ornl

NUREG/CR-3655
ORNL/TM-9068

OAK RIDGE
NATIONAL
LABORATORY

MARTIN MARIETTA

A Method for Analytical Evaluation of Computer-Based Decision Aids

W. B. Rouse
R. A. Kisner
P. R. Frey
S. H. Rouse

Work Prepared for the
U.S. Nuclear Regulatory Commission
under DOE Interagency Agreement 40-550-75

OPERATED BY
MARTIN MARIETTA ENERGY SYSTEMS, INC.
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

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

NUREG/CR-3655
ORNL/TM-9068
Distribution Category RX

A METHOD FOR ANALYTICAL EVALUATION OF COMPUTER-BASED DECISION AIDS

W. B. Rouse*
R. A. Kisner
P. R. Frey*
S. H. Rouse*

NRC MONITOR: J. P. Jenkins
Human Factors Branch
Division of Facility Operations

PROGRAM MANAGER: W. H. Sides, Jr.
Oak Ridge National Laboratory

PRINCIPAL INVESTIGATOR: R. A. Kisner
Oak Ridge National Laboratory

Manuscript Completed: April 1984
Date of Issue: July 1984

*Search Technology, Inc.

Work Prepared by
Search Technology, Inc.
25B Technology Park/Atlanta
Norcross, Georgia 30092
under ORNL Subcontract No. 62X-43185V
for Oak Ridge National Laboratory

Work Prepared for the
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
under DOE Interagency Agreement 40-550-75

NRC FIN No. B0438

Prepared by the
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831
operated by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under Contract No. DE-AC05-840R21400

PREFACE

This report is an outgrowth of work performed under the Oak Ridge National Laboratory (ORNL) research project Operational Aids for Nuclear Power Plant Operators. It attempts to summarize the results of two tasks of that project. In the first task, a review of operational and decision-making aids, twelve computer-based aids were analyzed with respect to their function and design. These particular aids were chosen because they added intelligence to the data collection and display process beyond merely rearranging and concentrating already existing data. Appendix A contains a summary of the data collected on these aids organized by the following topics:

1. problem definition
2. function
3. design
4. plant interface and environment
5. performance
6. operation
7. maintenance and testing
8. user training
9. documentation
10. work status

The second task developed a classification scheme and an evaluation method that would evaluate a proposed operational aid using the following criteria:

1. compliance with present and developing regulatory requirements and standards,

2. user operability,

3. system maintainability,

4. training support, and

5. documentation required for effective interface to the control room environment.

Appendix B, which contains a review of applicable U.S. Nuclear Regulatory Commission (NRC) documents and a categorization of acceptance criteria, addresses the first item; the remaining items are treated in the main body of the report. The methodology developed for classification and evaluation of operational aids builds on the results of other tasks completed under the operational aids program and cited in the text.

This report, which concludes the Operational Aids for Nuclear Power Plant Operators Program, should provide a reasonable basis for classifying and evaluating certain aspects of decision aids. The method described, however is not highly proceduralized, so the evaluator will have to exercise specific skills in judgment. The need for other extensions and refinements will likely become apparent with experience in using the proposed methodology.

CONTENTS

CONTENTS (continued)

CONTENTS (continued)

LIST OF FIGURES

LIST OF FIGURES (continued)

LIST OF ACRONYMS

ac	alternating current
ACCUM	accumulator actuation point
ADC	analog-to-digital converter
ADQ	automated data qualification
AID	alarm initiated display
AIDS	Abnormal Incident Decision Support (Atomic Energy of Canada Limited)
AIDS	Accident Identification and Display System (Wisconsin Electric Power Company)
BPO	Balance of plant operator
BWR	boiling water reactor
CANDU	Canadian natural-uranium, heavy-water-moderated and -cooled power reactors
CMM	channel malfunction monitor
CNTMT	containment
CR	control room
CRT	cathode-ray tube
CSF	critical safety function
DAP	data acquisition processor
DAS	data acquisition system
DASS	Disturbance Analysis and Surveillance System
DCP	display control processor
DCS	Display Control System (NUCLENET-1000)
DG	display generator
DMA	Diagnosis of Multiple Alarms
ECC	error checking and correction
EG&G	Idaho National Engineering Laboratory (EG&G Idaho, Inc.)
EOF	Emergency Operations Facility
EPRI	Electric Power Research Institute
EPROM	electrically programmable read-only memory
ERF	emergency response facilities
ESSS	Ebasco Safety Surveillance System
FFTF	Fast Flux Test Facility
FW	feedwater
GE	General Electric Company
GRS	Gesellschaft für Reaktorsicherheit
HALO	Handling Alarms with Logic
HFE	human factors engineering
HHSI	high head safety injection

HW	heavy water
ICC	Inadequate Core Cooling
IEEE	Institute of Electrical and Electronic Engineers, Inc.
INPO	Institute for Nuclear Power Operations
IO	input-output
IQ	information quality
IQF	information quality function
IRM	intermediate range monitor
ISOL	isolated
Kbyte	kilobyte
KTA	Standards Organization, Federal Republic of Germany
KWU	Kraftwerksunion
LHSI	low head safety injection
LOCA	loss-of-coolant accident
LOFT	loss of fluid test facility
LOSC	loss of secondary cooling
Mbyte	megabyte
MIDAS	Master Information Data Acquisition System
MTBF	mean time between failure
MTTR	mean time to repair
NDTT	nil ductility transition temperature
NRC	U.S. Nuclear Regulatory Commission
NSAC	Nuclear Safety Analysis Center
NSSS	nuclear steam system supplier
ODDS	Operational Diagnostics and Display System
P&ID	Piping and Instrumentation Diagram
PDC	program development center
PIE	Plant Incident Evaluator
PMS	performance monitoring system
PPS	Procedure Prompting System
PRA	probabilistic risk assessment
PRM	process radiation monitor
PRZR	pressurizer
psia	pounds per square inch, absolute
psig	pounds per square inch, gage
PTS	pressurized thermal shock
PWR	pressurized-water reactor
RAD	radiation
RAM	random access memory
RAU	remote analog unit
RCP	reactor coolant pressure

RCS	reactor cooling system
RG	Regulatory Guide
RDU	remote digital unit
RHR	residual heat removal
RO	reactor operator
RPS	Reactor Protection System
RPV	reactor pressure vessel
RV	reactor vessel
SAS	Safety Assessment System
SG	safety guide
SGTR	steam generator tube rupture
SPDS	safety parameter display system
SRL	Savannah River Laboratory
SRM	source-range monitor
SRO	senior reactor operator
SS	Shift Supervisor
SSPM	safety system performance monitor
SSR	safety system readiness
SSRM	safety system readiness monitor
STA	shift technical adviser
STAR	Disturbance Analysis and Surveillance System (Federal Republic of Germany)
TAF	top of active fuel
TC	thermocouple
TSC	Technical Support Center
TRU	test and reconfiguration unit
UL	Underwriters' Laboratories

ACKNOWLEDGMENTS

The authors gratefully acknowledge the contributions of many persons to the efforts reported here. Jens Rasmussen of the Riso National Laboratory provided important insights at a critical juncture of the project. Ruston Hunt and Michael Maddox of Search Technology, Inc., provided useful comments and suggestions throughout the course of the project. William Sides of Oak Ridge National Laboratory and James Jenkins of the U.S. Nuclear Regulatory Commission supplied valuable feedback during several project review meetings. All of the individuals and organizations who graciously supplied detailed information on their operational aid systems. Finally, the Institute of Nuclear Power Operations was very helpful in providing access to their Job and Task Analysis Data Base.

ABSTRACT

This report presents a proposed methodolgy that involves a two-stage process of classification and analytical evaluation of decision aids for nuclear power plant operators. The classification scheme relates any particular aid to one or more general decision-making tasks. Evaluation proceeds using a normative top-down design process based on the classification scheme and involves determining how various design issues associated with this process were resolved by the designer. The result is an assessment of the "understandability" of the aid as well as the identification of training and display requirements necessary to ensure understandability. The methodology is illustrated by applying it to the evaluation of an aid designed to support operators in recovery of critical safety functions at a pressurized-water reactor.

Two appendices are included. Appendix A contains information collected from manufacturers, developers, and users of operational aid systems. Appendix B is a review of NRC documents and guidelines that might apply to operational aids.

1. INTRODUCTION

In the wake of Three Mile Island and the subsequent requirements by the U.S. Nuclear Regulatory Commission (NRC) for the installation of safety parameter display systems (SPDSs) in all nuclear power plants (Ref. 1), electric utilities and system vendors have responded with a wide variety of SPDS alternatives. Many of these alternatives go beyond the NRC-dictated requirements and potentially provide a wider range of support for operator decision making. As a result, the considerable variety of options makes it difficult to compare and evaluate alternatives. This situation is not very different from that which exists in the military, where the variety of decision aids appears to be even greater (Refs. 2,3).

In fact, an initial survey of the alternatives might lead one to conclude that the proposed types of decision aids are substantially more numerous than the types of human decision making in need of support. This perception is, of course, due to a lack of standardization in terminology and, in some cases, rather sweeping claims by decision-aid designers. What is needed is a method for transcending the detailed engineering peculiarities of any particular aid and focusing on the nature of the general decision-making tasks supported. This report discusses such a method.

The essence of the method presented here is a two-stage process of classification and evaluation. The first stage, classification, maps any particular decision aid to one or more general decision-making tasks. The taxonomy of general decision-making tasks employed in this mapping is based on a conceptual model of human decision making (see Sect. 2). To illustrate the use of this model-based classification, four specific aids were classified: Diagnosis of Multiple Alarms (DMA), Safety Assessment System (SAS), Disturbance Analysis and Surveillance System (STAR), and Procedure Prompting System (PPS). This illustration leads to an interesting comparison of the aids, particularly in terms of the distinctions among them.

The second stage of the proposed method, evaluation, is based on a normative top-down view of a system design. In general, an aid is evaluated by first assuming that it was produced using this normative design process and then determining how the various design issues associated with this process were resolved by the designer. More specifically, an aid is evaluated in terms of the situations and tasks for which it was intended, the forms of information appropriate for each situation, the prototypical messages required to support each task, and the knowledge necessary to understand these messages. The result of evaluation is an assessment of "understandability," as well as the training and display requirements necessary to ensure understandability.

The top-down approach to classification and evaluation was chosen in order to avoid having to infer the purpose of the various attributes of any particular aid. Instead, the design objectives for the aid are used to determine the attributes that *should* be present. Given these requirements, the aid (as well as the design documentation and the designer) is then audited to determine how these attributes are realized. This approach supplies the evaluator with a series of top-down questions to be asked rather than a series of answers (i.e., the attributes of an existing aid) to be justified. In this way, as noted earlier, evaluation transcends the peculiarities of any particular aid and focuses on the extent to which decision making is actually supported.

Program Background

The NRC has sponsored a number of research programs aimed at simplifying operators' tasks and improving their performance in an effort to facilitate the safe operation of nuclear power plants under both normal and abnormal conditions. These programs include the addition of control room aids; more and better training, especially for handling emergencies; the development of better control room procedures; and increased automation. As the research program has progressed, it has become increasingly apparent that the focus should not be on the performance of the operator in isolation but rather on the functioning of the operator within the human-machine system as an entity. It is important not only to know the capabilities and limitations of the two major components--the human and the machine--but also to understand the interactions between them and the consequences of those interactions. With the human and the machine both acting properly as conceived by the system designers, the consequence is a smoothly operating plant. On the other hand, the consequence of improper performance by one component could be a serious degradation of the system that could be made worse or mitigated, depending on the response of the other component.

The Oak Ridge National Laboratory (ORNL) has been actively involved in the research of human-machine interactions since 1979, when (among other human factors programs) the Human Interactions Review Program began. The title of that program was later changed to Operational Aids for Nuclear Power Plant Operators to reflect the emphasis on real-time decision aids. The underlying theme of that research has been that the subject of human-machine interaction must be treated holistically, with the operating crew included as a system element. The program has had the overall goal of providing NRC with the technical basis for developing design requirements and review criteria, as well as assessing the improvements to plant safety for methods to enhance the capabilities of nuclear plant operators. To determine this technical basis two basic objectives were pursued: determine the role of the operating crew, and develop a method to characterize the function and effectiveness of operational aids that might be proposed for installation at nuclear power plants.

The program began by defining the operating crew's function, organization, and responses to the work environment (Refs. 4-14). Because of

the complexity of the subject and the paucity of specific research, it was necessary to build on a number of seemingly disparate research results, methods, techniques, and human-machine interface models. These indirectly related areas included operator acceptance of computerized aids (Refs. 15,16), allocation of control functions (Ref. 17-20), and modeling of human cognition (Refs. 21-23). The research in these areas has proved useful both within the Operational Aids Program and outside as well, stimulating research by others and providing useful design and evaluation tools. These findings together contribute to the first basic objective: to investigate the role of the operator.

The program has concluded by summarizing its findings relative to the second basic objective, that is, to develop a method for characterizing operational aids so that similarities and differences across aids and the meaning of those differences might be made apparent, thus paving the way for an objective evaluation of the usefulness of such aids. This report summarizes these findings in three parts: (1) presentation of the theory, the methodology, and an example of application; (2) reviewing 12 proposed and functioning computer-based operational aids for nuclear plant operators (Appendix A); and (3) reviewing NRC and other criteria and guidelines that could apply to operational aids not mandated by NRC (Appendix B). This program will allow NRC regulators to evaluate computer-based operational aids for nuclear power plant operation in order to determine the effects of an aid's proposed design on the operator's understanding of plant processes and to determine the implication of these processes on important operator decisions concerning plant safety.

2. OPERATOR DECISION MAKING

A recent survey of the decision-aiding literature (Ref. 3) concludes that virtually every aid reviewed is aimed at supporting one or more of three general decision-making tasks: (1) situation assessment, (2) planning and commitment, and (3) execution and monitoring. Figure 1 illustrates an elementary conceptual model of the basic relationships among these general tasks. Other aspects of the relationships among these tasks (e.g., iteration) are discussed in Sect. 2.1.

Situation assessment is required when the information received by an operator differs from his or her expectations in other than an acceptable manner. Unexpected deviations prompt the operator to question the validity of a priori assumptions regarding the status quo. This questioning leads to a search for an explanation of what has happened, is happening, or may happen. As "situation assessment" implies, its goal is to assess the underlying situation that produced the unexpected information.

Given an explanation of the new situation, the next general task is planning and commitment--which involves generating, evaluating, and selecting among alternative courses of action relative to criteria that reflect tradeoffs between possibly competing objectives (e.g., availability versus safety). In many engineering systems, alternative plans are readily available in terms of formal procedures for dealing with particular situations. Further, operators' training may, in effect, prescribe the course of action they will take so that alternatives need not be actively considered. However, when situations arise that were not anticipated in the design of the procedures or that are unfamiliar because they were not considered in the design of the training, operators can be required to pursue planning and commitment. In such situations, operators' decision-making and problem-solving abilities, as well as their breadth of experience, are likely to be crucial.

The third general decision-making task, execution and monitoring, involves implementing the plan selected, observing its consequences, and evaluating deviations of observed consequences from expectations. Most operator activities are dominated by execution and monitoring. The vast majority of the time, differences between observations and expectations are minor, and consequently situation assessment or planning and commitment are not required. However, when they are required (i.e., when the deviations are unacceptable), the role of the operator becomes central to ensuring continued system operations and safety.

2.1 RELATIONSHIPS AMONG DECISION-MAKING TASKS

Based on the above discussion, Fig. 1 can be modified to yield Fig. 2, which refines the description of the relationships among

Figure 1. Three general decision-making tasks.

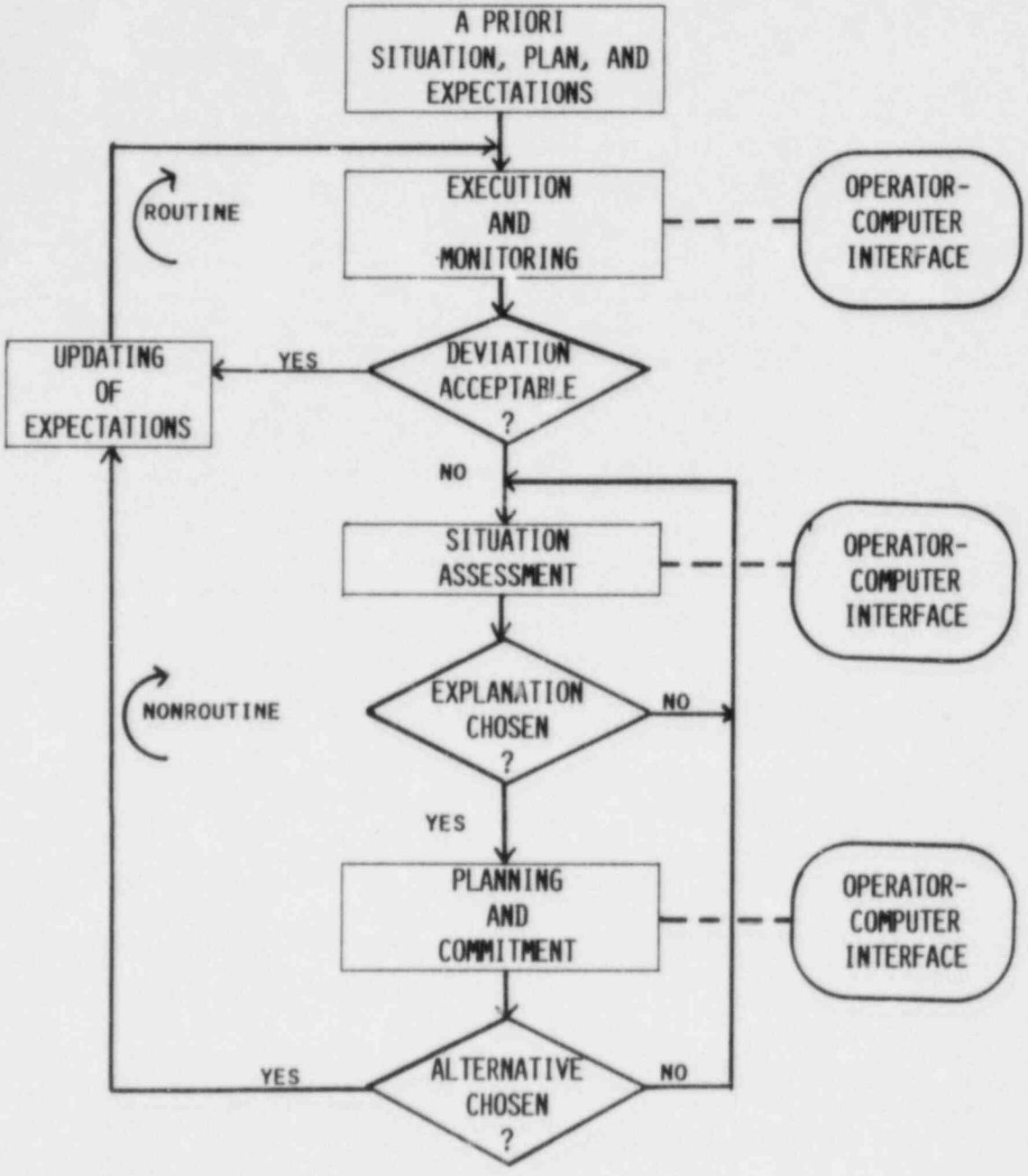


Figure 2. Relationships among decision-making tasks.

decision-making tasks. Four modifications are particularly noteworthy. First, in order to avoid the potentially misleading impression from Fig. 1 that situation assessment is always the initial decision-making task, Fig. 2 illustrates execution and monitoring as proceeding directly from the a priori situation, plan, and expectations.

A second noteworthy modification is the explicit updating of expectations. Execution of a plan seldom results in exactly what was expected; therefore, updating is required even if deviations are never sufficient to prompt situation assessment. This leads to the third important modification, namely, the discrimination between routine and nonroutine iterations through the decision-making process, as represented by the loops in Fig. 2. This distinction is useful for clarifying the differences between normal display scanning and problem-directed information seeking, where the former behavior is more pattern recognition oriented (i.e., skill based) and the latter behavior is more oriented toward problem solving (i.e., rule and knowledge based). As might be expected, these two processes require different forms of decision aiding.

The fourth and final noteworthy modification of this conceptual model of decision making involves the explicit indication of "operator-computer interface" in Fig. 2. Because the same information displays, input devices, and dialogue structure can support different decision-making tasks--albeit perhaps in different ways--the operator-computer interface is shown as common to each of the three general decision-making tasks. For example, the act of obtaining information from displays is not viewed as a separate decision-making task per se.

This distinction is quite important. It reflects the focus of this report: evaluating the extent to which an aid is likely to support operator decision making. This is quite a different focus from that found, for example, in NUREG-0700 (Ref. 24) where the emphasis is on human factors issues associated with basic display parameters rather than how the displayed information is used. While these two perspectives are different, however, they are not conflicting; in fact, they are complementary and necessary to an overall evaluation (see Sect. 4.3).

2.2 SUBTASKS OF GENERAL DECISION-MAKING TASKS

While execution and monitoring, situation assessment, and planning and commitment are the general decision-making tasks of interest, they are somewhat too broad in scope to provide the classification of decision functions needed to categorize aids. Thus these general tasks have been further subdivided as shown in Fig. 3. In contrast to Fig. 2, the ongoing processes involved with the operator-computer interface are *not* depicted in Fig. 3. This serves to emphasize the nature of utilizing the interface as a support function rather than a decision-making task.

Sections 2.2.1 through 2.2.4 elaborate upon the tasks shown in Fig. 3. To clarify the definitions presented, examples from four existing aids (DMA, SAS, STAR, and PPS) are used. These aids are considered in more

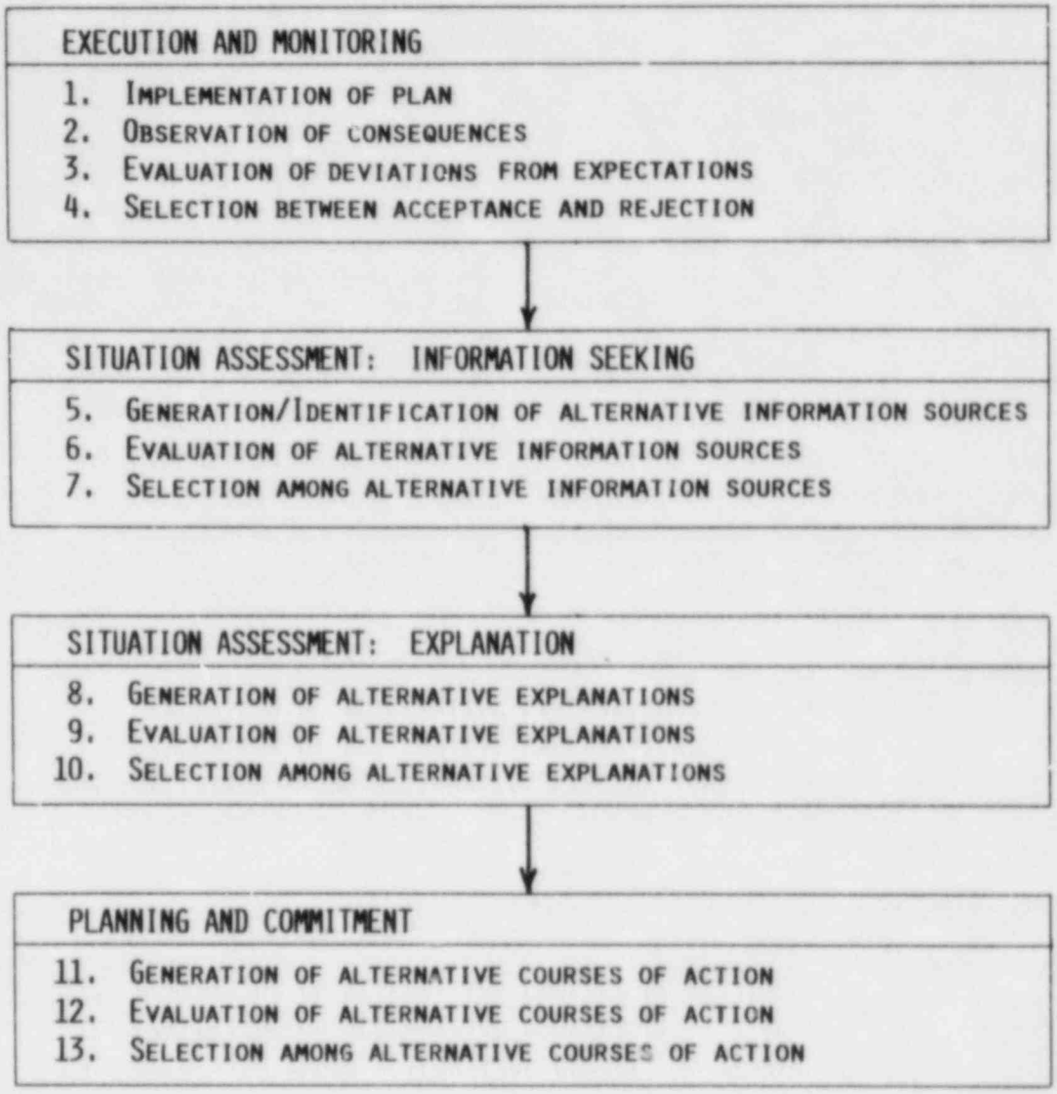


Figure 3. Subtasks of general decision-making tasks.

detail later in Sect. 3 and in Appendix A, where the complete set of functions provided by each aid is described.

2.2.1 Execution and Monitoring

Four subtasks comprise the range of operator activities during the execution and monitoring phase of decision making. As noted in Fig. 2, these subtasks apply to routine as well as nonroutine activities related to system operations.

1. Implementation of Plan. Given the a priori situation, plan, and expectations, the operator implements the plan through specific manual activities to exercise control and coordination of plant components. Typically, control activities center on communication and manipulation [e.g., supervisory senior reactor operator (SRO) instructions to other crew members reactor operators (RO) and balance of plant operators (BPO)]. Coordination activities contribute to sequencing and balancing the deployment of resources (e.g., use of crew members and alternative backup systems).

   In studying existing aids to identify aid functions that support decision tasks, it appears that plan implementation resides solely with a person and not a machine, at least for the aids reviewed in this study. Beyond the social/political constraints inhibiting development of a machine-controlled nuclear plant, all of the aids reviewed by the authors appear to be premised on the importance of the operator maintaining ultimate control. In other words, despite rapid advances in aiding technology, there does not appear to be any explicit objective of ultimately eliminating an operator's overall responsibility for managing events.

2. Observation of Consequences. Plans are normally implemented with anticipated consequences. The subtask of observing consequences involves acquiring information and correlating it with the course of action implemented. At this point the decision-making task requires further data: namely, an evaluation of deviations from expectations and a determination of whether or not these deviations are acceptable.

3. Evaluation of Deviations from Expectations. This subtask involves determining whether or not the actual course of events deviates significantly from what was anticipated to be the result of plan implementation. While some deviations are quite normal, excessive deviations indicate that something is awry (e.g., the situation assessment may have been wrong). The quantitative definition of *excessive* depends on the uncertainty associated with a priori expectations of consequences.

4. Selection Between Acceptance and Rejection. At this stage of the decision process, the operator is at the decision point of Fig. 2 that asks "deviation acceptable?" This decision represents the point at which the discrimination is made between routine and nonroutine

situations. Acceptance or rejection of the observed deviations as normal involves trading off the costs of false acceptance or rejection, in terms of the cost of incorrectly proceeding with execution and the cost of wrongly abandoning execution to pursue situation assessment and/or planning.

Given sufficient information, this selection task can be viewed as simply one of choosing the minimum expected cost alternative. However, since the probability and cost of selection errors are usually not explicit, this selection process is not very straightforward. Thus some form of computer aiding may be appropriate to assist the operator in identifying and resolving these tradeoffs and, more importantly, to assist the operator in identifying nonroutine situations.

An example of an aid that supports execution and monitoring tasks is provided in some of the functions of SAS. The top-level displays of SAS are designed to indicate "key parameters for assessing safety status of plant" and in this capacity support the observation of consequences task. In addition, three safety-related monitors of SAS support the observation, evaluation, and selection subtasks of execution and monitoring by using an algorithm to compare real-time data to data obtained from a tree-structured logic table.

2.2.2 Situation Assessment: Information Seeking

Situation assessment tasks are prompted by the observation of information that is inconsistent with expectations. One might be tempted to use the phrase "unanticipated event" to describe situations that are inconsistent with an operator's "internal model" of what should happen. However, the term *event* implies a well-defined, discrete situation--which is certainly not the only possibility. In the environment of a nuclear power control room, multiple indicators may point to an unusual situation, but the local manifestations of this situation may be distributed among many subsystems of the plant. Thus at this point in the decision-making process, the operator must often contend with complicated, redundant, and seemingly contradictory information. In fact, the widespread trend toward "symptom-based" procedures reflects a recognition of this possibility.

Situation assessment can be viewed as involving two phases: information seeking and explanation. The first phase, information seeking, includes generating/identifying, evaluating, and selecting among alternative information sources, which are usually fairly well defined in the operation of a nuclear power control room. They include displays, data bases (both hard-copy and computer-readable), and colleagues in the control room and elsewhere in the plant.

1. Generation/Identification of Alternative Information Sources. This subtask involves rapidly (and perhaps unconsciously) considering the large number of information sources available and delimiting a reasonable subset for further consideration. As an example, to enhance

DMA's primary function of detecting and locating leaks, control room radiation conditions and leak rate displays are used to generate/identify information related to overall plant safety.

2. Evaluation of Alternative Information Sources. This subtask involves assessing the relevance, information content, and resource requirements associated with alternative information sources. In the context of aids for nuclear power plant operators, this subtask could be supported by having the computer assess the relevance of the information on each display page to the critical safety functions currently being threatened. The aid could also support an operator in this subtask by assessing the consistency among multiple sources of information.

3. Selection Among Alternative Information Sources. This subtask basically involves the allocation of information acquisition resources (e.g., operator time and limited space on display pages) relative to criteria such as uncertainty reduction and resource constraints. Given the outputs of the evaluation task and explicit allocation criteria, selection in terms of resource allocation can be posed as a standard optimization problem. However, humans do not appear to approach selection quite so rigorously, partially because criteria are usually far from explicit. Selection may therefore provide opportunities for aiding.

As an illustration of one possible approach to aiding that supports situation assessment, as discussed in Sect. 3.3, STAR appears to support the operator in the processes of evaluating and selecting among alternative information sources via the function of suppressing nuisance alarms. By reducing the number of alarms requiring operator attention, STAR somewhat compensates for human limitations in making complicated tradeoffs and dealing with uncertainty and constraints.

2.2.3 Situation Assessment: Explanation

The explanation phase of situation assessment includes generating, evaluating, and selecting among alternative explanations of the situation.

1. Generating Alternative Explanations. This subtask involves synthesizing possible explanations of what has happened, is happening, and may happen. A typical a default explanation is that a priori expectations have been, are, or will be fulfilled. The process whereby other alternatives emerge appears to depend on previous experiences, pattern-recognition abilities, and perhaps creativity. Not too surprisingly, there appears to be a void in the support of this process by the prototype aids reviewed.

2. Evaluation of Alternative Explanations. This subtask involves finding the degree of correspondence between each candidate explanation and the assessed situation. For example, as discussed in Sect. 3.2, the accident identification and display system of SAS calculates a weighted factor for each of four major accidents and displays this

probability as a bar height to the operator. Beyond assessing the degree of fit (likelihood of correct selection), evaluation also includes determining the cost of both types of misevaluation (i.e., false acceptance or rejection of alternatives). In general, the cost of falsely accepting an alternative depends on the particular alternative that is consequently falsely rejected. In ambiguous situations where many alternative explanations are feasible, the interdependencies of these costs of error can be complicated and therefore difficult to keep in mind; this would seem to be a potential area for computer aiding.

3. Selection Among Alternative Explanations. This subtask involves trading off the feasible explanations in terms of the degree of correspondence with the assessed situation and the costs of false acceptance and rejection. For instance, evaluation and selection among alternative explanations are both involved in the DMA function of analyzing the need for the manual addition of emergency cooling water. If the values of all of the parameters associated with these tradeoffs were known, selection could be viewed as merely a cost-optimization problem. However, it is very unlikely that humans make selections this formally, partially because of inherent ambiguities in situations and explanations and partially due to human information processing limitations. Therefore, as with selection among information sources, selection among explanations may be an appropriate task for aiding.

2.2.4 Planning and Commitment

The planning and commitment task includes generating, evaluating, and selecting among alternative courses of action. This task differs from situation assessment primarily in terms of being purely future oriented and of emphasizing a sequence of actions over time rather than an assessment at a particular point in time. Thus situation assessment attempts to determine what has happened, is happening, or may happen, while planning and commitment focuses on manipulating future situations by choosing appropriate courses of action.

1. Generating Alternative Courses of Action. This subtask is similar to generating alternative explanations. Typically, the operator will consider courses of action that have been successfully used before in the given situation. Often, such courses of action or plans may be available in the form of procedures. Alternative plans also may emerge from experiences with analogous situations or, if absolutely necessary, from analytical study of the situation. The source of truly novel alternatives is difficult to pinpoint, which makes alternative generation a difficult process to aid; nevertheless, the subtask does support a design principle requiring sufficient system flexibility to avoid inhibiting creativity when it is needed.

2. Evaluation of Alternative Courses of Action. This subtask involves assessing or imagining the consequences of plans, both in terms of resource requirements and of impact on future situations. This type

of evaluation is usually performed by mapping (correctly or otherwise) from possible actions to previously experienced consequences. In many situations, training will enable reasonably accurate anticipation of effects of actions. When the cost of erroneous forecasting is high and time allows, evaluation of alternative actions may be performed using predictive models, perhaps the simplest operational form of which is a predictor display.

3. Selection Among Alternative Courses of Action. This subtask involves the allocation of action resources (people and equipment) subject to resource constraints and relative to criteria that assess the degree to which objectives are achieved over some planning horizon. As with the other types of selection tasks, given sufficient information, selection among alternative courses of action can be posed as a constrained optimization problem. However, the complexity of such a formulation dictates that unaided humans are very unlikely to pursue selection in this manner. While aiding may be possible, its feasibility is likely to depend totally on the amount of available information that humans have difficulty assessing and/or communicating.

An example of an aid that supports planning and commitment is PPS. It appears to support all planning and commitment tasks in determining the next attainable safe state and how to get there. As discussed in detail in Sect. 3.4, given a table of safe states and acceptable system configurations, PPS can generate, evaluate, and select a list of instructions appropriate for an off-normal condition. New instructions are generated, evaluated, and selected based on operator actions and plant response.

2.2.5 Common Attributes of Decision Making Tasks

The terms used in Fig. 3 and in Sects. 2.2.1 through 2.2.4 are designed to emphasize common attributes of operator decision-making tasks. Clearly, the three most central words in this formulation of the decision-making process are generation, evaluation, and selection relative to alternative information sources, explanations, courses of action, and deviations from expectations. Beyond these types of decisions, acquisition and integration of information as well as observation of consequences (*input*) and plan implementation (*output*) are the other activities depicted in Fig. 3. These input-output (I/O) types of activities involve less conscious decision making than generation, evaluation, and selection. Nevertheless, these I/O activities are good candidates for aiding in order to free humans to attend to generation, evaluation, and selection.

2.3 RELATIONSHIP OF PROPOSED MODEL TO EXISTING MODELS

In formulating the proposed conceptual model of the decision-making tasks required of nuclear power plant operators, the authors studied descriptions of several alternative models of operator behavior and decision making in the process-control domain. Most of these alternatives are summarized in the *Proceedings of the Workshop on Cognitive Modeling of*

Nuclear Plant Control Room Operators (Ref. 21). A recent comprehensive review of models in this area is provided by Rouse (Ref. 25). The most relevant of the alternative models are briefly reviewed in Sect. 2.3.1 and contrasted with the proposed model.

2.3.1 Alternative Models

The proposed model has many parallels with the authors' previous work on human problem solving (Ref. 26). Their most recent efforts in this area involve a model that includes three levels of decision making: recognition and classification, planning, and execution and monitoring. These three levels are virtually identical with those in Fig. 1. Depending on the type of information on which a decision is based, alternative decision processes are either state oriented or structure oriented. State-oriented processes are considered from an artificial intelligence perspective involving frames, scripts, and basic pattern recognition at the three levels. Structure-oriented processes involve basic principles, planning heuristics, and the use of functional structure at the three levels. In general, this model of human problem solving is very similar to the model proposed here; the main difference is that the proposed model explicitly considers decision functions, which is essential if decision aids are to be classified.

Rasmussen's pyramid of the mental activities encountered by the control operator in his thought processes and manual activities (Ref. 27) corresponds closely to the model proposed here. In general both models focus on relatively high-level activities dealing with planning and decision making. One major difference is that Rasmussen's model explicitly considers lower level mental activities that are only implicitly addressed by Rouse (Ref. 25). For example, the stereotyped and often unconscious mental activities that enable the operator to bypass certain intermediate states of knowledge are explicitly depicted by Rasmussen as "rule-based short cuts"; in contrast, Rouse aggregates these and other types of activities into the general category of S-rules.

A close comparison can be made with Rasmussen's model by correlating the situation assessment tasks and monitoring activities in Figs. 1 through 3 with the tasks on the left leg of Rasmussen's pyramid (i.e., knowledge-based analysis). The right leg of the pyramid corresponds to many of the planning and commitment tasks and execution tasks in the proposed model. Monitoring is an activity that Rasmussen uses to connect the right and left legs at the base of the pyramid.

Another model with close resemblance to the proposed model is discussed by Thorndyke (Ref. 28). Three general phases of the situation assessment and planning model [influenced by previous developments of Hayes-Roth (Ref. 29)] are in complete agreement with the proposed model: situation assessment (which includes both routine monitoring and anticipation/explanation of unusual events), planning, and plan execution. Thorndyke's model includes, in effect, a loop back to the planning and commitment phase of the proposed model to illustrate the iterative nature of planning as an aspect of problem solving.

A supervisory control model structure is offered by Baron (Ref. 30). Each portion of his model corresponds to some phase of decision making included in the proposed model:

1. display processor,
2. information processor,
3. situation assessor,
4. response selector/formulator, or
5. response effector.

The major distinction between Baron's model and the others discussed thus far is the control-theoretic approach to formulating and predicting operator behavior and decision making. Sheridan's model of human diagnostic behavior (Ref. 31) is similar in that it is also couched in control theory and state variables. While control-theoretic models of operator behavior have a rich history, such formulations may not be appropriate for higher level operator activities such as problem solving. It may be that control-theoretic part-task models are useful but that an overall framework premised on control-theoretic concepts is too constraining.

Siegel and Wolf (Ref. 32) have developed a "General Nuclear Power Plant Model," partially based on the Newell-Simon theory of problem solving (Ref. 33). In modeling the probability of a correct decision, Siegel and Wolf have formulated a mathematical expression that captures the difference between the ability required of the task and the operator's actual ability. Their model is noted in this discussion because it is an interesting mathematical model of the decision as an end product; however, Siegel and Wolf offer no description of the process of decision making by the operator. Thus the model is of limited use for guiding evaluation of aids for the decision-making process.

It should be emphasized, however, that this is not an inherent limitation of the Newell-Simon theory of human problem solving. Indeed, there are strong elements of this theory in the model of the authors as well as those of Rasmussen and Thorndyke. Thus, it is clear that Newell and Simon's seminal work has had a substantial impact on efforts in the cognitive modeling area.

2.3.2 An Alternative Taxonomy

Considering decision aiding from a very broad perspective, Rockmore et al. (Ref. 2) reviewed more than 75 decision aids that appeared to have potential relevance to decision making in the command and control task of target aggregation. In their categorization of aids they briefly identify the decision-making function(s) primarily supported by each aid. Five of the six functions appear similar to the proposed model:

1. information acquisition and fusion,
2. information retrieval,
3. information assessment,

4. plan generation, and
5. plan evaluation.

The sixth function, generic aid or aid in building aids, is not relevant to the issues of interest in this report.

Rockmore et al. include very limited discussion of these six decision-making functions. Thus it is unclear whether their first two functions map to the situation assessment phase of the proposed model, where information received by the operator conflicts with his or her expectations, or whether these functions correlate with the routine activity associated with observation of consequences and the evaluation of deviations from expectations. Nevertheless, there is general compatibility between these two conceptual models.

2.3.3 Summary

The proposed model of operator decision making is consistent with the various alternatives reported in the literature (Ref. 37). The proposed model does, however, provide more than just a synthesis of alternatives. It also describes operator decision making in terms of aidable functions rather than on the basis of elementary human information processing or aggregated system-oriented functions. This provides the necessary framework for classifying operator aids. The next consideration is the degree to which nuclear power plant operator decision making can be classified in terms of these general functions.

2.4 COMPARISON WITH A TAXONOMY OF OPERATOR TASKS

The conceptual model outlined earlier in this section will provide the foundation for classifying decision aids designed to assist nuclear power plant operators. Before discussing the classification of such aids, however, the proposed conceptual model should be compared with an existing taxonomy of tasks performed by nuclear power operators. Kisner and Frey (Ref. 4) have proposed such a taxonomy for both normal and emergency operations in nuclear power plants. They divide the operator's role into three general areas: supervision of plant operations, maintenance of equipment, and coordination of support activities. Kisner and Frey elaborate on tasks related to the first two areas. These tasks are listed in Fig. 4, with a numerical mapping by number to tasks listed in Fig. 3.

In general, this taxonomy is compatible with the model espoused in this report; most differences can be explained by the difference in perspective. The major thrust of the Kisner-Frey taxonomy appears to be supervisory and maintenance activities characterized by the execution and monitoring tasks found in Fig. 3. Planning is mentioned, but specific nuclear operator tasks are not elaborated on, and situation assessment tasks do not appear relevant. Thus while one might expect a taxonomy covering planning and diagnosis activities to correlate closely with the proposed conceptual model of general decision-making tasks, the two approaches to classification have different emphases: While Kisner and

1. Planning (11-13)*

2. Monitoring (1-3)

   Alarm monitoring
   State monitoring
   Signal verification
   System-operation verification
   Parameter-deviation detection

3. Controlling plant systems (1-3)

   Manual tasks
   Mechanized tasks
   Manual-automatic tasks
   Machine-automatic tasks

4. Diagnosing problems

   Problem anticipation (12)
   Problem solving (10, 13, 4)
   Reconfiguring (11-13)

5. Maintenance of equipment

   Planning (11-13)
   Testing (3, 9)
   Implementation (1, 2)
   Equipment modification (11-13, 1-4)

* Numbers in parentheses refer to decision making tasks in Figure 3.

Source: R.A. Kisner and P.R. Frey, "Functions and Operations of Nuclear Power Plant Crews," NUREG/CR-2587, ORNL/TM-8237, April 1982.

Figure 4. Taxonomy of nuclear plant operator role.

Frey focus on a systems-oriented identification of tasks, this report presents a behavior-oriented description of the process of decision making.

Additional explanations for the differences in the proposed conceptual model of decision making and the Kisner-Frey taxonomy emerge when one considers the source of information on which their taxonomy is based. Beginning with recently developed emergency procedures for nuclear power plants, Kisner and Frey infer the role of the operator "that had been intended by designers and trainers." While such an approach is an excellent way to begin an analysis of behavioral requirements, it is not sufficient because a description of the role of the operator based solely on a procedure-oriented perspective may be quite deficient with regard to planning and diagnostic behavior. As a result, the Kisner-Frey taxonomy omits the information-seeking and explanation tasks of the situation assessment phase emphasized in Figs. 1 through 3.

Kisner and Frey describe operator behavior via two conceptual models: a hierarchical model, which captures the goal-oriented behavior of the operator, and a process model, which captures fault diagnosis via procedural guidelines. Both models are applied to describing operator behavior in terms of the emergency procedures of three different types of plant. While the activities included in the models are relatively specific, they can be aggregated to correspond to the general level of tasks in Fig. 1. However, as might be expected based on the above discussion, the activities emphasize the iterative loop between planning and commitment and execution and monitoring.

In general, the conceptual model proposed in this report appears to be quite consistent with the results of the analysis of Kisner and Frey. Further, the proposed model provides significant elaboration in the area of planning and diagnosis, particularly with regard to the nonroutine aspects of a situation assessment. Thus the model encompasses a wider range of behaviors that potentially might be aided.

2.5 SUMMARY

Section 2 discusses the conceptual foundation of a scheme for classifying operator decision aids in terms of functions aided. It compares this foundation to various models discussed in the literature and to an existing taxonomy of operator tasks. At this point, the proposed conceptual model appears to be reasonable. The practicality of classifying aids on the basis of this model is the next issue of interest.

3. CLASSIFYING DECISION AIDS

To illustrate how decision aids can be classified based on the proposed conceptual model, this section considers four available decision aids. Chosen from the 20 decision aids described in the literature (most of which are summarized in Appendix A), the four aids were selected primarily because they were described with relative completeness and because they are in use in an operational facility. Furthermore, it seemed desirable to select a group of aids that supported a range of decision tasks in order to demonstrate the adaptability of the classification scheme. The aids chosen for this discussion are: DMA, SAS, STAR, and PPS.

The advantage of using the proposed model-based classification scheme is to allow one to capture the essence of the decision-making tasks supported by the functions of an aid. For each function described in the literature, a mapping was made to one or more of the decision-making tasks discussed in Sect. 2 and listed in Fig. 3. As illustrated in Sects. 4 and 5, this mapping allows evaluation issues to be raised in terms of the general decision-aiding objectives of an aid, rather than in terms of specific design features and nuances. At the end of this section, discussion focuses on a comparison of the four aids with respect to the type of decision-making tasks supported by each.

3.1 DIAGNOSIS OF MULTIPLE ALARMS (DMA)

3.1.1 Brief Description

DMA is installed at the Savannah River Laboratory (SRL) in three production reactors, where, unlike the typical nuclear power plant, plutonium is the end product of interest. The primary function of DMA is to assist the operator in identifying the location of leaks through analysis of multiple alarm patterns (Ref. 34). Rather than alarm prioritization, DMA focuses on evaluation of alarm patterns and problem location (i.e., leaks in the primary and secondary cooling systems). The aid offers advice by identifying the proper procedure for locating the leak.

3.1.2 Decision-Making Tasks Supported

Figure 5 lists the functions of DMA, and for each function a corresponding decision task is identified from the classification scheme of Fig. 3. DMA analyzes alarm patterns to detect and locate leaks. This involves three of the four subtasks of the execution and monitoring phase and accounts for the highest concentration of decision tasks, 34%. For environmental safety reasons, operators are motivated to avoid actuating the emergency core-cooling system. DMA supports operators in this task by assessing the situation relative to the need for additional manual

Function	Decision-Making Task (from Fig. 3)
1. Detect and locate leaks	1. Observation of consequences 2. Evaluation of deviations from expectations 3. Selection between acceptance and rejection
2. Analyze need for manual emergency cooling-water addition	1. Evaluation of alternative explanations 2. Selection among alternative explanations
3. Direct operators to the correct written procedure	1. Evaluation of alternative courses of action 2. Selection among alternative courses of action
4. Display leak rates	1. Generation/Identification of alternative information sources
5. Display control room radiation conditions	1. Generation/Identification of alternative information sources

Figure 5. Classification of diagnosis of multiple arms (DMA).

emergency cooling water. In this capacity DMA supports evaluation and selection among alternative explanation subtasks.

In the event of a leak, DMA will (via SRL's Automated Procedures System) advise the operator of the correct procedure to consult for controlling the problem, and an appropriate procedure is identified by evaluating and selecting among the alternative courses of action offered. Additional information is displayed to the operator regarding the rate of the leak and radiation conditions in the control room. These functions support the operator's need for information by displaying (i.e., generating/identifying) alternative sources of information.

3.2 SAFETY ASSESSMENT SYSTEM (SAS)

3.2.1 Brief Description

The motivation for developing SAS is stated as a need for an aid to assist the operator in assessing the safety status of the plant and in detecting abnormal conditions (Ref. 35). SAS is designed to fulfill the SPDS requirements for pressurized-water reactors and was developed for use at the Point Beach Nuclear Plant of Wisconsin Electric Power Company.

3.2.2 Decision-Making Tasks Supported

Figure 6 lists the functions of SAS, mapping them to one or more decision-making tasks identified in the classification scheme of Fig. 3. Most (nearly 80%) of the decision-making tasks supported by SAS can be categorized as execution and monitoring. Two functions (top-level displays and trend graphs) display output to the operator and support the observation-of-consequences subtask. Three monitor functions [safety system readiness (SSR), safety system performance, and critical safety] routinely assess the plant state, and thereby support the observation, evaluation, and selection subtasks of the execution and monitoring phase.

Two functions support the information seeking phase. The malfunction monitor acts as a filter for bad data and thus supports evaluation of alternative information sources, and the top-level message display lists the current value of key parameters among other variables related to plant state. After an off-normal condition has been detected, the three monitor displays feed information to the top-level message display in an effort to provide the operator with supporting information.

The SAS Accident Identification and Display System (AIDS) function offers a fixed set of alternative explanations (total of five) during an unusual condition. Each explanation is evaluated by AIDS and displayed to the operator, who must make the selection of explanation(s). Thus the function of AIDS can be stated simply as evaluation of alternative explanations.

Function	Decision-Making Task (from Fig. 3)
1. Top-level displays key parameters for assessing safety status of plant	1. Observation of consequences
2. Accident identification and display system	1. Evaluation of alternative explanations
3. Trend graphs of related parameters	1. Observation of consequences
4. Safety system readiness monitor to assess status of selected safety system	1. Observation of consequences 2. Evaluation of deviations from expectations 3. Selection between acceptance and rejection
5. Safety system performance monitor to assess systems sequencing and performance	1. Observation of consequences 2. Evaluation of deviations from expectations 3. Selection between acceptance and rejection
6. Critical safety function monitor which defines conditions to assess status of five critical safety functions	1. Observation of consequences 2. Evaluation of deviations from expectations 3. Selection between acceptance and rejection
7. Channel malfunction monitor to list data that have been rejected or deleted	1. Evaluation of alternative information sources
8. Top-level message display	1. Generation/Identification of alternative information sources

Figure 6. Classification of safety assessment system (SAS).

3.3 DISTURBANCE ANALYSIS AND SURVEILLANCE SYSTEM (STAR)

3.3.1 Brief Description

STAR was developed with a perspective slightly different from the previously described systems. The operator's fault-diagnosis activity is supported to enhance plant availability and safety (Refs. 36, 37). Developed for use at the Grafenrheinfeld pressurized-water reactor in the Federal Republic of Germany, STAR is an example of a "next-generation" SPDS, namely, a disturbance analysis and surveillance system (DASS).

3.3.2 Decision-Making Tasks Supported

Figure 7 maps the functions of STAR to the decision-making tasks outlined in Fig. 3. Like SAS, the highest percentage of decision-making tasks supported by STAR occur in the execution and monitoring phase. Terms such as *status surveillance, availability and operability*, and *verification* imply such tasks as observation of consequences, evaluation of deviations from expectations, and selection between acceptance and rejection.

Approximately 30% of the decision-making tasks supported involve the situation assessment phases concerning alternative information sources and explanations. The primary aid functions are concerned with "determine primary cause/plant state" and "suppress nuisance alarms."

The planning and commitment activity accounts for 20% of the decision-making tasks supported by STAR. Generation, evaluation, and selection among alternative courses of action are all represented in these functions. Implementation of cause-consequence diagrams by STAR enables it to "determine possible consequences" and "predict system behavior," which relate to the planning phase of decision making. That the automated procedural guide offers support in selecting an appropriate course of action with respect to small loss-of-coolant accidents (LOCAs) is implied in the function description.

3.4 PROCEDURE PROMPTING SYSTEM (PPS)

3.4.1 Brief Description

The Hanford Engineering Development Laboratory developed two aids for use in a liquid-metal fast-breeder reactor and has implemented them on a subsystem of the fast flux test facility (FFTF) (Ref. 38). Based on Rasmussen's model of operator behavior in large process control systems (Ref. 39) these aids have been designed to support nuclear operators in assessing the status of the plant and to guide operator actions during off-normal conditions. The system currently consists of two major components which will eventually be integrated: PPS and Master Information Data Acquisition System (MIDAS).

Function	Decision-Making Task (from Fig. 3)
1. Status surveillance of the process during normal and disturbed operation	1. Observation of consequences 2. Generation/Identification of alternative information sources
2. Availability and operability indication of automatic functions	1. Observation of consequences 2. Evaluation of deviations from expectations 3. Selection between acceptance and rejection
3. Verification of operation sequence of safety systems (post trip	1. Observation of consequences 2. Evaluation of deviations from expectations 3. Selection between acceptance and rejection
4. Determination of the primary cause of a disturbance	1. Evaluation of alternative explanations
5. Suppression of nuisance alarms	1. Evaluation of alternative information sources 2. Selection among alternative information sources
6. Determination of possible consequences of propagation of the disturbance	1. Generation of alternative courses of action 2. Evaluation of alternative courses of action
7. Surveillance of mass, energy, and anomalous plant states	1. Evaluation of alternative explanations
8. Surveillance of characteristic curves for components to obtain information about permissible operation of components	1. Evaluation of alternative explanations
9. Prediction of the behavior of systems or components by means of simulation models	1. Generation of alternative courses of action 2. Evaluation of alternative courses of action
10. Verification of data by consistency checks of instrumentation	1. Observation of consequences 2. Evaluation of deviations from expectations 3. Selection between acceptance and rejection
11. Annunciation of unanticipated circumstances	1. Evaluation of deviations from expectations 2. Selection between acceptance and rejection
12. Automated operation manual to guide operators through small loss of coolant accidents	1. Selection among alternative courses of action

Figure 7. Classification of disturbance analysis and surveillance system (STAR).

3.4.2 Decision-Making Tasks Supported

Figure 8 maps system functions to the proposed classification scheme (Fig. 3). MIDAS is primarily a data base maintaining information regarding plant status; it supports the necessary documentation and queries for maintenance of plant subsystems and components. The many objectives cited for MIDAS all focus on supporting the operator's need for information that will be used in decision making. Thus the classification of MIDAS tends to fall under one category, generation/identification of alternative information sources.

PPS is more than a data base; it assesses (or has access to) current plant status and, given an off-normal condition, can predict the next attainable safe state. In addition, the system generates appropriate procedures for the operator to execute and monitors operator actions for assessing new plant status. New procedures will be generated depending on the actions taken by the operator. These relatively sophisticated functions are distributed mostly across two decision tasks: execution and monitoring (33% of the system's decision tasks) and planning and commitment (33%). In assessing plant status, PPS also accounts for evaluation and selection among alternative explanations (23% of the system's decision tasks).

PPS demonstrates the preliminary feasibility of an expert system interacting with human operators in the control room. The lube-oil system for one of the main heat transport pumps on FFTF, for example, was modeled and run with PPS. Future work will concentrate on integrating MIDAS and PPS.

One of the unique aspects of PPS is reliance on a conceptual framework of operator behavior from a cognitive perspective, namely, adaptation of Rasmussen's model, to formulate the basis for system design. Another important distinction of PPS is the level of computer involvement, which, compared with the other aids included in this section, more closely attains the function of advisor/expert. The greatest limitation of the system is that it has not been tested on a full-scale system.

3.5 COMPARISON OF AIDS

Figure 9 provides a comparison of the above decision aids based on the proposed model-based classification. The check marks shown in each column were drawn from Figs. 5 through 8, which were generated by studying the documentation for the aids and using engineering/behavioral judgements. The fractions shown in Fig. 9 are simply the relative proportion of check marks in each of the four main categories.

SAS has relatively few functions supporting the explanation or the planning and commitment phase, whereas STAR and DMA are more evenly distributed across all tasks. The problem-solving perspective of STAR is naturally related to explanation and planning and commitment tasks, which are in fact supported by the cause-consequence diagrams used to model

Function	Decision-Making Task (from Fig. 3)
MIDAS	
PROVIDE INFORMATION REGARDING PLANT COMPONENT FUNCTIONS AND RELATIONSHIPS; STATUS OF PLANT WORK REQUESTS	1. GENERATION/IDENTIFICATION OF ALTERNATIVE INFORMATION SOURCES
PPS (LIMITED APPLICATION):	
1. IDENTIFY NEXT SAFE STATE	1. EVALUATION OF ALTERNATIVE EXPLANATIONS 2. SELECTION AMONG ALTERNATIVE EXPLANATIONS
2. PROVIDE SERIAL LIST OF INSTRUCTIONS TO OPERATOR FOR ANY COMPONENT FAILURE OR CHANGE OF STATE	1. GENERATION OF ALTERNATIVE COURSES OF ACTION 2. EVALUATION OF ALTERNATIVE COURSES OF ACTION 3. SELECTION AMONG ALTERNATIVE COURSES OF ACTION
3. TAKE INTO ACCOUNT ACTION TAKEN AND RESPOND WITH "NEW" PROCEDURE (VIA NO. 3)	1. OBSERVATION OF CONSEQUENCES 2. EVALUATION OF DEVIATIONS FROM EXPECTATIONS 3. SELECTION BETWEEN ACCEPTANCE AND REJECTION

Figure 8. Classification of procedure prompting system (PPS).

DECISION-MAKING TASKS	DMA	SAS	STAR	PPS
EXECUTION AND MONITORING	.34	.79	.50	.33
1. IMPLEMENTATION OF PLAN				
2. OBSERVATION OF CONSEQUENCES	✓	✓	✓	✓
3. EVALUATION OF DEVIATIONS FROM EXPECTATIONS	✓	✓	✓	✓
4. SELECTION BETWEEN ACCEPTANCE AND REJECTION	✓	✓	✓	✓
SITUATION ASSESSMENT: INFORMATION SEEKING	.22	.14	.17	.11
5. GENERATION/IDENTIFICATION OF ALTERNATIVE INFORMATION SOURCES	✓	✓	✓	✓
6. EVALUATION OF ALTERNATIVE INFORMATION SOURCES		✓	✓	
7. SELECTION AMONG ALTERNATIVE INFORMATION SOURCES			✓	
SITUATION ASSESSMENT: EXPLANATION	.22	.07	.12	.23
8. GENERATION OF ALTERNATIVE EXPLANATIONS				
9. EVALUATION OF ALTERNATIVE EXPLANATIONS	✓	✓	✓	✓
10. SELECTION AMONG ALTERNATIVE EXPLANATIONS	✓			✓
PLANNING AND COMMITMENT	.22	--	.21	.33
11. GENERATION OF ALTERNATIVE COURSES OF ACTION			✓	✓
12. EVALUATION OF ALTERNATIVE COURSES OF ACTION	✓		✓	✓
13. SELECTION AMONG ALTERNATIVE COURSES OF ACTION	✓		✓	✓

Figure 9. Comparison of decision aids.

plant behavior. DMA supports the planning and commitment task by providing advice to the operator in the form of procedure identification.

One distinction shared by DMA and SAS is their lack of predictive technologies. The state orientation of SAS and the reliance of DMA on logic trees and decision tables limit support of problem-solving tasks such as determining the cause of an unusual condition and predicting the consequences (plant behavior) of alternative courses of action.

The lack of functions to support plan implementation is a noteworthy limitation on the part of all of these operational aids. While the operator has primary responsibility for the manipulation of controls, man-machine task allocation with respect to plan implementation is not addressed. However, PPS demonstrates the feasibility of human-computer interaction, with comparatively more emphasis on computer advising in the planning and commitment task as well as in execution and monitoring. While plan implementation still resides with the operator, the system can account for operator actions and identify errors and can generate, evaluate, and select new procedures based on previously executed steps.

One caveat should be mentioned regarding the tasks of generating alternative courses of action and alternative explanations. The functions of most operational aids are little more sophisticated than look-up tables or logic trees. For such systems, the responsibility to generate new or truly unusual approaches will most likely reside with the operator. At the other end of the spectrum of prototype aids, the development of PPS demonstrates the feasibility of implementing software techniques for generating, evaluating, and selecting proceduralized steps to be executed by the operator. The degree of involvement on the part of the computer in terms of plant operations appears far more extensive than that of currently installed decision aids and suggests promising change for future aid design.

4. AN ANALYTICAL APPROACH TO EVALUATION

4.1 OVERALL APPROACH

The purpose of classifying a decision aid in the manner prescribed in Sect. 2 and illustrated in Sect. 3 is to set the stage for evaluation. Ideally, evaluation should begin with an analytical assessment of the aid and culminate in empirical validation of the aid's having achieved the design objectives pursued (i.e., successful support of the decision-making tasks of interest). However, the scope of this project limits the evaluation in this report to analytical rather than empirical methods. A further reason for this limitation is the fact that other recent efforts in the industry have produced a comprehensive methodology for empirical evaluation (Ref. 40).

Thus the overall approach presented in this report is purely a paper evaluation by a knowledgeable analyst, based mainly on design documentation as well as the additional information specified in this section. As a result, all conclusions must be drawn solely on the basis of careful examination of the aid, in terms of both design intentions and the product eventually realized.

One could argue that such an analytical evaluation is inherently limited in that design concepts and details may be reviewed but not tested. In a sense, an analytical evaluation can *verify* the tenability of a design but cannot *validate* the design in terms of having achieved the design objectives. Nevertheless, analytical evaluation can be a very efficient means of providing an assessment of an aid's potential for effectiveness.

Analytical evaluation can be very straightforward. If an analytical process such as developed by Frey and coworkers (Ref. 41) has been used to design the aid and the use and results of that process are well documented, then one need only audit the lines of reasoning and resulting design decisions from which the aid emerged. Unfortunately, such information is seldom available. The evaluation problem therefore becomes one of attempting to verify that a design is consistent with objectives that are usually only vaguely defined.

As stated, this is an almost impossible task. However, it is feasible if a design framework can be developed such that any aid can be viewed as if it had been designed using this framework. The remainder of this section describes such a framework as well as a process for using it for evaluation.

4.2 DESIGN FRAMEWORK

One must infer the designer's intentions to develop a design framework that can be reasonably assumed to reflect the (perhaps implicit) process pursued by a designer. Sections 2 and 3 of this report provide a strong basis for arguing that there are only 13 general decision-making tasks that an aid can support. Therefore, this section proceeds with the assumption that the designer of an aid intended to support 1 or more of these 13 general tasks.

Based on design documentation, and perhaps discussions with the designer, one can classify a designer's intentions in terms of support of one or more of the tasks in Fig. 3. The evaluative question then becomes whether or not the resulting aid provides the information necessary to perform the task(s). While it is not feasible within a general framework to specify the particular variables (e.g., which pressures and temperatures) that must be presented, it is possible to consider the types and forms of required information.

4.2.1 Types of Situations

One must define the situations in which the aid is likely to be employed to identify tasks and determine information requirements. For evaluation, one can use design documentation (and perhaps inquiries to the designer) to define these situations. Three general classes of situations are of interest. These classes can be described in terms of their *familiarity* and *frequency*, of which there are three meaningful combinations:

1. familiar and frequent,
2. familiar and infrequent, and
3. unfamiliar and infrequent.

Most situations are *familiar and frequent*. They are familiar in that the possibility of their occurrence has been anticipated. They are frequent in the sense that considerable experience is gained in dealing with them. For such situations, decision makers usually "know" what to do; when they observe the situation, their course of action is apparent. For example, upon observing a high pressure difference across the demineralizer filters in the condensate system in a nuclear power plant, the operator can immediately identify the situation as one or more clogged filters. (As an example from everyday life, a light that suddenly goes off will prompt immediate replacement of the bulb rather than an elaborate probe of the electrical system.)

Familiar and infrequent situations usually do not allow for such immediate action because the persons involved do not have much experience with these types of situations (even though the possibility of their occurrence was anticipated). As a result, a person may immediately hypothesize a course of action but collect a variety of information before pursuing it. As an example, a high-radiation alarm for the steam generator blowdown line in a pressurized-water reactor will quickly lead

to the hypothesis that a steam generator tube has ruptured. However, an operator will do considerable checking before pursuing the course of action appropriate for this situation. As an example from everyday life, if the only response is a weak "click" upon turning on the ignition of one's car, the hypothesis immediately chosen is likely to be a battery failure. Nevertheless, the driver will perform various tests before purchasing a new battery.

Unfamiliar and infrequent situations are those that are unanticipated by the decision maker and, by definition, seldom if ever previously experienced. As a result, the appropriate course of action is not at all obvious. Further, available procedures may be inadequate or even inappropriate for coping with the situation. Therefore, decision makers have to rely on knowledge that goes beyond situation-specific experiences and job aids. Almost all persons have encountered situations (e.g., automobile or home appliance failures) where the symptoms were totally inconsistent with their concept of the failures that were possible--those with which they were readily prepared to cope. Such a situation occurred at Three Mile Island.

Not all of the 13 general decision-making tasks are relevant to the three types of situations. (The relevance of tasks to situations is summarized in Fig. 10.) Because familiar and frequent situations are those in which the decision maker "knows what to do," the operator need not consider alternative information sources, explanations, and courses of action. Familiar and infrequent situations, on the other hand, require that the situation be verified prior to action. The verification process is likely to require consideration of sources of verifying information and alternative explanations. However, once the situation is verified, alternative courses of action need not be considered.

Unfamiliar, and by definition infrequent, situations are likely to require the full range of decision-making tasks. In synthesizing a course of action, the decision maker will usually have to consider a variety of hypotheses and options. This process tends to be far removed from "knowing what to do" and, it is worth noting, is one of the primary reasons why humans will continue to be vital elements of complex engineering systems.

4.2.2 Types of Strategies

As might be expected, decision makers approach the three types of situations quite differently (Refs. 25, 39). Familiar situations call upon humans' pattern recognition abilities, and problem-solving strategies tend to be *symptomatic* in the sense that observed patterns are mapped directly to likely solutions. Therefore, information to support this type of strategy should be pattern oriented and, in particular, should utilize patterns that are stereotypical for the population of decision makers of interest.

At the other extreme, unfamiliar situations call upon human analytical reasoning abilities, with the result that problem-solving strategies tend

DECISION-MAKING TASKS	TYPES OF SITUATION		
	FAMILIAR AND FREQUENT	FAMILIAR AND INFREQUENT	UNFAMILIAR AND INFREQUENT
EXECUTION AND MONITORING	YES	YES	YES
SITUATION ASSESSMENT	NO	YES	YES
PLANNING AND COMMITMENT	NO	NO	YES

Figure 10. Relevance of tasks of situation.

to be *topographic* in the sense that system functions and the relationships among these functions are explicitly considered in the search strategy. Information to support topographic strategies should be structure oriented and should emphasize causal relationships among subsystems. This will allow the symptom *tracing* that is typical for topographic strategies rather than the *mapping* from symptom to solution that is typical of symptomatic strategies.

Familiar and infrequent situations are likely to result in mixed strategies. Execution and monitoring will primarily be approached symptomatically, while some aspects of situation assessment may require a topographic approach. This does not necessarily imply that topographic or structural information will be explicitly displayed. With familiar situations it is quite likely that operators will have complete knowledge of the relevant structural information (i.e., will have a good "internal model"). However, if this structural information is to be used effectively to assess the situation, the information that does appear on the displays must be consistent with a topographic approach. Aggregated patterns would therefore be inappropriate; instead, displays should show disaggregated elements of information that allow humans to trace symptoms through their internal models of the system structure.

4.2.3 Forms of Information

The distinction between *aggregated patterns and disaggregated elements* is important for determining how the system state should be displayed. The term *state* is used here to denote both the values of essential physical variables (e.g., temperatures and pressures) and the status of configurational variables (e.g., pumps on or off and valves opened or closed).

For symptomatic strategies, system state should be displayed as an aggregated pattern. Some types of displays are excellent for emphasizing patterns. For example, N-fold circular profiles or iconic displays are oriented toward pattern recognition. As another example, some types of mimic displays involve simple outlines that allow the viewer to focus quickly on the desired portion of the display (e.g., an outline of the containment that partitions the display into the relevant variables inside and outside the containment).

In contrast, topographic strategies require that the system state be displayed as disaggregated elements. This is because particular variables such as temperatures, pressures, and valve positions are usually needed to trace through the topography of the system. A mimic display that explicitly depicts functional relationships, perhaps in block diagram fashion, is an example of a display that emphasizes elemental physical and configurational variables. In fact, any display that explicitly indicates a single state variable could be viewed as potentially supporting a topographic strategy.

The task and situation not only affect the choice between patterns and elements, but they also affect the extent to which information about

future system states is needed. *Current* information (which may include information related to past system states) is sufficient for familiar and frequent situations because the human decision maker "knows" what will happen. In contrast, unfamiliar and infrequent situations often require *projected* information, particularly for those tasks in the planning and commitment category. The intermediate type of situation (i.e., familiar and infrequent) may also benefit from projected information, by verifying that the situation is likely to evolve as hypothesized.

Thus forms of information can be described in terms of two dichotomies: (1) patterns versus elements and (2) current versus projected. The appropriateness of different forms for alternative combinations of tasks and situations is shown in Fig. 11. From this figure, one can see that the choice of task and type of situation dictates the form of information and, hence, the choice of how the information is displayed (e.g., analog versus digital, trend plots, or mimic displays).

The extent to which the resulting choices are appropriate depends on having correctly specified the tasks and situations. With regard to situations, this can be somewhat difficult because familiarity and frequency are defined at least partially, relative to particular individuals. Therefore, it is quite possible that a given situation will be familiar to one individual and unfamiliar to another.

This possibility usually results in display designers hedging by providing more elemental information than is strictly required, "just in case" particular individuals need it. Hedging also tends to occur when users are asked about what information they need. Numerous studies have shown that operators, managers, and commanders tend to overspecify their information requirements. Nevertheless, users often seem to find some "comfort" in additional and perhaps redundant information. Unfortunately, this can become a problem when display space is limited.

The approach advocated in this report is to assume the requirements in Fig. 11 to be a minimum. Additional information is acceptable to the extent that clutter and confusion are not likely to result. In other words, additional information is acceptable as long as basic human-factors incompatibilities do not arise.

An alternative approach is to design aids to adapt to individual users. Approaches to design of such aids are available (Ref. 3), but are beyond the scope of this report, as well as being beyond the range of current offerings in the nuclear power industry.

4.2.4 Prototypical Messages

Form is only one attribute of information displays. Of greater importance is *content* (i.e., the "what" as opposed to the "how"). Specifying the content of a display independent of any particular application is virtually impossible; without an application in mind, it is unreasonable to choose the particular variables to be displayed. It

DECISION-MAKING TASKS	TYPE OF SITUATION		
	FAMILIAR & FREQUENT	FAMILIAR & INFREQUENT	UNFAMILIAR & INFREQUENT
EXECUTION & MONITORING	CURRENT PATTERNS	CURRENT PATTERNS	CURRENT PATTERNS & ELEMENTS
SITUATION ASSESSMENT	—	CURRENT PATTERNS & PROJECTED ELEMENTS	CURRENT & PROJECTED ELEMENTS
PLANNING & COMMITMENT	—	—	CURRENT & PROJECTED ELEMENTS

Figure 11. Appropriate forms of information.

is possible however, to specify the nature of the *messages* that must be transmitted to support each task and situation. From this perspective, each information component of a display can be analytically evaluated in terms of its potential contribution to the transmission of one or more messages. The result will be identification of *missing* and *irrelevant* information components (i.e., portions of required messages that are not supported and information components that are not associated with any required messages, respectively.)

This type of analysis requires that one define a set of "prototypical" messages that are relevant to a range of applications. Considering the 13 general decision-making tasks in Fig. 3, 11 of them can be classified by one of three terms: (1) *generation/identification*, (2) *evaluation*, and (3) *selection*. A fairly general set of messages can be formulated for each of these terms. This set of messages is shown in Fig. 12, along with additional prototypical messages for execution and monitoring.

The genesis of this set was fairly straightforward. Messages for generation/identification are simply expressed in terms of alternative information sources, explanations, and courses of action. Messages for selection are also quite easy to envision; they simply specify the alternative that should be selected. Evaluation is much more complicated because it can involve deviations, confidence consequences, resource requirements, and comparisons of alternatives.

Given this set of prototypical messages, one is in a position to be much more specific about how an aid might support each of the 13 general decision-making tasks. Stated succinctly, in order for an aid to support a particular task, the display must provide at least one of the prototypical messages associated with the task. Of course, while Fig. 12 provides the alternative messages, one cannot dictate which alternatives are most appropriate without considering particular applications. For evaluation, this choice should be governed by the design documentation, probably augmented by discussions with the designer.

This top-down approach to selecting a set of messages provides an alternative means for dealing with the traditional problem of defining information requirements, which is typically pursued in a bottom-up manner (i.e., "up" from activity primitives rather than "down" from overall objectives). Once the messages/information requirements have been defined, one is in a position to determine the display elements and formats that will be used to "picture" the messages. Beyond the issue of form discussed earlier, more detailed issues include data characteristics and type of reading required (i.e., quantitative versus qualitative). Consideration of these issues is beyond the scope of this report. (Reference 41, which basically picks up where this report leaves off.)

4.2.5 Summary

The design framework is summarized in Fig. 13. By specifying the types of situation of interest, one defines the possible tasks of interest

IMPLEMENTATION:

1. THE COMPLETE [STEPS / PROCEDURES / GOALS] ARE . . .
2. THE CURRENT [STEP / PROCEDURE / GOAL] IS . . .
3. THE NEXT [STEP / PROCEDURE / GOAL] IS . . .

OBSERVATION:

THE CURRENT [STATE] IS . . .

GENERATION/IDENTIFICATION:

THE POSSIBLE [INFORMATION SOURCES / EXPLANATIONS / COURSES OF ACTION] ARE [A* / B / C] BECAUSE. . .

EVALUATION:

1. DEVIATION OF [STATE] IS [WITHIN EXPECTATIONS / OUTSIDE OF EXPECTATIONS]
2. CONFIDENCE IN [INFORMATION SOURCE / EXPLANATION / COURSE OF ACTION] IS [D* / E / F] BECAUSE. . .
3. CONSEQUENCES OF [EXPLANATION / COURSE OF ACTION] WILL BE [G* / H] BECAUSE. . .

Figure 12. Prototypical messages.

4. RESOURCES FOR [INFORMATION SOURCE / COURSE OF ACTION] WILL BE [I* / J] BECAUSE. . .

5. COMPARISON OF [INFORMATION SOURCES / EXPLANATIONS / COURSES OF ACTION] IN TERMS OF [K* / L / M] YIELDS RANK ORDERING OF...

SELECTION:

1. DEVIATION OF [STATE] IS [ACCEPTABLE / UNACCEPTABLE] BECAUSE. . .

2. THE BEST [INFORMATION SOURCE / EXPLANATION / COURSE OF ACTION] IS [A* / B / C] BECAUSE. . .

*A = DISPLAY ELEMENTS, DISPLAY PAGES, MANUALS, CREW MEMBERS
B = FEASIBLE SET OF FAILURES, POSSIBLE SITUATIONS, LIKELY CONTRIBUTING EVENTS/FACTORS
C = PROCEDURES, PLANS
D = ACCURACY, RELEVANCE
E = COMPLETENESS, APPROPRIATENESS
F = SUFFICIENCY, LIKELY SUCCESS
G = RESULTING STATE, RESULTING SITUATION, PROCEDURE IMPLIED
H = RESULTING STATE, RESULTING SITUATION
I = TIME, PERSONNEL
J = TIME, PERSONNEL, EQUIPMENT, INVENTORY
K = CONFIDENCE, RESOURCES
L = CONFIDENCE, CONSEQUENCES, URGENCY
M = CONFIDENCE, CONSEQUENCES, RESOURCES, URGENCY

Figure 12 (continued)

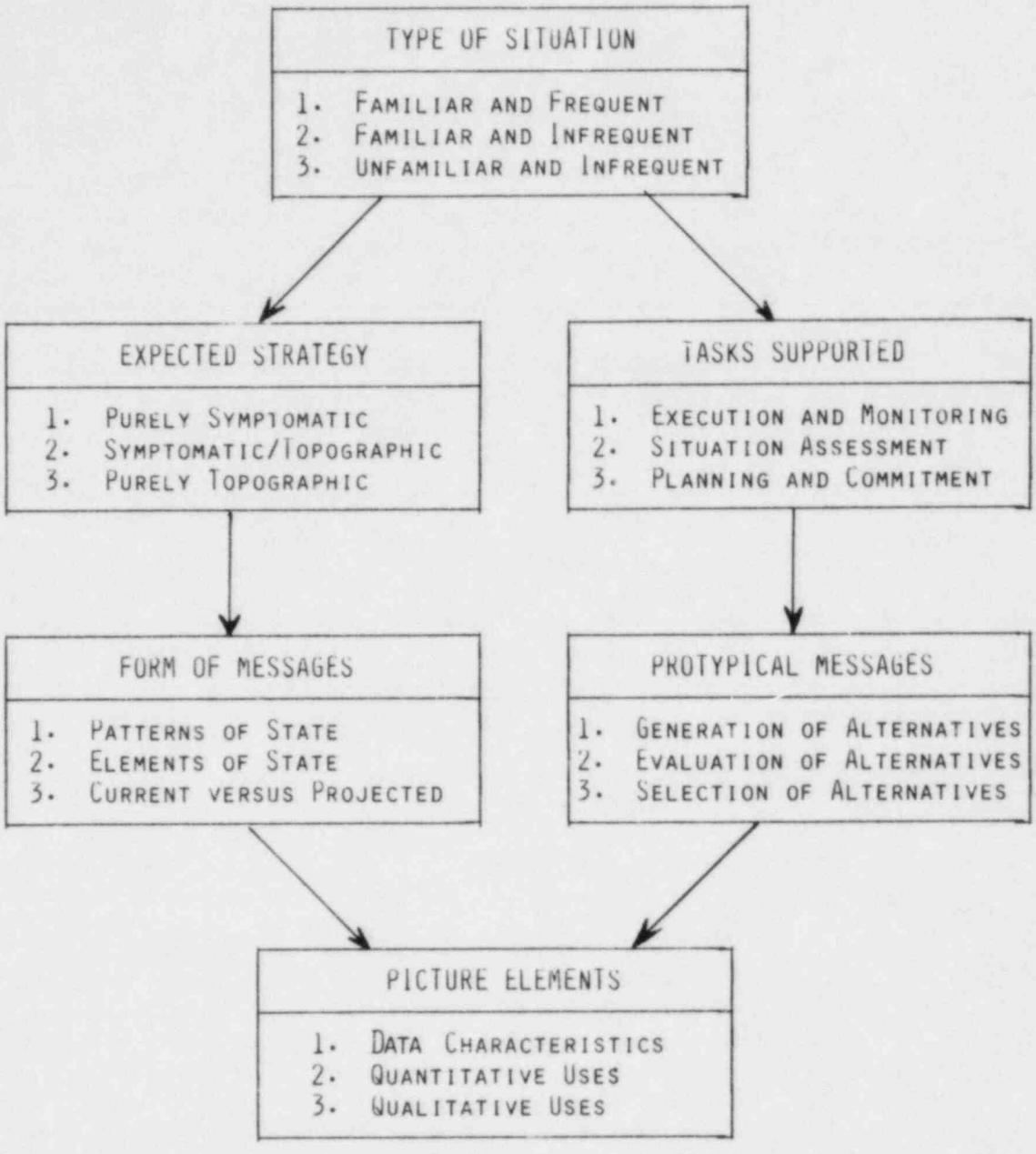


Figure 13. Summary of design framework.

(Fig. 10) as well as the expected strategy (see Sect. 4.2.1). The situations, tasks, and strategies dictate the appropriate forms of information (Fig. 11). Finally, tasks define the alternative prototypical messages that might be provided (Fig. 12). Given the types of messages and the general forms they should take (e.g., patterns versus elements), one is in a position to proceed with detailed design such as prescribed by Frey et al. (Ref. 41).

Figure 13 is not intended to imply that design and evaluation can be almost proceduralized. For example, as noted in Sect. 4.2.3, specifying the type of situation is not easy and requires knowledge of the training and experience of potential users of the aid, as well as front-end analysis of the events that are likely to present themselves. Figure 13 is simply a guide to what questions should be asked; it does not specify all of the answers.

4.3 EVALUATION

The design process outlined in Sect. 4.2 enables one to proceed from design objectives (i.e., situations and tasks) to information requirements (i.e., types and forms of messages) to particular displays using a design guide such as that given in Reference 41. This section discusses evaluation of the resulting displays. Specifically, it addresses the issue of assessing the operator knowledge required in order to understand the messages displayed.

The evaluation of *understandability* may be contrasted with evaluation of *effectiveness and compatibility* (Ref. 40). *Effectiveness* is the degree to which an aid supports achievement of design objectives. To the extent that effectiveness can be assessed analytically, the design process outlined in Sect. 4.2 ensures effectiveness. Further evaluation requires empirical testing, perhaps using the methodology proposed by Rouse (Ref. 40). *Compatibility* is the degree to which the demands that an aid places on users' sensorimotor abilities are within the human limitations of the population of users for which the system is designed. Thus a compatible system is one in which displays are readable, controls are reachable, and so forth. Assessment of compatibility is the essence of NUREG-0700 (Ref. 24) and therefore need not be discussed in detail in this report. Suffice it to say that compatibility is necessary for an aid to be successful. However, compatibility alone is not sufficient; understandability and effectiveness must also be ensured.

An aid is understandable to the extent that the information communicated to users is meaningful to them. To assess understandability one must first determine the knowledge that users must possess for them to understand the messages displayed. Once these knowledge requirements have been identified, one must then assess the extent to which users can be expected to have this knowledge. Any knowledge that is lacking can be designated as presenting a potential limit to understandability.

Knowledge requirements can be classified into three categories: (1) *display* (e.g., coding), (2) *command* (e.g., dialogue), and (3) *plant* (e.g., functions and locations). Using the finer grained classification provided in Fig. 14, one can consider each type of message as it is manifested on the display. Knowledge requirements in each category can then be identified, usually by or with the help of the designer or other individuals (operators) who are knowledgeable of the specific application for which the aid is intended.

Once all of the knowledge requirements have been identified, one then must assess the extent to which users will possess this knowledge. One approach is to employ a data base such as the Job and Task Analysis Data Base developed by the Institute of Nuclear Power Operations (INPO) (Ref. 42), which is particularly useful for assessing whether or not typical operators will have particular elements of *plant* knowledge. For *display* and *command* knowledge, one may have to consider what conventions are employed in the environment where the aid will be used.

If one cannot ensure that particular knowledge elements have been provided by typical operators' experience and training, then one must look elsewhere. Two other sources are possible: (1) operator training for using the aid and (2) other displays intrinsic to the aid or elsewhere in the control room. Knowledge requirements not satisfied by any of the above sources are deemed unsatisfied and, hence, potential limits to understandability.

The assessment of understandability proceeds as follows. First, the knowledge requirements for understanding each message (as manifested on the display) are identified. Second, the extent to which typical operators possess this knowledge (from experience, training, or other displays) is assessed. Finally, knowledge requirements not satisfied are deemed to reflect design inadequacies. The list of these inadequacies is the product of evaluation.

The use of a systematic design process such as proposed by Frey et al. (Ref. 41), will result in determination and satisfaction of knowledge requirements prior to evaluation. If such an approach is employed, the evaluation scheme described in this section is unlikely to yield many surprises (i.e., serious problems). Instead, it will serve mainly to verify compliance with the design process.

4.4 SUMMARY

Section 4 presents an analytical approach to evaluating the understandability of candidate operator aids, based on a normative view of how such aids should be designed. A candidate aid is classified using this framework (as illustrated in Sect. 3), and analysis then proceeds to identify any knowledge requirements that are not satisfied, thus potentially compromising understandability.

PLANT KNOWLEDGE

WHAT: CHARACTERISTICS (LOCATIONS, UNITS, CONTENTS, DEFINITIONS, DESIGN CHARACTERISTICS, INPUTS, OUTPUTS, SOURCES, LIMITS)
RELATIONSHIPS (SOURCES, INPUTS, OUTPUTS, INTERLOCKS, ORGANIZATION, DIFFERENCES)
PATTERNS (STATES, TRENDS, SEQUENCES, ALIGNMENTS)
SITUATIONS (STATES, MODES)
CRITERIA (PRIORTIES, LIMITS)
ANALOGIES (SIMILARITIES, DIFFERENCES)

HOW: FUNCTIONS (CAUSES, EFFECTS)
PROCEDURES(OPERATIONS)
STRATEGIES

WHY: REQUIREMENTS (PURPOSE, REASONS)
OBJECTIVES
OPERATIONAL BASES
LOGICAL BASES
PHYSICAL PRINCIPLES/THEORIES
MATHEMATICAL PRINCIPLES/THEORIES

DISPLAY KNOWLEDGE

TERMINOLOGY (LABELS, WORDS, ABBREVIATIONS)
SYMBOLOGY (SYMBOLS, CODING)
ELEMENTS (HOW TO READ OR INTERPRET ELEMENTS)
ORGANIZATION (RELATIONSHIPS AMONG DISPLAYS, CURRENT LOCATION)
DELAYS (DATA UPDATE, REDRAW TIME)

COMMAND KNOWLEDGE

TERMINOLOGY (COMMANDS, ARGUMENTS, ABBREVIATIONS)
SYMBOLOGY (SYMBOLS, CODING)
DEVICES (HOW TO USE DEVICES)
MODES (WHEN TO USE COMMANDS)
FEEDBACK (WHAT TO EXPECT)

Figure 14. Classification of knowledge requirements.

5. EXAMPLE APPLICATION OF EVALUATION METHODOLOGY

A hypothetical decision aid was designed and subsequently evaluated to illustrate the application of the proposed evaluation methodology and assess its practical utility. This section presents the aid, describes the application of the evaluation process, and discusses the results obtained. The general applicability of the proposed methodology is discussed in Sect. 6.

5.1 HYPOTHETICAL DECISION AID

The authors chose to develop a hypothetical decision aid to demonstrate the evaluation methodology because available information about existing aids was not sufficiently detailed to perform an evaluation without the risk of misrepresentation. Further, by developing the aid to be evaluated, they had access to *complete* design information and could therefore assess the need for such information.

The decision aid was developed to support operators of pressurized-water reactors (PWRs) in identifying which, if any, procedures should be performed to recover from a compromised critical safety function (CSF). The aid will provide operators with the text of the procedures on request.

The aid was designed using the methodology of Frey et al. (Ref. 41). The design documentation included system objectives and display and dialogue descriptions. This documentation is excerpted in this section to the extent necessary to illustrate the evaluation.

The authors envision most applications of the methodology espoused in this report to involve aids that were not designed in the systematic manner prescribed by Frey and his coworkers. This design method was used for this example, however, in order to illustrate what information is necessary for evaluation. The Frey method generates this information during design and prior to evaluation, but evaluation of aids that were not systematically designed and documented will require designers to reconstruct this information after design and during evaluation.

5.1.1 Design Objectives

The following design objectives were adopted:

1. This display system should operate as a real-time operational aid for protection of CSFs for a PWR. Specifically, the aid should assist in detection of the need for and choice of appropriate CSF recovery procedures using the decision algorithms provided by the Nuclear Steam System Supplier (NSSS).

2. The user of the system is the person with immediate responsibility and authority for the operation of the plant (shift supervisor).
3. The system should be used during all phases of power plant operation as well as post-trip activities until the plant has reached a safe shutdown state.
4. The displays should be available on the existing display device located on the shift supervisor's console.

5.1.2 Displays

To support these objectives, a hierarchical display system was developed which is composed of four levels as shown in Fig. 15. (The eight displays marked with an asterisk in Fig. 15 are shown in detail in Figs. 16 through 24. The remaining displays were not evaluated and are not presented here.)

5.1.2.1 Display Hierarchy

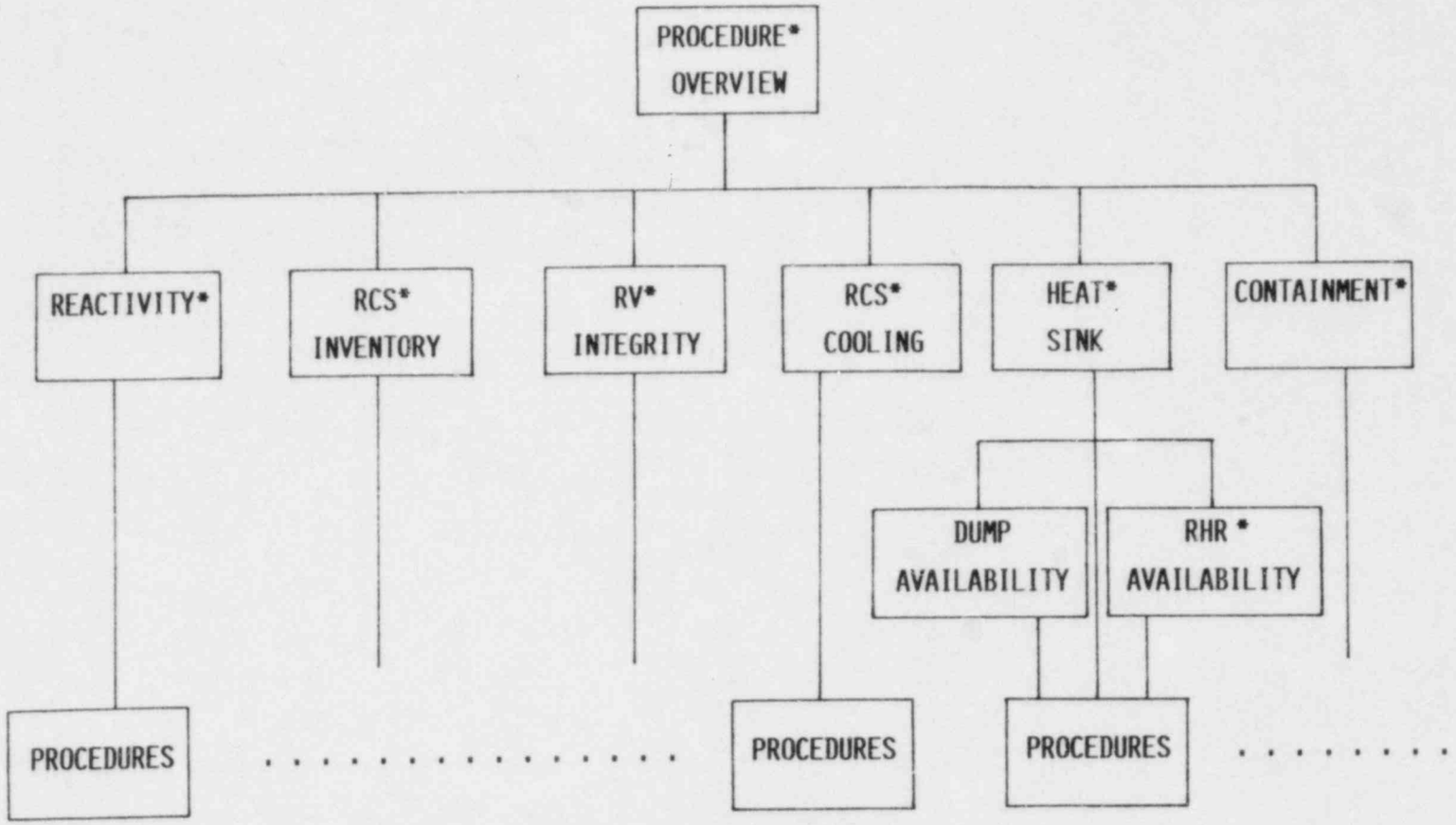
The first-level display (Fig. 16) is a procedure overview that displays the names of all active procedures (i.e., procedures whose entry conditions have been met) and their priorities. The second-level displays (Figs. 17 through 23) contain the plant parameters related to each CSF as well as the name of the current active procedure (if any) for that CSF. The third-level displays (an example is shown in Fig. 24) support the heat sink CSF only, and they contain information related to equipment availability. The fourth-level displays (not included) contain the text of the procedures. The left portion of each display is dedicated to an overview of the CSFs.

The box underneath the title of each second- and third-level display contains the number and name of the current active procedure, if any, for that CSF. The text that appears in that box consists of one line as shown in Fig. 25. The same text appears on the top-level display.

5.1.2.2 Display Coding

Three types of coding are used in these displays: color, texture, and blinking. Color coding is used on the CSF status boxes, procedure numbers, and parameter displays. When a CSF is not fully satisfied and may eventually require some operator action, a yellow background is used on the appropriate CSF box and procedure labels. When a CSF is challenged and prompt action is required, a magenta background is used. When a CSF is in jeopardy and immediate operator action is required, a red background is used. The parameters that indicate the violation of the CSF use the same color coding. Text is always displayed as white on black.

Texture coding is used in the CSF status boxes and the procedure numbers as a redundant coding technique for degree of compromise of the CSF (see Fig. 26). A lightly striped background is used with the yellow indications, a heavy stripe is used with the magenta, and a solid background is used with the red. Because the parameters are primarily for operator information only, texture coding is not used for those display elements.



* Displays Shown in Figures 16-24.

Figure 15. Display hierarchy.

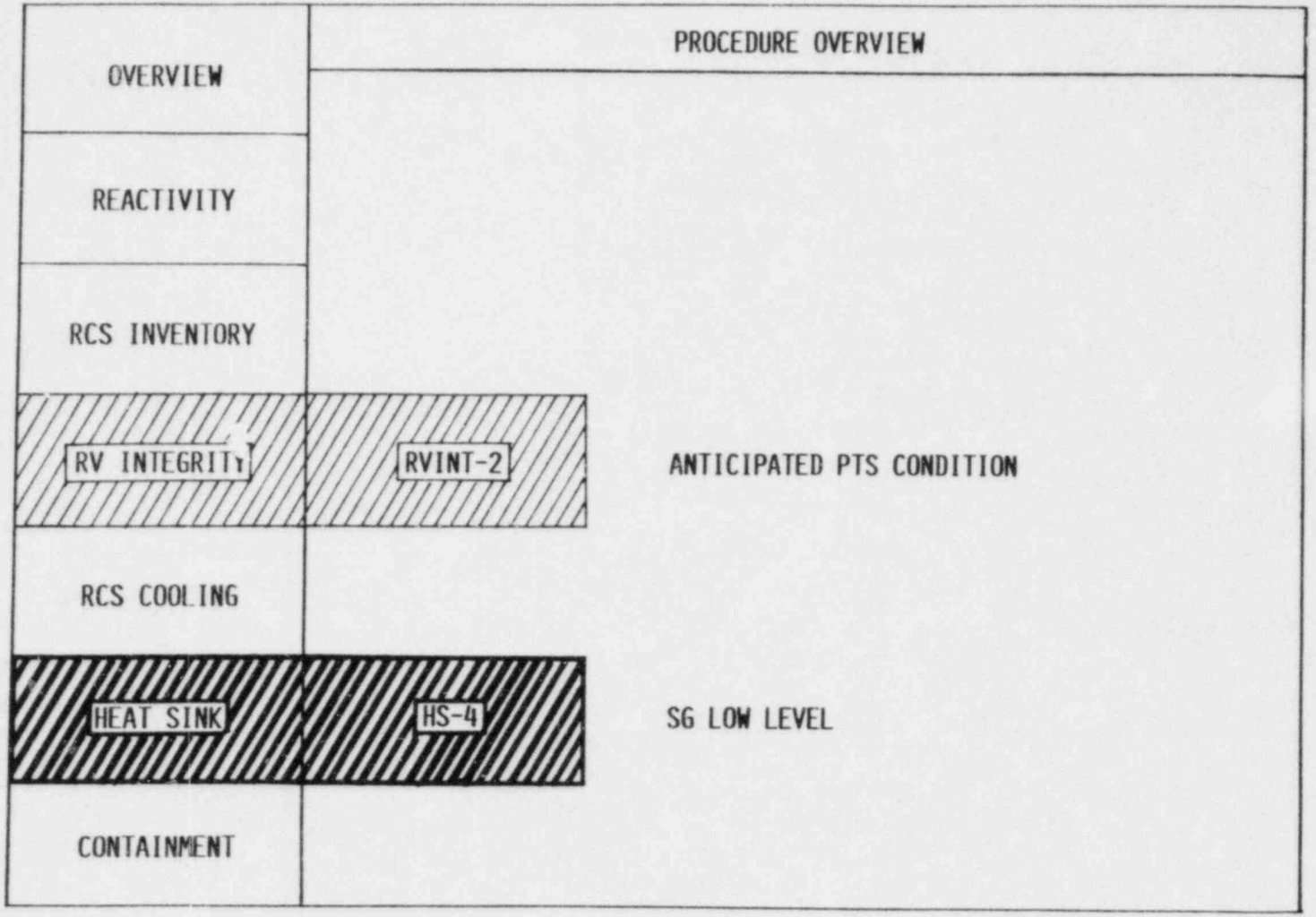


Figure 16. Top-level display: procedure overview.

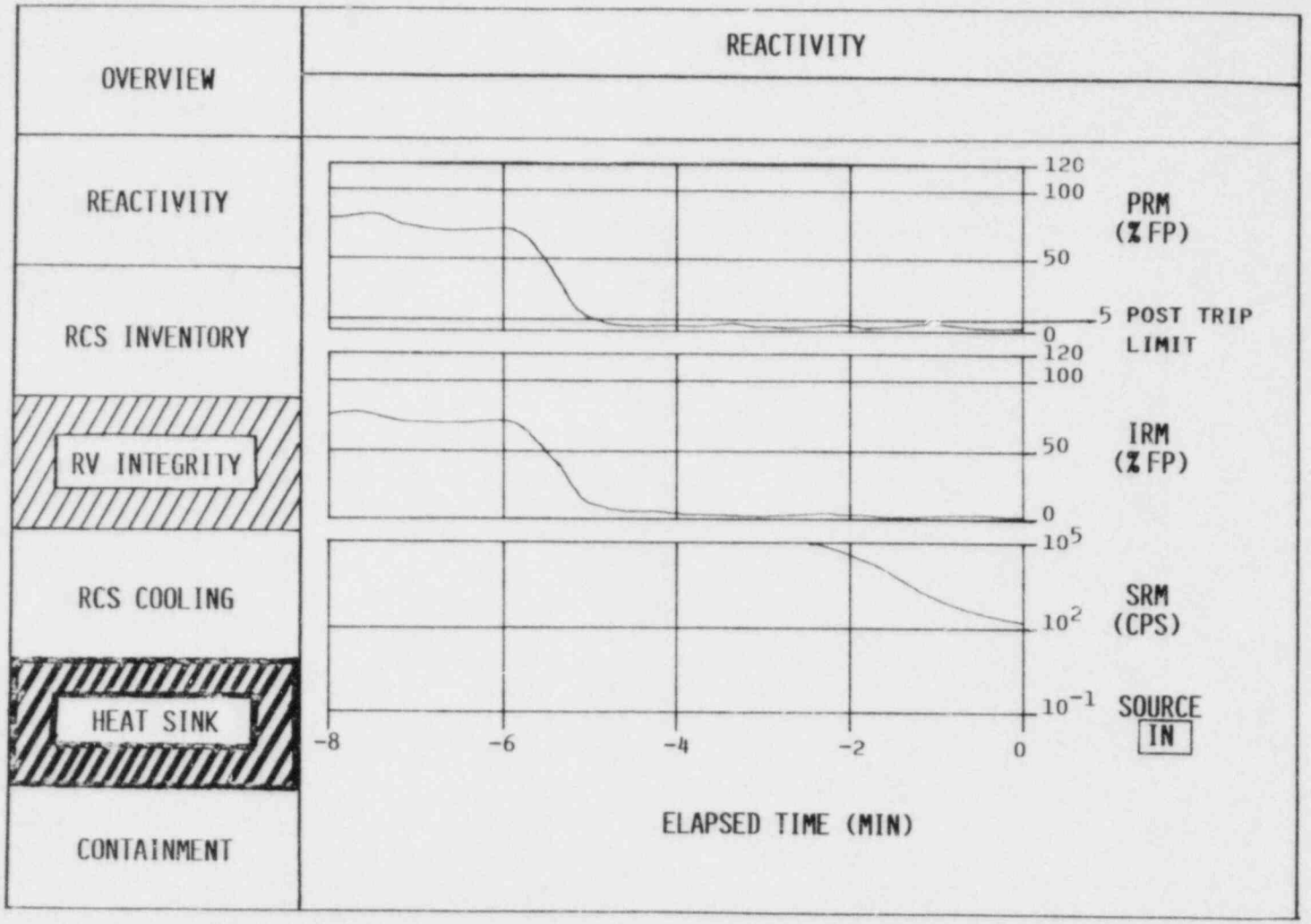


Figure 17. Second-level display: radioactivity.

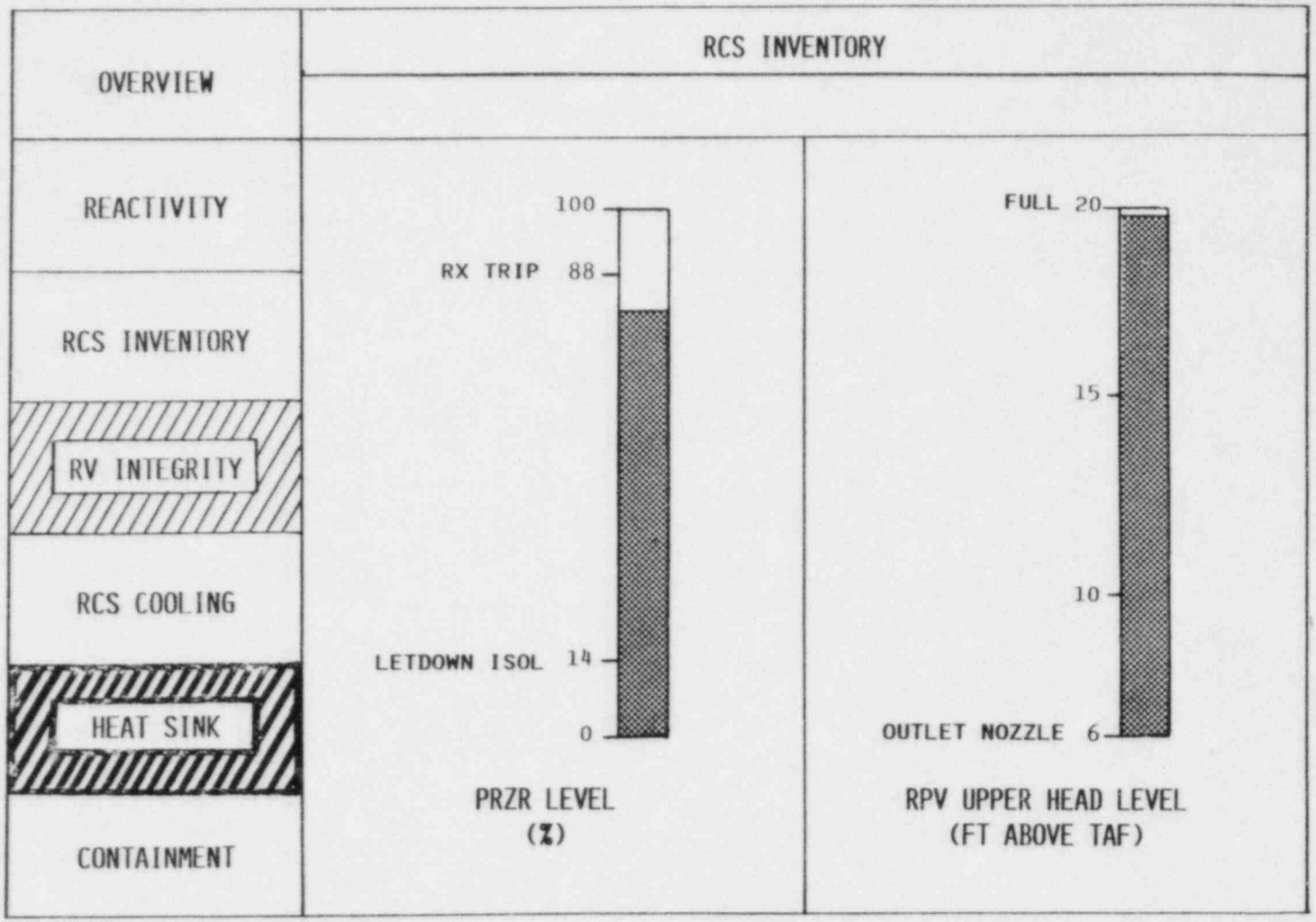


Figure 18. Second-level display: reactor cooling system (RCS) inventory.

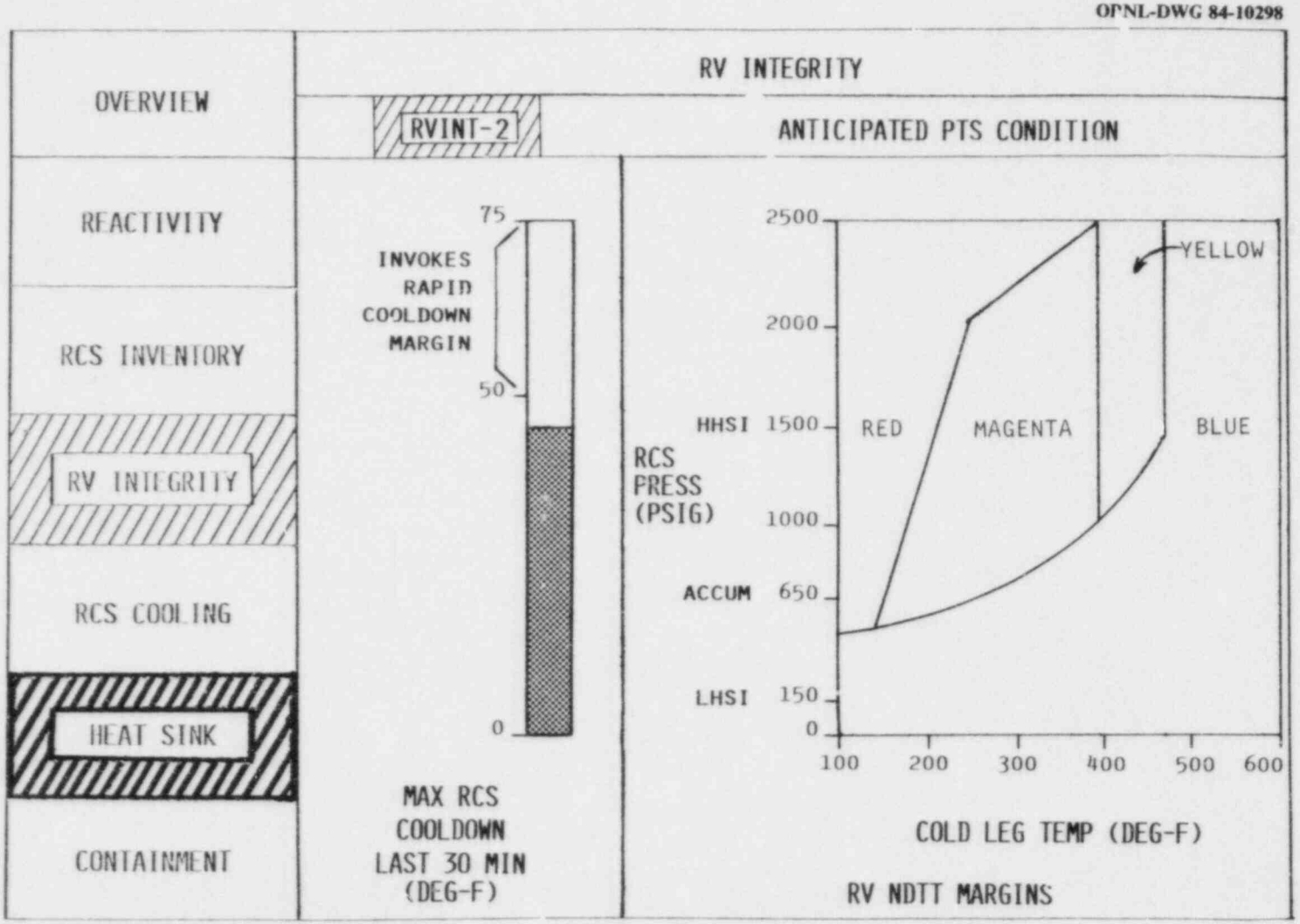


Figure 19. Second-level display: reactor vessel (RV) integrity with normal cooldown margins.

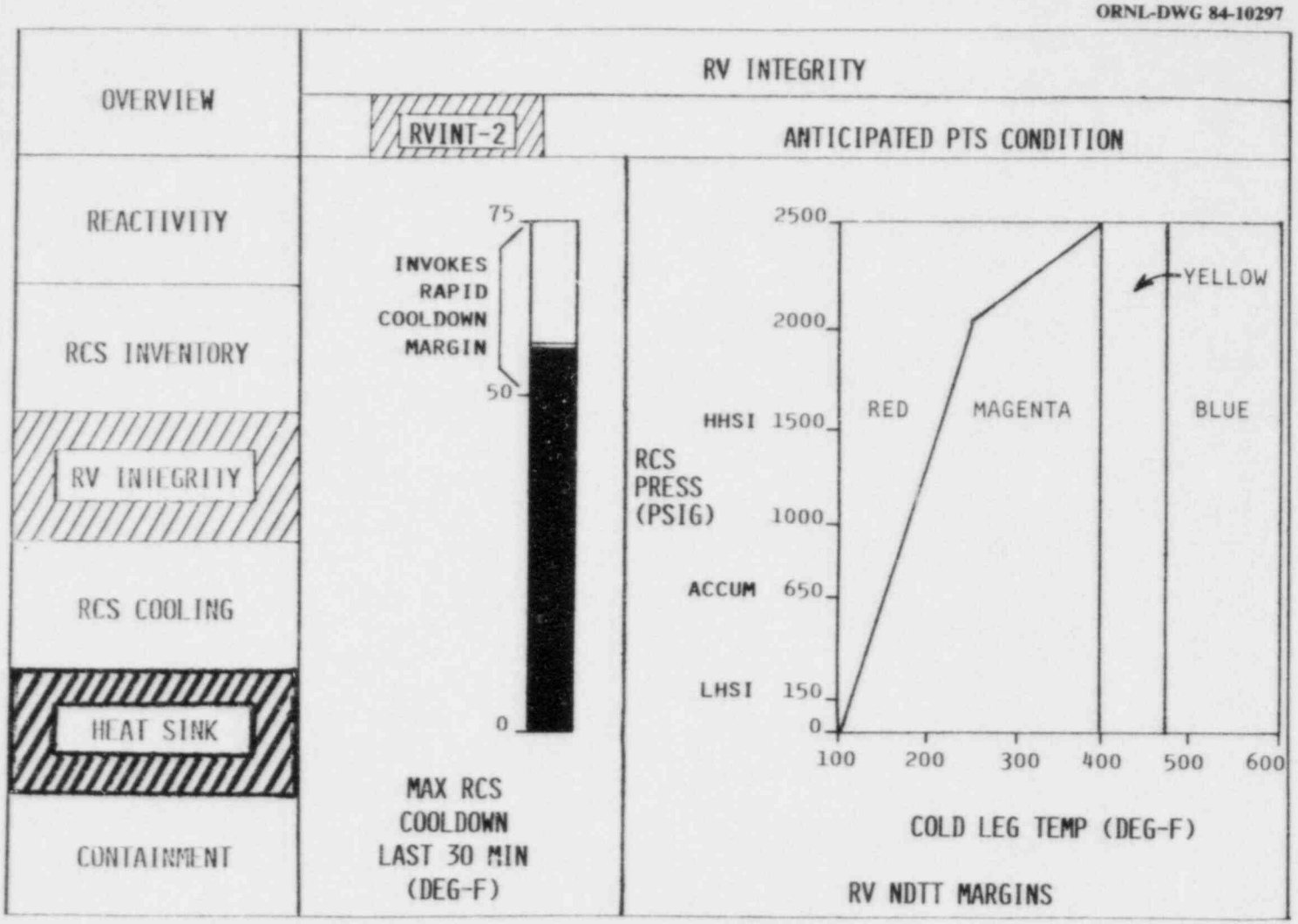


Figure 20. Second-level display: reactor vessel (RV) integrity with rapid cooldown margins.

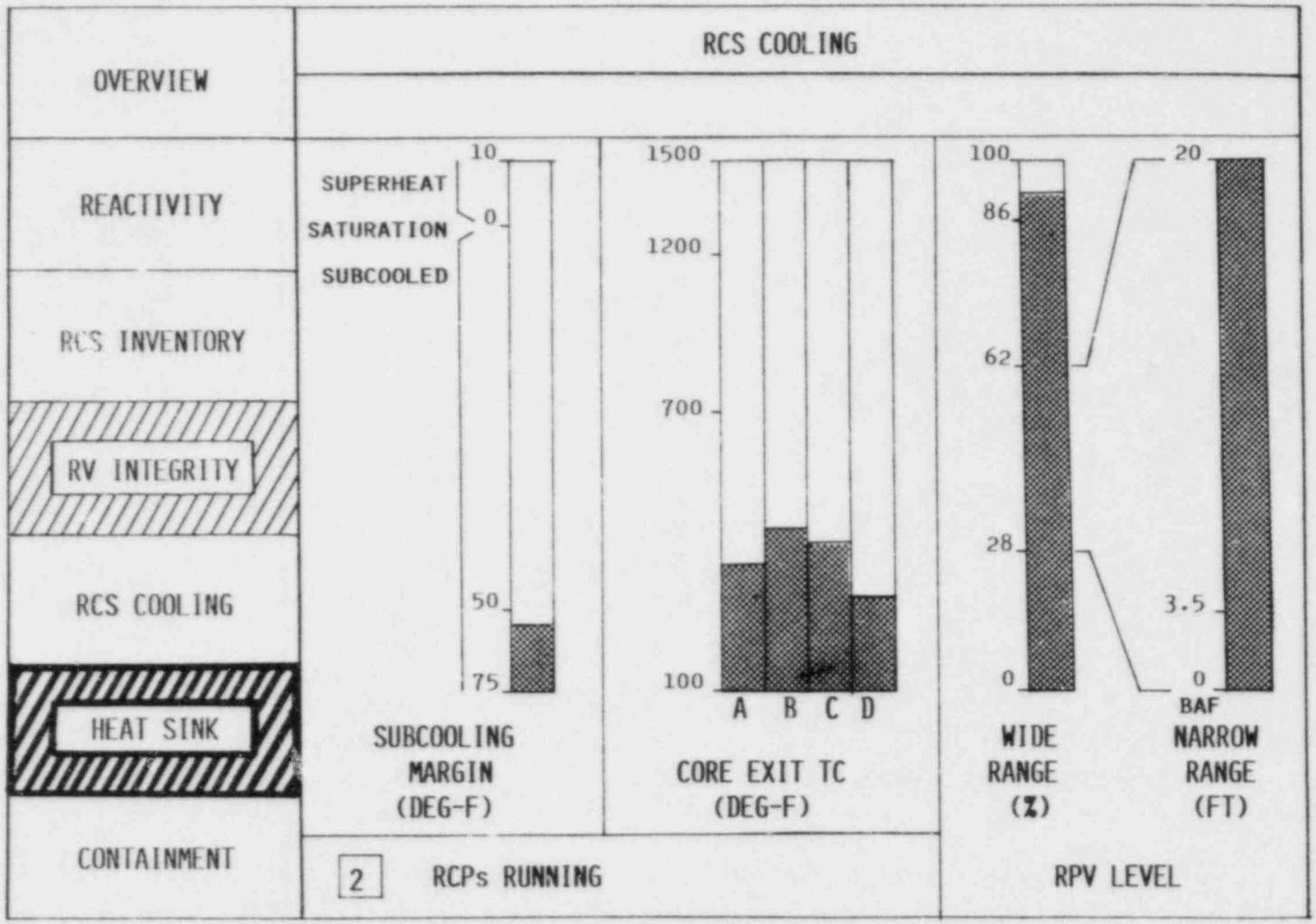


Figure 21. Second-level di play: reactor cooling system (RCS) cooling.

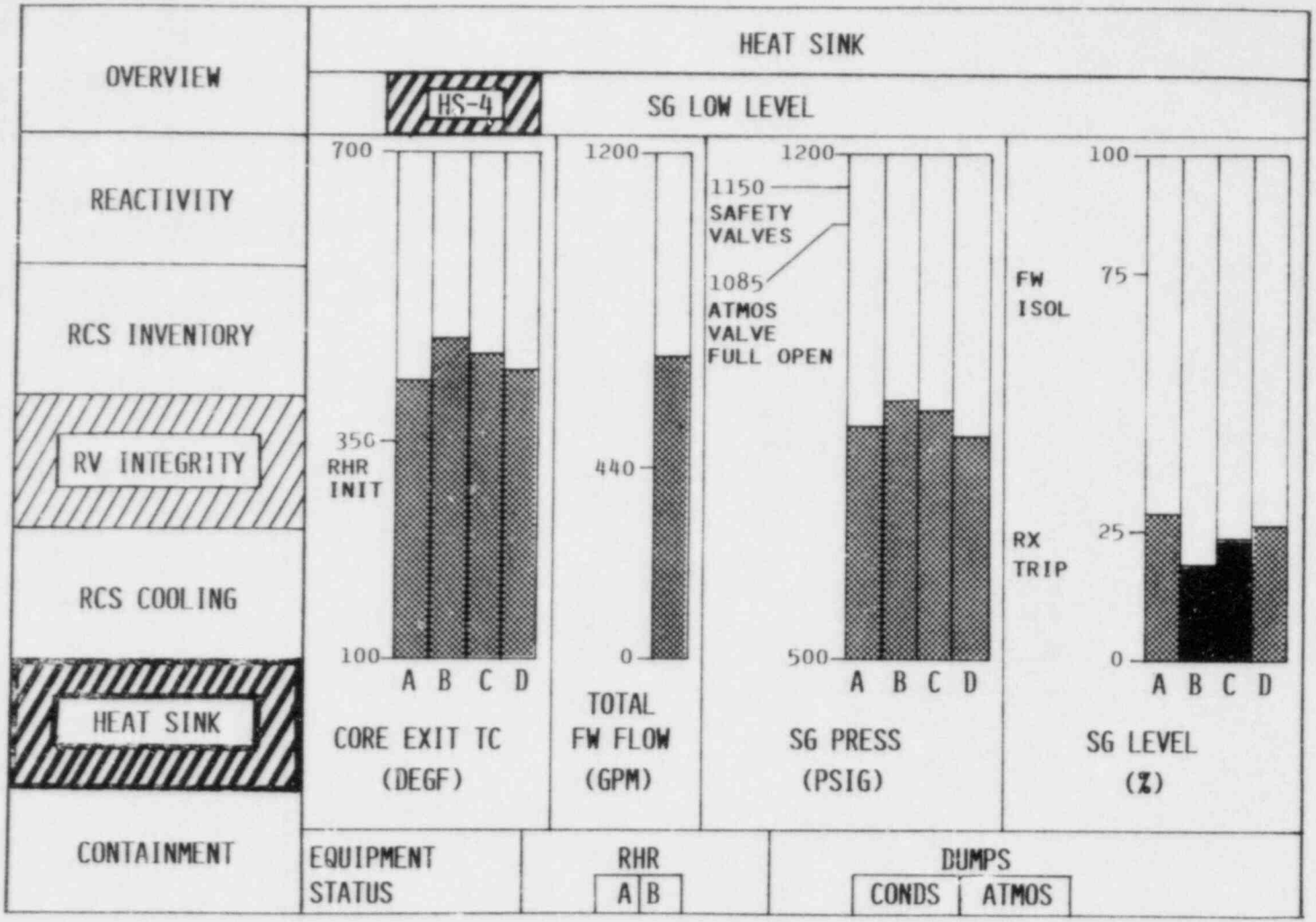


Figure 22. Second-level display: heat sink.

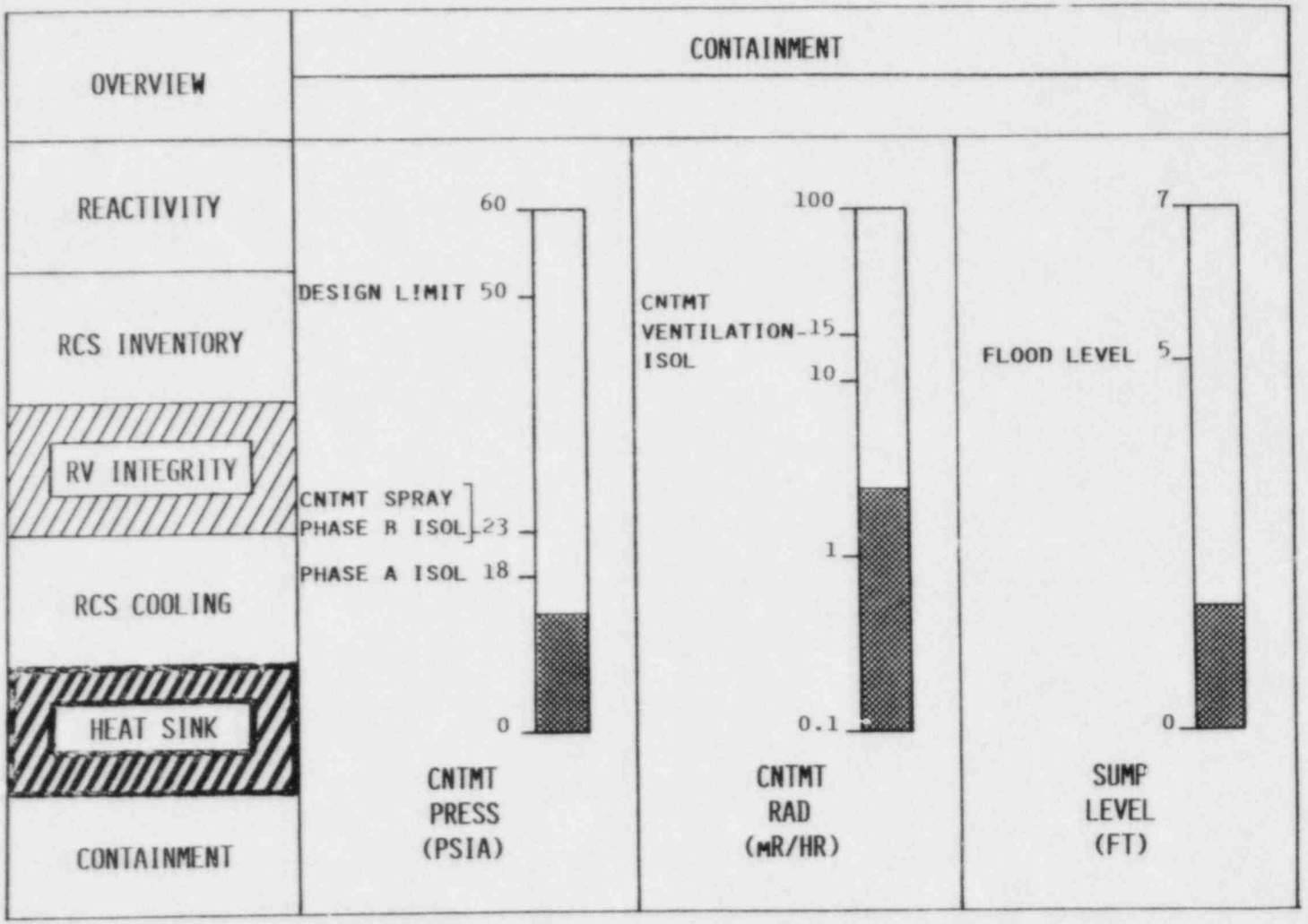


Figure 23. Second-level display: containment.

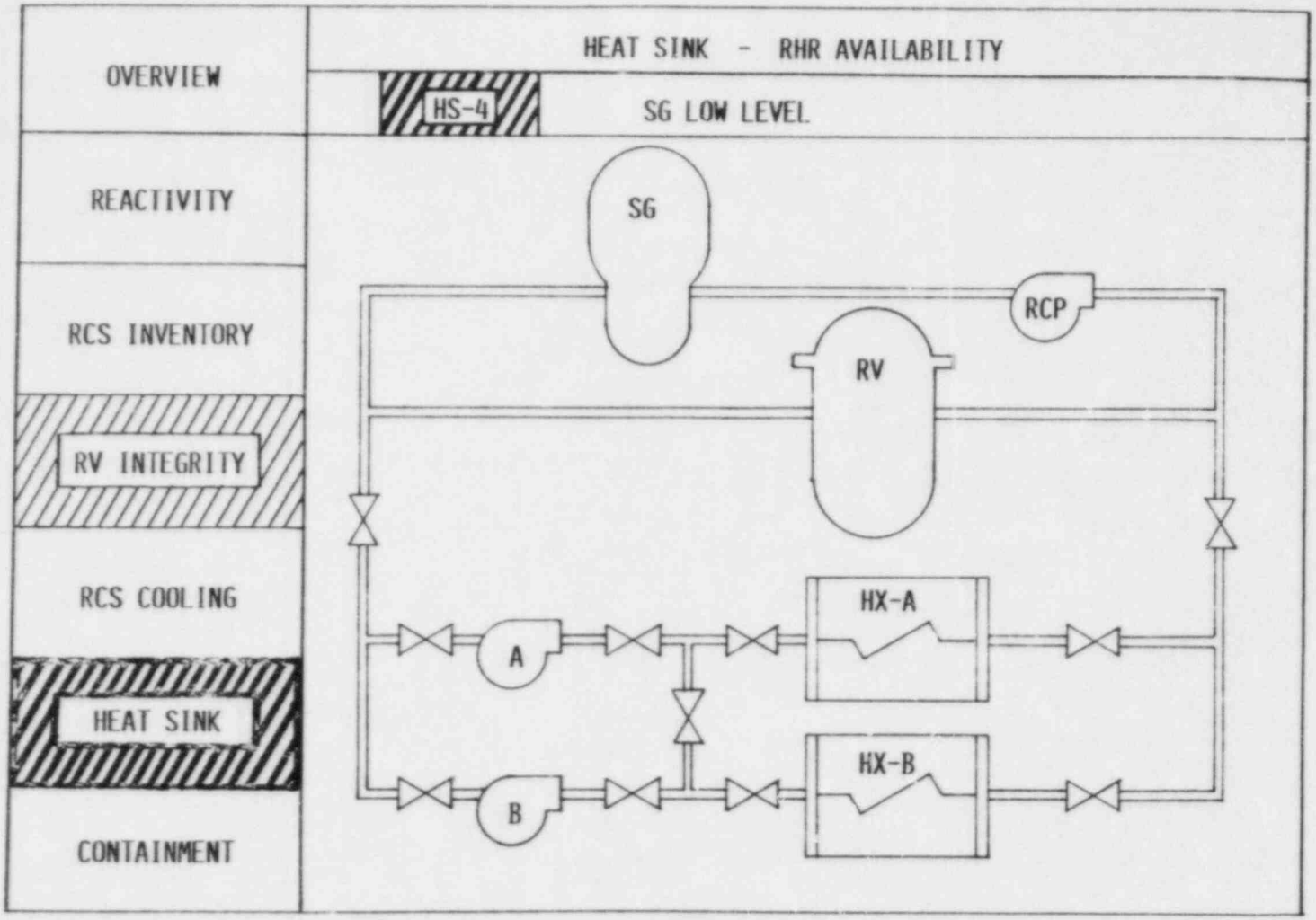


Figure 24. Third-level display: residual heat removal (RHR) availability.

REACTIVITY

REAC-1	CONTINUED NUCLEAR POWER GENERATION
REAC-2	LOSS OF CORE SHUTDOWN

RCS INVENTORY

RCSINV-1	PRESSURIZER FLOODING
RCSINV-2	LOW SYSTEM INVENTORY
RCSINV-3	VOIDS IN REACTOR VESSEL

RV INTEGRITY

RVINT-1	IMMINENT PTS CONDITION
RVINT-2	ANTICIPATED PTS CONDITION

RCS COOLING

RCSC-1	INADEQUATE CORE COOLING
RCSC-2	DEGRADED CORE COOLING
RCSC-3	POTENTIAL LOSS OF CORE COOLING
RCSC-4	SATURATED CORE COOLING CONDITIONS

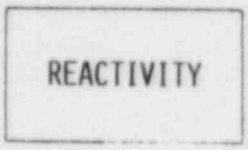
HEAT SINK

HS-1	LOSS OF SECONDARY HEAT SINK
HS-2	SG OVERPRESSURE
HS-3	SG HIGH LEVEL
HS-4	SG LOW LEVEL
HS-5	LOSS OF SG P RVS AND CONDS DUMP VALVES

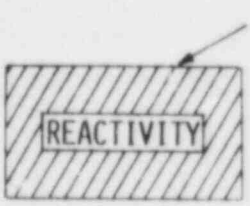
CONTAINMENT

CONT-1	HIGH CONTAINMENT PRESSURE
CONT-2	HIGH CONTAINMENT SUMP LEVEL
CONT-3	HIGH CONTAINMENT RADIATION LEVEL

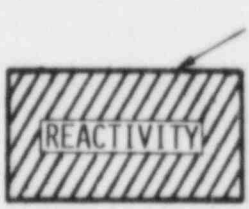
Figure 25. Text for the procedure overview and active procedure blocks.



CRITICAL SAFETY FUNCTION (CSF) SATISFIED.
OPERATOR ACTION NOT NEEDED.



CSF NOT FULLY SATISFIED.
OPERATOR ACTION MAY EVENTUALLY BE NEEDED.



CSF CHALLENGED.
PROMPT OPERATOR ACTION IS NECESSARY

CSF IN JEOPARDY.
IMMEDIATE OPERATOR ACTION IS REQUIRED.

NOTE: COLOR AND TEXTURE CODES ARE THE SAME FOR THE PROCEDURE NAMES.

Figure 26. Color and texture codes.

Blink coding is used to alert the user of a change in the status of one of the CSFs. When a CSF changes status, the alphanumerics in the corresponding CSF box blink from full to half intensity, with 75% duty cycle and a frequency of 1 Hz. The blinking continues until the user accesses the second-level display related to the CSF whose status changed.

5.1.2.3 Display Access

The displays are accessed through the use of a touch-sensitive screen over the cathode-ray tube (CRT) face. The active areas of the touch screen change with the display being viewed. The touch areas are summarized in Fig. 27.

All top- and second-level displays can be accessed from anywhere in the display hierarchy. Third-level displays can be reached only from the corresponding second-level display, while fourth-level displays can be reached from the top-level or the corresponding second- or third-level displays.

5.1.3 Summary

The objectives and display characteristics of the hypothetical aid have been briefly described. Evaluation of compatibility issues would require much more information than is presented here (e.g., character and symbol sizes, display resolution, refresh rates, and workspace layout). The design information presented to this point is, however, sufficient to begin analysis of the understandability of the aid.

5.2 EVALUATION OF THE DECISION AID

5.2.1 Specification of Situations and Tasks

As stated in the objectives, the purpose of this aid is to support identification and selection of appropriate procedures for protection of CSFs. Although it is hoped that CSFs are not compromised frequently, the possibility of this occurrence must be anticipated. Therefore, the situations of interest are *familiar* and *infrequent*.

Of course, it is quite likely that the aid would be used in the event of an unfamiliar failure or transient. However, this aid was designed to protect CSFs (a familiar problem) rather than to diagnose an unfamiliar failure. Thus the aid is used to deal with familiar and infrequent (or perhaps frequent) situations that may or may not arise as the result of an unfamiliar failure. To support diagnosis of unfamiliar failures (which was not a design objective), the aid would have to be redesigned and extended.

With the situations specified, the next step in the evaluation process is to determine which of the 13 decision tasks are supported by the aid. From the objectives, it appears that the only task supported is the selection among alternative courses of action (". . .the aid should

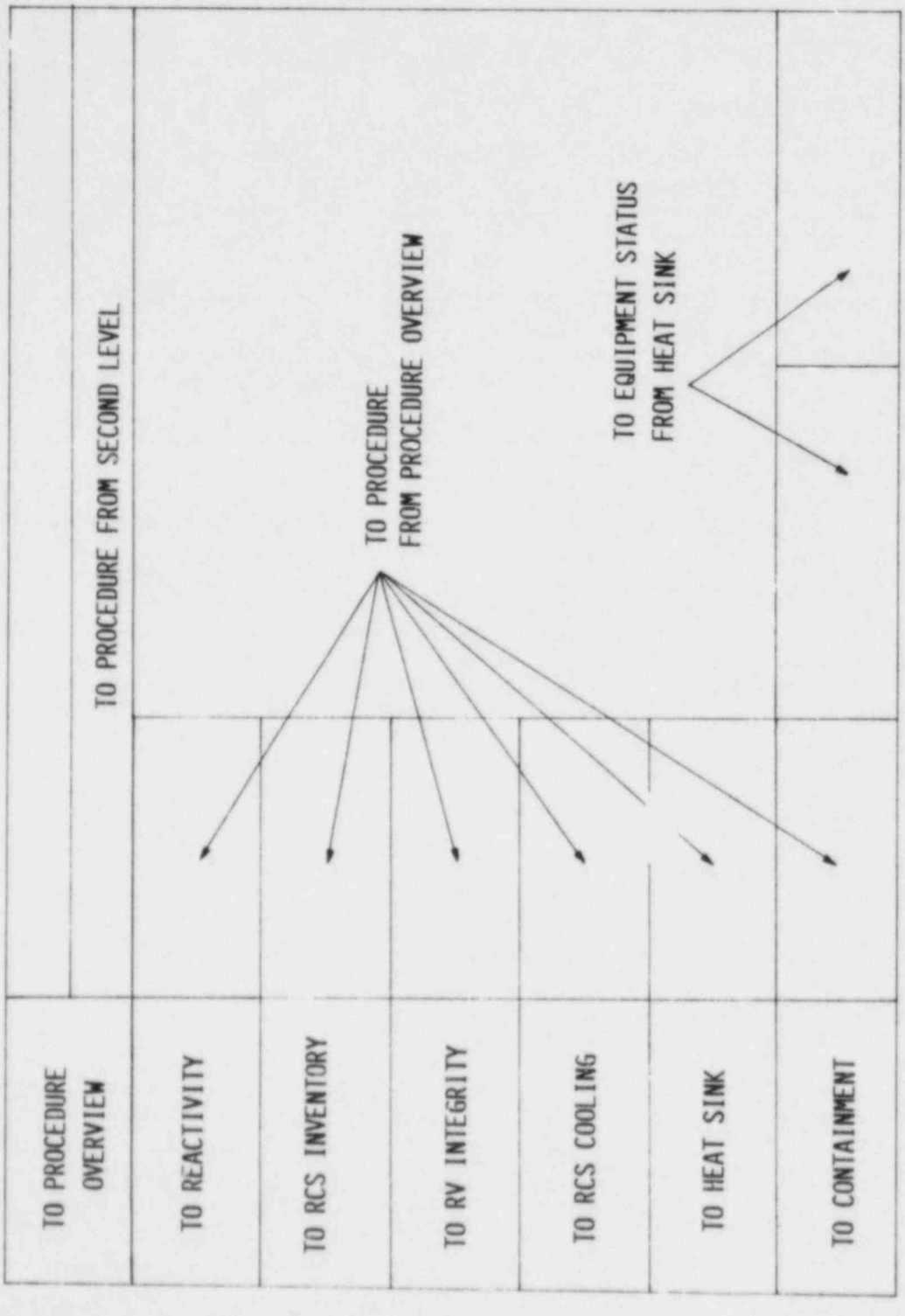


Figure 27. Touch screen active areas.

assist in the detection of the need for and the choice of the appropriate CSF recovery procedure . . ."). However, using Fig. 10 as a guide for further analysis of the displays resulted in identification of additional decision tasks that are supported. The following discussion presents the reasoning that led to these conclusions for each of the decision tasks.

1. Implementation of plan - Yes

   During normal plant operation, the aid does not support this decision task. However, once the operators begin performing the CSF recovery procedures, the aid becomes a resource to support this task by providing the procedures on the fourth-level displays.

2. Observation of consequences - Yes

   The aid displays the state of the plant as indicated by the parameters that are monitored. The portions of the display that support this task are the parameter display areas (column charts, etc.).

3. Evaluation of deviations from expectations - Yes

   The aid supports this task by checking the parameters against thresholds (expectations). These thresholds form a wide boundary within which the CSFs are satisfied and beyond which the CSFs are in various stages of compromise. The aid performs these threshold checks and indicates the results on the displays by color and texture coding on the picture elements.

4. Selection between acceptance and rejection - Yes

   The thresholds for the observed parameters are such that any parameter that crosses the threshold is unquestionably in an unacceptable range.

5. Generation of alternate information sources - Yes

   The aid supports this task by indicating, on any given page, that information to explain the current situation may be present on another page if another CSF is indicated as compromised.

6. Evaluation of alternative information sources - No

   The aid does not indicate anything about the quality of the information source or about the resources required to obtain the information.

7. Selection among alternative information sources - No

   The only sense in which the aid supports this task is that the designer has selected a set of parameters to be available to the

user. The aid does not select an information source and present it to the user for consideration.

8. Generation of alternative explanations - No

   The CSFs can be thought of as explanations in a limited sense. As explanations, they are functional answers to the question "What's wrong?," indicating areas where problems exist. However, the aid does not generate new explanations other than the status of the six CSFs.

9. Evaluation of alternative explanations - Yes

   The aid evaluates the extent to which the CSFs are satisfied, and evaluates the alternative explanations according to urgency or, in other terms, proximity to undesirable consequences. The urgency level is predetermined by decision trees and indicated on the display by color and texture coding in the CSF blocks.

10. Selection among alternative explanations - No

    This aid does not choose one of the CSFs as being the source of the problems. Several of the CSFs may be compromised simultaneously with the same level of urgency.

11. Generation of alternative courses of action - No

    This aid has a limited set of alternatives to suggest to the user. They are the procedures that were preselected by the designer. Because the aid does not generate new courses of action, it does not support this task.

12. Evaluation of alternative courses of action - No

    In a sense, the aid supports this task with the top-level display, where all active procedures are displayed. As noted in Item 9 above, the procedure labels are coded (color and texture) to indicate the relative urgency of the various courses of action. However, the aid does not provide the user with a comparison of the relative merits of the active procedures; the situations dictate the procedures.

13. Selection among alternative courses of action - No

    In a sense, the aid might support this task with the second-level displays, where one and only one procedure may be active at any one time for a given CSF. However, at the top level the aid may be recommending action on as many as six procedures at one time. Therefore, the aid does not support this task in an overall sense.

The specification of tasks is not as straightforward as the above discussion may lead one to conclude. While Fig. 10, in conjunction with design

documentation and discussions with the designer, provides some guidance, judgment is required. Once one concludes that a task is supported and then evaluates the aid with respect to the prototypical messages associated with the task, it is quite possible to conclude that a task is actually not supported by the aid. The methodology advocated in this report is thus iterative to some extent.

5.2.2 Prototypical Messages

Using the prototypical messages in Fig. 12 in conjunction with the displays (Figs. 16 through 24), the prototypical messages relevant to the above six decision tasks (i.e., numbers 1 through 5 and 9) were identified and are shown in Fig. 28. It is important to note that the tentative choices of prototypical messages are likely to have to be verified by discussions with the designer. For this example, of course, this was not a problem.

The message for the first task is included for illustrative purposes only, because the fourth-level displays are not analyzed in this example. The rationale ("because . . .") is omitted in each case because the hypothetical aid does not provide the rationale. The messages for tasks 5 and 9 are special cases of the general messages in Fig. 12 and reflect the specific content of the displays.

Once the relevant prototypical messages are identified, the next step is associating individual display elements with one or more messages. Using the displays, design documentation, and discussions with designers, this is reasonably straightforward. The results are shown in Fig. 29.

5.2.3 Forms of Information

The next step in the evaluation process is consideration of the forms of displayed information. Figure 11 suggests that current patterns and projected elements are the most appropriate forms for the situations and tasks supported by the hypothetical aid.

With regard to *current patterns*, many of the display elements emphasize qualitative readings. For example, the CSF status boxes on all displays and bar charts on many of the second-level displays (Figs. 18 through 23) are oriented toward immediate recognition of acceptable or unacceptable patterns. In fact, very little precise quantitative information can be gleaned from these displays.

Considering *projected elements*, the trend plots on the reactivity display (Fig. 17) and the parameter-parameter history on the reactor vessel (RV) integrity display (Figs. 19 and 20) certainly imply projected information. In addition, the four levels of color and texture coding for the CSF status boxes provide a projection of the urgency of each threatened CSF. These types of display elements would be suitable for supporting the mixed symptomatic/topographic strategy anticipated to be employed for situation assessment in familiar and infrequent situations.

TASK NO.	DECISION TASK	PROTOTYPICAL MESSAGE
*1	IMPLEMENTATION OF PLAN	THE CURRENT [STEP] IS . . .
2	OBSERVATION OF CONSEQUENCES	THE CURRENT [STATE] IS . . .
3	EVALUATION OF DEVIATIONS FROM EXPECTATIONS	DEVIATION OF [STATE] IS [WITHIN EXPECTATIONS / OUTSIDE OF EXPECTATIONS]
4	SELECTION BETWEEN ACCEPTANCE AND REJECTION	DEVIATION OF [STATE] IS [ACCEPTABLE / UNACCEPTABLE]
5	GENERATION OF ALTERNATIVE INFORMATION SOURCES	THE POSSIBLE [INFORMATION SOURCES] ARE [DISPLAY PAGES]
9	EVALUATION OF ALTERNATIVE EXPLANATIONS	COMPARISON OF [EXPLANATIONS] IN TERMS OF [URGENCY] YIELDS RANK ORDER OF . . .

* THIS TASK IS INCLUDED FOR ILLUSTRATIVE PURPOSES ONLY. NO FURTHER ANALYSIS IS PERFORMED ON THE FOURTH-LEVEL DISPLAYS.

Figure 28. Prototypical messages provided by the decision aid.

Display Element	Protoypical Message (See Figure 28)
Elements common to all displays (Figures 16-24)	
Title	1
CSF status	5,9
Elements common to 2nd and 3rd level displays Figures 17-24)	
Active procedure box	1
Procedure overview display (Figure 16)	
Procedure title list	1
Reactivity display (Figure 17)	
PRM trend	2,3,4
IRM trend	2,3,4
SRM trend	2,3,4
Source in/out indicator	2
RCS inventory display (Figure 18)	
PRZR level	2,3,4
RPV upper head level	2,3,4
RV integrity display (Figures 19 and 20)	
Max RCS cooldown	2,3,4
RV NDTT margin plot	2,3,4

Figure 29. Correlation of display elements with prototypical messages.

RCS COOLING DISPLAY (FIGURE 21)	
SUBCOOLING MARGIN	2,3,4
CORE EXIT TC	2,3,4
RPV WIDE RANGE LEVEL	2,3,4
RPV NARROW RANGE LEVEL	2,3,4
RCPS RUNNING INDICATOR	2,3,4
HEAT SINK DISPLAY (FIGURE 22)	
CORE EXIT TC	2,3,4
TOTAL FW FLOW	2,3,4
SG PRESSURE	2,3,4
SG LEVEL	2,3,4
RHR STATUS	2,3,4,5
DUMPS STATUS	2,3,4,5
CONTAINMENT DISPLAY (FIGURE 23)	
CNTMT PRESSURE	2,3,4
CNTMT RADIATION	2,3,4
SUMP LEVEL	2,3,4
HEAT SINK - RHR AVAILABILITY DISPLAY (FIGURE 24)	
MIMIC	2,3,4,9

Figure 29 (continued)

5.2.4 Knowledge Requirements

Using the knowledge taxonomy (Fig. 14) in conjunction with relationships between display elements and prototypical messages shown in Fig. 29 (and referenced to Fig. 28), the next step is identification of knowledge requirements in the display, command, and plant categories. To illustrate the results of this step, the knowledge requirements for RV integrity display (Figs. 19 and 20) are shown in Figs. 30 through 34.

Considerable judgment is needed when assessing knowledge requirements. While use of the taxonomy (Fig. 14) to audit the display elements (Figs. 19 and 20) provides some guidance, the process is far from algorithmic. (Section 6.3 discusses possible refinements to the methodology that would help in this area.)

Much of the analysis of information requirements may have been done in the process of designing an aid. Therefore, the extent of inference required may be less than implied in this section. However, as noted earlier, it is also likely that the proposed evaluation methodology will be applied to aids where literally no analysis of knowledge requirements was performed.

5.2.5 Assessment of Understandability

Given the knowledge requirements compiled in Figs. 30 through 34, the next step is assessing the extent to which these requirements are satisfied. Figure 35 provides an assessment of the extent to which requirements are met by three sources: (1) operators' prior training and experience, (2) training specifically for use of the aid, and (3) other displays or resources.

The degree to which knowledge requirements are satisfied by operators' prior training and experience was assessed by accessing the INPO Job and Task Analysis Data Base (Ref. 42). It was fairly straightforward to determine whether or not each knowledge requirement in Fig. 35 appears in the data base for the tasks for which the data base was developed. The *plant* knowledge found in the INPO data base can reasonably be assumed to be knowledge that operators will have *prior* to encountering a decision aid. This is because interaction with decision aids is a task that was not considered when developing the data base.

For information requirements not satisfied by prior training and experience, either operators have to be able to obtain this knowledge from other displays or resources or they have to be trained specifically to gain this knowledge. Figure 35 shows that many requirements will have to be satisfied by these means. The extent to which other displays and resources provide the requisite information is reasonably straightforward to assess. Training for use of the aid is more subtle.

To assess the extent to which training will satisfy the knowledge requirements shown in Fig. 35, one needs more than just the aid, design

DISPLAY: RV INTEGRITY (APPLICABLE TO ALL)

DISPLAY ELEMENT: CSF STATUS BOXES

PROTOTYPICAL MESSAGE: COMPARISON OF [EXPLANATIONS] IN TERMS OF [URGENCY] YIELDS RANK ORDER OF...

KNOWLEDGE REQUIREMENTS:

PLANT:
1. DEFINITION OF REACTIVITY
2. DEFINITION OF REACTOR COOLING SYSTEM INVENTORY
3. DEFINITION OF REACTOR VESSEL INTEGRITY
4. DEFINITION OF REACTOR COOLING SYSTEM COOLING
5. DEFINITION OF HEAT SINK
6. DEFINITION OF CONTAINMENT
7. PLANT STATE WITH LOSS OF REACTIVITY CONTROL
8. PLANT STATE WITH LOSS OF REACTOR COOLING SYSTEM INVENTORY
9. PLANT STATE WITH LOSS OF REACTOR VESSEL INTEGRITY
10. PLANT STATE WITH LOSS OF REACTOR COOLING SYSTEM COOLING
11. PLANT STATE WITH LOSS OF HEAT SINK
12. PLANT STATE WITH LOSS OF CONTAINMENT

DISPLAY:
1. DEFINITION OF COLOR CODING
2. DEFINITION OF TEXTURE CODING
3. DEFINITION OF BLINK CODING
4. HOW TO READ A STATUS INDICATOR
5. THAT RCS MEANS REACTOR COOLING SYSTEM
6. THAT RV MEANS REACTOR VESSEL

COMMAND: NONE

Figure 30. Knowledge requirements for critical safety function (CSF) status boxes display element: comparison and explanations.

DISPLAY: RV INTEGRITY

DISPLAY ELEMENT: CSF STATUS BOXES

PROTOTYPICAL MESSAGE: THE POSSIBLE INFORMATION SOURCES ARE [DISPLAY PAGES]

KNOWLEDGE REQUIREMENTS:

PLANT: NONE

DISPLAY:
1. ORGANIZATION OF DISPLAY HIERARCHY
2. GENERAL CONTENTS OF OTHER DISPLAY PAGES

COMMAND:
1. HOW TO ACCESS OTHER DISPLAY PAGES
2. HOW TO USE THE TOUCH SCREEN

Figure 31. Knowledge requirements for critical safety function (CSF) status boxes display element: identification of information sources.

DISPLAY: RV INTEGRITY

DISPLAY ELEMENT: ACTIVE PROCEDURE BOX

PROTOTYPICAL MESSAGE: THE CURRENT [PROCEDURE] IS...

KNOWLEDGE REQUIREMENTS:

PLANT:
1. DEFINITION OF PRESSURIZED THERMAL SHOCK CONDITION
2. DIFFERENCE BETWEEN ANTICIPATED AND IMMINENT PRESSURIZED THERMAL SHOCK CONDITION
3. HOW TO INITIATE THE PERFORMANCE OF THE PROCEDURES

DISPLAY:
1. LOCATION OF THE ACTIVE PROCEDURE BOX
2. THAT IF A PROCEDURE IS ACTIVE, ITS LABEL AND NAME ARE SHOWN IN THE ACTIVE PROCEDURE BOX
3. THAT THE PROCEDURES ARE ACCESSIBLE ON THE FOURTH-LEVEL DISPLAYS
4. THAT OTHER PROCEDURES ARE ALSO ACTIVE IF OTHER CSFS ARE INDICATED AS COMPROMISED
5. THAT PTS MEANS PRESSURIZED THERMAL SHOCK
6. DEFINITION OF COLOR CODING
7. DEFINITION OF TEXTURE CODING

COMMAND:
1. HOW TO ACCESS THE FOURTH-LEVEL DISPLAYS
2. HOW TO USE THE TOUCH SCREEN

Figure 32. Knowledge requirements for active procedure box display element.

DISPLAY:	RV INTEGRITY
DISPLAY ELEMENT:	MAX RCS COOLDOWN COLUMN CHART
PROTOTYPICAL MESSAGE:	THE CURRENT [STATE] IS...

KNOWLEDGE REQUIREMENTS:

PLANT:
1. DEFINITION OF REACTOR COOLING SYSTEM COOLDOWN
2. DEFINITION OF RAPID COOLDOWN MARGIN WITH RESPECT TO NIL DUCTILITY TRANSITION TEMPERATURE
3. DEFINITION OF DEGREES FAHRENHEIT

DISPLAY:
1. DEFINITION OF MAX RCS COOLDOWN LAST 30 MIN.
2. THAT DEG-F MEANS DEGREES FAHRENHEIT
3. RELATIONSHIP BETWEEN MAX RCS COOLDOWN LAST 30 MIN DISPLAY ELEMENT AND RV NDTT DISPLAY ELEMENT (THAT THE RV NDTT DISPLAY CHANGES WHEN MAX RCS COOLDOWN IN THE LAST 30 MINUTES INDICATES GREATER THAN 50 DEGREES FAHRENHEIT)
4. HOW TO READ A COLUMN CHART
5. DEFINITION OF COLOR CODING

COMMAND: NONE

Figure 33. Knowledge requirements for maximum reactor cooling system (RCS) cooldown column chart.

DISPLAY: RV INTEGRITY

DISPLAY ELEMENT: RV NDTT MARGINS PLOT

PROTOTYPICAL MESSAGE: THE CURRENT [STATE] IS...

KNOWLEDGE REQUIREMENTS:

PLANT:
1. DEFINITION OF REACTOR VESSEL NIL DUCTILITY TRANSITION TEMPERATURE MARGIN
2. DEFINITION OF COLD LEG TEMPERATURE
3. DEFINITION OF REACTOR COOLING SYSTEM PRESSURE
4. DEFINITION OF POUNDS PER SQUARE INCH-GAGE
5. DEFINITION OF DEGREES FAHRENHEIT
6. RELATIONSHIP OF REACTOR COOLING SYSTEM PRESSURE AND COLD LEG TEMPERATURE TO REACTOR VESSEL NIL DUCTILITY TRANSITION TEMPERATURE
7. EFFECT OF HIGH HEAD SAFETY INJECTION ON NIL DUCTILITY TRANSITION TEMPERATURE MARGIN

DISPLAY:
1. DEFINITION OF THE ZONES ON THE RV NDTT MARGIN PLOT
2. THAT RV NDTT MEANS REACTOR VESSEL NIL DUCTILITY TRANSITION TEMPERATURE
3. THAT DEG-F MEANS DEGREES FAHRENHEIT
4. THAT PSIG MEANS POUNDS PER SQUARE INCH-GAGE
5. THAT HHSI INIDCATES HIGH HEAD SAFETY INJECTION ACTUATION POINT
6. THAT LHSI INDICATES LOW HEAD SAFETY INJECTION ACTUATION POINT FOR REFERENCE
7. THAT ACCUM INDICATES ACCUMULATOR ACTUATION POINT FOR REFERENCE
8. HOW TO READ A PARAMETER-PARAMETER PLOT
9. DEFINITION OF COLOR CODING

COMMAND: NONE

Figure 34. Knowledge requirements for reactor vessel (RV) nil ductility transition temperature (NDTT) margins plot.

PLANT KNOWLEDGE	OPERATOR'S EXPERIENCE AND TRAINING	TRAINING FOR AID	OTHER DISPLAYS OR RESOURCES
Definition of reactivity	✓		
Definition of reactor cooling system inventory	✓		
Definition of reactor vessel integrity	✓		
Definition of reactor cooling system cooling	✓		
Definition of heat sink	✓		
Definition of containment	✓		
Definition of pressurized thermal shock condition	✓		
Definition of reactor vessel nil ductility transition temperature margin	✓		
Definition of rapid cooldown margins with respect to nil ductility transition temperature	✓		
Definition of reactor cooling system cooldown	✓		
Definition of cold leg temperature	✓		
Definition of reactor cooling system pressure	✓		
Definition of degrees Fahrenheit	✓		
Definition of pounds per square inch--gage	✓		
Plant state with loss of reactivity control	✓		✓
Plant state with loss of reactor cooling system inventory	✓		✓
Plant state with loss of reactor vessel integrity	✓		✓
Plant state with loss of reactor cooling system cooling	✓		✓
Plant state with loss of heat sink	✓		✓
Plant state with loss of containment	✓		✓
Relationship of reactor cooling system pressure and cold leg temperature to reactor vessel nil ductility transition temperature	✓		
Effect of high head safety injection on nil ductility transition temperature margin	✓		
Difference between anticipated and imminent pressurized thermal shock condition		✓	
How to initiate the performance of the procedures	✓		

Figure 35. Knowledge requirements summary for the reactor vessel (RV) integrity display.

Fig. 35 (continued)

DISPLAY KNOWLEDGE SUMMARY	OPERATOR'S EXPERIENCE AND TRAINING	TRAINING FOR AID	OTHER DISPLAYS OR RESOURCES
Definition of color coding		✓	
Definition of texture coding		✓	
Definition of blink coding		✓	
Definition of Max RCS Cooldown last 30 min	✓	✓	
Definition of the zones on the reactor vessel nil ductility transition temperature margin plot		✓	
How to read a status indicator	✓	✓	
How to read a column chart	✓	✓	
How to read a parameter-parameter plot	✓	✓	
Organization of display heirarchy	✓		
General contents of other display pages	✓		
Location of active procedure box	✓		
That if a procedure is active, its label and name are shown in the active procedure box		✓	
That the procedures are accessible on the fourth-level displays		✓	
That other procedures are also active if other Critical Safety Functions are indicated as compromised		✓	✓
Relationship between Max RCS Cooldown and RV NDTT Margin display elements (that the RV NDTT display element changes when Max RCS cooldown in last 30 min is indicating greater than 50 deg-F)		✓	
That PTS means pressurized thermal shock	✓	✓	
That RV NDTT means reactor vessel NIL ductility transition temperature	✓	✓	
That HHSI indicates high head safety injection actuation point	✓	✓	
That LHSI indicates low head safety injection actuation point for reference		✓	
That ACCUM indicates accumulator actuation point for reference		✓	
That DEG-F means degrees Fahrenheit	✓		
That PSIG means pounds per square inch--gauge	✓		
That RCS means reactor cooling system	✓	✓	
That RV means reactor vessel	✓	✓	
COMMAND KNOWLEDGE SUMMARY			
How to access all other displays		✓	
How to use the touch screen		✓	

documentation, and access to the designer. One must also have the program and the instructions for training in use of the aid.

If this type of information is not available, an alternative conclusion is: The aid will be understandable *if* a training program is devised to satisfy the knowledge requirements assigned to training. Thus the type of conclusion emerging from application of the proposed methodology is not simply whether or not an aid is understandable but also an assessment of what would be needed to ensure understandability. This is certainly much more useful than a simple "yes or no" type of evaluation.

5.3 SUMMARY OF EXAMPLE

The hypothetical example serves to illustrate how the proposed evaluation methodology can be applied to a realistic operator aid. While the analysis presented here is not complete, each step of the process outlined in Fig. 13 is illustrated sufficiently to provide an appreciation of how the methodology might be used. As discussed in Sect. 6, considerable work is needed to make the use of the methodology more straightforward and less dependent on "judgment." This example also serves to emphasize the nature of results typically obtained, which should include not only an assessment of understandability but also guidance on how deficiencies can be remedied.

6. DISCUSSION AND CONCLUSIONS

This report addresses the problem of evaluating decision aids for nuclear power plant operators. The scope of the effort was intentionally limited to analytical rather than empirical evaluation. The goal was not to replace empirical evaluation but instead to determine how definitive an analytical evaluation could be.

6.1 SUMMARY OF METHODOLOGY

The development of the methodology is based on the premise that each operator aid is representative of a general class of decision support systems for operators of dynamic engineering systems. Given this premise, the methodology is directed at this whole class of aids. This perspective allows the development (Sect. 2) of a scheme for classifying operator aids in terms of the general decision-making tasks supported. The practical utility of this classification scheme is illustrated (Sect. 3) by considering a number of existing aids and showing how they could readily be classified.

Having determined that all aids could be viewed as members of a general class, consideration then shifts to development (Sect. 4) of a normative top-down process for designing aids in this class. The process involves identifying the situations and tasks where the aid is to provide support and then the forms of information and prototypical messages necessary to provide the support. The final step of the detailed design is discussed briefly but not elaborated upon because it is the topic of available design guides.

An evaluation methodology is developed (Sect. 4) based on the assumption that any aid could be viewed as if it had been designed using the proposed normative design process. The basic idea is that by studying the aid and its design documentation, as well as talking with the designer and perhaps operators, one can infer the answers to the questions posed in the normative design process. The result is an association of each display element of the aid with one or more prototypical messages. One can then assess the knowledge requirements for understanding these messages. The final step is determining whether or not human operators meet these requirements--by prior training and experience, training for use of the aid, or other displays and resources (e.g., control panels or manuals). Knowledge requirements not met are potential limits to the understandability of the aid.

Application of the methodology is illustrated (Sect. 5) by applying it to the evaluation of a hypothetical aid for supporting recovery of critical safety functions in a PWR. The example serves to illustrate how each

step of the methodology is pursued, while also emphasizing the information (from design documentation and perhaps the designer and operators) necessary to answer the questions posed by the methodology. Even though only a portion of the aid is evaluated, the example also provides some indication of the effort necessary to pursue evaluation fully. Clearly, a complete evaluation would be a substantial effort.

6.2 METHODOLOGY STRENGTHS AND WEAKNESSES

One strength of the proposed methodology is that it provides a mechanism for classifying and comparing all operator aids in a very broad class. This should ease the evaluator's job and, once experience is gained with different types of aids, provide a means for detecting "common mode" problems with all aids of a particular classification. Another strength is that the methodology provides the highest level of analytical evaluation possible. It goes substantially beyond a classical human factors evaluation of compatibility and allows assessment of the understandability of the information presented. This is achieved by relying on a top-down view of design that focuses on the set of messages necessary to achieve design objectives rather than on the information requirements dictated by the results of traditional task analyses. By starting from "what should be" instead of "what is," a general set of evaluative questions can be posed which yields a highly directed evaluation process and allows extensive analytical evaluation.

Although it is not a primary goal, the methods presented in this report would also be very useful for design. This would be particularly true for the front-end portions of design, prior to actually laying out displays. Of course, the type of design process advocated in this report would be of great use if one anticipated using the proposed methodology to evaluate the resulting aid.

While the methodology has these strengths, it has two related weaknesses. First, it views any design as if a systematic design process had been pursued. In particular, it assumes that each element of information displayed by the aid is shown because it contributes to the achievement of one or more design objectives. However, some information will quite likely be included in the displays because of designers' "whims," that is, with no analytical justification for the information. The association of prototypical messages with such display elements will then be quite difficult.

A related weakness is that it will be difficult for a novice evaluator to apply the proposed methodology. As noted throughout this report, considerable judgment is needed to infer design intentions and, subsequently, to determine appropriate prototypical messages and knowledge requirements. Of course, this weakness, as well as that discussed above, is likely to be a limitation of any analytical evaluation methodology.

6.3 RECOMMENDATIONS FOR EXTENSIONS AND REFINEMENTS

As with most new methodologies, the greatest need is for the proposed methodology to be repeatedly applied and for those experiences to be used to provide more guidance to the evaluator, especially in areas where the evaluator now heavily relies upon judgment. This might also lead to empirical validation of the assertion that unfulfilled knowledge requirements, identified by the methodology tend to result in understandability limitations.

A more specific need involves extending the classification of decision-making tasks supported to include a dimension related to the sophistication of the aid. This would allow differentiation between the aids that can provide the rationale for their suggestions (e.g., expert systems) and those that are basically hard-wired algorithms. As a result, prototypical messages could be more definitive for each type of aid.

Another area where refinement is needed is in the knowledge taxonomy (Fig. 14), so that the determination of knowledge requirements can be more systematic and less dependent on judgment. As a result, evaluators would not need as much experience before being confident in their assessments. This is an area where success is quite likely with a fairly modest investment of resources.

The need for many other extensions and refinements is likely to emerge as experience in using the proposed methodology is gained. Therefore, the first priority should be that such applications be pursued.

REFERENCES

1. U.S. Nuclear Regulatory Commission, "Requirements for Emergency Response Capability." NUREG-0737, Supplement 1, December 1982.

2. A. J. Rockmore et al., "Decision Aids for Target Aggregation: Technology Review and Decision Aid Selection," Report 6459-200-1, Systems Control Technology, Palo Alto, California, May 1982.

3. W. B. Rouse and S. H. Rouse, "A Framework for Research on Adaptive Decision Aids," Search Technology, Inc., Report AFAMRL-TR-83-082, October 1983.

4. R. A. Kisner and P. R. Frey, "Functions and Operations of Nuclear Power Plant Crews," NUREG/CR-2587, ORNL/TM-8237, April 1982.

5. A. A. El-Bassioni, R. A. Hedrick, and R. W. Starostecki, "Review of Standards and Requirements Affecting Human Factors in Nuclear Power Plant Control Rooms," Science Applications, Inc., Report SAI 1-245-08-124-00, September 1980.

6. R. A. Kisner, A. M. Fullerton, P. R. Frey, and E. M. Dougherty, "A Taxonomy of the Nuclear Power Plant Operator's Role," presented at the Enlarged Halden Program Meeting on Process Computer Applications, Fredrickstad, Norway, June 14-19, 1981.

7. R. A. Kisner and G. F. Flanagan, "A Systems Approach to Defining Operator Roles," *IEEE Trans. Nucl. Science,* NS-28(1), 972-977 (1981).

8. M. Becker, R. C. Block, M. M. Danchak, R. R. Gay, D. R. Harris, and J. P. Tully, "A Systems Approach to Evaluation of Control Room Structure," BBH-81-1, Final Report, May 1981.

9. C. B. Oh, M. E. Watson, S. V. Asselin, A. R. Buhl, P. F. Knight, F. E. LeVert, and J. C. Robinson, "A Characterization of the Nuclear Power Plant Operator's Role," Technology for Energy Corp. Report TEC R-80-022, August 1, 1980.

10. S. V. Asselin and C. B. Oh, "A Characterization of the Nuclear Power Plant Operator's Role During Emergencies," ORNL/SUB-80/13852/1, August 1980.

11. C. B. Oh, E. M. Dougherty, and J. L. Hamrick, "Analysis of the Operator's Role During the Onset of an Emergency," Technology for Energy Corp. Report TEC R-81-004, February 27, 1981.

12. C. B. Oh, E. M. Dougherty, and J. L. Hamrick, "Analysis of the Operator's Role as Defined by Emergency Procedures Developed for a PWR and a BWR," Technology for Energy Corp. Report TEC R-81-018, June 19, 1981.

13. E. M. Dougherty, "Cognitive Demands on the Reactor Operator (as inferred from Emergency Operating Instructions)," Technology for Energy Corp. Report TEC R-81-014, June 30, 1981.

14. E. M. Dougherty, "Transitions in the Role of the Operator," Technology for Energy Corp. Report TEC R-81-015, June 30, 1981.

15. P. R. Frey and R. A. Kisner, "A Survey of Methods for Improving Operator Acceptance of Computerized Aids," NUREG/CR-2586, ORNL/TM-8236, April 1982.

16. P. R. Frey and R. A. Kisner, "A Survey of Methods for Improving Operator Acceptance of Computerized Aids," presented at the *Edison Electric Institute 1982 Engineering and Operating Computer Forum,* September 20-22, 1982, Denver, Colorado.

17. R. Pulliam, H. E. Price, J. Bongarra, C. R. Sawyer, and R. A. Kisner, "A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control," NUREG/CR-3331, ORNL/TM-8781, August 1983.

18. R. Pulliam and H. E. Price, "Allocating Functions to Man or Machine in Nuclear Power Plant Control," *Proc. Fifth Power Plant Dynamics, Control and Testing Symposium,* March 21-23, 1983, Knoxville, Tennessee.

19. R. Pulliam and H. E. Price, "Allocation of Functions to Man and Machine in the Automated Control Room," presented at the *Tenth Water Reactor Safety Research Information Meeting,* October 12-15, 1982, National Bureau of Standards, Gaithersburg, Maryland.

20. H. E. Price, R. E. Maisano, and H. P. Van Cott, "The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review," NUREG/CR-2623, ORNL/SUB/81-9027/1, November 1981.

21. L. S. Abbott and R. A. Kisner (Eds.), *Proceedings of the 1982 Workshop on Cognitive Modeling of Nuclear Plant Control Room Operators,* NUREG/CR-3114, ORNL/TM-8614, December 1982.

22. R. A. Kisner and T. B. Sheridan, "Computing and Cognition in Future Power Plant Operations," *Proc. Fifth Power Plant Dynamics, Control, and Testing Symposium,* March 21-13, 1983, Knoxville, Tennessee.

23. S. Baron, C. Feehrer, R. Maralidharan, R. Pew, and P. Horwitz, "An Approach to Modeling Supervisory Control of a Nuclear Power Plant," NUREG/CR-2988, ORNL/SUB/81-70523/1, October 1982.

24. U.S. Nuclear Regulatory Commission, "Guidelines for Control Room Design Reviews," NUREG-0700, September 1981.

25. W. B. Rouse, "Models of Human Problem Solving: Detection, Diagnosis, and Compensation for System Failures," *Automatica* 19(6), November 1983.

26. W. B. Rouse, "Outline of a Model of Human Problem Solving in Failure Situations," in L. S. Abbott and R. A. Kisner, Eds., *Proceedings of the 1982 Workshop on Cognitive Modeling of Nuclear Plant Control Room Operators*, NUREG/CR-3114, ORNL/TM-8614, December 1982.

27. J. Rasmussen, "The Role of Cognitive Models of Operators in the Design, Operation, and Licensing of Nuclear Power Plants," in *Proceedings of Workshop on Cognitive Modeling of Nuclear Plant Control Room Operators*, NUREG/CR-3114, ORNL/TM-8614, December 1982.

28. P. W. Thorndyke, "A Rule-Based Approach to Cognitive Modeling of Real-Time Decision Making," in L. S. Abbott and R. A. Kisner, Eds., *Proceedings of the 1982 Workshop on Cognitive Modeling of Nuclear Plant Control Room Operators*, NUREG/CR-3114, ORNL/TM-8614, December 1982.

29. B. Hayes-Roth and F. Hayes-Roth, "A Cognitive Model of Planning," *Cognitive Science*, 3, 1979.

30. S. Baron et al., "A Framework for Modeling Supervisory Control Behavior of Operators of Nuclear Power Plants," in L. S. Abbott and R. A. Kisner, Eds., *Proceedings of the 1982 Workshop on Cognitive Modeling of Nuclear Plant Control Room Operators*, NUREG/CR-3114, ORNL/TM-8614, December 1982.

31. T. B. Sheridan, "Cognitive Models and Computer Aids for Nuclear Plant Control Room Operators," in L. S. Abbott and R. A. Kisner, Eds., *Proceedings of the 1982 Workshop on Cognitive Modeling of Nuclear Plant Control Room Operators*, NUREG/CR-3114, ORNL/TM-8614, December 1982.

32. A. I. Siegel and J. J. Wolf, "Cognitive Models Embedded in System Simulation Models," in L. S. Abbott and R. A. Kisner, Eds., *Proceedings of the 1982 Workshop on Cognitive Modeling of Nuclear Plant Control Room Operators*, NUREG/CR-3114, ORNL/TM-8614, December 1982.

33. A. Newell and H. A. Simon, *Human Problem Solving*, Prentice-Hall, Englewood Cliffs, New Jersey, 1972.

34. K. L. Gimmy and E. Nomm, "Automatic Diagnosis of Multiple Alarms for Reactor Control Rooms," *Trans. Am. Nucl. Soc.* 41, 520 (1982).

35. R. A. Newton, R. C. Zyduck, and D. R. Johnson, "Using Cognitive Modeling to Improve the Man-Machine Interface," in L. S. Abbott and R. A. Kisner, Eds., *Proceedings of the 1982 Workshop on Cognitive Modeling of Nuclear Plant Control Room Operators*, NUREG/CR-3114, ORNL/TM-8614, December 1982.

36. L. Felkel, "STAR Disturbance Analysis and Surveillance System: Answers to Regulatory Review Questions," (correspondence to R. DiSalvo, U.S. Nuclear Regulatory Commission), Gesellschaft für Reaktorsicherheit (GRS) mbH, Garching, Federal Republic of Germany, June 1981.

37. W. E. Buttner et al., "STAR--A Concept for the Orthogonal Design of Man-Machine Interfaces with Application to Nuclear Power Plants," in G. Johannsen and J. E. Rijnsdorp, Eds., *Analysis, Design, and Evaluation of Man-Machine Systems*, IFAC/IFIP/IFORS/IEA, Baden-Baden, Federal Republic of Germany, September 1982.

38. S. E. Seeman, R. W. Colley, and R. C. Stratton, "Optimization of the Man-Machine Interface for LMFBRs," *Proceedings of the LMFBR Safety Topical Meeting*, Lyon, France, July 1982.

39. J. Rasmussen, "Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models," *IEEE Trans. Systems, Man, Cybernet.* SMC-13(3), 257-266 (May/June 1983).

40. W. B. Rouse, "Computer-Generated Display System Guidelines: Vol. 2, Developing an Evaluation Plan," Draft Report EPRI RP2184, February 1984.

41. P. R. Frey et al., "Computer-Generated Display System Guidelines: Vol. 1, Display Design," Draft Report EPRI RP2184, February 1984.

42. Institute of Nuclear Power Operations, "Job and Task Analysis Retrieval Manual," INPO Report, September 1983.

APPENDIX A

REVIEW OF OPERATIONAL AIDS FOR NUCLEAR POWER PLANT OPERATORS

A.1. INTRODUCTION

One of the subtasks of the Oak Ridge National Laboratory project, Operational Aids for Nuclear Reactor Operators, was to collect and classify information pertaining to a diversity of computer-based operational aids, primarily those aids that in some way support the cognitive behavior of the plant crew. The limited data base that resulted can assist in identifying the spectrum of possible aid functions and serve as the foundation for a comprehensive data base for future review processes.

Information concerning specific operational aids under development by various groups has been difficult to obtain by unorganized inquiry. Therefore, to enlarge and improve the data base, a questionnaire was prepared and used to canvass a limited number of manufacturers and developers. It was organized to include the following categories of information (the complete questionnaire is included in Sect. A.3):

1. problem definition
2. function
3. design
4. plant interface and environment
5. performance
6. operation
7. maintenance and testing
8. user training
9. documentation
10. work status

Responses to the questionnaire varied widely in detail and form, thus forcing distillation of the salient features of each operational aid from multiple information sources, including the initial questionnaire. These sources included technical and management presentations, technical papers and reports, personal discussions, taped responses, sales brochures, system specifications and schematics, and other documents. This type of data base should be viewed as dynamic, not static, owing to the nature of current trends in operational aid development. Thus the listings that follow in Sect. A.4 are neither exhaustive nor necessarily timely and represent only a cross section of the industry. The authors recommend that this data base be updated and expanded because of its potential usefulness to NRC and others.

A.2. GENERAL RESULTS

Data for this review were taken from the following operational aid systems:

1. AIDS - Abnormal Incident Decision Support (Atomic Energy of Canada)
2. DASS III - Disturbance Analysis and Surveillance System (EPRI-Electric Power Research Institute, Nuclear Power Division)
3. DCS - NUCLENET Display Control System (General Electric Company)
4. DMA - Diagnosis of Multiple Alarms (Savannah River Laboratory)
5. ESSS - Ebasco Safety Surveillance System (Ebasco Services)
6. HALO - Handling Alarms with Logic (Halden Reactor Project)
7. MIDAS - Master Information and Data Acquisition System (Hanford Engineering Development Laboratory)
8. ODDS - Operational Diagnostics and Display System (Idaho National Engineering Laboratory)
9. PIE - Plant Incident Evaluator (General Atomic Company)
10. PPS - Procedure Prompting System (Hanford Engineering Development Laboratory)
11. SAS - Safety Assessment System (Wisconsin Electric Power)
12. STAR - Disturbance Analysis and Surveillance System (Geselischaft für Reaktorsicherheit/Federal Republic of Germany)

The following general summary of the data is organized according to the major headings on the questionnaire to illustrate questionnaire organization.

Problem Definition. Six problem areas have been identified by the respondents:

1. Alarms cause operator confusion during normal and abnormal operation, with the number of alarms being great and their relevance not always clear.
2. Data rate (the quantity of information presented to the operator per unit of time) is high during fault conditions.
3. Data structure in the control room is suboptimal, bordering on no structure at all, which forces operators to expend mental and physical effort collecting and converting data.
4. Integration of systems, equipment, and information (inside and outside the control room) is not accomplished to a satisfactory degree.
5. Delayed detection of a deviation from normal leads to a degradation of plant safety because the inception of an event can often be traced back to the deviation of one or two parameters.
6. Incorrect diagnosis by the crew is a possibility even with ample time allowed for corrective action.
7. Procedures created by system experts are not exhaustive of all possible situations and combinations of situations.

Functions. Numerous functions have been incorporated by the aid designers. The following is a list of functions compiled from the 12 aids reviewed. (No one aid incorporated all of these functions.)

Discrete Alarms

1. Grouping alarms for operational or safety priority/significance
2. Grouping alarms for specific modes of operation or conditions of the plant
3. Suppression of nuisance and redundant alarms
4. Recognition of specific sequential and combinational patterns of alarms

Data

1. Validation of sensor data
2. Compression and grouping of data
3. Graphic display [piping and instrumentation diagrams (P&ID), functions, messages]
4. Trend analysis and display of parameter trends

Integration

1. Systems
   - Indication of configuration
   - Identification of mode and lineup
   - Indication of safety and control systems availability
   - Verification of operation
   - Indication of process status
   - Margin to technical specification
2. Components
   - Monitoring of specific equipment
   - Monitoring for prediction of failure
3. Procedures
   - Computer generation or retrieval of procedures
   - Monitoring procedures executed by the operator
   - Recommendations to the operator for specific tasks/actions

Diagnosis

1. Early detection and warning of disturbance
2. Identification of the cause of disturbance
3. Identification of the event in progress by probabilistic means
4. Indication of the presence of unanticipated circumstances for diagnosis
5. Prediction of the propagation of a disturbance
6. Prediction of the consequences of intended operator actions

For the aids surveyed the users that were intended for the system were varied and ranged from operators, shift supervisors, and shift technical advisors to plant engineers and their various combinations. The conditions under which the aids would be used also varied from aid to aid. Some aids are intended primarily for normal conditions only, some for abnormal conditions, and others for both. Most designers are reluctant to allow direct control of the plant by an operational aid, but, in fact, one aid surveyed is capable of scramming the reactor without operator intervention.

Design. Some aids are designed to exist as separate, stand-alone devices, but others are intended to be integrated into the plant control boards. In some cases, the option is left to the utility customer. Most designers are using modular software; some specify the use of verification and validation techniques. Almost universally, the cathode-ray tube (CRT) is used as the operator interface. Many aids have been prototyped on minicomputer systems, though most designers indicate the use of microcomputers for production equipment. Of the prototype aids now in existence, some have been tested on simulators, and a few have been tested in operating plants.

Plant Interface and Environment. Many of the aids require an equipment room for computers and memory drives. Computer equipment and peripherals are sensitive to ac power fluctuation, high temperature, high humidity, and dust. The aids require a tie-in to plant sensor signals; in some cases, additional sensors are required. The installation times for the aids generally extend over several plant outages.

Performance. Several respondents indicate goals of 99% equipment reliability. Predominant failure areas named were CRT, computer memory, data acquisition system (DAS), computer mainframe, and latent logic errors. Mean-time-between-failure (MTBF) and mean-time-to-repair (MTTR) data are generally not known for the aid systems. Response times of aids to a change in process state ranged from 1 s up, with no upper limits indicated in many cases. Response to an operator command ranged from 1 to 3 s for most aids. Input data verification was considered by some, with diverse schemes being employed to qualify data; some, however, did not specifically mention data verification as a part of the aid system.

Operation. Most aids employ CRT and function keyboard interfaces, and most are user interactive. Few designers, however, have considered the interaction between aid and existing procedures. Some have involved operators with the design of the aid or the testing process. Most designers consider the presence of existing control panels as sufficient information for independent verification of the conclusions rendered by an aid. Some go further by building in *scrutability* (i.e., they give the user a means to trace the development of an analysis). Regarding operator workload, no respondent could list specific operational tasks eliminated by aids, although general workload reductions were often cited.

Maintenance and Testing. Many aids are weak in this category. Some, however, include self-testing mechanisms.

Training. Operator training is needed for all systems. Some of the aids are self-explanatory, while others require that the operator be trained in the aid's use on a plant simulator. Designers vary in their opinions concerning how much knowledge should be required of the operator regarding the aid's method of performing its analysis. Some experience indicates that the more complete and detailed the operator's knowledge of the aid, the more the operator can follow the conclusions of the aid and use its information.

Documentation. Most aid designers have not addressed this subject thoroughly, because many aids are in the conceptual design state. Many designers plan to leave documentation to the customer.

Work Status. Of the 12 aids examined, three are installed and working at a power plant, two are installed at a plant simulator, and two are in the prototyping stage. The remaining aids are in the concept or laboratory development stages.

A.3. QUESTIONNAIRE

The following pages contain the specific questions used in the questionnaire. They were structured to elicit essay responses, which allowed for flexibility but demanded too much effort on the part of those responding. Thus the results are often shallow. A multichoice questionnaire, if properly structured, would have improved the data-collection process.

GUIDANCE QUESTIONS FOR REVIEW OF OPERATIONAL AIDS

PROBLEM

Identify the major problems related to operations or maintenance that prompted the development of the operational aid system. Which of these problems does the operational aid attempt to solve? Which category does the solution chosen best fit: interim, awaiting further resolution; adaptive, adding or modifying systems to supplement deficient equipment and functions; or corrective, changing existing equipment to completely eliminate the problem?

FUNCTION

ROLE/USER - Describe the operational aid system from a functional perspective. Include information about the functions the system performs and how these functions are performed. Identify the primary user(s) of the system and the plant conditions under which the system is expected to be used. Will the system support the operator in his function as a planner, monitor, controller, or diagnostician? Describe, using a block diagram, how operational aid functions relate to the operating crew and plant system.

MEMORY - Will the system maintain historical data? If so, how much information is stored and for how long? What means are provided to allow the operator access to the historical data?

CONTROL - Does the system perform any automatic control functions? Discuss the nature of the control actions and the control algorithms governing those actions.

DESIGN

SCHEME - Describe, using a schematic diagram, the electronic structure of the operational aid. Describe the physical outline of the aid using photographic or diagrammatic means.

COMPUTER - Describe the computer system used in the operational aid, including hardware and software structure.

VERIFICATION - Describe the methods used to verify and validate the design of the system. Include the hardware design review, software verification and validation, and verification of the accuracy and adequacy of the plant models.

STANDARDS - What standards have been used in the design and why were they chosen? Identify regulatory and non-regulatory standards, including equipment qualification for the system.

PLANT INTERFACE AND ENVIRONMENT

ISOLATION - How is the system isolated from the safety signals? Does the isolation comply with the requirements of IEEE 603?

INSTALLATION - Discuss the installation of the system. Provide the physical distribution of components within the plant. What components of the system are sensitive to temperature, humidity, air purity, C power fluctuations, or other environmental conditions? How are the acceptable environmental conditions around these components maintained? How much time is required for installation? Can installation be made in phases?

PERFORMANCE

RELIABILITY/ AVAILABILITY - Discuss the expected reliability characteristics to which the system has been designed. Identify the unreliability of the system, including both self-revealing and nonrevealing failure modes. Provide and justify the expected mean-time-to-failure and mean-time-to-repair data for the system. How has software reliability been factored into the overall reliability measure of the system?

RESPONSE TIME - Describe the response time characteristics of the system. To be included in this are the following: the maximum expected latency time between a change in a plant state or variable and the corresponding output from the system to the operator; the maximum expected response time of the system to operate commands; and the maximum data rates the system can withstand. Also describe the conditions under which these characteristics were determined.

VERIFICATION - Describe the methods which are used by the system to verify incoming data and identify the potential failures in the verification process.

OPERATION

INTERFACE - Describe the operator-system physical interface. Include a discussion of the human factors engineering features of the interface. Provide the results

of the evaluation of the interface using the guidelines set down in NUREG-0700.

INTERACTION - How have the operating procedures been changed to reflect the presence of the system? Has the system been integrated into the operational environment so that the user knows how the system relates to the other equipment in the control room? During which state of design, fabrication, installation, etc., did user involvement begin?

RESPONSIBILITY - How has the responsibility for operation of the aid been assigned? Is this a formal or an informal arrangement?

VERIFICATION - Discuss the methods available to the operating crew to verify the correctness of information from the system.

WORKLOAD - Describe the impact that the introduction of this system will have on the workload of the operating crew. What additional responsibilities does this system require of the operator (e.g., routine system backup, reinitialization of the system after failure, operational verification, emergency acknowledgments, action logs, and shift-change status reports)? What tasks have been eliminated to make time for operation of the system, especially during a burst of alarms?

COMMUNICATION - Is the user-system dialogue adaptable to the user's experience level? Has the structure and format of the user-system dialogue been adapted to the task and operational environment?

MAINTENANCE AND TESTING

Discuss the maintenance and testing requirements of the system. Identify the responsible organizations and their duties. Describe the methods used to verify the adequacy of the maintenance and testing procedures. What are the high-maintenance components of the system? To what extent are self-testing and on-line diagnostics used in the system?

USER TRAINING

What additional training does the operator need to use the system? Is it sufficient for the operator to know how to use the system or must he also know how the system performs the analysis? Does the system response during training accurately reflect the expected response during actual operation? Has a means of continued training of future users been adequately provided?

DOCUMENTATION

To what extent do the persons responsible for the system (both operational and maintenance) have control over the format and content of the system documentation? What procedures are followed to ensure that maintenance (both hardware and software) and operational documentation is kept current? Will documentation be available to the user prior to system start-up? Does the documentation reflect the user's perspective (as opposed to the designer's)?

WORK STATUS

In what state of development is the operational aid system: conceptual design, laboratory development, prototype, installed but not operational, or installed and operational? When is the aid expected to become operational?

A.4. OPERATIONAL AIDS DATA SHEETS

Responses to the questionnaire and other data sources were condensed and reformatted into data sheets. Editing of responses was minimized to avoid possible distortion of the data. The data sheet format follows along with the data sheets for each of the 12 aids reviewed (Sects. A.4.1 through A.4.12).

OPERATIONAL AIDS DATA SHEET FORMAT

SYSTEM NAME:

DEVELOPER:

INSTALLATION:

CONTACT PERSON:

DATE:

DATA:

1. PROBLEM

2. FUNCTION

- 2.1 ROLE/USER
  - 2.1.1 Functions
  - 2.1.2 Users
  - 2.1.3 Conditions
  - 2.1.4 Support
- 2.2 MEMORY
  - 2.2.1 Permanence
  - 2.2.2 User Access
- 2.3 CONTROL

3. DESIGN

- 3.1 SCHEME
- 3.2 COMPUTER HARDWARE
- 3.3 COMPUTER SOFTWARE
- 3.4 VERIFICATION
- 3.5 STANDARDS

4. PLANT INTERFACE AND ENVIRONMENT

- 4.1 ISOLATION
- 4.2 INSTALLATION
  - 4.2.1 Distribution of Components
  - 4.2.2 Environment-Related Sensitivities
  - 4.2.3 Installation Time

5. PERFORMANCE

- 5.1 RELIABILITY/AVAILABILITY
  - 5.1.1 Requirements
  - 5.1.2 Failure Modes
  - 5.1.3 MTBF
  - 5.1.4 MTTR

5.2 RESPONSE TIME
- 5.2.1 State Change Response
- 5.2.2 Operator Command Response
- 5.2.3 System Data Rate

5.3 INPUT DATA VERIFICATION

6. OPERATION

6.1 INTERFACE
6.2 INTERACTION
- 6.2.1 Integration with Procedures
- 6.2.2 Integration with Other Control Room Equipment
- 6.2.3 User Involvement

6.3 RESPONSIBILITY OF OPERATION
6.4 CREW VERIFICATION OF SYSTEM RESPONSE
6.5 WORKLOAD
- 6.5.1 Tasks Added
- 6.5.2 Tasks Eliminated

6.6 COMMUNICATION
- 6.6.1 Dialogue Adaptability to User Experience
- 6.6.2 Dialogue Structured to Task

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS
7.2 RESPONSIBLE ORGANIZATIONS
7.3 METHODS FOR VERIFICATION
7.4 HIGH-MAINTENANCE COMPONENTS
7.5 SELF-TESTING/DIAGNOSTICS

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED
8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED
8.3 USE OF SYSTEM DURING TRAINING
8.4 FUTURE USERS

9. DOCUMENTATION

9.1 USER CONTROL
9.2 CURRENCY
9.3 AVAILABILITY
9.4 PERSPECTIVE

10. WORK STATUS

10.1 CURRENT
10.2 EXPECTED OPERATION

A.4.1 OPERATIONAL AIDS DATA SHEET: ABNORMAL INCIDENT DECISION SUPPORT (AIDS)

SYSTEM NAME: AIDS - Abnormal Incident Decision Support

DEVELOPER: Atomic Energy of Canada Limited/Engineering Company

INSTALLATION: No specific target identified

CONTACT PERSON: M. A. Sillamaa

DATE: December 1982

DATA:

1. PROBLEM

There is a need to assist the operator during abnormal incidents by providing up-front alarm analysis and predictive capability. No specific operational problem was identified.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function 1 -

Identify specific accident in progress if possible.

e.g., loss of high-pressure service water due to pump PHS137 failure or pipe PTPB19-6 break

Method. Pattern recognition based on alarm trees.

Function 2 -

Identify specific abnormal function.

e.g., loss of heat sink

Method. Comparison of a combination of measured variables and derived variables (e.g., inlet subcooling) to limits.

Function 3 -

Identify if major pieces of equipment are under mechanical stress.

Method. Spectrum analysis of acoustical or process signals related to the equipment.

Function 4 -

Analysis-data storage and recall for past accident evaluation and reporting.

Method. Storage on hard disk.

2.1.2 User - Control room operator.

2.1.3 Condition - Abnormal incidents.

2.1.4 Support - Support operator in diagnostics and decision-making at incipient stages of an accident.

2.2 MEMORY - Historical data needed for prediction (Function 2) and past incident analysis and reporting (Function 4).

- Analysis models.

2.3 CONTROL - No direct control on process indicated; however, computer control is used in CANDU reactors.

3. DESIGN

3.1 SCHEME - Computers and displays will be separate from the control and safety computers.

3.2 COMPUTER HARDWARE - None selected, probably a super-mini (e.g., Sel-Gould; Perkin-Elmer).

3.3 COMPUTER SOFTWARE - None selected (trend toward simple programs with multiple self-checks).

3.4 VERIFICATION - Independent validation team; models used in system and models used to test a system derived from a common source (previous safety analyses).

3.5 STANDARDS - Normal engineering quality assurance program.

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Separate computers from control or safety computers. Common signal sources with other computers. Buffering techniques will be used to prevent interference.

4.2 INSTALLATION - Not specified.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY - No special requirements identified at this time.

5.2 RESPONSE TIME - 2 to 5 s for analysis results, variable with type of analysis.

5.3 INPUT DATA VERIFICATION - (1) irrationality checks; (2) physical redundancy checks; (3) analytical redundancy checks; (4) time averaging to achieve noise filtering and dynamic compensation.

6. OPERATION

6.1 INTERFACE - Dedicated displays for retrofits to existing stations; probably dual function display units, stored by control computers or AIDS computers, in new stations. Keyboard will probably be divided into three groups: numeric keys for data entry, control keys to control data entry, and function keys to initiate displays and analysis routines to be compatible with keyboards for other computer applications. No human factor guidelines.

6.2 INTERACTION -

6.2.1 Integration with Procedures - The system is capable of recalling procedures.

6.2.2 Integration with Other Control Room Equipment - On retrofits, separate display/keyboard units; in new stations, same display as used with control computers.

6.2.3 User Involvement - System requirements (i.e., functional contents and performance and human-machine interface) worked out mainly in consultation with unit operators. Operators will be involved in evaluating the prototype.

6.3 RESPONSIBILITY OF OPERATION - Plant operators.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - Other instruments and displays are available for verification of diagnosis.

6.5 WORKLOAD -

6.5.1 Tasks Added - Monitoring AIDS system and verification after an event.

6.5.2 Tasks Eliminated - Lookup of certain procedures performed automatically.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - Facility will be provided to adjust dialogue/display contents easily at the station (i.e., display templates will be used with a display compiler; displays will be generated in real time from the compiled templates plus read plant data).

6.6.2 Dialogue Structured to Task - Yes, specific function keys will probably be used.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - Not yet specified.

7.2 RESPONSIBLE ORGANIZATIONS - Station staff.

7.3 METHODS FOR VERIFICATION - Separate validation and software unit provided for station staff to verify changes.

7.4 HIGH-MAINTENANCE COMPONENTS - Not yet known.

7.5 SELF-TESTING/DIAGNOSTICS - Facilities standardly designed into CANDU computer systems will be provided.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - (1) in system facilities for operators; (2) in system contents, structure, software tools, hardware for maintenance purposes.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - Specialist in station staff will be required for software and hardware maintenance at the plant.

8.3 USE OF SYSTEM DURING TRAINING - Potentially to be included with plant simulator, if it exists, for a station.

8.4 FUTURE USERS - Not specified.

9. DOCUMENTATION

9.1 USER CONTROL - Passes to station staff on installation.

9.2 CURRENCY - Not specified.

9.3 AVAILABILITY - Proprietary.

9.4 PERSPECTIVE - Documentation standard to CANDU plants; some from designer perspective, some from user perspective.

10. WORK STATUS

10.1 CURRENT - Aid is in the concept state. A feasibility analysis is under way. Prototype development next.

10.2 EXPECTED OPERATION - Not known.

A.4.2 OPERATIONAL AIDS DATA SHEET: DISTURBANCE ANALYSIS AND SURVEILLANCE SYSTEM (DASS III)

SYSTEM NAME: DASS III System - Disturbance Analysis and Surveillance System (Phase III)

DEVELOPER: Electric Power Research Institute/Nuclear Safety Analysis Center (NSAC)

INSTALLATION: None specified

CONTACT PERSON: D. G. Cain, NSAC

DATE: January 1983

DATA:

1. PROBLEM

With a lack of integration of plant instrumentation, the operator needs assistance to accurately analyze and assess a disturbance.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Functions -

General Category	DASS Function
A. Overhead Functions	1. Proper interpretation and validation of process variables
	2. Identification of the plant mode of operation
	3. Integrated display of all DASS output
B. Surveillance Functions	4. Surveillance of system/subsystem configuration
	5. Verification that automatic control and protection system functions occurred
	6. Surveillance of margin to technical specifications

	7. Determine the status of the critical safety and availability requirements
C. Diagnosis Functions	8. Recognize the significance of alarms
	9. Disturbance detection by parameter analysis
	10. Determine the cause of the disturbance
D. Corrective Action or Procedures Functions	11. Determine the best corrective action
	12. Assistance in monitoring normal and off-normal operating procedures
E. Simulation Function	13. Predict the future propagation of disturbances
	14. Evaluation of possible control actions prior to initiation

Methods. Not given (trend away from cause-consequence implementation).

2.1.2 User - Shift supervisor.

2.1.3 Condition - Off normal.

2.1.4 Support - Supports shift supervisor in his role as a systems diagnostician, planner, and monitor (at systems level). Problem solving and decision making are primarily made by shift supervisor but with support from the other members of the crew.

2.2 MEMORY - DASS apparently has data storage and retrieval capability with user access through the functions provided.

2.3 CONTROL - No control process.

3. DESIGN

3.1 SCHEME - DASS is intended to be placed in proximity to the shift supervisor's area.

3.2 COMPUTER HARDWARE - Not specified.

3.3 COMPUTER SOFTWARE - FORTRAN 77.

3.4 VERIFICATION - Verification will be done when software package is actually adapted to specific user system.

3.4 STANDARDS - Will comply with standards as they evolve.

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Not specified.

4.2 INSTALLATION - Not specified.

4.2.1 Distribution of Components - Not specified.

4.2.2 Environment-Related Sensitivities - Not specified.

4.2.3 Installation Time - Not specified.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY -

5.1.1 Requirements - Reliability will equal SPDS (99%).

5.1.2 Failure Modes - Not specified.

5.1.3 MTBF - Not specified.

5.1.4 MTTR - Not specified.

5.2 RESPONSE TIME -

5.2.1 State Change Response - Less than 5 s.

5.2.2 Operator Command Response - Graphics response in 2 to 5 s.

5.2.3 System Data Rate - Update of information in 5 s. Must ensure that alarms are synchronized with actual control board.

5.3 INPUT DATA VERIFICATION - Same as SPDS.

6. OPERATION

6.1 INTERFACE - Various means are being considered, viz., keys, buttons, plasma screens, touch panels, etc. Human factors will be considered and complete system will be evaluated prior to selection.

6.2 INTERACTION -

6.2.1 Integration with Procedures - Automated monitoring of procedures will be included in initial DASS implementation.

6.2.2 Integration with Other Control Room Equipment - SPDS and process computer upgrade.

6.2.3 User Involvement - Some operator involvement at early stages.

6.3 RESPONSIBILITY OF OPERATION - Not specified.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - Backup information would be supplied by the control board operators.

6.5 WORKLOAD -

6.5.1 Tasks Added - A modifiction of crew structure, training, method of solving problems, and a redistribution of workload would be necessary.

6.5.2 Tasks Eliminated - Net workload should be reduced during accident situations because of enhanced information integration. Unlikely to affect control functions.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - Can be made to adapt to specific user.

6.6.2 Dialogue Structured to Task - Can be made to adapt to varying tasks.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - Will be developed later.

7.2 RESPONSIBLE ORGANIZATIONS - Will be developed later.

7.3 METHODS FOR VERIFICATION - Will be developed later.

7.4 HIGH-MAINTENANCE COMPONENTS - Will be developed later.

7.5 SELF-TESTING/DIAGNOSTICS - Will be developed later.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - Additional training necessary.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - Supports operator understanding of plant systems, critical instruments, and critical safety and availability requirements.

8.3 USE OF SYSTEM DURING TRAINING - Response of system under simulator conditions should reflect expected response on an actual plant but may differ depending on simulator veracity.

8.4 FUTURE USERS - Not specified.

9. DOCUMENTATION

9.1 USER CONTROL - Will be developed later.

9.2 CURRENCY - Will be developed later.

9.3 AVAILABILITY - Will be developed later.

9.4 PERSPECTIVE - Will be developed later.

10. WORK STATUS

10.1 CURRENT - Laboratory development.

10.2 EXPECTED OPERATION - None known.

A.4.3 OPERATIONAL AIDS DATA SHEET: DISPLAY CONTROL SYSTEM (DCS) - NUCLENET-1000

SYSTEM NAME: DCS - NUCLENET-1000 DISPLAY CONTROL SYSTEM

DEVELOPER: General Electric Company/Nuclear Energy Business Group

INSTALLATION: None at operating plants. Two at simulator facilities: BWR/6 Training Center, Tulsa, Oklahoma; BWR Services Training Center, San Jose, California

CONTACT PERSON: Leonard C. Pugh

DATE: June 23, 1982

DATA:

1. PROBLEM

Prior to NUCLENET-1000 there had never been any concerted effort to provide a human factors engineered control facility for nuclear power plants. Operators and maintainers had been forced to conform to the limitations of the hardware and software given to them. Panels were devised with controls and displays purchased as off-the-shelf components. Software and hardware were provided that met the needs of the designer, not necessarily the needs of the user.

A new computer-driven display system was designed to bring normal operations (and normally expected operational perturbations) information to the operator (and supervisory personnel).

The initiation of this solution effort began in 1971. The first implementation was installed in the field in late 1977, the second in 1978, and the third in 1981.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function 1 -

Alarm initiated display (AID) - The objective of AID is to provide early warning about the off-normal state of the primary AID variable, when such state has the potential for loss of power generation capability. This enables the operator to prevent an unscheduled outage of the plant for given plant conditions, because for each AID, there exists at least one alternative course of action (utilizing the control-room-operator interface), which can prevent either a pretrip alarm or trip of the reactor protection system.

Method. When a specified AID variable is found to be outside predetermined limits and an associated trigger logic expression is satisfied, an alphanumeric descriptor of this variable, with its numeric value, in engineering units is displayed, in the reserved area.

Function 2 -

Presentation of supportive data, which includes the status or value of those process variables that are helpful in determining the (normally anticipated) cause of the off-standard condition(s) of the specified AID variable.

Method. Associated with Function 1.

Function 3 -

Presentation of color- and shape-coded graphic displays generated as a result of operational information needs analyses for each process system. The system has the capability of 100 different dynamic display formats. Sixty-three were predesigned by GE, with the remainder to be designed as information needs change, due to process maturation.

Method. Associated with Function 1.

2.1.2 User - Real-time information for operating personnel and near real-time information for supervisory personnel.

2.1.3 Condition - Primarily pretrip conditions.

2.1.4 Support - DCS and subsystem AID should present the information in the best possible manner, which would prompt the trained operator to make cognitive, knowledge-based, response to that information. It cannot direct the activities of the operator.

2.2 MEMORY - The DCS is required neither to do numeric analysis nor to maintain historical data, because there is also a performance monitoring system (PMS) of mainframe computers to perform these functions. The PMS communicates with the DCS via a common core and a common drum memory and provides the limited historical data required for minute-to-minute operation of the plant. Examples of such data are vessel heatup rate and power versus core flow relationship. The PMS provides historical data via trend recorders, CRT displays (not

real-time), and high-speed line printers. Data retention for long-term storage is via magnetic tape.

2.3 CONTROL - System performs no automatic control functions, but it does perform automatic intersystem data transfer and automatic AID.

3. DESIGN

3.1 SCHEME - The DCS is physically integrated with the NUCLENET-1000 control complex console. A family of 63 display formats are available.

3.2 COMPUTER HARDWARE - Remote analog and remote digital units (RAUs & RDUs), under the control of data acquisition processors (DAPs), scan the analog and digital measurements, respectively, from process instrumentation. Signals are conditioned, and analog measurements digitized. The resulting data are sent to the DAPs from the RAUs and RDUs, as directed by the DAPs.

DAPs adjust the data by performing gain compensation, offset correction, digital filtering, sensor drift limiting, and sensor calibration. The data are checked for error conditions, range limits, and significant changes. Data that change significantly are converted to engineering units and sent by each of the DAPs to both of the display control processors (DCPs).

The DCPs are arranged in a redundant configuration, with the inactive DCP acting as an operational standby to the active DCP. Both DCPs operate on the same process data from the DAPs, with only the active DCP being able to communicate with the display generators (DGs). All processors are Honeywell 4500s.

Each DCP updates its data base with data from the DAPs; formats the data in accordance with the formats selected for each video monitor; and, in the case of the active DCP, outputs the formatted data to the video monitors through the DG.

The DCS is under the surveillance of an independent test and reconfiguration unit (TRU). The TRU determines the operational status of the major elements of the DCS, indicates this status to the operator, and activates switchover hardware in the event of a failure of the active DCP or one of the DAPs.

3.3 COMPUTER SOFTWARE - Not specified.

3.4 VERIFICATION - A dynamic mock-up of the operator/computer interface was built in GE's Engineering Lab. This mock-up was driven by the DCS hardware. This hardware, which was also used for the software development and test, was later shipped to our staging area for integration with the remainder of the control complex for a final system factory test, prior to shipment of the control complex to the utility site for installation.

Formal hardware design reviews are standard procedure for GE. Software verification was accomplished as a continuation of the development and test, because the entire system was available for such exercising.

3.5 STANDARDS - The only standard which was applicable to the DCS, at the time of the design, was Underwriters Laboratories (UL) 492: Radio & Television Receiving Appliances, paragraph 157; and Picture Tube Enclosure, paragraph 158.

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Regulatory Guide 1.75, physical independence of electrical systems, was the only regulatory action which had to be directly incorporated. At the time of the design it was the only regulatory action that applied to a non-Class 1E system design. Optically isolated inputs, from the few Class 1E circuits involved, provided the compliance with the requirements of RG 1.75.

4.2 INSTALLATION -

4.2.1 Distribution of Components - The system is part of an integrated control complex and usually is installed as a package. There is a provision for certain I/O units to be installed for customer use, external to the control complex.

4.2.2 Environment-Related Sensitivities - No specific sensitivities indicated; however, if the control complex is installed as designed, all components are located within the controlled environment of the control complex.

4.2.3 Installation Time - Because DCS comes with NUCLENET-1000, the system requires no additional time for installation, and with the exception mentioned above, there is no necessity for phased installation.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY -

5.1.1 Requirements - System reliability greater than 0.995. Unavailability no greater than 0.5% for any 90-day period. Confirmed by operational data.

5.1.2 Failure Modes - Drum memory failure and CRT failure are common failure modes.

5.1.3 MTBF - Not specified.

5.1.4 MTTR - Drum replacement: 4 h.
CRT replacement: 30 min.

5.2 RESPONSE TIME -

5.2.1 State Change Response -

Response Time. DCS response time is no greater than 250 ms and is defined as the duration of time between the instant a significant change occurs in the process and the instant the information is displayed. This delay does not include the delays caused by signal conditioning, filtering (within or without the DCS), inherent sensor delay, or any other delay caused by the components that are not part of the DCS.

Analog Signals. To ensure readibility, analog signals displayed as digital number are updated once per second.

Digital Signals. Digital signals are updated once per second.

5.2.2 Operator Command Response - 1 s.

5.2.3 System Data Rate - Response requirements of 250 ms apply to a maximum of 25 signals (analog, digital, or combination). The maximum number of signals given above is based upon a detailed transient analysis of the BWR, using transient analysis data for Chapter 15 of the Safety Analysis Report. Intrasystem maximum data rate is 230,000 baud.

5.3 INPUT DATA VERIFICATION -

Error Condition. A check is made to determine if acquired analog input values are within the operating range of the

analog-to-digital converter (ADC). Values exceeding the range of the ADC are considered low confidence. A check is made to determine if an open sensor error has occurred. This check is made on thermocouples only. The open sensor error is considered low-confidence data. All errors are uniquely noted as part of point data. The last good value is retained as the value of the input for processing and displaying. Each sensor in the failed state continues to be scanned. When the failure is corrected, the sensor is automatically returned to normal processing. An error for one sensor does not cause any reading of other sensors to read erroneously.

Sensor Range Limit Check. Analog inputs are compared against preassigned high- and low-sensor-range limits. Values changing to outside of the sensor-range limits are indicated as low-confidence data. Sensor-range limits cannot be changed by the operator from the control room (using the DCS/operator interface). Changes must be made using the PMS.

Validity Checks. Each signal, as it is received in a logic module, is checked for conformance with an anticipated value. This information is used for failure analysis.

Signal Transformation. Reference signals are processed through a comprehensive set of logical and arithmetic operations. These operations are intended to exercise basic logic components contained within the logic module. The results are predictable if all components are functioning correctly. If any one component fails, the results will indicate an error.

6. OPERATION

6.1 INTERFACE - The Display Control System (DCS) is a dual redundant (2 × 2) system of mainframe computers, with an integral test and reconfiguration unit (TRU), which provides real-time operating information to the operator via ten color CRTs, and near real-time operating information to the supervisory personnel via two color CRTs.

The color video monitor displays are controlled by either of two operator action paths: a master display select matrix (of backlighted pushbuttons) or a format select switch and a system select switch group associated with each CRT. Included with each switch group is a menu pushbutton (momentary), and a change enable pushbutton (also momentary).

One of the format select switch positions is indicated as the MASTER position. When the individual format select switches are in the MASTER position, the format displayed will be one which is assigned to a given phase of plant operation. The

master display select matrix communicates to the machine the particular phase of plant operation which the operator is performing.

The DCS formats employ the following color coding:

Green - Used only for lines and symbols in process diagrams to represent static system components, i.e., pumps, motors, valves, and, piping that are not dynamically presented in a given format. Selected for this association because the static elements make up the larger part of the display for a process control application and because a green hue has been demonstrated to be the least visually fatiguing of the available hues.

Cyan - Used as a supporting hue and applied to alphanumeric identification, scales, and borders.

Yellow - Applied to all dynamic process variable display elements, such as bar graphs and digital data. Selected for this application because of the intensity of its hue. Yellow allows the operator to scan the display and easily identify dynamic information.

Red - Restricted to use as a visual hue for abnormal conditions. Should any variable exceed process limits, the data (bar graph and/or digital) normally displayed in yellow, changes to red. Selected because of the traditional, preestablished psychological associations (populational stereotype) with such conditions and because intensity allows minimal visual search.

White - Used as a reference mark on scales, adjacent to bar graphs, to indicate process limits or to present low-confidence data.

Magenta - May be used in place of red.

Dark Blue - Shall not be used, because its visual loss against the normal background color.

Black - Used as normal background color.

No evaluation has been made using the guidelines of NUREG-0700, but the results of GE studies that differ from NUREG-0700 have been provided to the Human Factors Engineering Branch for consideration in the revision of NUREG-0700.

6.2 INTERACTION -

6.2.1 Integration with Procedures - System was included in the first draft of the operating procedures.

6.2.2 Integration with Other Control Room Equipment - Yes, the system has been integrated into the operational environment so that the user knows how the system relates to the other equipment in the control room.

6.2.3 User Involvement - User involvement began during the conceptual design phase. One licensed senior reactor operator represented the ultimate user until the mock-up state of the design, when other operations personnel were brought in to perform operator duties for task analyses.

6.3 RESPONSIBILITY OF OPERATION - The assignment to the operator is a formal one. The assignment to supervisory personnel is an informal one. It is intended that any person authorized to enter the control complex, who is not the operator at the controls, use the supervisory monitoring console to retrieve information, so that the operator need not be distracted from his primary duties. Operator is responsible for reinitialization after power failure.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - The system presents all dynamic data, which are not determined to be off-normal, in yellow. Off-normal dynamic data are presented in red. Dynamic data that the system determines to be low confidence (or suspect as to correctness) are presented in white. Each display format contains a 24-h clock in the lower right-hand corner to indicate display dynamicity.

System software has been tested and verified. The system hardware is under the surveillance of the test and reconfiguration unit, with automatic or manual reconfiguration capability.

Hardware configuration is displayed to the operator on a standby information panel, which is located immediately behind the NUCLENET control console. This panel is provided for the remote possibility (calculated reliability >0.995) that a complete failure of the DCS occurs. All hard-wired data displayed on the standby information panel are provided as a result of the operational needs analyses and are input to the DCS.

If the operator has reason to question the validity of the information displayed on the CRTs, a direct comparison can be

made. Not all data input to the DCS are also displayed on the standby information panel; only that information required to allow continued steady-state power operations, reasonable power maneuvers in the run mode, or a safe shutdown, without reliance on the DCS, is also displayed.

6.5 WORKLOAD -

6.5.1 Tasks Added - Reinitialize after power failure.

6.5.2 Tasks Eliminated - This system constitutes only a part of the total integrated design. It may decrease information search task time, by retrieving those data that are pertinent to the task at hand. It attempts to present data in a cognitive form, which closely approximates the operator's mental model of the process, thus reducing his internal information processing tasks. It provides hierachical display of the individual process systems involved, as well as matrix displays of integrated plant operation.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - Documented but not adaptable.

6.6.2 Dialogue Structured to Task - Yes, dialogue is user oriented.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - Test and reconfiguration unit (TRU) monitors DCS.

7.2 RESPONSIBLE ORGANIZATIONS - Maintenance of hardware is the responsibility of the customer's electronic maintenance organization.

7.3 METHODS FOR VERIFICATION - Not specified.

7.4 HIGH-MAINTENANCE COMPONENTS - Highest maintenance components are the CRTs.

7.5 SELF-TESTING/DIAGNOSTICS - In TRU.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - The operator requires no additional training beyond that currently included in the operator training program, because this is not a backfit product.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - It is sufficient for the operator to know how to use the system, because it currently performs no analysis.

8.3 USE OF SYSTEM DURING TRAINING - The system response during training accurately reflects the expected response during actual operation, because the integrated design is reproduced in full-scale simulators. One simulator is customer owned, the other is the property of GE, and the latter has been used for operator training for two years.

8.4 FUTURE USERS - Both simulators will be used for continued training of future users.

9. DOCUMENTATION

9.1 USER CONTROL - Up to customer.

9.2 CURRENCY - Up to customer.

9.3 AVAILABILITY - Available to user prior to system start-up.

9.4 PERSPECTIVE - User oriented.

10. WORK STATUS

10.1 CURRENT - The operational aid system, as a part of the integrated design, is installed and operational, even though the power plants they serve do not yet have operating licenses. The aid is being used during the preoperational tests of the plant.

10.2 EXPECTED OPERATION - Not specified.

A.4.4 OPERATIONAL AIDS DATA SHEET: DIAGNOSIS OF MULTIPLE ALARMS (DMA)

SYSTEM NAME: DMA - Diagnosis of Multiple Alarms

DEVELOPER: Savannah River Laboratory

INSTALLATION: SRL Production Reactor K

CONTACT PERSON: Kris L. Gimmy, Nuclear Engineering Division

DATE: April 30, 1982

DATA:

1. PROBLEM

When a true process casualty or accident occurs, the operator may be confronted with 50 to 100 alarms within a few seconds. He has no way of comprehending this, particularly if it is a pattern that he has not seen before.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function -

DMA recognizes patterns on the annunciator plates, while factoring in some analog data, and gives a clear indication of the source of the alarms and the location of the problem. These are displayed to the operator. DMA is not an alarm prioritization system.

Method. Unlike the work on the STAR system in Germany, SRL is starting from the accident end and working backward toward the cause and effect end (i.e., not starting the analysis with things such as lube-oil pumps, rather with things like breaks in the primary coolant system). Currently about 40 alarm trees in the system are in operation.

2.1.2 User - Control room operator.

2.1.3 Condition - Only for the most serious conditions. Does not respond to single alarms, but only to the 20 or 30 accidents that will lead either to a loss of coolant or loss of circulation in the primary loop.

2.1.4 Support - Supports operator in his role as a diagnostician.

2.2 MEMORY - None.

2.3 CONTROL - None.

3. DESIGN

3.1 SCHEME - DMA is to be integrated with closed-circuit monitors of process piping. The DMA uses data already available in the control computers plus the data from about 150 annunciators that are bought in the conventional digital inputs.

3.2 COMPUTER HARDWARE - Primarily a software system residing in existing computers: two Perkin-Elmer Model 816E with 64 K RAM, 1-MB fixed-head disk; Computer Products scanner multiplexed through Cunningham cross-bar system. Conrac video display unit.

3.3 COMPUTER SOFTWARE - Not specified (40% of software is audit related).

3.4 VERIFICATION - This system was extensively prototyped and tested in an SRL laboratory before it was installed. The method of verification or validation was to build a complete prototype in SRL shops and to operate it for several months using simulated inputs from low-level voltage sources before installing it in a reactor.

3.5 STANDARDS - The standards used in the design of DMA are primarily the DuPont design standards for computer systems.

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Safety systems temperature signals which are used by the control computer (hence DMA) are isolated by swamping resistors. The method of averaging signals yields 1000-to-1 isolation from feedback problems.

4.2 INSTALLATION -

4.2.1 Distribution of Components - The control computers are located in a room separate from the control room in their own carefully controlled environment (i.e., typical computer room: special air conditioners, etc.).

4.2.2 Environment-Related Sensitivities - The computer system is sensitive to ac power fluctuations. If the plant power bus drops to about 88% of normal voltage, both safety computers will go inoperative giving a reactor scram. This has happened on a couple of occasions.

4.2.3 Installation Time - Not specified.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY -

5.1.1 Requirements - Not specified.

5.1.2 Failure Modes - Scanner card failure and mainframe failures.

5.1.3 MTBF - Computer: 1 month.
Low-level analog-scanner system: 1 week.

5.1.4 MTTR - Computer: 2 h.
Low-level analog-scanner system: 10 min.

5.2 RESPONSE TIME -

5.2.1 State Change Response - 30 s maximum.

5.2.2 Operator Command Response - Not given.

5.2.3 System Data Rate - 1000 points per s (safety computer).

5.3 INPUT DATA VERIFICATION -

Performed in software. No further information given.

6. OPERATION

6.1 INTERFACE - The DMA does not receive much operator input; however, there is a four-position switch from which the operator indicates the basic state of the reactor, whether it is loaded or unloaded, whether it is at power or shutdown. The switch position determines some of the ground rules for the alarm analysis. The interfaces have not been evaluated against NUREG-0700.

6.2 INTERACTION -

6.2.1 Integration with Procedures - Procedures reflect DMA.

6.2.2 Integration with Other Control Room Equipment - DMA is integrated functionally with other control room equipment.

6.2.3 User Involvement - User involvement began during the prototype stage, where the system was running in the laboratory for about six months before control room installation.

6.3 RESPONSIBILITY OF OPERATION - The responsibility for operating the aid is with the people that operate the reactor. No computer specialists are on shift; hence, any technical advice that they need is vested in the written procedures. Operators are responsible for reinitializing after power failure. This is done by pushing one button.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - The operating crew decides the correctness of the system. They do this by responding to the internal self-revealing diagnostics that are built into the software.

6.5 WORKLOAD -

6.5.1 Tasks Added - Not specified.

6.5.2 Tasks Eliminated - Not specified.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - None.

6.6.2 Dialogue Structured to Task - Very little dialogue. Operators are not required to know any special computer language.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - Not specified.

7.2 RESPONSIBLE ORGANIZATIONS - Maintenance is the responsibility of the plant instrument group. A special division is devoted to computer repair, with people that are specially trained, having been to manufacturer's schools. Blueprints and spare parts are available. A laboratory computer system is at their disposal, which was used for program development; they can use it for testing repair parts.

7.3 METHODS FOR VERIFICATION - Not specified.

7.4 HIGH-MAINTENANCE COMPONENTS - Scanners in the control computer (which is the host for DMA).

7.5 SELF-TESTING/DIAGNOSTICS - Yes, used to a great extent.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - The operator receives training on how to use the system as part of his training to become a reactor operator.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - Not specified (very little operator memorization).

8.3 USE OF SYSTEM DURING TRAINING - Extensive.

8.4 FUTURE USERS - Program development center (PDC) used for continued training for future users.

9. DOCUMENTATION

9.1 USER CONTROL - All software for the computer systems is prepared by the plant technical group, specifically the reactor technology group, which has been doing the work for 15 years. A strict administrative procedure exists on how the software is to be documented. Every piece of software is documented by a program abstract as well as a listing. A program abstract gives all of the formulae used in that specific module. It describes the limitation of the mathematics, and a flowchart is included that describes the logical decisions, branching, etc.

9.2 CURRENCY - Updated. Every time the program is changed, the documentation is changed and reviewed by the reactor department and by the reactor technology department.

9.3 AVAILABILITY - Not specified directly, but apparently available to the operator if needed.

9.4 PERSPECTIVE - Software is computer programmer oriented; procedures are operations oriented.

10. WORK STATUS

10.1 CURRENT - DMA is installed at the K reactor and is under test.

10.2 EXPECTED OPERATION - Operation at other two reactors by 1983.

A.4.5 OPERATIONAL AIDS DATA SHEET: EBASCO SAFETY SURVEILLANCE SYSTEM (ESSS)

SYSTEM NAME: ESSS - Ebasco Safety Surveillance System

DEVELOPER: Ebasco Services Incorporated

INSTALLATION: None

CONTACT PERSON: Shaikh Moinul Matin

DATE: January 1983

DATA:

1. PROBLEM

Operation's problems affect availability safety, security, and efficiency of nuclear power plants. Early warning and correction can help to maintain the plant in its original intended (optimum) state. To achieve this, a surveillance system that detects the slightest degradation can be implemented. All plant component failures and malfunctions, if investigated far enough, begin as a single degradation of one parameter. The time history of pattern of degradations of various parameters is the telltale of the event to follow and possible remedial actions. Rather than devise a system dedicated to analysis (post accident), the ESSS is primarily designed on the philosophy of flagging plant degradations before the situation is severe enough to warrant safety actions. Thus, if a plant can be kept within the original licensed envelope, the plant is safe. This improves the plant availability also.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function -

Alert and advise of deviation from normal before serious problems develop.

Method. Proprietary time history pattern recognition system implementing artificial intelligence.

2.1.2 User - Plant supervision - all levels.

2.1.3 Condition - Normal (preaccident) operation; limited use in accident.

2.1.4 Support - Supports operator in monitoring, diagnostics, and maintenance.

2.2 MEMORY - Logs operator decisions and events for future analysis.

2.3 CONTROL - Does not alter controls in the control room, but can independently scram the reactor.

3. DESIGN

3.1 SCHEME - ESSS is to be integrated with other consoles in control room.

3.2 COMPUTER HARDWARE - Distributed microprocessors, plus dedicated minicomputer.

3.3 COMPUTER SOFTWARE - Proprietary. Has self-checking programs. Artificial intelligence system capable of learning, adapting, and self-criticizing.

3.4 VERIFICATION - Two modes exist. One examines the integrity of certain sensor signals, while the other confirms whether the signal is valid or not, for the intended use. The system realizes that validity of a signal changes with the intended use.

3.5 STANDARDS - According to developer, ESSS performs well beyond the requirements of NUREG-0696, NUREG-0700, and Regulatory Guide 1.92, Revision 2.

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Signals for this system are isolated (as close to sensors as possible) from the existing electronics and are expected to be in compliance with IEEE 603. Ebasco system failure will not affect the usual operations of the plant except that the assistance it provides to the operator will not be present.

4.2 INSTALLATION -

4.2.1 Distribution of Components - Plant specific. Additional sensors may be needed.

4.2.2 Environment-Related Sensitivities - Designed for control room environment and some transient environments.

4.2.3 Installation Time - Installed during regular plant outages; no additional downtime is necessary.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY -

5.1.1 Requirements - The ESSS developers are aiming for a 2.2% improvement in plant availability by the use of ESSS. No reliability figure given for ESSS. System is constantly self-criticizing.

5.1.2 Failure Modes - Developers consider the worst failure mode loss of ESSS function. Because it does not alter the operations or procedures of normal control room activities, it cannot degrade the reliability of plant controls.

5.1.3 MTBF - Not given.

5.1.4 MTTR - Not given.

5.2 RESPONSE TIME -

5.2.1 State Change Response - Time not specified; however, ESSS will respond to parameter out of tolerance by 0.1% or at most 1.0%.

5.2.2 Operator Command Response - Not given.

5.2.3 System Data Rate - Not given.

5.3 INPUT DATA VERIFICATION - Various techniques are used for verification and validation of signals and data. These include redundant sensors, additional calculations, periodic testing, etc., to achieve a certain level of reliability of the information which is used in making decisions.

6. OPERATION

6.1 INTERFACE - Interactive consoles and displays. Conforms to human factors guidelines of NUREG-700.

6.2 INTERACTION -

6.2.1 Integration with Procedures - Can be reflected in procedures only if desired by client.

6.2.2 Integration with Other Control Room Equipment - An issue to be discussed with the client.

6.2.3 User Involvement - Developers feel that user involvement should be minimum or none at all.

6.3 RESPONSIBILITY OF OPERATION - Not directly addressed. Developers feel the responsibility of operation of the system and for the maintenance staff is an issue to be addressed with the specific client utility.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - Plant instruments available for verification.

6.5 WORKLOAD -

6.5.1 Tasks Added - Monitoring ESSS.

6.5.2 Tasks Eliminated - Monitoring of diverse plant instruments.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - Dynamic adaptation possible because of artificial intelligence.

6.6.2 Dialogue Structured to Tasks - To be accomplished within a specific time. These are pertinent to the specific plant.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - No requirement placed on control room personnel.

7.2 RESPONSIBLE ORGANIZATIONS - Support group responsible for maintenance and testing of ESSS.

7.3 METHODS FOR VERIFICATION - Self-checks by various validation techniques.

7.4 HIGH-MAINTENANCE COMPONENTS - None specified.

7.5 SELF-TESTING/DIAGNOSTICS - Yes, proprietary, based on pattern recognition.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - Operator training or familiarity with the system can be achieved on the training simulator, or in the control room.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - Operators do not have to understand the operation of the ESSS in order to use it effectively.

8.3 USE OF SYSTEM DURING TRAINING - Eventually by use of the training simulator.

8.4 FUTURE USERS - Trained by system or simulator.

9. DOCUMENTATION

9.1 USER CONTROL - Not specified.

9.2 CURRENCY - Not specified.

9.3 AVAILABILITY - Not specified.

9.4 PERSPECTIVE - Not specified.

10. WORK STATUS

10.1 CURRENT - Work is in progress along with the development of software and algorithms. Developers are in search of prospective clients for possible fundings to build a prototype, demonstrate system on his plant. ESSS can be implementd in stages such that the first stage satisfies the NRC requirements NUREG-0696. Stages can be added on later. Beside safety enhancement and NRC requirements, plant availability improvement is the chief benefit derived from the implementation of such a system. Numerical estimate of availability improvement is being developed.

10.2 EXPECTED OPERATION - Unknown.

A.4.6 OPERATIONAL AIDS DATA SHEET: HANDLING ALARMS WITH LOGIC (HALO)

SYSTEM NAME: HALO - Handling Alarms with Logic

DEVELOPER: Halden Reactor Project/Norway

INSTALLATION: Halden Experimental Facility

CONTACT PERSON: Smidt Olsen

DATE: February 23, 1982

DATA:

1. PROBLEM

Operator is in most need of support during first stages of decision making because:

1. data flow rate is too high during major disturbances, and

2. essential information during major disturbances is scattered over the control boards.

The HALO concept is to automatically check that all required actions take place. Alarming occurs if these actions do not occur. The concept can be adapted to both existing control rooms and new control rooms.

The operator needs a simplified presentation of the plant status in order to maintain a clear overview, and he also needs detailed information to support his diagnostic work. The HALO alarm-presentation concept reflects this duality of needs by separating the presentation of information needed for overview from the detailed information needed for diagnostic work.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function 1 -

Alarm if automatic functions that should follow a trip are not carried out.

Method. Suppress signals that indicate function is being carried out.

Function 2 -

Alarm extraction through suppression of alarms that result from normal consequences of process conditions.

Method. Combinational and sequence logic and time delay.

Function 3 -

Display overview and detailed alarm information.

Method. A hierarchical alarm display concept is used. This consists of an overview picture, which utilizes information coding methods other than text (i.e., symbols and colors) and a hierarchy of detail pictures where the alarm information is integrated with other process information. In addition, the concept includes ordinary alarm text displays.

Function 4 -

List and sort alarms of recent history.

Method. An alarm record is maintained on mass storage. Different search profiles are available for the operator.

Function 5 -

Implementation and updating of the on-line system.

Method. An off-line program accepts the definition of process signals and alarm condition in "plain language" and translates this information into suitable form for the on-line part.

2.1.2 User - Shift supervisor and control room operators.

2.1.3 Condition - Used under all conditions from operating to post scram.

2.1.4 Support - Support the operator as a process monitor and diagnostician.

2.2 MEMORY - Alarm record maintained so that the operators are able to sort and list alarms from the recent history.

2.3 CONTROL - None directly; indirectly through the operator.

3. DESIGN

3.1 SCHEME - Not available.

3.2 COMPUTER HARDWARE - Prototype developed on minicomputer equipment. Final system will use distributed dedicated microcomputers. Electromechanical storage devices (e.g., magnetic disks) will be avoided because of reliability and speed considerations. System will be modular, with each module a self-contained unit that can talk asynchronously to other modules through a data bus. A transfer rate of 1 to 2 Mbytes/s is expected. A proposed system: each single board computer has a storage capacity of 128 Kbytes of RAM plus 8 K of EPROM for the basic software. An additional card containing 512 Kbytes of RAM can be plugged into the local bus extension.

3.3 COMPUTER SOFTWARE - System is functionally divided into an off-line and on-line part. The off-line part translates information from operators into the internal data structures for later use by the on-line system. The on-line part runs continuously and generates alarms based on the off-line edited a priori data. The off-line program is a batch process. The on-line program consists of four parts: (1) registration (raw process data collection); (2) preprocessing (range, limit, validation, and consistency checks); (3) alarm generation (logic); and (4) presentation (overview, detail, and text displays).

3.4 VERIFICATION - Planned.

3.5 STANDARDS - Designers believe none apply.

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Will not interfere with safety.

4.2 INSTALLATION -

4.2.1 Distribution of Components - Instrument cabinets and control room.

4.2.2 Environment-Related Sensitivities - Needs air conditioning and humidity control.

4.2.3 Installation Time - Several shutdowns needed. Phased approach possible.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY -

5.1.1 Requirements - <1% unavailability.

5.1.2 Failure Modes - Latent errors possible due to the nature of the process and the way the logic is established.

5.1.3 MTBF - Not specified.

5.1.4 MTTR - Not specified.

5.2 RESPONSE TIME -

5.2.1 State Change Response - 1 s.

5.2.2 Operator Command Response - 1 to 2 s.

5.2.3 System Data Rate - Not assigned.

5.3 INPUT DATA VERIFICATION - Limit check, range check, consistency check, and majority voting.

6. OPERATION

6.1 INTERFACE - One CRT for overview; one or more CRTs for working alarm system. Tracker ball, numerical pad, or touch-screen interface needed. Color and blink are used for coding. Specific layout is dependent on control room. There are in principle three kinds of displays for presentation of alarms that the operators can request on different screens in the control room: an overview picture, detailed alarm group pictures, and alarm texts.

(a) In the overview picture there is a schematic diagram of the whole process. The overview is divided into areas representing subsystems in the process. When one or more alarms in a subsystem are active, the corresponding area in the overview picture is given the actual alarm color. When there are not any active alarms in a subsystem, the corresponding area in the picture is given a color (one of two), which indicates whether or not the subsystem is operating. It is assumed that a proper criterion for this can be found for each subsystem, e.g., a neutron flux for the reactor, pressure for different pressure vessels, flow for steam lines or condensate and feed water systems, etc. Because some of the alarms cannot be directly related to the main process diagram, they are

grouped together by their origin and are given a special symbol in the overview picture (high radiation level, high room temperature, fault in pressurized gas delivery system, etc.). As a result, each alarm belongs to an alarm group which is represented by an area on the overview.

The objective of using this kind of an overview picture is to give the operator the possibility to obtain with a glance the main status as well as the alarm situation of the process. There will not be any text in the overview picture.

(b) The alarm group detail pictures are schematic diagrams that can display individual alarms in a way similar to the overview; for example, the detail picture for the plant electric power supply systems would be a rather detailed one-line diagram. Correspondingly for the high room temperature alarms, the detail picture would show the alarming sensor location on a map of the plant buildings. In addition, some alphanumeric information (e.g., room number or circuit breaker code) can be given.

(c) The alarm text displays are lists of alarm indications in chronological order of occurrence. Each such indication includes the time when set, identification code, and alarm message in plain language. A list can contain all current alarms or only alarms belonging to selected alarm groups and alarm urgency classes. Any combination of these selection criteria can be used to form a new alarm list. For example, all highest urgency alarms can be shown on one screen and all the rest on another screen or only the alarms in the condenser, or condensate and feedwater system can be selected to be listed.

6.2 INTERACTION -

6.2.1 Integration with Procedures - None specified.

6.2.2 Integration with Other Control Room Equipment - Not specified.

6.2.3 User Involvement - Nuclear operators have participated in design.

6.3 RESPONSIBILITY OF OPERATION - Not specified.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - Operator may inspect plant signals to detect faulty signal. This may be entered into HALO. HALO will then disregard that signal.

6.5 WORKLOAD -

6.5.1 Tasks Added - Monitor and operate HALO.

6.5.2 Tasks Eliminated - Collecting plant alarm data, recognizing individual alarms, summarizing process status.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - Not specified.

6.6.2 Dialogue Structured to Task - Function-oriented keyboard.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - Not specified.

7.2 RESPONSIBLE ORGANIZATIONS - Not specified.

7.3 METHODS FOR VERIFICATION - Not specified.

7.4 HIGH-MAINTENANCE COMPONENTS - Not specified.

7.5 SELF-TESTING/DIAGNOSTICS - Not specified.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - Some training needed for functional keyboard and tracker ball.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - Not necessary for operator to know how HALO performs its analysis, although such knowledge may build up user confidence.

8.3 USE OF SYSTEM DURING TRAINING - Not specified.

8.4 FUTURE USERS - Not specified.

9. DOCUMENTATION

9.1 USER CONTROL - Not specified.

9.2 CURRENCY - Not specified.

9.3 AVAILABILITY - Not specified.

9.4 PERSPECTIVE - Not specified.

10. WORK STATUS

10.1 CURRENT - Laboratory development with one small prototype running at Halden experimental facility.

10.2 EXPECTED OPERATION - Not specified.

A.4.7 OPERATIONAL AIDS DATA SHEET: MASTER INFORMATION AND DATA ACQUISITION SYSTEM (MIDAS)

SYSTEM NAME: MIDAS - Master Information and Data Acquisition System

DEVELOPER: Hanford Engineering Development Laboratory
Westinghouse Hanford Company

INSTALLATION: Fast Flux Test Facility (FFTF)

CONTACT PERSON: S. E. Seeman

DATE: December 1982

DATA:

1. PROBLEM

In previous systems the operator relied on long lists, memory, and his own knowledge of the plant to determine the functional relationships of equipment in the plant and whether or not these pieces could be released for maintenance. Several information sources in combination give the operator knowledge of the state of the plant and allow him to decide whether or not to release the components for work. Use of this distributed information requires human's data gathering and logical powers. In many situations this is done under stress, such as multiple requests for work on different parts of the plant. The MIDAS sytem was developed to consolidate these information sources. The operator uses this system to help him make decisions about whether or not to allow maintenance or repair work to be done on the plant.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function 1 -

Supply predesignated technical information concerning plant components.

Method. Not specified.

Function 2 -

Integrate the plant components by function.

Method. Not specified.

Function 3 -

Provide variable query and sort capability.

Method. Not specified.

Function 4 -

Provide variable reporting capability.

Method. Not specified.

Function 5 -

Maintain work document status.

Method. Not specified.

Function 6 -

Maintain component status of components affected by work documents.

Method. Not specified.

Function 7 -

Provide a high level of control and visibility of processed work.

Method. Not specified.

2.1.2 User - Plant operator.

2.1.3 Condition - Used under all conditions.

2.1.4 Support - Supports user as planner.

2.2 MEMORY - Not specified.

2.3 CONTROL - None.

3. DESIGN

3.1 SCHEME - Not specified.

3.2 COMPUTER HARDWARE - Not specified.

3.3 COMPUTER SOFTWARE - Not specified.

3.4 VERIFICATION - Not specified.

3.5 STANDARDS - Not specified.

4. PLANT INTERFACE AND ENVIRONMENT - Not specified.

5. PERFORMANCE - Not specified.

6. OPERATION - Not specified.

7. MAINTENANCE AND TESTING - Not specified.

8. USER TRAINING - Not specified.

9. DOCUMENTATION - Not specfied.

10. WORK STATUS - In use at FFTF.

A.4.8 OPERATIONAL AIDS DATA SHEET: OPERATIONAL DIAGNOSTICS AND DISPLAY SYSTEM (ODDS)

SYSTEM NAME: ODDS - Operational Diagnostics and Display System

DEVELOPER: Idaho National Engineering Laboratory

INSTALLATION: LOFT

CONTACT PERSON: Eddie A. Krantz

DATE: March 4, 1982

DATA:

1. PROBLEM

Control rooms display over 2000 individual readings. Relating these readings during a transient to the predicted behavior as documented in technical manuals is impractical. Rules are thus applied to interpret readings and generate behavior. A higher principle of operation can be applied by relating the function state of the plant to analytical predictions of behavior via computer technology.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function 1 -

Generate diagnostic-oriented graphics.

Method. Color CRT graphics program developed at LOFT.

Function 2 -

Generate diagnostic messages.

Method. Computer calculation based on measured quantities.

2.1.2 User - Control room operators and supervisors.

2.1.3 Condition - Seems to apply to all conditions of plant.

2.1.4 Support - Supports operator as a monitor of the state of the plant and as a diagnostician.

2.2 MEMORY - Trend information is held for operator recall.

2.3 CONTROL - Not specified.

3. DESIGN

3.1 SCHEME - ODDS is a part of an NRC research program at LOFT. The design appears to be stand alone (from control boards), and it changes as new ideas and concepts are added and removed.

3.2 COMPUTER HARDWARE - Magnetic tape; 80 MB disk; Ramtek 6200A; Prime 550 mainframe.

3.3 COMPUTER SOFTWARE - Not specified.

3.4 VERIFICATION - Verified by experimentation and administrative procedures.

3.5 STANDARDS - Internal standards used for software configuration control, operation of data acquisition and visual display system, conduct of LOFT operation, calibration, and assignment of responsibility.

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Safety signal isolation observed.

4.2 INSTALLATION -

4.2.1 Distribution of Components - Equipment closet for mainframe and memory. Three Ramtecs in control room area. One Ramtec in technical support center.

4.2.2 Environment-Related Sensitivities - Heat in equipment closet. Disk is sensitive to temperature.

4.2.3 Installation Time - Not specified.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY -

5.1.1 Requirements - Not specified.

5.1.2 Failure Modes - Disk failure; CRT failure.

5.1.3 MTBF - Not specified.

5.1.4 MTTR - Not specified.

5.2 RESPONSE TIME -

5.2.1 State Change Response - Not specified directly.

5.2.2 Operator Command Response - 3 s (2.5-s system response time + 0.5 s as CRT graphics draw time).

5.2.3 System Data Rate - 9600 baud lines to LOFT data acquisition system and color terminals.

5.3 INPUT DATA VERIFICATION - Automated data qualification (ADQ) system has been developed using information quality functions (IQFs) and estimated data quality indication. This system has not been integrated with ODDS.

6. OPERATION

6.1 INTERFACE - Operator interface consists of CRTs and terminal keyboards. The types of graphics used fall under the following categories:

1. Process schematics (mimic diagrams)
2. Operating maps
3. Event (accident) signatures
4. Trends
5. Procedural tools (e.g., response trees)

6.2 INTERACTION -

6.2.1 Integration with Procedures - Not specified.

6.2.2 Integration with Other Control Room Equipment - Not specified.

6.2.3 User Involvement - Complete user involvement. Operators even invent displays.

6.3 RESPONSIBILITY OF OPERATION - Not specified.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - Independent verification via control boards.

6.5 WORKLOAD -

6.5.1 Tasks Added - Not specified (operating keyboards).

6.5.2 Tasks Eliminated - Status indication made easier.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - Displays are constantly being adapted.

6.6.2 Dialogue Structured to Task - No, alphanumeric keyboard used.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - Not specified.

7.2 RESPONSIBLE ORGANIZATIONS - Not specified (LOFT personnel).

7.3 METHODS FOR VERIFICATION - Not specified.

7.4 HIGH-MAINTENANCE COMPONENTS - Disk storage; CRT.

7.5 SELF-TESTING/DIAGNOSTICS - Some.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - Training needed.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - Some knowledge needed.

8.3 USE OF SYSTEM DURING TRAINING - Not specified.

8.4 FUTURE USERS - Not specified.

9. DOCUMENTATION

9.1 USER CONTROL - Not clear.

9.2 CURRENCY - Not specified.

9.3 AVAILABILITY - Not specified.

9.4 PERSPECTIVE - Not specified.

10. WORK STATUS

10.1 CURRENT - System in use at LOFT since February 1980.

10.2 EXPECTED OPERATION - Not for use other than LOFT.

A.4.9 OPERATIONAL AIDS DATA SHEET: PLANT INCIDENT EVALUATOR (PIE)

SYSTEM NAME: PIE - Plant Incident Evaluator

DEVELOPER: General Atomic Company

INSTALLATION: None specified at this time

CONTACT PERSON: William R. Davidson

DATE: February 9, 1982

DATA:

1. PROBLEM

Fault diagnosis in operating reactors can be complicated by an overabundance of signals and meters, only a few of which are relevant at any given time. A related weakness in the overall design/operation sequence in current use is that most of the detailed system performance evaluations performed are not fully used in plant operations. Though this may not be a "problem," it is a waste of resources.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function -

Provides operator with diagnostic information to recognize possible plant system malfunctions.

Method. Based on systems analysis performed during plant design. Results of probabilistic risk analysis (PRA) are used to generate fault trees and prioritize the possible diagnosis. Displays are data driven rather than programmed.

2.1.2 User - Control room operator, senior shift advisor.

2.1.3 Condition - Abnormal events.

2.1.4 Support - Support operator in problem recognition and diagnostic tasks.

2.2 MEMORY - No historical data retained. Uses instantaneous rather than time-dependent plant information for calculations.

2.3 CONTROL - No direct automatic control functions are attempted.

3. DESIGN

3.1 SCHEME - Stand alone or link with plant computer. Three-step design process is used to custom design system for each plant:

(1) Probabilistic risk assessment (PRA). Implementation begins with the use of PRA techniques to determine the causes and consequences of significant events and to rank them according to their risk contribution. PRA is used in part because the methodology develops event tree and fault tree structures to define accident scenarios. It is used also because it provides event sequence probabilities, which are needed to rank the importance of various sequences. Finally, it is used to determine which events are most essential to detect.

Because risk equals the probability of an event times the consequences of that event, once the acceptable risk level is established, selection of the specific events that must be detected to meet the risk criterion uniformly is therefore a logical and consistent procedure.

(2) Engineering evaluation. Following the PRA assessment, a deterministic evaluation identifies suitable means for the detection of the preselected events and appraises the adequacy of the installed or planned instrumentation. If the equipment is determined to be inadequate or insufficient, the owner is informed and recommendations are made for additional measurements.

(3) Development of status vectors and message text. After the deterministic evaluation, the various plant disturbance matrices are the sets of states that identify events which carry a risk above an acceptable value. Corresponding messages to be transmitted to the reactor operator and the senior shift advisor are then formulated. These matrices and the messages that they trigger are then installed as a data base within the PIE system and become part of a unique design for the plant assessed.

3.2 COMPUTER HARDWARE - Prototype on LSI-11.

3.3 COMPUTER SOFTWARE - FORTRAN coded.

3.4 VERIFICATION - None formally.

3.5 STANDARDS - None given.

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Signal isolation has not been addressed. PIE can derive signals from plant instrumentation, plant computer or PIE may be resident in plant computer.

4.2 INSTALLATION -

4.2.1 Distribution of Components - For stand-alone system, the display and processor are housed together.

4.2.2 Environment-Related Sensitivities - Will add slight heat load. Disk drives are dust sensitive.

4.2.3 Installation Time - Not specified.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY - Not a concern. Software reliability is testable.

5.2 RESPONSE TIME -

5.2.1 State Change Response - Varies according to scope of diagnostic software desired.

5.2.2 Operator Command Response - Not given (response primarily data driven).

5.2.3 System Data Rate - Not given.

5.3 INPUT DATA VERIFICATION - None indicated.

6. OPERATION

6.1 INTERFACE - Color CRT and lighted mimic boards. Alphanumeric keyboard on prototype. Color graphics are cited as being designed to high human engineering standards. No guidelines cited.

6.2 INTERACTION -

6.2.1 Integration with Procedures - Not addressed.

6.2.2 Integration with Other Control Room Equipment - Not addressed.

6.2.3 User Involvement - None with operator; some with utility engineering.

6.3 RESPONSIBILITY OF OPERATION - Control room operators.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - Redundancy of information provided by existing displays.

6.5 WORKLOAD -

6.5.1 Tasks Added - Monitor PIE.

6.5.2 Tasks Eliminated - Some information gathering eliminated because PIE provides compressed data.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - Fixed during custom design process.

6.6.2 Dialogue Structured to Task - Task independent. System responds to plant conditions without interaction.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - Unevaluated.

7.2 RESPONSIBLE ORGANIZATIONS - Unevaluated.

7.3 METHODS FOR VERIFICATION - Unevaluated.

7.4 HIGH-MAINTENANCE COMPONENTS - Unevaluated.

7.5 SELF-TESTING/DIAGNOSTICS - Unevaluated.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - In principle, the system is self-explanatory, and only minor training requirements might be anticipated. This would need to be explored further in simulator testing.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - Not specified.

8.3 USE OF SYSTEM DURING TRAINING - Not specified.

8.4 FUTURE USERS - Not specified.

9. DOCUMENTATION

9.1 USER CONTROL - Unaddressed.

9.2 CURRENCY - Unaddressed.

9.3 AVAILABILITY - Unaddressed.

9.4 PERSPECTIVE - Unaddressed.

10. WORK STATUS

10.1 CURRENT - A small prototype system was developed and has been operating, in conjunction with a computer simulation of reactor operations, for over a year. Future plans are not final.

10.2 EXPECTED OPERATION - Unknown.

A.4.10 OPERATIONAL AIDS DATA SHEET: PROCEDURE PROMPTING SYSTEM (PPS)

SYSTEM NAME: PPS - Procedure Prompting System

DEVELOPER: Hanford Engineering Development Laboratory
Westinghouse Hanford Company

INSTALLATION: Lube Oil System Model for Fast Flux Test Facility (FFTF)

CONTACT PERSON: S. E. Seeman

DATE: December 1982

DATA:

1. PROBLEM

Present procedures for control of nuclear power plants during off-normal conditions are generally based on the question "what if." That is, ahead of time, systems experts, including operators, sit down and answer the questions "what if this component were to fail," or "what if this sensor should give a high reading." For large processes such as nuclear power plants there are many situations that can happen in combination, and indeed there are some that can happen that are not considered at the time probable. Not enough time or resources are available to analyze all of the situations and prepare a manageable set of procedures that can be assimilated and effectively used in controlling the plant.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function 1 -

Identify the closest safe state to the current failed state.

Method. Not specified.

Function 2 -

Provide serial list of instructions to operator for any component failure or change of state.

Method. Not specified.

Function 3 -

Take into account action taken and respond with "new" procedure.

Method. Not specified.

2.1.2 User - Currently experimental applications.

2.1.3 Condition - Used under failed conditions.

2.1.4 Support - Supports user as controller.

2.2 MEMORY - Not specified.

2.3 CONTROL - None.

3. DESIGN

3.1 SCHEME - PPS is implemented with a computer model of the lube-oil system, and the user interface consists of a color graphics display for a system schematic and an alphanumeric display for the procedures.

3.2 COMPUTER HARDWARE - Not specified.

3.3 COMPUTER SOFTWARE - Not specified.

3.4 VERIFICATION - Not specified.

3.5 STANDARDS - Not specified.

4. PLANT INTERFACE AND ENVIRONMENT - Experimental.

5. PERFORMANCE - Not specified.

6. OPERATION - Not specified.

7. MAINTENANCE AND TESTING - Not specified.

8. USER TRAINING - Not specified.

9. DOCUMENTATION - Not specified.

10. WORK STATUS - Laboratory development.

A.4.11 OPERATIONAL AIDS DATA SHEET: SAFETY ASSESSMENT SYSTEM (SAS)

SYSTEM NAME: SAS - Safety Assessment System

DEVELOPER: Wisconsin Electric Power Company and Pressurized Water Reactor (PWR) Owners Group

INSTALLATION: Point Beach Nuclear Plant

CONTACT PERSON: Roger Newton

DATE: May 5, 1982

DATA:

1. PROBLEM

Accident analyses indicate that operators have difficulty assessing the state of the plant with respect to safety. Also, conditions of the plant are often not available to other utility personnel in a timely manner at locations other than the control room.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function 1 -

Top-level displays (three modes: normal operation; heatup/cooldown; cold shutdown).

Method. Display key parameters necessary to assess the safety status of the plant during normal and off-normal conditions. Variety of display techniques is used on color CRTs.

Function 2 -

Accident identification and display system (AIDS).

Method. The accident identification module (AIDS) of the SAS calculates a weighted indicator for each of four major accidents: LOCA, SGTR, LOSC, and ICC. This probability is then displayed to the operator as a bar height on a CRT display.

Function 3 -

Trend graphs of related parameters.

Method. Trend graphs for the last 30 min of operation are available to the operator. Predefined groups of related parameters are displayed on the CRT.

The group selection is controlled by the function keypad, for the primary CRT. Color enhancement and other human factors considerations were used in the display format development in order to highlight important information.

Function 4 -

Safety system readiness monitor (SSRM), which assesses the status of selected safety system.

Method. The SSRM algorithm is based on a tree-structured logic table that is compared to real-time data in order to assess "readiness." Since there are significant variations in safety system designs, instrumentation, etc., between different plants, a general SSRM software package would be very difficult (or impossible) to develop. Instead, the approach taken in SAS was to develop a generic "core" software package to analyze any logic tree and to provide a mechanism whereby each site unique tree can be input to a computer. In this way, plant uniqueness can be easily accommodated and the generic software can be verified and used at any installation.

Function 5 -

Safety system performance monitor (SSPM), which assesses safety systems sequencing and performance.

Method. Same as Function 4.

Function 6 -

Critical safety function (CSF) monitor, which defines conditions to assess the status of five critical safety functions.

Method. The CSF module continuously monitors the status of selected parameters and applies the status to define paths on "trees" (one for each area). The decision process is such that

only one path on each tree can be defined at any one time. That path results in an endpoint that either shows the CSF as satisfied or references a recovery procedure. The current status (endpoint) for all six CSFs is displayed on a summary page.

Function 7 -

Channel malfunction monitor (CMM), which lists data that have been rejected or deleted.

Method. Monitors rejected inputs.

Function 8 -

Top-level message display.

Method. A message area which indicates the mode selected, date, time, and the current value of some key parameters, and notifies the operator of off-normal conditions as monitored by the readiness monitor, performance monitor, critical safety function monitor, and channel malfunction.

2.1.2 User - RO and SRO [Primary cathode-ray tube (CRT)]; SS and STA (Secondary CRT).

2.1.3 Condition - Normal and abnormal conditions.

2.1.4 Support - Supports operator in evaluating safety status and detecting abnormal conditions.

2.2 MEMORY - Trend information held and displayed.

2.3 CONTROL - No control.

3. DESIGN

3.1 SCHEME - For the generic SAS, a primary CRT and a secondary CRT are used to present all graphical displays. There are 21 displays available on the primary CRT and 41 available on the secondary CRT. The number and availability of secondary displays will vary for the site-specific installation. All graphics displays are presented to the control room operator on high-resolution, multicolor CRTs. The SAS software is designed to be expandable to accommodate the many additional secondary CRT displays for a specific power plant.

3.2 COMPUTER HARDWARE - Redundant SEL Concept 32/37 (32-bit 16 MB core memory); Chromatics CGC 7900.

3.3 COMPUTER SOFTWARE - The major modules in the SAS software are:

SASP - main processor module.
DISPLAY - module to generate the output to the display generator.
SSM - safety system monitor module - includes a safety system readiness monitor, a safety system performance monitor, and a predictive safety system readiness monitor.
ANSI F77 FORTRAN-coded mainframe
PASCAL, C, BASIC-coded display units.

3.4 VERIFICATION - During the course of software development, a set of static test cases was developed that test the key features of each software module. Furthermore, static system test cases have been developed and used to verify the correct operability of the total system. A set of dynamic test cases has been generated by recording nuclear plant simulator data on magnetic tape from a number of different plant transients which test the dynamic behavior of the system under "read" conditions. A design review that compares these test results to the original functional and design specifications has been performed.

3.5 STANDARDS - Not specified.

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Date derived from sensor inputs in most cases. Isolation from plant safety system not specified.

4.2 INSTALLATION -

4.2.1 Distribution of Components - CRTs in control room. Other equipment not specified.

4.2.2 Environment-Related Sensitivities - Not specified.

4.2.3 Installation Time - Not specified.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY -

5.1.1 Requirements - Not specified.

5.1.2 Failure Modes - Not specified.

5.1.3 MTBR - Not specified.

5.1.4 MTTR - Not specified.

5.2 RESPONSE TIME -

5.2.1 State Change Response - Not given.

5.2.2 Operator Command Response - Less than 2 s.

5.2.3 System Data Rate - Mainframe 26.67 MB per s. Display data update 19.2 K baud using standard RS232 protocol.

5.3 INPUT DATA VERIFICATION - The data displayed by the SAS are validated by comparing redundant sensors, checking the value against reasonable limits, calculating rates of change, and/or checking temperature-versus-pressure curves. Invalid data are rejected by the SAS logic.

6. OPERATION

6.1 INTERFACE - Operator interfaces with SAS via CRTs and keyboards. The CRTs are readable to 15 ft for mode displays, 6 ft for supporting displays, and 28 in. for text. A summary of the features of primary and secondary CRTs follows:

Primary CRT	Secondary CRT
1. Implements SPDS	1. Provides detailed information
2. Has function keyboard	2. Has full keyboard
3. Is centrally located	3. Is located near the SS desk
4. Is used by RO and SRO	4. Is used by SS and STA

6.2 INTERACTION -

6.2.1 Integration with Procedures - Not specified.

6.2.2 Integration with Other Control Room Equipment - Not specified.

6.2.3 User Involvement - User involvement at operations level. Operators assisted in generating AIDS model. Operators tested.

6.3 RESPONSIBILITY OF OPERATION - Operators and supervisors.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - May verify by independent means.

6.5 WORKLOAD -

6.5.1 Tasks Added - Operation of SAS.

6.5.2 Tasks Eliminated - None.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - Fixed to some level of experience at design.

6.6.2 Dialogue Structured to Task - Function-oriented communication with SAS for operators and a more flexible communication possible for supervisors.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - Not specified.

7.2 RESPONSIBLE ORGANIZATIONS - Owner utility.

7.3 METHODS FOR VERIFICATION - Not specified.

7.4 HIGH-MAINTENANCE COMPONENTS - Not specified.

7.5 SELF-TESTING/DIAGNOSTICS - Some.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - Yes, self-programmed training course has been developed using videotape and a training manual.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - Yes, especially for AIDS.

8.3 USE OF SYSTEM DURING TRAINING - Not specified.

8.4 FUTURE USERS - Not specified.

9. DOCUMENTATION

9.1 USER CONTROL - Up to utility.

9.2 CURRENCY - Up to utility.

9.3 AVAILABILITY - Generic documentation available now including listings, diagrams, and implementation guide.

9.4 PERSPECTIVE - Operations oriented.

10. WORK STATUS

10.1 CURRENT - Installation and test.

10.2 EXPECTED OPERATION - Not specified.

A.4.12 OPERATIONAL AIDS DATA SHEET: DISTURBANCE ANALYSIS AND SURVEILLANCE SYSTEM (STAR)

SYSTEM NAME: STAR - Disturbance Analysis and Surveillance System

DEVELOPER: Gesellschaft für Reaktorsicherheit (GRS) mbH

INSTALLATION: Grafenrheinfeld (1300-MWe Kraftwerksunion-PWR)

CONTACT PERSON: Lothar Felkel

DATE: March 1982 (Initial information 8/81)

DATA:

1. PROBLEM

Undiagnosed disturbances may lead to deterioration in operating status, actuation of protection systems, damage to equipment, and release of radiation. The original goal of STAR, improve plant availability, was expanded to include safety. STAR will be an auxiliary system in the control room to supplement the function of existing equipment.

2. FUNCTION

2.1 ROLE/USER -

2.1.1 Function 1 -

Status surveillance of the process during normal and disturbed operation.

Method. Logical and chronological combination of primary process data and, where necessary, inclusion of more sophisticated modeling.

Function 2 -

Availability and operability indication of automatic functions.

Method. Same as Function 1.

Function 3 -

Verification of operation sequence of safety systems (post trip).

Method. Same as Function 1.

Function 4 -

Determination of the primary cause of a disturbance.

Method. Starting with the occurrence of an undesired event, the disturbance analysis system traces back through the stored fault trees to the possible causes of the disturbance and displays these to the operator.

Function 5 -

Suppression of nuisance alarms.

Method. By means of the cause-consequence diagrams, an entire sequence of events, the starting events only, or the final event only of the disturbance sequence may be displayed to the operator, thus reducing the amount of extraneous alarms. For the scrutability of the conclusions drawn by the disturbance analysis system, an option is provided for displaying to the operator all information that belongs to the sequence.

Function 6 -

Determination of possible consequences of propagation of the disturbance.

Method. The same method as for Function 4 applies. The fault tree can be traced in the opposite direction to find possible consequences of the actual situation.

Function 7 -

Surveillance of mass, energy, and momentum balances to determine anomalous plant states.

Method. Evaluation of balance equations, supplying them on-line with process data.

Function 8 -

Surveillance of characteristic curves for components to obtain information about permissible operation of components.

Method. The curves, described in terms of analytical functions or by tables of data, can be included in the cause-consequence diagrams to allow the checking of the characteristics of components.

Function 9 -

Prediction of the behavior of systems or components by means of simulation models (later implementation).

Method. Construction of simple analytic mathematical models.

Function 10 -

Verification of data by consistency checks of instrumentation.

Method. Diverse information from the process instrumentation can be used to check the plausibility of information delivered from sensors according to physical behavior. Retrofitting addition, or relocation, of instrumentation may become necessary.

Function 11 -

Annunciation of nonanticipated circumstances.

Method. If pattern of process signals does not match cause-consequence descriptions, unanticipated situation is reported to operator.

Function 12 -

Automated operation mode to guide operators through small LOCAs.

Method. Look-up tables of procedures logically connected to cause-consequence diagrams.

2.1.2 User - Primarily plant operators. Under difficult situations, systems may be used by shift supervisors, plant engineers, and specialists.

2.1.3 Condition - Used under all conditions.

2.1.4 Support - Supports operator as a monitor and diagnostician.

2.2 MEMORY -

1. Plant data collected and stored for real-time internal use by machine.

2. Plant data collected every 5 s for up to a 24-h period for trend analysis by operator.

3. Operator accesses and commands are recorded for future task analysis.

2.3 CONTROL - System performs monitoring function. Control loop is closed through the operating crew only.

3. DESIGN

3.1 SCHEME - STAR is being tested outside of the control room area to avoid biasing the operators. STAR receives it data from the plant computer.

3.2 COMPUTER HARDWARE - Not specified.

3.3 COMPUTER SOFTWARE - Not specified (automatic software analysis used).

3.4 VERIFICATION - Models are checked for syntax deficiencies. Cause-consequence descriptions are submitted to a fault tree analysis for evaluation of cut sets. Models are compared with plant simulator. STAR also was operated during hot engineering commissioning phase of Grafenrheinfeld plant. This last check uncovered plant design errors.

3.5 STANDARDS - Reliability requirements and display design requirements (German KTA rule No. 3901).

4. PLANT INTERFACE AND ENVIRONMENT

4.1 ISOLATION - Grafenrheinfeld installation isolated by plant computer. Complies with West German standard KTA 3501.

4.2 INSTALLATION -

4.2.1 Distribution of Components - Computers and peripheral equipment are located in a computer room, so is the operator interface (which will be moved to the control room after its feasibility has been proven). The central connection rack is located in a room below the control room and the instrumentation at the point of measurement.

4.2.2 Environment-Related Sensitivities - Almost all components are sensitive to temperature, humidity, air purity, ac power fluctuations, and so on. Therefore, the rooms in which they are located are equipped with air conditioning, which is required for control room equipment anyway. The systems may be very sensitive to ac power fluctuations; therefore, buffer batteries or flywheel support is a necessity. Problems occurred in the Grafenrheinfeld plant with dust in the computer room. Air purity is very poor.

4.2.3 Installation Time - Apart from the wiring of the sensors and the connections to the computer systems, the installation is an everyday task for computer manufacturers.

5. PERFORMANCE

5.1 RELIABILITY/AVAILABILITY -

5.1.1 Requirements - Must be 100 times more reliable than human reliability.

5.1.2 Failure Modes - Not specified.

5.1.3 MTBF - Not specified.

5.1.4 MTTR - Not specified.

5.2 RESPONSE TIME -

5.2.1 State Change Response - Less than 1 s for indication that something is happening, but time to completion is open.

5.2.2 Operator Command Response - Less than 1 s.

5.2.3 System Data Rate - High (uses multiple processors, shared memory, and array processors). System performs analysis on all data continuously - not data driven.

5.3 INPUT DATA VERIFICATION - The sophistication with which the incoming data are treated varies with the importance of the process signals. Safety-related signals are verified by majority voting. Operational status signals, which may carry noise induced from several sources, are subjected to sophisticated filtering methods, and predicted values are compared to measured values. Also the process signals are checked as to whether they exceeded their nominal ranges. For a collection of signals, a consistency check is performed by relating diverse measurements according to physical insights.

6. OPERATION

6.1 INTERFACE - Operators communicate with the on-line STAR system via two high-quality color display screens, a function keyboard, an alphanumeric keyboard, and tracker ball.

On one screen an alarm and summary overview picture is normally presented; on the other, a detailed presentation of a disturbance analysis from any subsystem. The operator may request different mimic diagrams containing on-line plant information to confirm conclusions by the analysis.

Alarms are presented on the screen as text strings consisting of subsystem identification and message. The same applies to detailed information about a disturbance. Because the amount of information can be larger than can be contained in one screen image, the information occupies more pages. In the upper right corner of the picture, the current page number and the total number of pages available are listed. To page, the operator uses specific keys.

From each function it is possible to branch out to details by tracker ball addressing. The details may be either a new picture or new information in the one currently displayed.

The standard alphanumeric keyboard is used for entering commands or other information to the system. To facilitate this each screen image contains a so-called dialogue area.

The dialogue text has a "dialogue color" in contrast with the operator's input, which appears in an "operator color." If accepted by the input check software, the operator color is replaced by an accepted color. A feature of the dialogue system is that the keyboard has a tabular function that automatically moves the input cursor to the first position of the following input field when the tabulator key is pushed. This facilitates the input of commands that require several parameters. The dialogue also includes error messages presented when the input check software detects an operator input area.

The dialogue area also contains one part that is called the operator message field, in which area the operator is alerted to and given responses to specific inquiries. For example, the operator will be notified when there are changes in the data background and when the image presently displayed does not contain the latest information available. Images are not updated immediately because this might disrupt the operator's train of thought. Rather, he is informed about the obsolescence of data that he is currently observing.

Specific guidelines to be considered in the development of the operator interface were not available at the time the development started. However, the application of the extended STAR system in the Biblis plant will be designed according to the guidelines set up in NUREG-700 and other German standards if they are available.

6.2 INTERACTION -

6.2.1 Integration with Procedures - Has not begun, but will be integrated.

6.2.2 Integration with Other Control Room Equipment - Has not begun, but will be integrated.

6.2.3 User Involvement - Not specified.

6.3 RESPONSIBILITY OF OPERATION - Plant operators.

6.4 CREW VERIFICATION OF SYSTEM RESPONSE - The system is provided with a great extent of scrutability. Therefore, if some of the information is not well understood by the operator, he can trace back through the analysis path to verify the plausibility of each step of the computation.

6.5 WORKLOAD -

6.5.1 Tasks Added - Frequent use; verification; reports to shift technical advisor.

6.5.2 Tasks Eliminated - None.

6.6 COMMUNICATION -

6.6.1 Dialogue Adaptability to User Experience - Some because of scrutability.

6.6.2 Dialogue Structured to Task - Yes, function orientation.

7. MAINTENANCE AND TESTING

7.1 REQUIREMENTS - Not specified.

7.2 RESPONSIBLE ORGANIZATIONS - For the development and application of the STAR system in Grafenrheinfeld, maintenance and testing will be performed by those organizations that have designed the system (GRS and KWU).

7.3 METHODS FOR VERIFICATION - A verification process will be used.

7.4 HIGH-MAINTENANCE COMPONENTS - The high-maintenance components of the hardware can be ordered as follows: power supply, peripheral equipment with many mechanical parts, and peripheral equipment with high-precision adjustment requirements (disk, magnetic tape).

7.5 SELF-TESTING/DIAGNOSTICS - Self-testing is realized as far as the computer performs built-in error checking and correction (ECC). On-line diagnostic tools are provided to facilitate the test of the software and associated technological data background. In an application beyond that of a research and development project, self-testing of the software and hardware as well as redundant computer structures will be used to further improve the overall system reliability.

8. USER TRAINING

8.1 ADDITIONAL TRAINING NEEDED - The training the operator needs depends on the degree of complexity of the specific function that he is using. For the simpler functions, about 3 h of instruction is sufficient. For the more sophisticted functions (disturbance analysis, post-trip analysis, using the system as an information tool in a knowledge-based task) he needs a three-day course in operating the system. However, this does not include training in the basic plant functions, which he is assumed to have completed already.

8.2 EXTENT OF KNOWLEDGE OF SYSTEM NEEDED - Experience has shown that when the operator is missing one piece of information in his mental model, he can hardly follow the conclusions of the system. He must be able to verify how the system derived the final information.

8.3 USE OF SYSTEM DURING TRAINING - Not specified.

8.4 FUTURE USERS - Not specified.

9. DOCUMENTATION

9.1 USER CONTROL - Efforts are being made to formalize and computerize the documentation.

9.2 CURRENCY - German plants have groups responsible for keeping overall documentation current.

9.3 AVAILABILITY - Not specified.

9.4 PERSPECTIVE - Not specified.

10. WORK STATUS

10.1 CURRENT - Operational.

10.2 EXPECTED OPERATION - Biblis: 1983.

APPENDIX B

RESULTS OF U.S. NUCLEAR REGULATORY COMMISSION DOCUMENT REVIEW AND CATEGORIZATION OF CRITERIA THAT MAY APPLY TO OPERATIONAL AIDS

B.1. INTRODUCTION

The materials included in Sect. B.3 comprise a review of U.S. Nuclear Regulatory Commission (NRC) and other documents as outlined in one of the tasks of the Operational Aids for Nuclear Reactor Operators program plan. The purpose of the review is to indicate specific requirements, criteria, and suggestions for NRC acceptance of operational aids for nuclear power plant operating crews. (Section B.2 provides a list of the documents reviewed.) Although specific and quantifiable requirements were found, they were intended to apply specifically to emergency response facilities (ERFs), especially safety parameter display systems (SPDSs), and to instrumentation for postaccident monitoring [NRC Regulatory Guide (RG) 1.97]. Section B.3 outlines the criteria and suggestions extracted.

The review considers only computer-based operational aids* that have not been solicited or required by NRC. An operational aid that functions to satisfy a requirement for the implementation of postaccident monitoring instrumentation, SPDS, or ERF already comes under the jurisdiction of specific guidelines for those systems. The instance of an operational aid implemented apart from an NRC requirement poses a problem for regulators because of potential effects on plant safety through interaction with other plant systems and procedures. Review of an unsolicited operational aid is at the discretion of NRC. As stated in NUREG-0835, "The addition of diagnostic techniques must not compromise the primary SPDS function and is subject to review prior to implementation." This statement, although intended to apply to future, expanded functions of SPDSs, potentially can be applied to operational aids apart from an SPDS.

An operational aid, classified as not functioning in the capacity as an SPDS or as RG 1.97-related equipment, must still meet a small number of specific requirements that relate to gross interactions with other systems; however, a large quantity of implied requirements also may be applied if guidelines are interpreted loosely. The implied requirements, which may be taken as suggestions, must be applied with caution because they were originally intended for more restricted usage. In this review, the requirements and suggestions have been ranged according to "must do" and "should do" categories respectively. The latter category, because it contains the bulk of the entries, is subdivided in a manner similar to that used for the data collection task, the results of which appear in Appendix A. These subdivisions are

---

*The concept of an operational aid, as it is used here, is one of a backfit system that in some way enhances the decision-making abilities of control room operators.

1. problem definition
2. function
3. design
4. plant interface
5. performance
6. operation
7. maintenance and testing
8. user training
9. documentation
10. work status

Within each of these subdivisions, an attempt was made to rank the entries according to their importance to safety. Section B.4 contains the ranking and categorization.

From the requirements collected, two classes of functions implementable by operational aids have been derived: those that are endorsed (recommended or implied) and those that are excluded. These functions are listed without ranking in Sect. B.5 according to their data source. Because of specific observations made in it, NUREG/CR-2587(1) is included as a data source for the recommended functions.* The findings in the contractor reports represent the opinions of their authors and may not have full endorsement by NRC. Thus their recommendations should be used with caution.

Review guidelines that were oriented toward the cognitive and information processing aspects of human-system interaction were solicited from NRC regulatory staff members who may be in a position to review specific candidate operational aids. These working notes were distilled, and their essence is listed below along with some comments from an independent reviewer. These recommendations and comments, like those contained in contractor reports, may not have full NRC endorsement.

1. Display images should aid the operators' data-sampling strategy in collecting data for assigned functions and tasks.
2. Display images should contain information resulting from processing and integration of data. (Reviewer raises the point that "raw" data may be more effective in some instances.)
3. Display images should contain information and data that support "response thresholds for operators." (Reviewer suggests that the conclusion may be premature.)
4. Display images should contain information and data that can allow the limited sampling rate of the human data acquisition system (DAS) to handle the entire system bandwidth.
5. The method used to manage data and information should be structured to support the execution of the operators' allocated tasks and functions. A specific example is the support needed for sequential decision making performed by operators after a reactor trip.

---

*NUREG/CR-2586(2) may also provide a source of information for excluded functions because of its specific operator acceptance data, but it is not included in this review.

6. Top-level display images should support the operators' model of the plant process in both normal and abnormal plant operations such as design-basis events.
7. Display images and data/information management schemes should strive to keep the operators abreast of the state of the plant.

B.2. DOCUMENTS INCLUDED IN THE REVIEW

1. U.S. NRC Regulatory Guide 1.97 (Task RS 917-4), Revision 2, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," December 1980.

2. NUREG-0696, U.S. Nuclear Regulatory Commission, Final Report, "Functional Criteria for Emergency Response Facilities," February 1981.

3. NUREG-0700, U.S. Nuclear Regulatory Commission, "Guidelines for Control Room Design Reviews," September 1981.

4. NUREG-0814, U.S. Nuclear Regulatory Commission, S. Ramos, Draft, "Methodology for Evaluation of Emergency Response Facilities," August 1981.

5. NUREG-0835, U.S. Nuclear Regulatory Commission, Draft Report, "Human Factors Acceptance Criteria for the Safety Parameter Display System," October 1981.

6. SECY 82-111B, U.S. Nuclear Regulatory Commission, "Requirements for Emergency Response Capability," September 8, 1982.

7. IEEE Std. 566-1977, The Institute of Electrical and Electronics Engineers, Inc., "IEEE Recommended Practice for the Design of Display and Control Facilities for Central Control Rooms of Nuclear Power Generating Stations," 1977.

B.3. CRITERIA AND SUGGESTIONS EXTRACTED FROM VARIOUS DOCUMENTS THAT APPLY TO OPERATIONAL AIDS

1. U.S. NRC Regulatory Guide 1.97 (Task RS 917-4), Revision 2, December 1980:

   "INSTRUMENTATION FOR LIGHT-WATER-COOLED NUCLEAR POWER PLANTS TO ASSESS PLANT AND ENVIRONS CONDITIONS DURING AND FOLLOWING AN ACCIDENT"

   APPLICATION:

   Instrumentation specifically for monitoring plant variables and systems during and following an accident in a light-water-cooled nuclear power plant.

   SUMMARY:

   General Comment--measurement of a single key variable is not sufficient to indicate accomplishment of a given safety function.

   Design Criteria--(Type A variable) [Sect. 1.3.1, pp. 4 through 5]
   - should be Class 1E and seismic qualified
   - should be designed so that single failure will not prevent operation
   - should be isolated as necessary from safety system signals
   - should be powered by uninterruptible power source
   - should be available prior to accident
   - should follow quality assurance plan
   - should provide continuous indication
   - should provide recording of instrumentation output

2. NUREG-0696, U.S. Nuclear Regulatory Commission, Final Report, February 1981:

   "FUNCTIONAL CRITERIA FOR EMERGENCY RESPONSE FACILITIES"

   APPLICATION:

   Facilities and systems that make up the total ERFs: control room, on-site technical support center, on-site operational support center, near-site emergency operations facility, SPDS, and nuclear data link.

SUMMARY:

ERFs in General --

Responsibility of licensee [Sect. 1.2, pp. 2 through 3]:
- diagnose abnormal conditions
- perform corrective actions
- mitigate abnormal conditions
- manage plant operations
- manage emergency response
- inform federal, state, and local officials
- recommend public protection measures
- restore plant to a safe condition
- recover from abnormal condition

Function of ERFs [Sect. 1.3, p. 3]:
- help reactor operations determine plant safety status
- relieve reactor operators of peripheral duties and communications not directly related to reactor system manipulation
- prevent congestion in the control room
- provide technical assistance to operators
- coordinate emergency response
- provide on-site and off-site communications
- become center for development of recommendations
- provide data to NRC for analysis
- acquire and control safety-related data

Safety Parameter Display System (SPDS)
[Sect. 5, pp. 24 through 27]--

General function and operation:
- indicate safety status
- be common to TSC, CR, and EOF
- operate in normal and emergency conditions
- be capable of future expandability
- have very high reliability--unavailability of 0.01 above cold shutdown and 0.2 at cold shutdown
- continuously indicate plant parameters related to safety
- assist in detection of abnormal condition
- concentrate a specific set of parameters
- be designed to good human factors engineering (HFE) principles
- use validated data
- be reflected in procedures and training
- present trend information or derivatives
- supply information to other systems
- be isolated from safety signal
- not interfere physically with access to other systems or displays

Design of display:
- incorporate HFE principles
- use format that is as simple as possible
- be pattern coded
- be oriented for each mode of plant operation
- include single primary display format for
  - reactivity control
  - reactor core cooling and primary heat removal
  - reactor coolant integrity
  - radioactivity control
  - containment integrity
- allow secondary formats
- be automatic or operator selected
- use audible alert
- be flexible

DAS [Sect. 7, pp. 31 through 34] --

- must provide signals to the DAS that are not processed by a software-programmable device
- must have safety signal isolation
- must be able to cope with external demands for its resources
- must have internal calibration and self-diagnostics
- must have verification and testing
- must have quality assurance program for software changes
- must be protected against interference and unauthorized manipulation
- must accommodate maximum data throughput

3. NUREG-0700, U.S. Nuclear Regulatory Commission, September 1981:

"GUIDELINES FOR CONTROL ROOM DESIGN REVIEWS"

APPLICATION:

Guidance for control room design review. Affects all equipment in control room.

SUMMARY:

General Comment--The guide often asks: Is the allocation of functions as it is now (at the time of the analysis) effective? For example can functions allocated to the control room crew be accomplished within (1) structure of the procedure and (2) design of the control room as it exists?

Criteria by Section--

Alarms [6.3]
- be prioritized (four levels maximum)
- be accompanied by general coding and arrangement guides

Controls [6.4]
- adequate
- economic of space
- anthropometic in design
- compatible with emergency gear (e.g., masks and gloves)
- protected against accidental activation
- functionally coded

Display [6.5]
- give complete information
- eliminate unnecessary information
- provide redundant information for backup only
- make distinction between information pertaining to whether operation of equipment or systems has been demanded or information pertaining to the actual status of same
- have self-evident display failure
- be designed so that operator does not have to mentally convert between scales or metrics
- have terms used by displays that correspond with same terms in procedures
- have color coding that is redundant with another cue and consistent in meaning

Labels [6.6]
- hierarchical scheme recommended

Process Computers [6.7]
- protection against changes being made by unauthorized personnel
- securely stored copy of operating software
- two-step data- or function-entry process
- dialogue based on operator's point of view (i.e., logical, consistent, and tuned to user population)
- word entry that does not exceed seven characters
- use of abbreviated words for system input but unabbreviated words for system output
- system that prompts user
- data input string that is correctable without complete reentry
- retention of sequential file of operator entries
- QWERTY keyboard
- function controls grouped near cathode-ray tube (CRT) and distinct from other keys (avoidance of multiple mode)
- delay message presented to maintain operator attention if response time for any query exceeds 3 s (see Exhibit 6.7-6, pp. 6.7 through 13 of Sect. 6.7)
- hard-copy procedures for computer operation

Allocation of Function (Appendix B)
- mandatory consideration of function allocation (B-15)
- monitoring of plant safety function made the responsibility of human operator
- workload allocated to humans not in excess of their ability
- time allotment compatible with human capability

4. NUREG-0814, U.S. Nuclear Regulatory Commission, August 1981, S. Ramos, Draft:

"METHODOLOGY FOR EVALUATION OF EME..GENCY RESPONSE FACILITIES"

APPLICATION:

Use by NRC staff in reviewing ERF conceptual designs.

SUMMARY:

The report, which is basically a questionnaire, is intended to prompt the reviewers to be systematic and exhaustive when reviewing ERFs.

General Questions Pertaining to Operational Aids -- [Sect. 2, pp. 2-1 through 2-6]

- What are the layouts of equipment at operator work stations?
- What is the flow of information between persons and groups?
- Where are data displayed?
- Is equipment anthropometically designed?
- Is there sufficient space for repair, maintenance, and testing?

DAS [Sect. 6, pp. 6-1 through 6-8]--

- Questions probe DAS environment, physical security, and access.
- Questions inquire about computer hardware and software.
- System must be able to cope with conflicting requests for system resources.
- Manual data entry must be verifiable.

SPDS (Display) [Sect. 7, pp. 7-1 through 7-8]--

- display of trend information
- dedicated terminal
- hard-copy device
- CRT: 80 characters × 24 lines
- low-noise printer

- 512 × 256 addressable points (minimum)
- 0.05-in. vector line (maximum)
- 50 full-screen vectors/s (minimum)
- 30-Hz refresh (minimum)
- 3-s response time to 90% of queries (minimum)
- most important information in upper right quadrant
- labeling of every display page
- 30-s maximum time to enter request for information

Documentation [Section 9.1, pp. 9-1 through 9-3]--

- functional system documentation
- hardware documentation
- software documentation
- users manual (should include following)
  - table of contents
  - description of use
  - system start-up procedure
  - system failure procedure
  - reference to support services
  - operating instructions for each piece of equipment
  - operating instructions for each request

Training include requirements [Sect. 9.2, p. 9-3]--

Quality Assurance include requirements [Sect. 9.3, pp. 9-3 through 9-5]--

5. NUREG-0835, U.S. Nuclear Regulatory Commission, October 1981, Draft:

"HUMAN FACTORS ACCEPTANCE CRITERIA FOR THE SAFETY PARAMETER DISPLAY SYSTEM"

APPLICATION:

SPDS as defined in NUREG-0696.

SUMMARY:

Scope [Sect. 2.0, pp. 1 through 3]--

- minimum set of plant parameters from which reactor operators may assess safety status of plant operation
- abnormal operating conditions detectable by SPDS and control room operators, as a unit
- SPDS functional criteria, as a minimum, met by a system representing an SPDS (other functions possible)
- CRT or other display types possible
- Chernoff faces and Fourier plots not acceptable

General Acceptance Criteria [Sect. 3.0, pp. 3 through 9]--

- monitor during normal operations
- instruments analogous to aircraft status instruments
- operator training is required
- design that considers operator needs
- incorporation of perceptual aids
- functional qualification program
- incorporation of HFE
- display of abnormal conditions must be distinct from display of normal conditions
- trend information for primary data set
- recalled additional data through secondary display format
- alphanumeric, symbolic, or graphic display
- analog or digital display
- readily interpretable changes in value
- linear relationship between measured variable and displayed variable (preferable-nonlinear may be necessary in some cases)
- trend information as the key to severity determination
- 30 min of trend (acceptable)
- direct association between display pattern and plant status

Specific Functional Criteria [Sect. 4.0, pp. 9 through 33]--

Primary function:
- for rapid detection of an abnormal condition

Secondary functions:
- that do not impair primary function
- which crew must be trained for

Future functions:
- for expansion of SPDS into a more comprehensive operational aid--subject to review

Data validation:
- validation where practicable
- identification of unvalidated data

Timeliness/Accuracy of data:
- sampling rate such that no loss of data
- sense-to-display delay less than 2 s
- accuracy enough to discriminate between normal and abnormal conditions

Comprehension:
- operator comprehension should take only seconds (if more than about 2 min, the design is unacceptable)

Trend:
- frequency bandwidth enough to display all meaningful information
- unambiguous time derivatives

Recall:
- data not lost due to electrical failures

Mode:
- display for each plant mode

Display:
- automatic or manual, but with manual override
- gradual change that is not interpretable as mode change

Readability:
- much detail is available; for example, see "Computer-Generated Display System Guide," Volume 1, P. R. Frey and W. H. Sides, EPRI Interim Report, March 1984.

Staff:
- trained for use on SPDS
- have users manual available
- acceptable without computer programming training

Interaction:
- system that contains operator interactive devices
- display that positively acknowledges operator requests
- rapid response time (undue response time unacceptable)
- function keys preferred

Failure recognition:
- system that provides for rapid operator recognition of SPDS failure

Audible Alarms:
- sound on abnormal conditions independent of annunciator system

6. SECY 82-111B, U.S. Nuclear Regulatory Commission, September 8, 1982:

"REQUIREMENTS FOR EMERGENCY RESPONSE CAPABILITY"

APPLICATION:

SPDS, Emergency Operating Procedures, RG 1.97, ERFs.

SUMMARY:

This letter qualifies and emphasizes material in NUREGs 0696, 0700, 0799, 0801, 0814, 0818, 0835, and RG 1.23, 1.97, 1.101, and 1.47.

The following taken from Supplement 1 to NUREG-0737, contained within SECY 82-111B.

Qualifies SPDS [Sect. 4.2, p. 13]--

- need not meet single failure criteria
- need not be qualified to meet Class 1E
- need not be seismically qualified
- need not have secondary backup for seismic qualification

Emphasizes [Sect. 4.0, pp. 12 through 16]--

- SPDS, instrumentation based on RG 1.97, control room review, function-oriented emergency operating procedures, and integrated staff training for operator comprehensibility and successful operator intervention [see Sect. 3.1, p. 6]
- SPDS location convenient to the control room operators
- SPDS for use during normal and abnormal conditions, especially useful during anticipated transients and the initial phase of an accident
- continuous display of status information
- isolation from interference with safety systems
- necessary instructions for operator action with and without SPDS
- application of human factors principles
- task and function analysis as the basis for designing and verifying SPDS
- display and control requirements compared with control room inventory to identify missing displays and controls

7. IEEE Std. 566-1977, The Institute of Electrical and Electronics Engineers, Inc.:

"IEEE RECOMMENDED PRACTICE FOR THE DESIGN OF DISPLAY AND CONTROL FACILITIES FOR CENTRAL CONTROL ROOMS OF NUCLEAR POWER GENERATING STATIONS"

APPLICATION:

Aid to designers in selecting information and control devices for use in the central control room.

SUMMARY:

Design Bases for Operational Aid--

- operating modes of plant
- responsibility of operator with respect to operational aid - quantity of stimulus produced by operational aid to avoid sensory saturation

Usage Analysis--

- priority of information
- plant systems related to the information or analysis
- operating modes
- frequency of use
- response times
- relationship to safety systems

Functional Considerations--

Display:
- accessibility of information
- readabiity and comprehension of display
- indication of abnormal condition

Control:
- amount of operator interaction required to operate the operational aid
- number of controls or sequence of actions required to accomplish a given function

Identification:
- ease of identification

Conventions:
- population stereotype
- consistency with other systems

Location:
- should not block view or impede traffic patterns

Layout:
- minimum operator motion required

Status:
- readily indicate whether operational aid is in or out of service

Communications:
- operational aid that does not divert operator attention away from his or her principal duties

B.4. REQUIREMENTS FOR OPERATIONAL AIDS

(Excluding SPDS and instrumentation to satisfy RG 1.97)

MUSTS

1. Must be isolated from interference with safety systems [RG 1.97, NUREG/0696, SECY 82-111B]
2. Must not block view of or physically interfere with access to other systems or displays [NUREG/0696, IEEE Std. 566-1977]
3. Must not impede traffic patterns within the control room [NUREG-0696, IEEE Std. 566-1977]
4. Must not divert operator attention away from his principal duties [IEEE Std. 566-1977]
5. Must incorporate anthropometric design of controls and displays [NUREG/0696, SECY 82-111B]
6. Must not use Chernoff faces for display of information [NUREG/0835]

SHOULDS [taken from all reviewed documents; some categories have no requirements]

(Material is organized to fit Operational Aid Data Sheet; requirements are preceded by hyphen.)

1. Problem Definition (section does not apply)

2. Function
   - 2.1 Role/User
     - 2.1.1 Functions and methods of implementation
       - Task and function analysis should serve as the basis for designing and verifying an operational aid. Also, a comparison should be made between the display and control requirements and the control room inventory to identify missing displays information and controls.
       - Allocation of function should be considered.
     - 2.1.2 System users (none)
     - 2.1.3 Conditions of use
       - System should operate in normal and emergency conditions.
       - Distinction should be made between information pertaining to whether operation of equipment or systems has been demanded or pertaining to the actual status of same.
     - 2.1.4 Operator support
       - Design should consider operator's needs.
       - System should assist in detecting abnormal conditions.

2.2 Memory
- Sequential file of operator entries should be retained.

2.2.1 Permanence
- For trend information, 30 min is acceptable.

2.2.2 User access
- System should be protected against interference and unauthorized manipulation.

2.3 Control (none)

3. Design

3.1 Scheme
- Design should be simple and space economic.
- Quality assurance should be applied to operational aid development.
- Operational aid should be able to cope with conflicting requests.
- Design should allow for future expandability.

3.2 Computer hardware (none)
3.3 Computer software (none)
3.4 Verification (none)
3.5 Standards (none)

4. Plant Interface and Environment

4.1 Isolation (none)
4.2 Installation
4.2.1 Distribution of components within plant (none).
4.2.2 Environment-related sensitivities (none).
4.2.3 Installation time requirement (none).

5. Performance

5.1 Reliability/Availability

5.1.1 Requirements
- System should perform with high reliability (>0.01; >0.2 cold shutdown--these apply to SPDS)

5.1.2 Failure modes
- Operational aid failure should be self-evident

5.1.3 MTBF (none)
5.1.4 MTTR (none)

5.2 Response time
- Time allotment should be compatible with human capability.

5.2.1 State change response time
- Sense-to-display delays should be less than 2 s.

5.2.2 Operator command response time
- Maximum response time to 90% of queries should be 3 s.
- If response time for any query exceeds 3 s, a delay message should be represented to maintain operator attention (see Exhibit 6.7-6, p. 6.7-13 of Sect. 6.7, NUREG-0700).

5.2.3 System data rates
- Date sampling rate should not lead to loss of data.
- System should accommodate maximum data throughput.

5.3 Input data verification
- Data validation should be used where practicable; the use of unvalidated data should be so indicated.
- Manual data entry should be verifiable.

6. Operation

6.1 Interface (general)
- Conventions should conform to population stereotypes and be consistent with other equipment and systems.
- Color coding should be redundant with other cues and consistent in meaning.
- Hierarchical labeling scheme is recommended.
- Displays should be readable and comprehensible.
- Operator's comprehension of the display should not take several minutes.
- Abbreviate words where possible.
- Display may be analog or digital.
- Display may be alphanumeric, symbolic, or graphic.

Interface (CRT and related hardware)

- Function controls should be grouped near applicable CRT and distinct from other keys (also avoid multiple mode QWERTY keys).
- Terminal should have QWERTY keyboard where alphanumeric entry is needed.
- Word entry should not exceed seven characters.
- Two-step data or function entry is preferred for CRT:
  80 characters × 24 lines
  512 × 256 addressable points (minute)
  0.05-in. vector line (maximum)
  50 full-screen vectors/second (minute)
  30-Hz refresh rate (minute)
- Every page of CRT display should be labeled.
- Upper right quadrant should generally be used for most important information.
- Chernoff faces are not acceptable.

6.2 Interaction

6.2.1 Integration with procedures
- Operational aid should be reflected in procedures and training.
- Terms used by displays should correspond with same terms in procedures and on other equipment.

6.2.2 Integration with other control room equipment
- Operational aid should be integrated with control room for operator comprehensibility and successful operator intervention.

6.2.3 User involvement

6.3 Responsibility of operation
- Display may be manual or automatic.

6.4 Crew verification of system response (none)

6.5 Workload
6.5.1 Additional tasks
- Workload allocated to humans should not exceed ability.

6.5.2 Tasks eliminated
- Operational aid should be designed for minimum operator motion.
- Unncessary information should be eliminated.

6.5.3 Cognitive
- Alarm prioritization should have a four-level maximum.
- Operator should not have to mentally convert between scales or metrics.

6.6 Communication
6.6.1 Adaptability to user experience
- Linear relationship between measured variable and displayed variable is preferred, although nonlinear relationship may be needed in some cases.

6.6.2 Dialogue structured to task
- Dialogue should be based on operator's point of view.
- System should prompt user.
- Maximum time to enter request for information should be 30 s.
- Data input string should be correctable without complete reentry.

7. Maintenance and Testing
7.1 Requirements (none)
7.2 Responsible organizations and duties (none)
7.3 Methods used to verify accomplishment (none)
7.4 High-maintenance components (none)
7.5 Self-testing and on-line diagnostics (none)

8. User Training
8.1 Additional training needed
- Personnel should be trained for using operational aid.
- Instructions for operation without operational aid should be available.

8.2 Extent of knowledge of system needed (none)
8.3 Use of system during training (none)
8.4 Future users (none)

9. Documentation
- Operational aid should be documented by user's manual or minimum.

9.1 User control of documentation (none)
9.2 Currency (none)
9.3 Availability (none)
9.4 Perspective (none)

10. Work Status (section does not apply)
10.1 Current
10.2 Expected operation

B.5. OPERATIONAL AID FUNCTIONS

B.5.1 FUNCTIONS AND ACTIVITIES ENDORSED (RECOMMENDED OR IMPLIED) FOR OPERATIONAL AID IMPLEMENTATION

NUREG-0696

- Assist reactor operators in determining plant safety status
- Relieve reactor operators of peripheral duties and communications not directly related to reactor system manipulation
- Provide remote data display for personnel and consultants to prevent congestion in control room
- Assist reactor operators in accomplishing on-site and off-site communications
- Improve detection of abnormal conditions
- Validate data

NUREG-0700

- Assist reactor operators in prioritizing alarm information
- Help prevent accidental activation of systems or equipment
- Help eliminate unnecessary information
- Provide a sequential record of operator actions

NUREG-0835

- Validate data
- Diagnose problem
- Recognize system failures

NUREG/CR-2587 (R. A. Kisner and P. R. Frey, "Functions and Operation of Nuclear Power Plant Crews," April 1982.)

- Assist operators in monitoring plant systems to detect discrepancies and deviations at the lowest possible level in the hierarchy of a system
- Assist operators in verifying that systems about to be called into service, already in service, or removed from service are functioning properly
- Provide systematic and consistent display of data
- Assist operators in verifying that the procedures in use apply to the actual circumstances facing the operator
- Prepare operators for exercising control over degraded systems (i.e., a system functioning below the level of automation intended by the designer)
- Assist operators in validating data prior to acting on them
- Assist operators in diagnosing problems

B.5.2 FUNCTIONS, ACTIVITIES, AND DEVICES THAT SHOULD BE EXCLUDED FROM IMPLEMENTATION

NUREG-0696
- Signals to SPDS or other ERFs that have been processed by a software-programmable device
- Direct interference with safety systems

NUREG-0700
- Prioritization of alarms by greater than four levels
- Display of incomplete information, which requires an excessive effort by operators to supplement it with information from other locations and displays
- Confusing displays that fail to distinguish between demand for operation and actual status
- Systems whose functions are unverifiable, results untestable, and failures not evident
- Display of data that requires operator to mentally convert between scales or metrics
- Monitoring and diagnosis of plant safety functions in such a manner that the human operator is no longer responsible for final determination of safety status
- Systems that force workload or time allotments to exceed human capability

NUREG-0814
- Systems that cannot handle conflicting requests for resources
- Loud printers

NUREG-0835
- Chernoff faces
- Automatic systems that have no manual override (applies mainly to SPDS)

SECY 82-111B
- Isolated functions not integrated into operations

IEEE STD 566-1977
- Functions with failure modes that are not readily apparent
- Functions that divert operator attention away from principal duties

APPENDIX B REFERENCES

1. R. A. Kisner and P. R. Frey, "Functions and Operations of Nuclear Power Plant Crews," NUREG/CR-2587, ORNL/TM-8237, April 1982.

2. P. R. Frey and R. A. Kisner, "A Survey of Methods for Improving Operator Acceptance of Computerized Aids," NUREG/CR-2586, ORNL/TM-8236, April 1982.

NUREG/CR-3655
ORNL/TM-9068
NRC Distribution Category RX

INTERNAL DISTRIBUTION

1. J. L. Anderson
2. H. Gray
3. P. M. Haas
4. E. W. Hagen
5-14. R. A. Kisner
15. A. P. Malinauskas
16. F. R. Mynatt
17. L. C. Oakes
18. T. W. Reddoch
19. W. H. Sides, Jr.
20. M. J. Kopp (Advisor)
21. P. F. McCrea (Advisor)
22. P. W. Murrill (Advisor)
23. H. M. Paynter (Advisor)
24. H. E. Trammell (Advisor)
25-26. Central Research Library
27-29. Document Reference Section
30-31. Laboratory Records Department
32. Laboratory Records, ORNL RC
33. ORNL Patent Section
34. I&C Publications Office

EXTERNAL DISTRIBUTION

35. Assistant Manager for Energy Research and Development, DOE Oak Ridge Operations Office, Oak Ridge, TN 37831
36. A. D. Alley, General Electric Co. Advanced Nuclear Technology Operation, P. O. Box 3508, MS-S29, Sunnyvale, CA 94088
37. S. Baron, Vice President, Information Sciences Division, Bolt, Beranek, and Newman, Inc., 10 Moulton St., Cambridge, MA 02238
38. Leo Beltracchi, Senior Human Factors Engineer, Human Factors Engineering Branch, Division of Human Factors Safety, Office of NRR, U.S. Nuclear Regulatory Commission, Washington, DC 20555
39. D. G. Cain, Program Manager, Nuclear Safety Analysis Center, 3412 Hillview Avenue, P. O. Box 10412, Palo Alto, CA 94303
40. Julian M. Christiansen, Universal Energy Systems, 4401 Dayton-Xenia Road, Dayton, OH 45432
41. William R. Corcoran, Director, Plant Engineering, Nuclear Power Systems, Combustion Engineering, Inc., MS 9482421, 1000 Prospect Hill Road, Windsor, CT 06095
42. W. R. Davidson, General Atomic Company, P. O. Box 81608, San Diego, CA 92138
43. Paul E. Dietz, Project Manager, Criteria & Analysis Division, Institute of Nuclear Power Operations, 1820 Waterplace, Atlanta, GA 30339
44. David E. Embry, 1 School House, Higher Lane, Dalton, Parbold, Lancashire WN8 7RP, England
45. Donald Farr, Director, Human Factors Systems, Science Applications, Inc., 1710 Goodridge Drive, McLean, VA 22102
46. Lothar Felkel, GRS, Forschungsgelände, 8046 Garching, Federal Republic of Germany
47. Joseph R. Fragola, Science Applications, Inc., 274 Madison Avenue, Suite 1501, New York, NY 10016

48. P. R. Frey, Senior Scientist, Search Technology, Inc., 25B Technology Park/Atlanta, Norcross, GA 30092
49. Walter Gilmore, EG&G Idaho Inc., P. O. Box 1625, Idaho Falls, ID 83415
50. Kris L. Gimmy, E. I. duPont de Nemours & Co., Savannah River Laboratory, Aiken, SC 29801
51. Lewis F. Hanes, Manager, Human Sciences Group, Bldg. 801-3, C-8, Westinghouse R&D Center, 1310 Beulah Road, Pittsburgh, PA 15235
52. Eric Hollnagel, OECD Halden Reactor Project, P. O. Box 173-N, 1751 Halden, Norway

53-67. J. P. Jenkins, Senior Engineering Psychologist, U. S. Nuclear Regulatory Commission, RES/DFO/HFB, MS 1130SS, Washington, DC 20555

68. E. A. Krantz, EG&G Idaho Inc., P. O. Box 1625, INEL, Idaho Falls, ID 83415
69. S. M. Matin, Ebasco Services, Inc., Advanced Technology Department, Two World Trade Center, New York, NY 10048
70. O. R. Meyer, Idaho National Engineering Laboratory, Box 1625, Willow Creek Building, Idaho Falls, ID 83415
71. Neville Moray, Professor, University of Toronto, Department of Industrial Engineering, Toronto, Ontario, Canada M5S 1A4
72. Kenneth G. Murphy, Jr., Nuclear Engineer, Division of Risk Analysis, Office of RES, U. S. Nuclear Regulatory Commission, Washington, DC 20555
73. William R. Nelson, Engineering Specialist, Idaho National Engineering Lab., EG&G Idaho, Inc., P. O. Box 1625, Idaho Falls, ID 83415
74. Roger A. Newton, Superintendent, Reactor Engineering, Wisconsin Electric Power Company, 231 W. Michigan, P. O. Box 2046, Milwaukee, WI 53201
75. John F. O'Brien, Project Manager, Nuclear Engineering & Operations Dept., Electric Power Research Institute, 3412 Hillview Avenue, P. O. Box 10412, Palo Alto, CA 94303
76. Charles M. Overbey, Human Engineering Section Leader, Division of Facility Operations, RES/DFO/HFB, U. S. Nuclear Regulatory Commission, Washington, DC 20555
77. Richard W. Pew, Principal Scientist, Bolt, Beranek & Newman, Inc., 10 Moulton Street, Cambridge, MA 02238
78. Leonard C. Pugh, General Electric Company Advanced Nuclear Technology Operation, P. O. Box 3508, MS-S29, Sunnyvale, CA 94088
79. Jens Rasmussen, Head, Electronics Dept. RISO National Laboratory, Postbox 49, DK-4000 Roskilde, Denmark

80-89. William B. Rouse, President, Search Technology, Inc., 25B Technology Park/Atlanta, Norcross, GA 30092

90. Thomas G. Ryan, Senior Engineering Psychologist, RES/DFO/HFB, U. S. NRC, Washington, DC 20555
91. S. E. Seeman, Westinghouse Hanford Company, Hanford Engineering Development Laboratory, P. O. Box 1970, Richland, WA 99352
92. Thomas B. Sheridan, Professor, Massachusetts Institute of Technology, Building 1, Room 110, MIT, Cambridge, MA 02139

93. M. A. Sillamaa, Atomic Energy of Canada Limited, Engineering Company, Sheridan Park Research Community, Mississauga, Ontario L5K 1B2 Canada
94. H. Smidt-Olsen, Institutt for Energiteknikk, Halden Reactor Project, P. O. Box 173, N-1751 Halden, Norway
95. Brian Tolley, Commission of the European Communities, Directorate of Science, Research and Development, Rue de la Loi Zoo, 1049, Brussels, Belgium
96. Jussi K. Vaurio, Program Manager, Fast Reactor Safety Technology, Management Center, Argonne National Laboratory, 9700 South Cass Avenue, Argonne, IL 60439
97. J. G. Wohl, Vice President R&D, Alpha Tech Inc., 3 New England Executive Park, Burlington, MA 01803
98. David D. Woods, Research Psychologist, Westinghouse Research & Development, Pittsburgh, PA 15235
99. J. Wreathall, Executive Engineer, NUS, 910 Clopper Road, Gaithersburg, MD 20878
100. DOE Technical Information Center, Oak Ridge, TN 37831
101-500. Given distribution as shown in NRC Category RX (10 copies NTIS)

☆U.S. GOVERNMENT PRINTING OFFICE:1984 -746 -067/ 4086 REGION NO. 4

NRC FORM 335 (11 81)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)
NUREG/CR-3655
ORNL/TM-9068

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)
A Method for Analytical Evaluation of Computer-Based Decision Aids

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
W. B. Rouse, R. A. Kisner, P. R. Frey, and S. H. Rouse

5. DATE REPORT COMPLETED
MONTH: March | YEAR: 1984

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Oak Ridge National Laboratory
P. O. Box X
Oak Ridge, TN 37831
and
Search Technology, Inc.
25B Technology Park/Atlanta
Nrocross, GA 30092

DATE REPORT ISSUED
MONTH: July | YEAR: 1984

6. (Leave blank)

8. (Leave blank)

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Human Factors and Safeguards Branch
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10. PROJECT/TASK/WORK UNIT NO.

11. FIN NO.
B0438

13. TYPE OF REPORT
Final

PERIOD COVERED (Inclusive dates)

15. SUPPLEMENTARY NOTES

14. (Leave blank)

16. ABSTRACT (200 words or less)

This report presents a proposed methodology that involves a two-stage process of classification and analytical evaluation of decision aids for nuclear power plant operators. The classification scheme relates any particular aid to one or more general decision-making tasks. Evaluation proceeds using a normative top-down design process based on the classification scheme and involves determining how various design issues associated with this process were resolved by the designer. The result is an assessment of the "understandability" of the aid as well as the identification of training and display requirements necessary to ensure understandability. The methodology is illustrated by applying it to the evaluation of an aid designed to support operators in recovery of critical safety functions at a pressurized-water reactor.

Two appendices are included. Appendix A contains information collected from manufacturers, developers, and users of operational aid systems. Appendix B is a review of NRC documents and guidelines that might apply to operational aids.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

Operational Aids; Decision Aids;
Decision Making; System Evaluation

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS (This report)
unclassified

21. NO. OF PAGES

20. SECURITY CLASS (This page)
unclassified

22. PRICE
$

120555078877 1 1AN1R5
US NRC
ADM-DIV OF TIDC
POLICY & PUB MGT BR-PDR NUREG
W-501
WASHINGTON DC 20555