a rate greater than an operator's ability to process them, the following receptor response (no feedback is assumed) to the overload may occur: (1) the signals are ignored, (2) the signals are selectively processed, or (3) the signals are terminated by closing receptor ports.

Human-Control Interface (F3)

If an operator receives a clear transmission, he processes the signal within an interval of time, as previously described (Fig. 5). The appropriate mode of response is selected (e.g., arms, hands, and fingers). In connection with the ability to process DASS information and the ability to carry out a physical response, the operator actuates specific controls. Some responses involve single acts, but others involve multiple acts, including sequential acts, which must occur in a specified period of time. While crossing the human-control junction, the physical responses are subject to interference that could result in (1) inadvertent actuation of controls, (2) failure to actuate controls, (3) actuation of controls in a wrong sequence, (4) incorrect performance of an action, and (5) failure to respond within allotted times.

However, with successful and timely contact with controls, muscular forces are exerted to move controls. Coordination is also required to carry out precise adjustments subject to the following problems:

(1) the control is moved in a wrong direction, (2) the control movement is too fast or too slow, or (3) the control is made dysfunctional.

Fig. 4. DASS-Human (F2) mode receptor specificity. (Only one-direction flow is considered.)

Fig. 5. DASS-Control (F3).

A similar logic may be applied to characterize the more realistic, but complex, case involving feedback. Rate of information transmission, mode of transmission, rate of feedback flow, operator response time, noise, input mode, and sources of interference are some independent factors to be evaluated. In addition, many input modes flow into few channels, and few output modes flow into potentially many controls (Fig. 6). A balance must be derived between the input of flow and outputs so that potentially critical information queues do not build, i.e., a methodology should be developed to resolve information overload problems.

Operationalizing the Conceptual Scheme

To facilitate an evaluation of the mode-receptor interfaces, specifications may provide guidance in assessing the integrity of engineered interfaces as proposed in the design stages. Military type specifications may be considered.³ Specifications define input and output characteristics at the interface with respect to hardware. Evaluations may also include plant simulation testing to empirically evaluate design-specific interfaces. In addition, computer simulation of operator reception, processing, and response could be useful in deriving quantitative measures of the mode-receptor interface. Quantitative examples are provided below.

Fig. 6. Relationship between input receptors and output appendages.

If quantitative measures of the interfaces are not possible, then qualitative criteria based on subjective evaluations could be considered to ensure that human factor principles are met. Qualitative testing could also be used, such as a "walk through" exercise, to determine how an operator may respond under a hypothesized set of conditions. Again, plant simulators could provide qualitative indications of how an operator may behave in connection with specific interface designs. However, most likely, an evaluation of the integrity of engineered human interfaces will include both qualitative and quantitative measures.

1. Quantitative inputs

- a. Determine the rate of information displayed to the operator (the rate is the amount of information presented per unit time).
- b. Determine the maximum number of annunciators which may be actuated in a specified interval of time.
- c. Determine the sound intensity level of alarms.
- d. Determine the intensity of annunciator lights with respect to normal and abnormal operating environments likely to be encountered.
- e. Determine the maximum number of colors to be displayed on a CRT at any one time.
- f. Determine the specific colors (wave length or frequencies) to be used in CRTs for each application, e.g., important systems may be displayed in yellow if indicated through experimentation or human factor principles.
- g. Determine the "size" of LED meters and the maximum distance at which they can be read with a high probability of accuracy.
- h. Determine the minimum distance between specific components (e.g., buttons, switches, levers) and sets of components.
- i. Determine the probability that a specified signal will remain undetected under a predefined set of operating conditions.

2. Quantitative outputs

- a. Determine the maximum and minimum distances between specific DASS controls, displays, or annunciators, and DASS-assisted reactor controls.
- b. Determine the maximum or minimum forces required to actuate a switch.

- c. Determine the maximum straight-line viewing distance and the maximum viewing angle in a three-dimensional space between a display and a control rated to the display.
- d. Determine whether the quality of information displayed on a CRT, intended for an operator in a predefined region, yields a correct response by 90% or greater of the operators tested under varying conditions.

The following discussion describes examples of qualitative criteria.

1. Qualitative inputs

Most of the inputs which directly affect the operator are produced by the displays and signals in the control room. Other inputs affecting the operator, including physical and psychological environmental characteristics, are not discussed here. Criteria to be considered in design of displays and signals are as follows:

- a. The operator should be able to respond in the shortest possible time, if indicated.
- b. The operator should be able to correlate easily and quickly the qualitative audio signals with the displayed, quantitative visual information.
- c. The operator should be able to associate the appropriate control option with a specific disturbance.
- d. The operator should be able to identify the gravity of any situation from any location.
- e. The operator should be able to easily discern the plant status from a quick survey of the displays.

2. Visual displays

Visual displays are suitable for long, complex, or abstract messages. If there is no urgency, a visual display should be sufficient. Should the message require storage or repeated referrals, a visual display (preferably hard copy) is necessary. Visual displays are preferred when auditory channels are overloaded or unsuitable, when many different messages are displayed simultaneously, or when the operator is confined to one spot.

With these characteristics as guidelines, the principles for visual display are defined as follows:

- a. The message should be of an appropriate size for the distance from which it must be read.

- b. There must be proper (sufficient, but not too much) illumination.
- c. The display should be designed such that parallax does not occur due to the angle from which the instrument must be read.
- d. The display must coordinate with the entire system: the displays should be consistently located, either functionally, sequentially, or combined, e.g., sequentially within each function; and the displays should be easily and correctly identified.
- e. The display should be compatible with associated controls, i.e., adjacent or mimic layout.
- f. Displays should be compatible with the general environment.
- g. Displays should be compatible with operator cognitive characteristics.

3. Auditory signals

Auditory signals are more suitable for short, simple messages which will not be needed for future reference. They are necessary for urgent messages. Auditory messages are preferred if visual channels are overloaded, the environment is unsuitable, or the operator must change locations frequently. The auditory channel also detects a signal amid noise very well.

With these characteristics as the basis, the principles of auditory display are as follows:

- a. A signal should alert an operator regardless of his location.
- b. A signal should not be too startling.
- c. A signal should give some indication of the severity of the malfunction
- d. A signal should not convey too much information.
- e. A signal should be located in close proximity to controls.
- f. The number of false alarms should be a minimum.

Errors Due to Design of Instrumentation Requiring Sensor Perception

Many errors are due to system and component design and the required method of human response rather than to human fallibility. Some examples of system-induced errors are:

1. Poor response time due to remote location of the sensor.
2. Inability to read instruments or discern sufficient detail to effect a correct response, due to the following:
 - a. nonconformance with anthropometric standards,
 - b. illegible copy (e.g., chart recorders),
 - c. poorly scaled instruments (e.g., meters),
 - d. multiple variables per display,
 - e. too many displays and signals, especially during an emergency,
 - f. poor location (height, angle, etc.),
 - g. glare or poor illumination,
 - h. instrument failure,
 - i. too much noise.
3. False alarms.
4. Incorrect response due to inconsistent color codes.
5. Incorrect or late response due to lack of timely feedback.

Factors to be Considered in Design of System with Respect
to Operator Output

Outputs

Output by the operator results from a decision and is realized through control manipulation. Some criteria for consideration in control design are listed below:

1. Controls should be compatible with action to be produced.
2. Controls should be easily identified by coding according to:
 - a. shape,
 - b. size,
 - c. labels,
 - d. colors.

4. Controls should be arranged logically:
 - a. standardized,
 - b. separated (especially emergency controls),
 - c. sequentially (for sequential operations),
 - d. functionally (by system).
5. Controls should conform to anthropometric standards.

Controls, as the output response of the operator, depend on his senses of vision and touch. Also to be considered in the location of such controls are the physical characteristics of the operator. Because operators vary in size, strength, and agility much more than in auditory and visual abilities (which are correctable), control placement should meet much stricter standards than those for displays to accommodate a large percentage of the operator population. Therefore, principles of control design are defined as:

1. Controls should match the physical dimensions of the operator in terms of his reach (span), field of vision (dependent on height), and amount of force required.
2. Controls should be quickly accessible (not remote).
3. Controls should be easily identified.
4. Controls should be logically arranged.
5. Emergency controls should be separated and shielded to avoid accidental actuation.
6. Controls should be compatible with associated displays by being located in close proximity to them and by following a mimic layout.

Errors due to design of controls

The errors associated with the manipulation of controls to effect a desired response are as follows:

1. Substitution of one control for another due to
 - a. lack of uniform placement,
 - b. inadequate separation,
 - c. lack of coding.

2. Errors in adjustment of a given control due to
 - a. judgmental error of the required speed of movement of control,
 - b. wrong position selection on multipositional switches,
 - c. wrong sequence execution due to lack of sequential arrangement.
3. Forgetting to manipulate a control (due to remote location).
4. Wrong direction selected on two-way direction switches not conforming to stereotypes.
5. Unintentional actuation due to
 - a. controls being too nearly alike in appearance,
 - b. controls in a poor location,
 - c. necessity of maintenance.
6. Inability to reach controls.

REFERENCES

1. A. Chapnis, *Man Machine Engineering*, Wadsworth Publishing, Inc., Belmont, CA, 1965.
2. A. D. Swain and H. E. Gultman, Handbook of Human Reliability Analysis for Nuclear Power Plant Operations (Draft), SAND 79-1529, Sandia Laboratories (September 1979).
3. "Human Engineering Design Criteria for Military Systems, Equipment and Facilities," MIL-STD-1472B, Department of Defense (December 31, 1974).
4. E. Buffa, *Modern Production Management*, 4th ed., Wiley, New York, 1973.
5. O. Johansson, Wredenberg, *Disturbance Analysis System Study*, KI/Studsvuk-F11, Kollektivforskningsparterna (November 1978).
6. R. Grumbach and H. Hoermann, "On-Line Diagnosis of Plant Disturbances," Gesellschaft Fue Reaktorsicherheit, MBH, D-8046, Garching.
7. "Human Factors Review of Nuclear Power Plant Control Room Design," Electric Power Research Institute, EPRI NP-309 (March 1977).
8. A. B. Long, "Technical Assessment of Disturbance Analysis Systems," prepared for publication in the *Nuclear Safety Journal*, Electric Power Research Institute (April 1979).
9. "Human Factors Methods for Nuclear Control Room Design," Electric Power Research Insitiute, EPRI NP-1118-SY (June 1979).
10. Combustion Engineering, Inc., and Systems Controls, Inc., "On-Time Power Plant Disturbance Analysis Systems," Electric Power Research Institute, EPRI Project RP891 (June 1979).
11. "Criteria for Safety Related Operator Actions," ANS 58.8 (ANSI N660), Rev. 1, Draft 2 (March 1979).
12. W. R. Corcoran et al., "The Operator's Role and Safety Functions," a paper given at Workshop on Licensing and Technical Issues - Post TMI, sponsored by the Atomic Industrial Forum, March 9-12, 1980, Washington, D.C.; G-E Power Systems, Combustion Engineering, Inc., Windsor, Conn., TIS-6555.

NUREG/CR-1760
ORNL/NUREG/TM-396
Dist. Category R1

INTERNAL DISTRIBUTION

1. J. L. Anderson
2. S. J. Ball
3. R. S. Booth
4. N. E. Clapp, Jr.
5. F. H. Clark
6. G. F. Flanagan
7. D. N. Fry
8. P. M. Haas
9. E. W. Hagen
10. J. M. Jansen
11. E. B. Johnson
12. R. K. Kibbe
13. R. A. Kisner
14. R. C. Kryter
15. F. C. Maienschein
16. F. R. Mynatt
17. G. S. Sadowski
18. R. L. Shepard
- 19-23. W. H. Sides
- 24-25. Central Research Library
26. Document Reference Section
- 27-28. Laboratory Records Department
29. Laboratory Records, ORNL R.C.
30. ORNL Patent Section

EXTERNAL DISTRIBUTION

31. R. DiSalvo, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555
32. Office of Assistant Manager for Energy Research and Development, DOE, ORO
- 33-34. Technical Information Center, DOE
- 35-334. Given distribution in Category R1, basic list