ACCESSION NUMBER ML003714955

NUREG/CR-xxxx
BNL-NUREG xxxx

Advanced Alarm Systems
Revision of Guidance and Its Technical Basis

Prepared by
William S. Brown, John M. O'Hara, and James C. Higgins

Brookhaven National Laboratory

Prepared for
U.S. Nuclear Regulatory Commission

NUREG/CR
BNL-NUREG

Advanced Alarm Systems: Revision of Guidance and Its Technical Basis

Manuscript Completed:
Date Published:

Prepared by
William S. Brown, John M. O'Hara, and James C. Higgins

Brookhaven National Laboratory
Upton, NY 11973-5000

Prepared for
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC JCN W-6290

ABSTRACT

The objective of this study was to update and revise Nuclear Regulatory Commission's (NRC) guidance for reviewing alarm system design in the Human-System Interface Design Review Guideline (NUREG-0700, Revision 1). The revisions were based on recent NRC research on the effects of alarm system design characteristics on operator performance and on a study examining the introduction of new computer-based human-system interface systems into conventional nuclear power plants. In addition this present study examined research on alarm systems published since the NRC's previous development of guidance for alarm systems, published in Human Factors Engineering Guidance for the Review of Advanced Alarm Systems (NUREG/CR-6105). Specifically, where supported by the technical bases, changes were made to the alarm system characterization, HFE guidelines, and the previously identified human performance issues. While the characterization of alarm systems in NUREG/CR-6105 did a reasonable job of representing their functional characteristics, it did not sufficiently address all aspects of alarm systems that are important to a design review. Thus, the characterization was expanded to (1) better illustrate the relationship of the alarm system to the plant's processes and systems, and (2) more clearly indicate the relationship between the human-system interface aspects of the alarm design and the guidance in NUREG-0700, Rev. 1. The research covered many aspects of alarm system design. Accordingly, modifications have been made in most of the elements of the characterization. In general, the research provided confirmatory data that was used to clarify the guidelines. In addition, several new guidelines were developed and the criteria of some existing guidelines were modified or supplemented based on this recent research. Several human performance issues were identified in recent literature. In most cases, they reflect those previously identified in earlier phases of this project. This information was used to revise issues, where appropriate. The changes to the characterization and HFE guidelines discussed in this document were reviewed and will be incorporated into NUREG-0700, Revision 2.

TABLE OF CONTENTS

Page

ABSTRACT . . . iii
LIST OF FIGURES . . . vii
EXECUTIVE SUMMARY . . . ix
PREFACE . . . xiii
ACRONYMS . . . xv

1 INTRODUCTION . . . 1-1

2 OBJECTIVE . . . 2-1

3 METHODOLOGY . . . 3-1

3.1 Overview . . . 3-1

3.2 Characterization of the Alarm System . . . 3-2

3.3 Development of the Technical Basis . . . 3-2

3.4 Development of Guidelines and Documentation . . . 3-4

3.5 Identification of Issues . . . 3-5

3.6 Peer Review . . . 3-5

4 RESULTS . . . 4-1

4.1 Basis for the Modifications to the Alarm System Characterization . . . 4-1

4.1.1 Evaluation of Recent Research: Descriptions of Alarm System Designs . . . 4-1
4.1.2 Modifications to the Alarm System Characterization . . . 4-8

4.2 Guidelines for HFE Design Review . . . 4-9

4.2.1 General Guidelines . . . 4-9

4.2.1.1 Evaluation of Recent Research . . . 4-9
4.2.1.2 Modifications to General Guidelines for Alarm Systems . . . 4-11

4.2.2 Alarm Definition . . . 4-12

4.2.2.1 Evaluation of Recent Research . . . 4-12
4.2.2.2 Modifications to Alarm Definition Guidelines . . . 4-14

4.2.3 Alarm Processing and Reduction . . . 4-14

4.2.3.1 Evaluation of Recent Research . . . 4-14
4.2.3.2 Modifications to Guidelines for Alarm Processing and Reduction . . . 4-16

4.2.4 Prioritization and Availability of Alarms 4-17

4.2.4.1 Evaluation of Recent Research 4-17
4.2.4.2 Modifications to Guidelines on Alarm Prioritization and Availability 4-19

4.2.5 Display 4-19

4.2.5.1 Visual Displays 4-20

4.2.5.1.1 Evaluation of Recent Research 4-20
4.2.5.1.2 Modifications to Visual Display Guidelines 4-22

4.2.5.2 Auditory Signals 4-22

4.2.5.2.1 Evaluation of Recent Research 4-23
4.2.5.2.2 Modifications to Guidelines for Auditory Signals 4-26

4.2.6 Control 4-27

4.2.6.1 Evaluation of Recent Research 4-27
4.2.6.2 Modifications to Guidelines for Alarm Control 4-27

4.2.7 Automated, Dynamic, and Modifiable Features 4-28

4.2.8 Reliability, Test, Maintenance, and Failure Indications 4-28

4.2.9 Alarm Response Procedures 4-29

4.2.9.1 Evaluation of Recent Research 4-29
4.2.9.2 Modifications to Guidelines for Alarm Response Procedures 4-29

4.2.10 Control-Display Integration and Layout 4-29

4.2.10.1 Evaluation of Recent Research 4-29
4.2.10.2 Modifications to Guidelines for Control-Display Integration and Layout . . 4-30

4.3 Human Performance Issues 4-30

5 DISCUSSION 5-1

6 REFERENCES 6-1

APPENDIX A Alarm System Characterization A-1

APPENDIX B Alarm System Guidelines B-1

APPENDIX C Alarm System Human Performance Issues C-1

LIST OF FIGURES

3.1 Major steps in developing NUREG-0700 3-2

3.2 Technical basis and process for developing guidance 3-3

3.3 Example of an alarm system design review guideline 3-6

EXECUTIVE SUMMARY

The alarm system is one of the primary means by which process abnormalities and failures are brought to plant personnel's attention. The need to improve the human factors engineering (HFE) of alarm systems has led to the development of advanced, computer-based alarm systems. The goal of such systems is to assist the operator by processing alarm data, and to improve the presentation of this information. This technology promises to provide a means of correcting many known deficiencies in alarm systems. Advanced, computer-based alarm systems are available as upgrades to existing human-system interfaces (HSIs), and are included in new control room designs.

The U.S. Nuclear Regulatory Commission (NRC) reviews the HFE aspects of control rooms to ensure that their design meets good human factors engineering principles and that the operator's performance and reliability are appropriately supported to protect public health and safety. The Human-System Interface Design Review Guideline, NUREG-0700, Rev. 1, was developed to provide guidance on HFE for the NRC. The NRC staff uses NUREG-0700 for (1) reviewing submittals of HSI designs prepared by licensees or applicants for a license or design certification of a commercial nuclear power plant (NPP), and (2) undertaking HSI reviews that could be included in an inspection or other types of regulatory review of HSI designs, or incidents involving human performance. It describes those aspects of the HSI design review process that are important to identifying and resolving human engineering discrepancies that could adversely affect plant safety. NUREG-0700 also has detailed HFE guidelines for assessing the implementation of HSI designs.

Alarm systems are key elements of control rooms because of the complexity of the process control task. Accordingly, NRC conducted a program of research aimed at developing a technical basis for reviewing advanced alarm systems. In an earlier NRC project, the key design features of advanced alarm systems were characterized, and HFE review guidance was developed and documented in *Human Factors Engineering Guidance for Advanced Alarm Systems*, NUREG/CR-6105. The guidance was based on a variety of sources, including HFE guidelines and standards, industry experience, and literature on features of alarm system design and their effects on operator performance. The guidance was subsequently integrated into Section 4 of NUREG-0700, Rev. 1.

Since the publication of this guidance, there has been a considerable amount of research on alarm systems that may have implications for developing new guidance or for revising the existing guidance. The purpose of the study reported here was to examine recent research and expand and revise the guidance to maintain it as state-of-the-art alarm system design review guidance.

Thus, the objective of this study was to review recent literature and, where supported by the technical bases in that literature, to address the following:

1. Revise and expand the alarm characterization in NUREG/CR-6105.

2. Revise and expand the HFE design review guidance:

    - Develop new review guidance to address alarm system design characteristics, or human performance issues not fully covered in NUREG-0700, Rev. 1

    - Revise the existing review guidance for alarm designs in NUREG-0700, Rev. 1

    - Augment the technical basis of existing guidance with confirmatory information

3. Identify human performance issues.

The methodology used to accomplish these objectives was the general NUREG-0700 methodology for guidance development. The revisions to the characterization and guidance were based on recent NRC research on the effects of alarm system design characteristics on operator performance and on a study examining the introduction of new computer-based human-system interface systems into conventional nuclear power plants. In addition we examined

research on alarm systems published since the NRC's previous development of guidance for alarm systems, published in NUREG/CR-6105.

The results for each objective will be briefly summarized below.

Alarm System Characterization

A system characterization is important because it provided a structure within which the reviewer could request information about a system and with which to structure the guidance. Existing alarm systems were reviewed and compared with the alarm characterization previously developed in NUREG/CR-6105. While the characterization reasonably represented the functional characteristics of alarm systems, it did not adequately address all aspects that are important to an HFE design review. Thus, the characterization was expanded to (1) better illustrate the relationship of the alarm system to the processes and systems of the plant, and (2) more clearly indicate the relationships between the HSI aspects of the alarm system and the guidance.

HFE Design Review Guidelines

Recent research has addressed many aspects of alarm system design, and as a result, modifications were made to most of the elements of the alarm system characterization. In general, the research yielded confirmatory data which could be used to further clarify the guidelines. In addition, where supported by the literature, new guidelines were developed.

The guidelines were organized and specified in a standard format and were organized as follows:

- General Guidelines
- Alarm Definition
- Alarm Processing
- Alarm Prioritization and Message Availability
- Display
  - General Alarm Display Guidelines
  - Display of High-Priority Alarms
  - Display of Alarm Status
  - Display of Shared Alarms
  - Alarm Messages
  - Coding Methods
  - Display Layout and Organization
- User-System Interaction
  - General Guidelines
  - Silence Functions
  - Acknowledge Functions
  - Reset Functions
  - Alarm Management
  - Automatic Features
- Control Devices
- Backup, Test, Maintenance, and Failure Indication Features
  - Reliability
  - Test
  - Maintenance
  - Failure Indication
- Alarm Response Procedures
- Control-Display Integration and Layout

The guidance was then peer reviewed and revised. This new guidance will be integrated into NUREG-0700.

Human Performance Issues

Where there was insufficient information for the technical basis upon which to develop valid design review guidance, an issue was defined. Several human performance issues were identified in recent literature. However, in most cases, they reflect ones already identified in earlier phases of this NRC project.

The issues were organized into the following categories. General issues dealt with the overall purpose and design of alarm systems, e.g., how to design alarm setpoints based on a two-stage alerted monitor approach to alarms. The second category of alarms was related to processing methods, e.g., the relationship of processing complexity to operator performance and how to design more effective alarms to support secondary event detection. The third category of alarms addressed display issues, e.g., formulating rules to allocate individual alarms to different types of alarm displays, such as messages or tiles. The fourth category of alarm issues dealt with controls, e.g., the determination of how to automate various alarm functions.

In conclusion, the studies reviewed have strengthened the alarm system design review guidance and its technical basis, especially for alarm processing and alarm availability. Three areas were especially reinforced. The first is the desirability of alarm processing and its operational acceptability. The second is the importance of providing access to suppressed alarms. The third is the need to provide information on the alarm's reliability and information to enable operators to confirm the validity of alarms in the extremely complex and noisy control room.

PREFACE

Brookhaven National Laboratory (BNL) prepared this report for the Division of Systems Technology of the U.S. Nuclear Regulatory Commission's (NRC's) Office of Nuclear Regulatory Research as part of the requirements of the *Advanced Alarm System Review Criteria* project (FIN W-6290). Jerry Wachtel (301 415-6498; jxw4@nrc.gov) is the NRC's Project Manager for this work. BNL's Principal Investigator is John O'Hara (631 344-3638; ohara@bnl.gov).

ACRONYMS

ABB-CE	Asea-Brown-Bovari-Combustion Engineering
ABWR	advanced boiling water reactor
ADIOS	Alarm and Diagnosis - Integrated Operator Support
AECL	Atomic Energy of Canada, Limited
AIW	annunciation interrogation workstation
AP600	advanced PWR design (Westinghouse)
APWR	advanced pressurized water reactor
ARP	alarm response procedure
CAMLS	CANDU Annunciation Message List System
CANDU	Canadian Deuterium Uranium
CPIAS	Critical Parameter Indication and Alarm System
CRT	cathode ray tube
EdF	Electricité de France
HAMMLAB	HAlden Man-Machine LABoratory
HFE	human factors engineering
HSI	human-system interface
I&C	instrumentation and control
KAERI	Korean Atomic Energy Research Institute
NOK	Nordostchweizerische Kraftewerke AG
NORS	NOkia Research Simulator
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
P&ID	piping and instrumentation diagram
PIPS	Plant Information Processing System
RTD	Resistance temperature detectors
SART	silence, acknowledge, reset, and test
SDCV	spatially dedicated, continuously visible (display)
VDU	video display unit

11 INTRODUCTION

The alarm system is one of the primary means by which process abnormalities and failures are brought to plant personnel's attention. The need to improve the human factors engineering (HFE) of alarm systems has led to the development of advanced, computer-based alarm systems. The goal of such systems is to assist the operator by processing alarm data, and to improve the presentation of this information. This technology promises to provide a means of correcting many known deficiencies in alarm systems. Advanced, computer-based alarm systems are available as upgrades to existing human-system interfaces (HSIs), and are included in new control room designs.

The U.S. Nuclear Regulatory Commission (NRC) reviews the HFE aspects of control rooms to ensure that their design meets good human factors engineering principles and that the operator's performance and reliability are appropriately supported to protect public health and safety. Alarm systems are key elements of control rooms because of the complexity of the process control task. Accordingly, NRC conducted a program of research aimed at developing a technical basis for reviewing advanced alarm systems.

In an earlier NRC project, the key design features of advanced alarm systems were characterized, and HFE review guidance was developed and documented in *Human Factors Engineering Guidance for Advanced Alarm Systems*, NUREG/CR-6105 (O'Hara, Brown, Higgins, and Stubler, 1994). The guidance was based on a variety of sources, including HFE guidelines and standards, industry experience, and literature on features of alarm system design and their effects on operator performance (see Section 3.1 of the present report for a detailed discussion of guidance development). The guidance was subsequently integrated into Section 4 of *The Human-System Interface Design Review Guideline*, NUREG-0700, Rev. 1 (O'Hara et al., 1996).

Since the publication of this guidance, there has been a considerable amount of research on alarm systems that may have implications for developing new guidance or revising it. The new literature can be divided into three categories: NRC research, industry research, and general research on supervisory control.

Two recent studies by the NRC are relevant to alarm systems. The first, conducted in an earlier phase of this project, specifically addressed the characteristics of alarm systems. During the development of the alarm system guidance discussed above, several human performance issues were identified. These were areas in which data were lacking, or where findings conflicted. The issues were prioritized, and from this analysis, those associated with the visual display of alarm information and simple alarm processing prioritization and filtering methods were rated as having the highest priority. To address this need, regulatory research was conducted on these issues (O'Hara, Brown, Hallbert, Skrånning, Persensky, and Wachtel, 2000).

The primary purpose of the research, referred to in this report as the *NRC alarm study*, was to evaluate the impact of the alarm system design on the performance of the plant and on operators understanding of the potential safety issues, and to provide data from which to develop design review guidance. Three alarm system design characteristics were studied: (1) alarm processing (degree of alarm reduction); (2) alarm availability (dynamic prioritization and suppression); and (3) alarm display (a dedicated tile format, a mixed tile and message list format, and a format in which alarm information is integrated into the process displays). The alarm characteristics were combined into eight separate experimental conditions. Six two-person crews of professional nuclear power plant (NPP) operators participated in the study. Following training, each crew completed 16 test trials, two trials in each of the eight experimental conditions (one with a low-complexity scenario, and one with a high-complexity scenario). Measures were obtained of plant performance, operator task performance, situation awareness, and workload. In addition, the operators' ratings and evaluations were obtained.

A second NRC study on alarm systems assessed the impact of introducing advanced HSI technologies into the control room of a conventional nuclear power plant (Roth and O'Hara, 1998). This technology included an advanced alarm system as well as computer-based procedures and an advanced display system. The study explored the effect of the new systems on the cognitive functioning of individual crew members, and on the structure and functioning of the crew as a team. The latter information was obtained by observing five crews of professional

operators during full-scope training simulations of plant disturbances. In addition, operators and other knowledgeable utility and vendor personnel were interviewed.

The results of both studies have many implications for existing guidance. Within the context of NUREG-0700, regulatory research can play two important roles in establishing guidance: developing its technical basis, and confirming the guidance (O'Hara, Brown, and Nasta, 1996). First, when the technical basis does not exist in other source materials, the experimental results can fill the knowledge gap, i.e., provide the information upon which design review guidance can be developed. Second, when the guidance has been based on other sources of information, such as technical papers, testing may be necessary to gain confirmatory evidence that (1) the guidance is an acceptable extraction, synthesis, or interpretation of the data, and (2) that the guidance is appropriate to an NPP application. Confirmatory research is most important for new guidance that was not developed from already existing guidelines. The NRC alarm study served both purposes: to evaluate the effects of specific alarm system characteristics on performance to establish a technical basis upon which to develop design review guidance; and, to authenticate the selected alarm system guidance.

A second source of information stems from continuing research on alarm system concepts by the nuclear and other complex systems industries (such as process control and aviation). This work reflects both the increasing technological capabilities to address alarm system issues, and their widely recognized importance in effective process control. Up-to-date information on the work of alarm system designers in both U.S. industries and research organizations and those overseas has been published in the proceedings of several conferences (e.g., the "Specialists' Meeting on Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants" sponsored by the International Atomic Energy Agency held in Chalk River, Canada, October 1996). The papers on plant alarm systems typically describe new (or enhanced) systems or approaches that offer better support for operator actions, or cover specific shortcomings of existing approaches. A subset of these papers also report the results of evaluations of the systems' performance.

Finally, there has been an increasing interest in supervisory control performance and in the design and effectiveness of alarm systems, and a significant number of papers on these topics have appeared in the general HFE literature, e.g., the special issue of *Ergonomics* (1995, Vol. 38) on Warnings in Research and Practice. The implications of the findings on alarm guidance from these three areas are the subject of this report.

12 OBJECTIVE

The objective of this study was to review recent literature and, where supported by the technical bases in that literature, to address the following:

1. Revise and expand the alarm characterization in NUREG/CR-6105.

2. Revise and expand the HFE design review guidance:

    - Develop new review guidance to address alarm system design characteristics, or human performance issues not fully covered in NUREG-0700, Rev 1

    - Revise the existing review guidance for alarm designs in NUREG-0700, Rev. 1

    - Augment the technical basis of existing guidance with confirmatory information

13. Identify human performance issues.

3 METHODOLOGY

The methodology used in this study is an application of the general NUREG-0700 methodology for guidance development (O'Hara, Brown, and Nasta, 1996). In this section, the general methodology is described including its application in this study.

3.1 Overview

This section describes the rationale for guidance development. Figure 3.1 shows the methodology for the overall guidance development for NUREG-0700. The portion of the methodology discussed in this report is boxed in the figure.

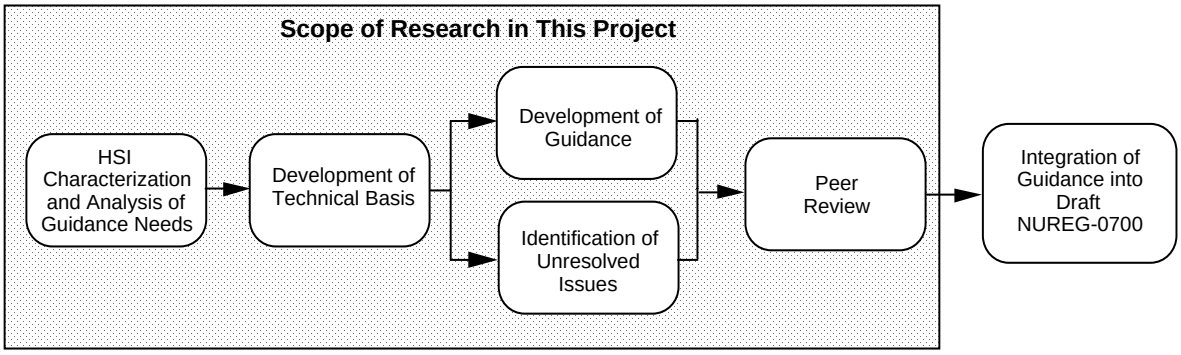

Figure 3.1 Major steps in developing NUREG-0700 guidance

The methodology was guided by the following objectives:

- Establish a process that will result in valid, technically defensible review criteria.
- Establish a generalizable process that can be applied to any aspect of HSI technology for which review guidance is needed.
- Establish a process that optimally uses available resources, i.e., develop a cost-effective methodology.

The methodology places a high priority on establishing the validity of the guidelines. Validity is defined along two dimensions: internal and external validity. Internal validity is the degree to which the individual guidelines are based on an auditable technical basis. The technical basis is the information upon which the guideline is established and justified. The technical bases vary for individual guidelines. Some guidelines may be based on technical conclusions from a study of empirical research, some on a consensus of existing standards, while others are based on judgement that a guideline represents good practices based on the information reviewed. Maintaining an audit trail from each guideline to its technical basis serves several purposes by enabling the following:

- Technical merit of the guideline to be evaluated by others
- A more informed application of the guideline since its basis is available to users
- Deviations or exceptions to the guideline to be evaluated

External validity is the degree to which the guidelines are independently peer reviewed. Peer review is a good method of screening guidelines for conformance to accepted HFE practices and for comparing guidelines to the practical operational experience of HSIs in real systems.

For individual guidelines, these forms of validity can be inherited from the source documents that form their technical basis. Some HFE standards and guidance documents, for example, already have good internal and external validity. If validity is not inherited, however, it should be established as part of the process for guidance development. Methodology was established to provide validity both inherited from its technical basis and through developing and evaluating guidance.

Figure 3.2 shows the process used to develop the technical basis and guidance. The process emphasizes information sources that have the highest degree of internal and external validity for developing the technical basis. Thus, primary and secondary source documents were sought as sources of guidance first, followed by tertiary source documents, basic literature, industry experience, and other sources. From these, we identified design principles and lessons from industry experience. Using this technical basis as a foundation, the guidance was developed. The guidance was peer reviewed and revised accordingly. For specific aspects of the topic, in which the technical basis was inadequate for developing guidance, we defined unresolved research issues. Thus, the technical basis led to the development of both guidance and issues. The resulting guidance documentation includes HFE guidelines, technical basis, the development methodology, and unresolved research issues.

Each of the steps of this research – topic characterization, development of technical basis, guidance development and documentation, identification of issues, and peer review – is discussed in greater detail in the sections that follow.

3.2 Characterization of the Alarm System

The first step in developing guidance was to identify the areas for which it was needed. This was accomplished by developing a characterization framework for alarm systems. The characterization identified the dimensions and characteristics along which alarm systems can be defined. The characterization is important because it provides a structure within which the reviewer can request information about a specific system being reviewed. It also provided the structure for HFE guidance organization.

A preliminary characterization was presented in NUREG/CR-6105. We developed this further by reviewing several new alarm system design descriptions to identify any changes needed to ensure that the characterization can be broadly applied to a wide range of alarm system designs. The results of the alarm system review are in Section 4.1 and the new characterization is presented in Appendix A.

3.3 Development of the Technical Basis

We began to formulate detailed review guidelines by collecting technical information on which guidance would be based (Figure 3.2). Our earlier alarm guidance development had already utilized many of the types of information identified in the figure, especially primary and secondary source documents. In this effort to update and revise the guidance, we focused on information from basic literature and original research.

When guidance was based on basic literature, engineering judgement was required to generalize from the unique aspects of individual experiments and studies to actual applications in the workplace. This is because individual experiments have unique constraints that limit their generalizability (such as their unique participants, types of tasks performed, and types of equipment used). For example, laboratory experiments often do not involve tasks of the complexity of NPP operations, and most experiments do not examine tasks under the same performance shaping factors (such as rotating shifts, stress, and fatigue) that exist in a work environment. While information from research is a valuable part of developing guidance, it usually cannot be blindly adopted. Thus, the results must be

interpreted in the context of real-world tasks and systems, which involves judgement based on professional and operational experience.

Finally, as discussed in Section 1, some information was identified in original research. A full account of the research is published elsewhere (O'Hara et al., 2000; Roth and O'Hara, 1998). Original research has the advantage of enabling a study to be focused on the specific issues that need to be addressed in guidance development. However, because of the time and resources required to conduct original research, it is only used when important information is needed that cannot be obtained through other means.

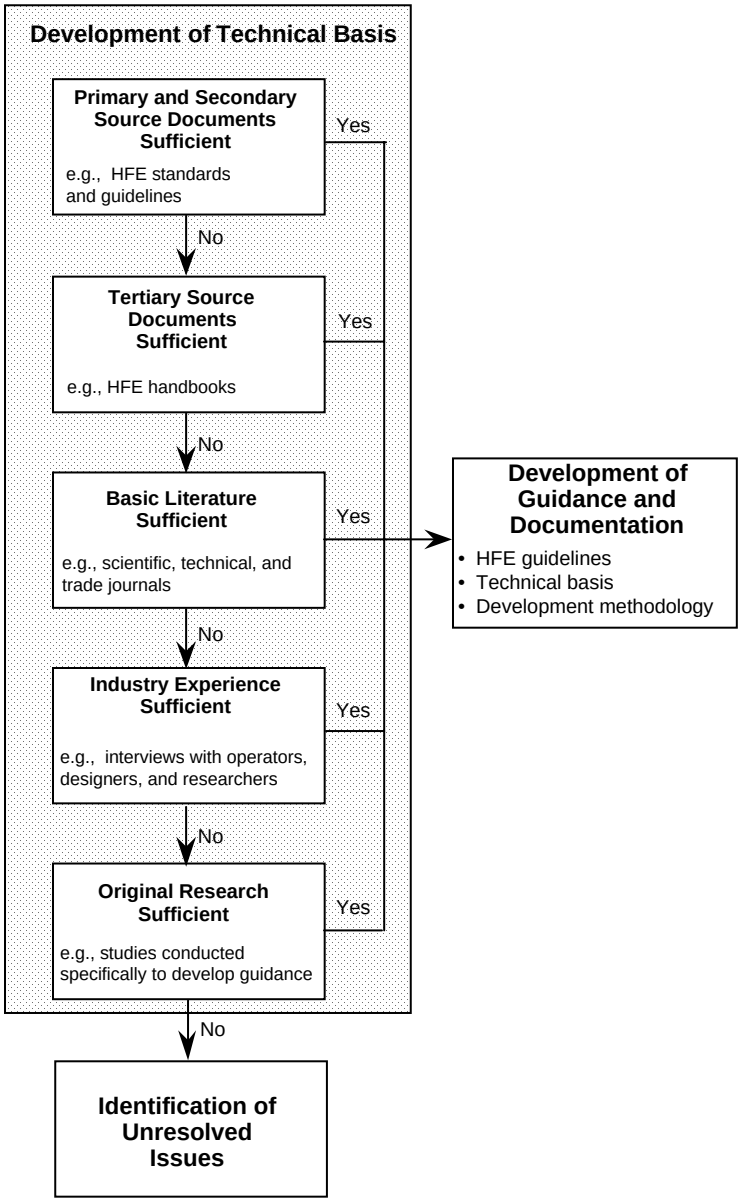

Figure 3.2 Technical basis and process for developing guidance

3.4 Development of Guidelines and Documentation

Once the technical information was assembled, a draft set of new guidelines was developed. The methodology was conservative in the sense that guidelines were developed or modified only for those aspects of alarm design that, in our interpretation, were supported by the literature. In addition to supporting guidance development, recent research was also reviewed to identify whether the results suggest changes or modifications to the existing guidance in NUREG-0700, Rev 1. Where new research provided a sufficient technical basis, the guidance was modified. This typically resulted in a modification to the *Review Criterion* or to the *Additional Information* components of the guidance, which provides information to support the interpretation of the guidance (guidance components are described below).

Finally, the research was reviewed to identify whether the results support the technical basis of the guidance in NUREG-0700, Rev 1. This technical basis is documented in NUREG/CR-6105. Where new research supports and augments the technical basis of a guideline, the *Discussion* component of the guidance was modified to include the new, confirmatory information.

The guidelines adopted the standard format in NUREG-0700, Rev. 1. An example is presented below:

4.3-2 Alarm Reduction

The number of alarm messages presented to the crew during off-normal conditions should be reduced by alarm processing techniques (from a no processing baseline) to support the crew's ability to detect, understand, and act upon all alarms that are important to the plant condition within the necessary time.

ADDITIONAL INFORMATION: Since there is no specific guidance on the degree of alarm reduction required to support operator performance, the designer should evaluate the system with operators to assess the effectiveness of the alarm reduction process. This assessment should include evaluations that simulate the operation of the alarm system under situations that activate multiple alarm conditions and/or generate increased operator workload. The use of dynamic mockups and prototypes of the alarm system and dynamic control room simulators should be considered when developing these assessments.[6105]

Discussion: While it is clear that the number of unprocessed alarms is overwhelming to operators and that processing techniques can reduce the number of alarms (Cory et al., 1993; Gertman et al., 1986), little research exists that provides more specific guidance on what number of alarms is an appropriate target. Hollywell and Marshall (1994) found that operators preferred CRT alarm message rates of not more than 15 messages per minute and that when the rate increased the number of missed alarms increased. This of course depends on the alarm display and types of message design implemented. It has also been found that reducing the number of alarms by 50% has little effect on operator performance (Baker, 1985a). In terms of operator processing of alarm information, it is probably inappropriate to specify alarm reduction in terms of absolute numbers of alarms (a metric often used to assess alarm reduction schemes). Demands on operator information processing depends not specifically on the absolute number of alarms, but on their rate, their recognizability as familiar patterns, their predictability, and the complexity of the operator's ongoing task. In addition, this guideline is consistent with the high-level design review principles of Cognitive Compatibility, Situation Awareness, Task Compatibility, and Timeliness.

Figure 3.3 Example of an alarm system design review guideline

Each of the guidelines is composed of the following components:

Guideline Number – Within each section, individual guidelines are numbered consecutively. Each guideline has a number which reflects its section and subsection location, followed by a dash, and then its unique number.

Guideline Title – Each guideline has a brief, unique, descriptive title.

Review Criterion – Each guideline contains a statement of an HSI characteristic so that the reviewer may judge the HSI's acceptability. The criterion is not a requirement, and discrepant characteristics may be judged acceptable based on the procedures in the review process.

Additional Information – For many guidelines, there is additional information which may address clarifications, examples, exceptions, and details on measurements, figures, or tables. This information is intended to support the reviewer's interpretation or application of the guideline.

Discussion – This section summarizes the technical basis on which the guideline was developed. It may identify the primary source documents, the technical literature such as journal articles, or the general principle from which the guideline was derived. This section will be removed when the guidance is integrated into NUREG-0700.

In place of the Discussion section will be a Source field.

Source – The source field identifies the NUREG/CR (or other document) containing the technical basis and development methodology for the guideline. As is the standard practice, the source field will cite this document as it will appear in its final form.

A discussion of the guidance modifications and their technical bases are in Section 4.2 and the revised guidance is presented in Appendix B.

3.5 Identification of Issues

A preliminary identification of alarm system issues was presented in previous publications (O'Hara and Brown, 1991a; O'Hara and Brown, 1991b). A summary of those issues is presented in Appendix C. Recent research was reviewed to determine whether the results indicated human performance issues not previously identified or suggested new interpretations of existing issues.

From a research standpoint, issues reflect aspects of the design and use of alarm systems that will require additional investigation to resolve. From a design review standpoint, issues reflect aspects of design and use that will have to be addressed on a case-by-case basis. For example, an issue can be addressed as part of design-specific tests and evaluations.

The results of the issue identification are in Section 4.3.

3.6 Peer Review

The resulting technical basis and guidance was submitted for review by individuals with knowledge and expertise related to alarm systems. Included were reviews by personnel from the U.S. NRC with expertise in HFE and related engineering fields. Human factors specialists who are external to the NRC and have expertise in human performance in complex systems, such as NPPs and aviation, conducted additional reviews. These external reviews included evaluations of the topic characterization along the criteria of clarity, accuracy, and completeness, and the technical basis along the criteria of organization, necessity, sufficiency, resolution, and basis. Comments from the peer reviews were incorporated into the current version of this document.

4 RESULTS

This section is divided into three subsections. The first addresses the alarm system characterization. The adequacy of the characterization of alarm system features and functions is best evaluated by comparing it to recent descriptions of such systems. In Section 4.1, several new systems are described with the intent to identify aspects of the characterization that warrant further development. The second addresses HFE design review guidelines. In Section 4.2, the human performance research related to alarm systems is evaluated for its implications for the HFE design review guidelines. The third identifies new human performance issues. In Section 4.3, the new human performance issues are identified.

The discussion in each section is divided into two subsections: Evaluation of Recent Research, and Modifications. In the Evaluation section, pertinent material is summarized and its relevance to the alarm guidance evaluated. Where warranted, this information is divided into the three categories of literature discussed above (system descriptions and evaluations, NRC research, and general HFE literature). In the Modifications section, the implications for the characterization, guidelines, or issues are identified.

In the appendices to this document, the implementation of the revisions is discussed. Appendix A contains the revised characterization. Appendix B contains the alarm system review guidance from NUREG-0700 and the Discussion sections from NUREG/CR-6105,both modified as described in this report. Appendix C summarizes human performance issues related to alarm systems.

4.1 Basis for the Modifications to the Alarm System Characterization

4.1.1 Evaluation of Recent Research: Descriptions of Alarm System Designs

This section gives general description of new alarm system designs. As several of these systems are still under development, some of the details may have changed from these descriptions.

The purpose of this section is to (1) identify recent trends in alarm system design and the types of characteristics and features that are being developed, and (2) determine whether the characterization should be modified.

The systems described are representative of new alarm system developments:

- Atomic Energy of Canada, Limited (AECL) CANDU Annunciation Message List System
- Electricité de France (EdF) N4 Plant Alarm System
- Westinghouse AWARE System
- Asea-Brown-Bovari-Combustion Engineering (ABB-CE) NUPLEX 80+ Alarm System
- Mitsubishi Atomic Power Industries Dynamic Priorities Alarm System
- Toshiba and Hitachi Advanced Boiling Water Reactor Alarm System
- Halden Computerized Alarm System for HAMMLAB

These descriptions were based on published literature, observations of the systems made during site visits, and discussions with alarm system designers. Following the system descriptions, the general trends in alarm system design that they reflect are summarized.

4 RESULTS

AECL CANDU Annunciation Message List System

Current Canadian Deuterium Uranium (CANDU) plants in Canada have relatively advanced alarm systems in comparison to most U.S. plants. In the Darlington plant, annunciator tiles and alarms presented via cathode ray tubes (CRT) devices are organized by control panel section; only alarms that are relevant to the control panel section are displayed. The alarm system CRTs show detailed alarm information in a list format. Information is grouped and color coded by priority using four levels: red, blue, white, and yellow. A separate and smaller color coding scheme is used for the annunciator tiles (e.g., the channel trip tile for the plant shutdown system is red). In the Pickering B control room, annunciator tiles are distributed among the relevant control sections, but detailed alarm information is displayed on two CRTs located in the center of the control panel. This information is presented using a list format and is color coded by plant system; there is no grouping by priority. Alarm information appears chronologically, starting with the top row of the left CRT. When all of the rows are filled on the left CRT, the information then appears on the top line of the right CRT. When all rows of the right are filled, the messages on the left CRT are overwritten. Once an alarm message has been overwritten, it can only be accessed from computer printouts.

To improve the alarm design, AECL is developing the CANDU Annunciation Message List System (CAMLS) with features that could be incorporated into other new and existing CRs (Davey, Feher, and Guo, 1995). CAMLS includes a console-based annunciation interrogation workstation (AIW) that provides access to real-time and historical alarm message logs, detailed alarm information, alarm response procedures, and supporting displays and flowcharts. A central annunciation message list is displayed on two side-by-side CRT displays, separate from the AIW, so that the most current alarm status is continuously available.

Alarms are indicated by a momentary tone, which eliminates the need for the operators to silence the alarm. Alarm acknowledgment and reset functions are effectuated with a single button. Acknowledgment of an alarm automatically presents detailed alarm information and alarm response procedures. No acknowledgment is required for low-priority alarms when those of higher priority are acknowledged. In addition, no acknowledgment is needed for status messages.

Alarm messages are color coded by priority based on the plant's mode, consequences (i.e., to safety, power generation, and plant equipment), and the operator's response requirements (e.g., type of response and available time). The full-text alarm messages make only limited use of abbreviations and acronyms. AECL found that using them increases the operator's workload and the opportunity for errors of interpretation. Thus, full-text messages may improve the use of alarm information.

Alarms are reduced by a variety of processing strategies. This includes reducing redundant and low-information alarms associated with particular plant modes, events, and process and equipment states. Additional reduction is accomplished by the following means:

- Having dynamic alarm setpoints (e.g., setpoints that change as a function of operating context)
- Coalescing similar messages (e.g., using a single message to reduce the number of individual messages from systems with redundant sensors, and using a single message to indicate a higher-level status that is derived from multiple plant parameters)
- Validating signals to ensure the integrity of sensor data
- Reducing alarm chatter (e.g., employing techniques to reduce the onset or effects of alarms associated with a parameter that oscillates across an alarm threshold)
- Separating fault and status annunciation messages (e.g., fault messages are grouped by priority, and status messages chronologically)

In addition to reducing alarms, conditional alarm generation is employed to create messages for expected alarms that have not occurred, and messages for impending violations of alarm limits based on the rate of change of a variable and its margin to the alarm setpoint.

EdF N4 Plant Alarm System

The EdF N4C alarm system contains four categories of alarms (Pirus, 1996):

- Red indicates personnel actions that must be taken quickly
- Yellow indicates personnel actions that can be delayed
- White indicates that an automatic action has been initiated
- Green indicates a protection system has been activated.

The information is presented on four CRTs. One each is dedicated to Red and Yellow alarms. Green and white alarms are shown on the third CRT, and the fourth is used to store alarms. The alarms are presented as text messages. From the alarm CRTs, operators have access to additional information on alarm sheets; these sheets are similar to alarm response procedures and include a more detailed explanation of its cause, and potential risks. They contain verification data, a list of associated automatic actions, consequent risks, and required operator actions. The alarm sheets are fully integrated with the instrumentation and control (I&C) system, so that the operator has all the information needed to take action on the alarm sheet display, and can take control actions directly through the display.

Many processing strategies are applied to reduce the number of alarms, including data validation, functional validation (e.g., suppressing the alarms that are consequences of the initial cause), and situation validation (e.g, ensuring an alarm is relevant in the current plant mode). According to Pirus (1996), fewer than 20 alarms are displayed for any transient. Thus, for example, in a house-load rejection transient, the system in an earlier plant design displayed 45 alarms to the operator, while the N4 displays only two. The operator can access all suppressed alarms through the alarm keyboard.

Westinghouse AWARE System

Westinghouse's AWARE alarm system is part of the AP600 HSI concept. Westinghouse is installing a tailored version of AWARE as part of its upgrade of Beznau Units 1 and 2 of the Nordostchweizerische Kraftewerke AG (NOK) plant in Switzerland. The AWARE system design is described in several papers (Carrera and Easter, 1991; Easter and Lot, 1992). The system was also studied as part of NOK's control room modernization, and its effect on the crew's performance was explored in a related NRC project (Roth and O'Hara, 1998).

The system has two main components: (1) an Overview Panel, and (2) a Support Panel. The Overview Panel is composed of a set of alarm message windows at the top of the control board. They are vacuum-fluorescent devices that display computer-generated alarm text messages of up to 80 characters. The alarm windows are analogous to traditional tile alarms in most U.S. plants, but allow changes to be made in the text shown in the windows. The alarm system preserves some of the strengths of a conventional tile-based annunciator system; namely, it retains multiple, parallel-presented, dedicated-position alarm windows, while taking advantage of the flexibility afforded by using computer-generated alarm text.

The Overview Panel encompasses 254 alarm message windows, approximately one-third to one-fourth more than the number of tiles in the usual annunciator-tile system. The database contains approximately 6,000 distinct alarm messages. They are grouped and assigned to alarm windows on the Overview Panel based on a plant function organization scheme.

Only one alarm message can be displayed in an alarm window at once. However, more than one alarm message associated with a given alarm window can be active at the same time. Therefore, a prioritization scheme was defined to establish which alarm message will be displayed in an Overview Panel window when more than one is activated. The alarms not displayed are stored in a queue of active messages associated with a particular Overview Panel window. In that case, a symbol appears in the alarm message window to alert the operators that messages are queued up. The lower-priority messages in the queue can be accessed from the Support Panel.

A key feature distinguishing this alarm system from other computer-based alarm systems is that its layout is based on a functional goal-means decomposition of the plant (Rasmussen, 1986). Rasmussen (1986) viewed human performance as representing behavior organized and controlled at various levels of abstraction, including perception, rules, and knowledge. Operators are characterized as flexible in their ability to respond to the situation. This characterization of action, being based upon various levels or depths of processing, led to the categorization of operator's performance into three classes: skill-based, rule-based, and knowledge-based. Higher levels of abstraction enable behavior to be *goal* directed. These levels can serve to define goals for lower levels. So, for example, the goal to define the present state of the system can structure the set of observations made at the lower level of abstraction. When a target or desired state is identified, it becomes a goal, and the tasks and procedures to be used to achieve that state are defined. These are the *means* by which goals are accomplished.

This general approach was proposed as a possible way to enhance alarm systems (Beattie and Vicente, 1996). Further, prioritization of alarm messages is only performed within narrowly defined queues of alarms that all relate to the same plant function; they are not prioritized across functions. This contrasts with many other computerized alarm systems that assign each alarm a predefined urgency for operators' action, with some always coded as "high" urgency, and others always coded as "low" urgency. In the AWARE alarm system, operators do not have to evaluate an alarm's relative priority. Those appearing in the alarm windows at any given time are expected to be dealt with by the operators.

The Support Panel is displayed via two video display units (VDUs). The VDUs are high-resolution, color, graphic workstations. The operator interacts with the Support Panel with a mouse-driven cursor. The highest level screen is a graphic representation of the overview panel. One display shows a reduced version of the Overview Panel that allows the user to see in which areas there are alarms. From the Support Panel, operators can access all active alarms in a queue, and so examine the list of alarm messages whose low priority did not permit them to be displayed on the Overview Panel, or those alarms that recently were "bumped" off the Overview Panel by higher priority messages. The operator can zoom-in on those of interest. The panel can be used to obtain additional information about an alarm or group of them. Operators also can see the logic behind any alarm message, the set-points and inputs to the logic, and various parsings of the chronological alarm message list. The support panel also contains the alarm system's controls for silence, acknowledge, reset, and test (SART) functions.

ABB-CE System 80+ Alarm System

Asea Brown Boveri - Combustion Engineering (ABB-CE) has an advanced alarm system that is part of its System 80+ control room design (Bryan and Fuld, 1995). Information is supplied to the operator in many ways, including through a dedicated tile display and through the integration of alarm information into process monitoring displays. For the dedicated alarm displays, the System 80+ control room contains the Discrete Indication and Alarm System (DIAS) which consists of alarm tile displays that are spatially dedicated and exhibited on electro-luminescent panels at the specific control panels where the relevant controls are located. The alarm tiles contain groups of alarms that are functionally related and located on the uppermost vertical section of the operator's sitdown workstation. A momentary tone is the initial audible alert of the transition of one or more alarms to new or cleared states for priority 1 or 2 alarms. A momentary reminder tone sends a recurring alert if priority 1 or 2 alarms remain unacknowledged. The alarm tones are emitted from the console where the alarm display is located.

The alarm tile display system conveys the meaning and importance of alarm conditions through a hierarchical classification (component, process, success path, and critical function) of alarm conditions and spatial dedication of alarm messages. Alarm tiles are established for the following:

- Critical Safety Functions
- Critical Power Production Functions
- Success Path performance
- Success Path availability
- Damage to major equipment
- Personnel hazard

Individual alarm tiles can indicate either the highest priority new or cleared alarm while continuing to exhibit the highest priority existing alarm. An alarm tile stop-flash capability is available for use during situations of high alarm activity; it focuses attention on new priority 1 alarms by temporarily stopping the flashing of all other unacknowledged alarm states.

Inputs to the alarm-tile display are made through touch screens. Alarm condition messages are automatically shown when an alarm tile acknowledgment is received. Unacknowledged alarms on a single tile are acknowledged through the display as a group.

In addition to the dedicated tile display, alarm information is integrated with the process displays. For example, alarms related to the critical safety functions are presented on the Integrated Process Status Overview Display (IPSO), the highest-level monitoring display, contained on a large screen overview visible from anywhere in the control room (or at individual workstations). The more detailed process displays in the data processing system also contain alarm indications.

The alarm tile display system is coordinated with the display system such that (1) the same coding schemes are used for indicating an alarm's priority and status, (2) similar alarm messages appear in both message windows, and (3) alarms that are acknowledged by the operator on one system are also acknowledged on the other.

The system uses alarm processing to reduce nuisance alarms. The techniques include signal validation, component availability processing, equipment status dependency, and plant mode dependency.

Bryan and Fuld (1995) emphasize the importance of using alarm system validation to ensure that the alarm management approach, an integral part of the overall HSI, is effective. They advocate employing "...simulated operating exercises in a full-scope, dynamic environment."

<u>Mitsubishi Atomic Power Industries' Dynamic Priorities Alarm System</u>

The Dynamic Priorities Alarm System (DPAS) developed by Mitsubishi Atomic Power Industries (MAPI) displays alarms on a combination of tiles and VDUs (Fujita, 1989). Each alarm can be lit in three colors. Color supports operators in distinguishing between status and alarm information. The prioritization scheme is as follows:

- Red denotes process abnormalities and component and system failures requiring operators' action
- Yellow signals cautionary information that automatic system and component actuation is needed
- Green indicates status information.

DPAS reduces the number of high-priority alarms through mode, multi-setpoint, and cause-consequence processing. The Mode Rule states that if a system is not in service, all the system's alarms are downgraded to green; for example, charging pump alarms change to green after a safety injection. The Multi-Setpoint Rule states that if there

are multiple set-points alarms, the less important ones are downgraded to green after a new alarm indicates a more severe condition. For example, a tank's low-level alarm turns green after the low-low level setpoint is reached. The Cause-Consequence Rule states that if an alarm occurs as a consequence of another alarmed condition, then the second one will be downgraded to yellow or green. For example, if a pump trip alarm is red, the low pressure alarm is yellow to indicate an automatic control function, and the pump autostart alarm is green.

Toshiba and Hitachi's ABWR Alarm System

The Advanced Boiling Water Reactor (ABWR) is a joint design by General Electric (GE), Toshiba, and Hitachi under the direction of the Tokyo Electric Power Company (TEPCO). The HSI is being primarily designed by Toshiba (for the Kashiwazaki-Karawa Unit 6, K-6) and Hitachi (for the K-7). Toshiba's control room is referred to as APODIA (Advanced Plant Operation by Display Information and Automation) and the Hitachi control room is called NUCAMM-90 (Nuclear Power Plant Control Complex with Advanced Man-Machine Interfaces for the 1990s).

Toshiba's APODIA has a three-level alarm system. The "plant-level" alarms will be related to the plant's overall status, the status of safety systems, and the status of important parameters. These alarms will be displayed on dedicated tiles on the large overview display. "System-level" alarms will indicate the status of each system and will be located as fixed tiles on the main operation console. Finally, "equipment-level" alarms will be presented via CRT message displays.

The Hitachi NUCAM-90 has two modes of alarm presentation. About one hundred and thirty annunciator tiles for important alarms are located on the large overview display. The rest of the alarms, approximately 1,500, are presented on CRTs. Three color-coded levels are used. Red signifies major alarms, such as a reactor trip. Blue indicates important system-level alarms. Importance is determined by the plant's present condition. The remaining ones are white.

A simple suppression system is used to suppress mode related alarms and redundant alarms. The suppression system is controlled by the operator; i.e., it can be turned on or off at the push of a button.

Halden Computerized Alarm System for HAMMLAB

An alarm system presently developed for the Man-Machine Laboratory (HAMMLAB) at the Halden Reactor Project is the Computerized Alarm System for the HAMMLAB (CASH) system (Førdestrømmen et al., 1994; Førdestrømmen et al., 1995; Miazza, Torralba, B., Karstad, T., Moum, B., and Follesø, K. (1994), 1993). CASH is designed to present alarms by integrated graphics and message lists. There are three levels of displays: overview displays (there is one overview display for reactor operations and turbine operations), NORS (NOkia Research Simulator) detailed process mimic displays (these are more detailed process formats), and selective alarm displays.

The CASH overview displays combine spatial dedication and message lists, a feature similar to AWARE. The overview displays are organized into nine windows based on major systems, such as containment, reactor, turbine, and pressurizer. A darkboard concept is used such that if no alarms appear in a system's window, the operator can rapidly determine that the status of that system is fine. The alarm messages presented in the overview are not fully detailed messages (e.g., set points are not shown). Complete detail is given on the selective alarm displays.

The NORS displays are graphic representations of plant systems with imbedded alarm information. The selective displays show detailed alarm messages and allow operators to undertake various sorting and trending functions, including grouping alarms by system, priority, time, and suppression.

CASH employs extensive alarm processing capabilities. The overview display (OD) filter removes alarms from overview displays. The suppressed alarms are available to operators on process displays and supplemental displays. Other alarms are removed by overview and process display (O&PD) filtering which suppresses alarms from both the overview and process displays.

Alarms are reduced by several processing methods (called structuring):

- Plant Mode Structuring – suppression based on defined plant modes (power operations, start-up, hot stand-by, hot shutdown, cold shutdown, and refueling)

- Plant System State Structuring – suppression based on the status of major plant components (e.g., if a process is bypassed, all alarms associated with it are suppressed)

- Logic Structuring – suppression based on various types of logical analysis (e.g., use of time delay)

- Dynamic Suppression Limit – suppression of alarms known to be associated with well-known disturbances, such as turbine trip. At such times, the parameters exceed their setpoints in expected ways and can be described by bounding curves (a curve representing the expected change in a parameter over time). In this type of processing, changing parameters are monitored to determine whether they are changing along the normal pattern. If so, the alarms are suppressed. If a parameter changes in an unexpected way, an alarm is generated.

- Inhibiting Alarms – suppression of alarms for components that are unavailable due to maintenance.

Non-Nuclear Process Control Plant Alarm Systems

Fossil-fuel power plants and petrochemical plants were visited as part of a related NRC project and information was collected about their alarm systems (O'Hara, Stubler, and Higgins, 1996). Most plants originally were equipped with annunciator-based systems, but most have been upgraded to CRT-based alarms. These plants tend to use the standard alarm system provided by their distributed control system vendors, which use lists as the primary presentation format. In some cases, this was augmented by a smaller set of alarm displays, specially designed for the plant, that use mimic and other formats. From interviews with plant personnel, the petrochemical plants appear more likely than fossil-fuel plants to develop additional alarm displays to augment the vendors' standard displays.

The petrochemical plants and some fossil-fuel plants augment the CRT-based alarm displays with annunciator tiles. Alarms mostly are shown via the CRTs while the most critical alarm conditions (e.g., related to operation of the safety interlock system) are indicated via a small set of annunciator tiles (Shaw, 1993). The annunciators offer a spatially dedicated, continuously displayed representation of these critical alarms to help operators cope with the high volume of alarms that occur during upsets.

The annunciators may or may not be completely separate from the CRT-based alarm system of the digital control system. For example, digital point sensors, such as level switches, can be wired directly to the annunciators, and then, using auxiliary contacts, wired to the CRT-based alarm system through the digital control system. Analog signals, such as temperatures, can be wired directly to the digital control system's analog input system, and then connected through the digital system to the annunciators. Thus, the CRT-based alarm system and the annunciator system may display the same, similar, or completely different alarm information depending on whether their signals are connected.

None of the fossil-fuel or petrochemical plants visited use alarm reduction methods. However, it was found some of the newer high-performance distributed control systems marketed to these plants can suppress or filter alarms that convey little useful information, especially after a major trip.

Detailed information describing alarm conditions is usually shown separately from displays that alert operators to their onset. In one petrochemical plant, when the operator acknowledges a new alarm, the alerting display is removed and replaced with a list supplying detailed information about the alarm condition. This was considered to be an improvement over the original alarm systems that provided alert information via annunciator tiles but no detailed information.

Both fossil-fuel and petrochemical plants reported using event sequence recorders to help operators diagnose the cause of the alarm. These devices record the onset of alarms in precise time intervals, and so allow operators to determine the order in which they occurred. Event sequence recorders support operators in determining which plant fault was the likely cause of an event.

General Trends in Recent Design of Alarm Systems

1. Alarm systems are being designed as integrated systems. Historically, they resulted from subsystem designers identifying what system parameters operators needed to be aware of. There was no guiding philosophy about what constitutes an alarm and no uniform design process for determining this. Most of the systems described above result from a design process focused on developing an alarm system within the context of an understanding of the operational problems of earlier approaches.

2. Alarm processing and reduction are major thrusts of newer alarm systems. This change reflects an understanding that the major issue in usability of alarm systems is the sheer number of alarms that come in during disturbances.

3. Most of the alarm systems described above utilize various levels of alarm information that require variable display techniques. For example, one alarm display may present auditory alerts and a brief visual identification of which alarm occurred, with more detailed information about the alarm given elsewhere or upon the operator's request. A system that combines tiles and message lists is an example. Sometimes a third layer of information is present – links to additional information, such as piping and instrumentation diagrams (P&IDs) and alarm response procedures. The newer designs appear to recognize that each display technique has strengths and weaknesses, and that multiple display formats are needed to accomplish all the functions of the alarm system.

4. Perhaps the most significant aspect of the systems described above is their alarm management facilities. With them, operators can interrogate the alarm system, for example, to obtain more detailed alarm information and to sort alarms for specific purposes.

5. Advanced alarm system features are being retrofitted into current plants. Several of the systems described above, e.g., AWARE and DPAS, are specifically designed for use in both new plants and for control room upgrades and modernization.

4.1.2 Modifications to the Alarm System Characterization

These trends, as well as most of the detailed alarm system characteristics, such as types of alarm processing strategies, are completely consistent with the alarm system characterization in NUREG/CR-6105. However, the characterization appears limited in two respects: physical alarm system components, and alarm management facilities.

While the earlier characterization reasonably represented the functional characteristics of the HSI aspects of alarm systems, it did not sufficiently cover the relationship of the alarm system to the rest of the plant. Thus, the characterization was expanded to better illustrate engineering aspects of alarm systems, i.e., sensors and processors, and their relationship to the alarm system's functionality.

In addition, alarm management functions were not adequately addressed. These functions were implicit in the discussion of expanded (beyond SART) control requirements in more advanced systems, e.g., provisions for operator-defined setpoints and the capability for sorting alarm lists. However, many new systems have fully featured alarm management capabilities. Thus, the characterization was modified to better reflect these management functions. (The specific techniques, not functions, for performing alarm management functions are related to the general issue of interface management, which is discussed in another NRC project, described by O'Hara, Stubler, and Nasta, 1998). The revised characterization is in Appendix A.

4.2 Guidelines for HFE Design Review

The results are organized around the basic structure of the review guidance for alarm systems design in NUREG-0700, Rev. 1.

4.2.1 General Guidelines

General characteristics include the basic functions associated with alarm systems (e.g., to alert the operator, to guide the operator's actions, to assist in monitoring plant events, and to facilitate the operator's interaction with the plant), and the relationship between the alarm system and the rest of the HSI. NUREG-0700, Section 4.1, describes the functional criteria for the alarm system and the general principles to which it should conform, such as consistency with the main control room HSI. It also includes validation of the alarm system. The primary issue here is the fundamental question of what the alarm system is intended to do.

4.2.1.1 Evaluation of Recent Research

System Descriptions and Evaluations

The basic functional requirements of the alarm system stated in Section 4.1, General Guidelines (i.e., alerting the operator to deviations, informing the operator of its priority, guiding the operator's response, and confirming whether the response was effective) are reflected in current conceptualizations of alarm system functions. For example, the requirements stated for the alarm system of the Kansai APWR main control board are exactly those stated above (Shimada, Yamamoto, Tani, and Kobashi, 1996). Other designers, while acknowledging the foregoing basic functions, have also explicitly recognized the importance of the operator's use of the information that the alarm system supplies. Designers planning improvements to the Darlington (CANDU) annunciation system (Long and Davey, 1996) state that to fulfill its basic functions, the system must do the following:

- detect and, perhaps, predict the occurrence of changes in the plant
- alert users to changes important for the current operating situation such that
  - only operationally relevant changes are annunciated
  - the demands imposed on users' attention to recognize the changes fit with the demands of other concurrent control room tasks
- point users to additional plant information to understand and respond to changes

This statement is significant in that it apparently promotes consideration of operators' cognitive limitations at the level of a functional requirement; alarm processing and a closer coordination of the alarm system with other information sources in the control room are specifically called for. Similarly, designers of the man-machine interface system for future Korean plants (Lee, Hur, Shin, Koo, and Park, 1996), established the following design bases of the alarm system:

- providing the operator with alarms in a timely manner
- reducing the number of alarms effectively to reduce the operator's workload
- integrating with other information systems to facilitate the operator's tasks

Thus, alarm reduction (processing) and the relationships of the alarm system to other information sources are highlighted, along with the basic alerting function of the alarm system.

NRC Research

The NRC alarm study (O'Hara et al., 2000) found that while operators had definite preferences and opinions about the value of the varying alarm displays and processing features, the effects of varying these features were modest. The authors pointed out that the HSI components in the simulator control room were relatively advanced in comparison to US plants, and generally more representative of advanced control room designs, such as may be found in the ABWR and AP600. The interface was VDU-based with hierarchical processing displays that gave a graphic overview at the top, and detailed process mimics below. The interface included extensive trending capability. Operators made great use of these features and did not want to remove them in favor of supplemental alarm displays. The displays provided more data integration and high-level information than would be found in a conventional control room where those functions are mainly served by the operators, based on the display of individual parameters.

Therefore, it is possible that (1) the operators can compensate for possible deficiencies in the alarm design with advanced displays, and (2), more significantly, that the alarm system plays a somewhat different role in an advanced control room because of the improved information system compared to that of conventional control rooms. In some respects, the broad role of the alarm system in conventional plants may partly be a function of a relatively poor information system. For example, operators in conventional plants use the alarm system to determine the overall status of the plant's systems and functions. In an advanced control room, such as the one used in the study, this assessment can be accomplished by the high-level displays. Advanced control room designs seem to reflect a better understanding of the operator's information needs.

The observed reluctance of operators to remove trends in order to access additional alarm information, was very similar to observations made during plant modernizations with computer-based alarms and displays (Roth and O'Hara, 1998). In general, the operators in both studies were reluctant to retrieve alarm information not in view (either on supplemental alarm lists or further down an alarm list).

General HFE Literature

As technology advances and information becomes integrated, the relationship between "alarm systems" and "plant display systems" becomes blurred. This leads to a focus on how to represent information about the plant to the operators, rather than on the design of alarm systems. Feher et al. (1996) noted that current approaches to alarm systems identify the need to "...alert operating personnel by redirecting their attention to important 'information' about the plant."

Stanton (1994a) points out that the confusion over the role of the alarm system stems from the vague definition of an 'alarm.' For example, an alarm may be an thought of as an attention-getting signal or as a piece of information. Likewise, the alarm system will serve various functions depending on the operational context and the operators' requirements and goals.

Roth, Mumaw, Vicente, and Burns (1997) conducted extensive observations and interviews of nuclear power plant operators to understand their cognitive activity during normal operations. They concluded that monitoring during normal operations is an active process involving selective attention rather than being a vigilance task. According to Roth et al., monitoring to support situation assessment and response planning is knowledge-driven, and is based principally on the operators' situation model (i.e., their mental representation of the state of the plant). Monitoring to support situation assessment includes confirming expectations about the plant's state, pursuing unexpected findings, checking for likely problems, validating initial indications, and interpreting specific indications. Response planning includes assessing goal achievement, determining potential side-effects of planned actions, estimating the viability of contemplated responses, and confirming of actions and their effects. Roth et al. (see also Vicente, Burns, Mumaw, and Roth, 1996) identified several strategies that operators may employ in dealing with alarm system interfaces to enhance the information available and reduce cognitive demands. Among these are enhancing the salience of selected signals and reducing "noise" or clutter, establishing bases for monitoring trends in parameters, creating new alarms or reminder indications, and creating external cues about the configuration of the

interface. Thus, operators apparently sought to modify the alarm system to give them better support under normal operating conditions for a broad range of functions that were not necessarily designed into the system.

Woods (1995) used the results of field studies of operators in various contexts to characterize the cognitive activities involved in fault management. He focused on abnormal operations, emphasizing on potential problems associated with alarms. For operators to maintain a coherent situation assessment during disturbances, they must direct their attention appropriately. Woods portrays alarm systems as automated agents that can assist operators by directing their attention to important new information. Effective direction of attention depends on the operators "...somehow being able to notice potentially interesting changes without drawing or interfering with limited attentional resources." That is, they must evaluate whether or not new information warrants a shift of attention without interrupting ongoing cognitive activity. An example of the importance of this principal is the reluctance to shift attention away from interface management tasks, as noted in the NRC research.

This perspective suggests that the attention-directing role of alarm systems should be considered in their design. Woods claims that if alarms are designed so as to unavoidably redirect operators' attention, the operators' situation assessment may be fragmented and they may be unable to develop an integrated response to an event. Operators' attempts to deal with the demands associated with forced but unwarranted interruptions in ongoing activity or shifts in attention may also cause them to ignore or disable alarms.

While the functional requirements for the alarm system assume the existence of a process deviation, Roth et al. show that operators actively use the alarm system to monitor the plant during normal operations. Accordingly, if explicit support for routine monitoring is not part of the overall information system, it should be recognized that the alarm system may have to serve this function in addition to those specified in the guideline. Furthermore, as Woods points out, the alarm system must be effective in the context of ongoing fault management, and the information it provides must not only meet the operators' requirements but must also be made available in ways that will not unnecessarily disrupt the operators' response to deviations. Specifically, the alarm system should direct attention to information without inappropriately demanding attention.

It might be expected that alarm systems will be designed to give more support for monitoring and for the effective direction of the operator's attention, while playing less of a role in supplying the operator with data (which will increasingly be provided by systems designed specifically to do so). However, the roles of the alarm system and of other information sources in the control room are not yet distinct. The amount of plant information that ought to be provided by the alarm system depends to a great extent on whether (and how readily) that information is available by other means.

4.2.1.2 Modifications to General Guidelines for Alarm Systems

The information reviewed above indicates that alarm systems are expected to support a variety of functions. They are expected to alert operators to changes in the process; this function is closest to the conventional definition of an alarm. However, alarm systems are also used to monitor the state of the process and plant equipment, in the absence (or in the aftermath) of process disturbance. (Roth et al. made observations suggesting that the mere absence of alarm indications is not sufficient for operators who are monitoring processes). Alarm systems also are expected to show information about the overall state of the process and plant equipment. This informative function may have evolved because conventional control room alarms gave an effective presentation of information needed by operators, but not readily available by other means within the HSI. The findings of the NRC alarm study suggest that the way in which an alarm system presents information may be related to the design of the information systems in general.

Modifications to the general guidance for alarm systems (see Appendix B) call attention to their wider functions and requirements:

- Guideline 4.1-1, Alarm System Functional Criteria – a statement was added to Additional Information that the functions required of the alarm system may depend on the design of the plant's information system and

operator's goals in using the alarm system. (Note that in Revision 0, this guideline had an incorrect title; the correct title was added.

- A new guideline, Guideline 4.1-2, Operator Verification of Alarms was created to address the need for operators to confirm alarm information. (The subsequent alarm numbers in Section 4.1 were changed consecutively). The subsequent guideline numbers were modified accordingly.

In addition, the findings confirm the need for careful analysis of the functionality of replacement alarm systems upgrades. This is noted in the modification to the following guideline:

- Guideline 4.1-3, Alarm System Upgrade Functionality – the guideline was modified to indicate the importance of analyzing functionality on the basis of not only the alarm system but the information system in general.

Based on reviewers' comments, a guideline was added to emphasize the importance of consistency with procedures as well as with the control room HSI:

- Guideline 4.1-5, Consistency with Emergency Operating Procedures, was added and subsequent guidelines where renumbered.

4.2.2 Alarm Definition

Alarm definition is the specification of the types of process parameters selected to be monitored and displayed by the alarm system, and the setpoints to be used to represent those parameters. Guidance is given in NUREG-0700, Part 2, Section 4.2. The timeliness of alarms and the avoidance of nuisance alarms due to poor setpoint selection are discussed in this context, as is the darkboard concept. The problems posed by nuisance alarms have long been recognized by alarm system designers and they struggle with the tradeoffs inherent in reducing these alarms without depriving operators of needed information. In recent years, there has been growing interest among human factors researchers in the effects of the alarm system's characteristics on the performance of supervisory controllers (see the discussion of the "alerted monitor system" in NUREG/CR-6105).

4.2.2.1 Evaluation of Recent Research

<u>System Descriptions and Evaluations</u>

Designers are faced with the dual imperatives of timeliness (i.e., ample warning of parameter deviations so that corrective actions can be taken promptly) and avoidance of nuisance alarms. System descriptions typically include signal processing techniques aimed at mitigating alarms arising from acceptable parameter fluctuations (see discussion of processing). Some techniques (such as using deadbands on annunciation thresholds) achieve their aim at the cost of presenting less accurate information to the operators since they amount to raising the threshold of the alarm. In the improved alarm strategy for CANDU plants, Davey et al., (1995) noted that warning of conditions potentially leading to upsets is enhanced by including rate and margin generation (i.e., assisting operators' judgements of trends with information based on rate and margin calculations).

Thus, there are techniques that may help achieve timeliness without setting overly conservative parameter thresholds.

<u>General HFE Literature</u>

The issue underlying the above topics is the way in which 'false alarms' may affect operators' performance, especially their confidence in the alarm system. The discussion associated with NUREG-0700 Guideline 4.2-3, Setpoint Determination and Nuisance Alarm Avoidance, briefly describes an 'alerted monitor' model of the operators' interaction with automated monitoring (i.e., alarm) systems. It is pointed out that the choice of alarm

setpoints will influence operators' tendencies to respond to them , and that the resulting performance may not be optimal.

In recent years, there have been several laboratory studies of the effects of alarm system characteristics on human performance during monitoring. These studies examined the effect of the alarm system's reliability, people's responses, and further elaborated on the alerted monitor analysis of monitoring performance. Some of this work is reviewed below.

Bliss, Gilson, and Deaton (1995) explored the factors influencing the 'cry-wolf' effect, i.e., mistrust of alarms, using a procedure that demonstrated the mistrust in a laboratory context. They examined subjects' responses to alarms of varying reliability in a dual-task paradigm, measuring the accuracy and speed of responses to alarms which occurred as the subjects performed a cognitively demanding primary task. Different groups of subjects responded to alarms of different reliability; specifically, they were exposed to conditions in which the proportion of 'true' alarms was either .25, .50, or .75. The alarm signals, visually presented on a VDU positioned 90º to the side of the primary task display, reflected three levels of urgency and were accompanied by an appropriate auditory signal lasting two seconds. Subjects responded to the alarm by positioning a cursor and clicking in a designated area; thus, they had to stop attending to the primary task to respond to the alarms. The subjects' only indication of whether an alarm was 'true' was the feedback given after each. Monetary rewards and penalties were assessed based on their responses; the running total was continuously displayed during a session. The range of the monetary contingencies varied directly with the urgency of the alarm. Most subjects' rate of responding to alarms roughly matched the expected probability of a true alarm; high-urgency alarms were responded to more often than low-urgency alarms, regardless of an alarm's reliability. However, response time did not differ as a function of either the alarm's reliability or urgency. The authors suggest that avoiding false alarms is critical in designing alarm systems because of the sensitivity of subjects' responses to their reliability. These findings are consistent with the observation that reliability is an important aspect of monitoring performance in general (Mumaw et al., 1996).

Bliss and McAbee (1995) considered whether differences in the criticality of the primary task would affect subjects' responses to alarms under circumstances similar to those described above. The criticality of the primary task was manipulated by adjusting the penalties (points lost) for marginal performance. Subjects responded to a greater proportion of alarms when the primary task criticality was low than when it was moderate or high. The results are interpreted as indicating that the effects of an operator's mistrust of alarm systems may be exacerbated when the tasks are most demanding. The authors suggest that redundant alarm systems might be used to increase reliability, or the alarm response might be undertaken during critical periods by a second operator who does not have primary responsibility for the critical task.

In another study using procedures similar to those described above, Bliss, Dunn, and Fuller (1995) investigated methods for increasing the frequency with which personnel responded to the alarms. The experiment indicated that letting subjects know that alarms would be more reliable than they had been in a previous session increased the rate of responding to the alarms. The authors conclude that since the rate of response was sensitive to the information given to the subjects, training might encourage more appropriate responses to alarms by operators of complex processes.

Bliss, Jeans, and Piroux (1996) examined the effects of supplying information about the overall reliability of an alarm system and the validity of individual alarms. Subjects responded to alarms while simultaneously carrying out a compensatory tracking task (to simulate the division of attention typical of operational environments). Two types of information about the reliability of the alarm signals were defined. Information about the validity of individual alarm signals was reflected by the readings on computer-presented gauges. A deviation of a specified size indicated that the current alarm was true; no deviation indicated that the alarm was false. Information about the overall reliability consisted of verbal instructions to the subject, as in previous experiments. Different groups received one or the other type of information, both types, or no information on reliability. The frequency, appropriateness, and latency of responses were recorded. Subjects who received information about overall reliability responded more often than the other groups. Those receiving information about the validity of individual alarms responded to fewer

alarms, but were correct more often. From these results, the authors recommended that redundant sources of information should be made available to operators for every alarmed condition as far as possible.

The overall findings of Bliss and his colleagues point to several general conclusions. First, subjects' confidence in alarms (i.e., their likelihood to respond to them) is apparently readily influenced by their experience of situational contingencies. This is not surprising in circumstances where there is no other basis for responding (i.e., no real process context). Second, subjects use information to adjust their response strategy, and respond more appropriately, to the extent the information is correct. Perhaps most significant, is the demonstration that responding (or not responding) to alarm signals depends on the subject's concurrent demands. When demand is high, subjects appear reluctant to devote resources to responding to signals if the payoff is uncertain.

Beattie and Vicente (1996) found that some alarm systems are deficient in supporting plant conditions other than full power, e.g., during maintenance outages.

4.2.2.2 Modifications to Alarm Definition Guidelines

Based on the foregoing findings, the following changes to the guidance have been made:

- Guideline 4.2-1, Alarm Selection – an item was added to the criteria to include monitoring of plant modes from full power to shutdown. The Additional Information was modified to cover the same issue. In addition, a Discussion section was included describing the Beattie and Vicente (1996) study linked to this modification. Beattie and Vicente (1996) found that some alarm systems are deficient in supporting plant conditions other than full power, e.g., during maintenance outages.

- Guideline 4.2-3, Setpoint Determination and Nuisance Alarm Avoidance – a statement was added to Additional Information about the effects of false alarms on an operator's performance. A caution was included that attempts to avoid or reduce nuisance alarms that may result in important information being withheld from operators. A brief review of the research findings on the reliability of alarms was added to the discussion, and the guideline title was changed to reflect the importance of setpoints.

4.2.3 Alarm Processing and Reduction

Processing is a fundamental aspect of alarm system design since it determines which alarms are presented to the operating crew. Alarms in conventional plants tend to overwhelm operators during transients because of the many nearly simultaneous annunciator activations with varying relevance to the operator's tasks. Alarm processing techniques were developed to support operators in coping with the volume of alarms, to identify which alarms are significant, and to reduce the need to infer the plant's conditions.

Part 2, Section 4.3, of NUREG-0700 has guidance for reviewing the processing of alarm data, from simple processes, such as signal validation to more complex alarm-reduction strategies.

4.2.3.1 Evaluation of Recent Research

<u>System Descriptions and Evaluations</u>

Most of the current alarm designs reduce the number of alarms presented to operators by applying processing of one kind or another. The systems described in recent proceedings typically mention many of the alarm processing techniques in NUREG-0700's guidance for alarm processing and reduction. For example, the ADIOS (Alarm and Diagnosis - Integrated Operator Support) system developed by KAERI (Kim et al., 1996) bases processing on plant mode, equipment status (which is included in logical consequences processing), and multi-setpoint relationships. The designers also are considering status-alarm separation, alarm validation, and signal generation.

The PIPS (Plant Information Processing System) being developed for future Korean nuclear power plants by KAERI (Suh et al., 1996) uses time delay and deadbanding to reduce nuisance alarms; equipment status dependency is also used. Suh et al. mention that "...any alarm has variable alarm setpoints assigned which are a function of plant operating mode." While the NUREG-0700 guideline for mode dependence does not formally exclude the possibility that acceptable operating ranges for some parameters may differ based on plant mode, the guideline's additional information section implies that an alarm is either operationally relevant or not. The CPIAS (Critical Parameter Indication and Alarm System) also being developed by KAERI for future plants will apparently use mode-dependent alarm setpoints (Lee et al., 1996); other processing techniques CPIAS will use are status-alarm separation, mode and equipment state dependence, cause-consequence, and time delay processing.

The CAMLS design (Davey et al., 1995) uses a variety of processing techniques and changes in alarm presentation and control features to enhance its effectiveness. Processing according to plant modes, events, and equipment states is used to temporarily suppress the display of alarms. Chatter filters, such as deadbanding and time delay, and signal validation are used to reduce nuisance and spurious alarms. Alarm generation is employed for events that are expected but do not occur and for advanced warning of parameter excursions ('rate and margin message generation'); this second type of alarm generation is not among those explicitly included in NUREG-0700's alarm processing guidance. The strategy described by Davey et al. also includes 'dynamic thresholding' of setpoints for a few parameters; i.e., alarm thresholds depend on operating context (e.g., reactor power), as in the PIPS described above. To further lessen the number of messages, similar alarm messages are coalesced by the system. Individual messages are replaced by summary messages that may reflect the status of a plant parameter (as indicated by multiple sensors), or may indicate a higher-order condition which the operators would otherwise have to deduce from the values of several parameters. This technique, especially the latter variety, can be considered a form of alarm generation processing which provides higher-level information.

NRC Research

The NRC alarm study examined the effects on performance of reducing alarms. Reduction was accomplished by two categories of methods based upon how the information that operators receive is affected. Nuisance Alarm Processing techniques eliminate alarms that are irrelevant to the current mode of the plant, e.g., a low-temperature alarm on a line that is out of service for maintenance. These techniques achieve a moderate reduction in alarms (called Tier 1 processing). Redundant Alarm Processing techniques analyze alarms to determine which are less important because they duplicate information given by other alarms. These techniques were combined with the Nuisance processing techniques to reduce alarms even further (Tier 2 processing). In addition, a baseline condition with no processing served for comparison (Tier 0 processing).

Tier 1 processing reduced the number of alarms to approximately 50 percent of the Tier 0 baseline. Tier 2 generated only about 25 percent of Tier 0. Operators clearly preferred the maximum reduction because it simplified the identification and understanding of important alarms. Based on their assessments of the alarms that were eliminated by the processing rules, the operators judged the techniques to be acceptable because in none of the sixteen scenarios used did they find that important information was missing. Thus, based on the degree of alarm reduction, the operator's preference for maximum reduction, and their verification that important alarms were not removed, processing was successful. However, processing had only a minor effect on objective performance measures (see O'Hara et al., 2000, for a detailed discussion of these findings).

Roth and O'Hara (1998) observed crews during their initial training with a new system which included an advanced alarm system. The alarm system displayed alerts when an automatic safety system did not actuate as expected or when an event was not proceeding as expected. Operators repeatedly remarked that this support for detecting unexpected events was a particular strength of the advanced system, since aid was most useful in circumstances that were out of the ordinary.

General HFE Literature

McDonald, Gilson, Mouloua, and Deaton (1995) extended the 'cry-wolf' research (see Section 4.2 above) to situations in which multiple alarms are presented simultaneously. Using methods similar to those of Bliss et al., they examined whether subjects' confidence in the validity of alarms is influenced by the number of other alarms present in a display. The subjects, undergraduate students, were informed that the probability of a given 'test' alarm being valid was 50%. The 'test' alarm was one of six elements presented in a rectangular array. In any single trial, up to five of the other elements were active along with the 'test' alarm. For each trial, subjects recorded their confidence that the 'test' alarm was valid. There was a roughly linear relationship between the number of other alarms present and subjects' confidence in the 'test' alarm despite the fact that the subjects knew the actual probability. The results were interpreted as showing a natural tendency for people to consider additional indications as confirmatory evidence. The authors suggested that if alarms are systematically grouped (as often is the case) this tendency might lead to faster, more accurate responses. However, they point out that there are circumstances, e.g., multiple unrelated failures, in which the assumption of relatedness is not appropriate.

In a similar experiment, McDonald, Gilson, and Mouloua (1996) demonstrated that confidence in an alarm's validity was influenced by the number and proximity of other active alarms. Subjects were again told that the probability that a particular 'test' alarm was true was 50%; this 'test' indicator was the topmost of seven similar ones in a vertical array. In any trial, from zero to three of the other alarms were active; the distance between the 'test' alarm and the other active alarm(s) varied. Subjects judged the probability that the 'test' alarm was valid. The results show simple linear relationships between both number and proximity of other alarms and reported confidence. The authors interpret the results as demonstrating natural tendencies to attribute common causes to events, depending on the way in which they are manifested.

The tendencies of subjects in these studies to respond in a way contrary to what they knew about the probability of a valid alarm may partly reflect experimental demand characteristics. The subjects were undergraduate students, not process experts, and they were responding to alarms *per se*, not to the inferred state of a process with which they were very familiar. However, since their responses also might reflect strong, perceptually based effects, some implications for alarm presentation can be cautiously considered. In a well-designed spatially dedicated display, the alarms close to one another are often related; they may be separate manifestations of an underlying fault and thus increase the operators' confidence that a problem exists. This would be augmented by the effects demonstrated in these studies. However, if multiple alarms were related to the same signal, i.e., if the information was not independent, the phenomenon demonstrated in the study would predispose the operators to false confidence. Then, the effects of alarm suppression would be expected to depend on the relationships among the alarms and the operators' training. If operators are uncertain about the degree of independence of the alarms, or do not fully understand the processing logic underlying the displays, they may revert to response tendencies similar to those demonstrated by McDonald and his colleagues.

4.2.3.2 Modifications to Guidelines for Alarm Processing and Reduction

The NRC alarm study confirmed the acceptability of various alarm processing techniques; the joint application of the techniques did not pose any problems. In the Roth and O'Hara study, operators commented favorably on generating alarms that indicated deviations from expected developments. However, at the same time, they recommended further reductions in other types of alarm presentations, such as 'status' or expected conditions. Accordingly, the following changes to the guidance have been made:

- The section title was changed from "Alarm Processing and Reduction" to "Alarm Processing" because these are separate functions. Reduction is accomplished by processing techniques.

- Guideline 4.3-1, Assured Functionality under High Alarm Conditions – as the NRC alarm study indicated, assuring the functionality of the alarm system under high alarm conditions is extremely difficult, even when there is extensive processing and this is not related to processing alone. The Additional Information and

Discussion sections have been modified to describe the study's findings and the need to consider alternative forms of display to achieve the objective of this guideline.

- Guideline 4.3-2, Alarm Reduction – the Discussion was modified to include the NRC alarm study. It also was modified to include Woods' (1995) view, discussed in Section 4.2.1.1, that the problem lies with demands imposed on attention and information processes, rather than the mere number of alarms. It may not be necessary to reduce the number of alarms if they are presented in ways that impose fewer demands (i.e., if the alarms did not unconditionally demand an immediate shift in the operators' attention).

- Guideline 4.3-4, Time Delay Processing – (1) deadbanding was added to the guideline, (2) the Additional Information was modified to deal with the effect of timeliness of information, (3) the Discussion was modified to include the findings from the NRC alarm study, and (4) the title of this guideline was changed to Parameter Stability Processing to better reflect its expanded scope.

- Guideline 4.3-5, Alarm-Status Separation – the Discussion was modified to include the NRC alarm study.

- Guideline 4.3-7, Mode Dependence Processing – the Additional Information was modified to include mode-dependent alarm thresholds and now cites Guideline 4.7-7, Automatic Mode-Defined Setpoints; the Discussion was modified to include the NRC alarm study.

- Guideline 4.3-8, System Configuration Processing – the Discussion was modified to include the NRC alarm study.

- Guideline 4.3-9, Logical Consequences Processing – the Discussion was modified to include the findings of the NRC alarm study.

- Guideline 4.3-11, Absence of Expected Alarm Patterns – the Discussion was modified to include Roth and O'Hara's (1998) findings on generating alarms.

- Guideline 4.3-12, Intelligibility of Processed Alarm Information – the Discussion was modified to include the NRC alarm study findings and the research demonstrating response biases associated with collateral alarms in the absence of knowledge about the relationships among alarms.

4.2.4 Alarm Prioritization and Availability

Alarm prioritization refers to the determination of the relative importance to the operating crew of all present alarm conditions following processing. Alarm message availability refers to the process by which alarm messages are selected for presentation to the operators based on the priority of their alarm conditions. Thus, while two alarm messages may be valid for current plant conditions, one may be very important to the operator's role and should be emphasized, while the other message may be of little importance and should be de-emphasized. This approach focuses the operators' attention on the alarm messages the greatest operational significance.

NUREG-0700, Part 2, Section 4.4, has review guidance for establishing prioritization criteria and implementing them. In addition, guidance is given for alarm availability, i.e., the method by which the results of alarm processing are made available to the operating crew through filtering, suppression, or coded prioritization.

4.2.4.1 Evaluation of Recent Research

<u>System Descriptions and Evaluations</u>

In describing the Sizewell B alarm system, Hickling (1994) notes that the significance of an alarm to operators depends on four factors: urgency, safety consequences, productivity consequences, relevance to the task at hand. He observes that it is impossible to define a single 'importance' dimension, but suggests that in future, the concept of

critical safety functions could be extended to identify the most threatening alarms. Hickling also suggests that allowing the operators to sort alarms according to any of the four factors might be effective.

Prioritization based on urgency and plant safety are called for in the NUREG-0700 guidance; these two factors are those most frequently cited in descriptions of advanced alarm systems. Alarm processing for the Electricité de France (EdF) N4 control room categorizes and color codes alarms based on the time available for the operators to act, and on a dynamic, situation-specific gravity (i.e., consequence) classification (Pirus, 1996). Alarms are color coded and segregated by urgency, and ordered within these categories by gravity; other orderings of the lists are available. The most urgent (red) alarms signify actions that must be taken within 5 to 15 minutes; actions that can be taken after 15 minutes are lower in priority (yellow). Actions that must be accomplished within 5 minutes are automated. PIPS also bases prioritization on urgency (Suh et al., 1996), and equates the time within which a response is required with the alarm's severity. Details of the display of priority are not given.

NRC Research

The NRC alarm study examined the effects on performance of the method by which the results of alarm processing are disclosed to the operating crew. The specific techniques used were suppression and dynamic prioritization. With suppression, less important alarms are not presented to the operators, but can be accessed by request or by the alarm system based upon changing plant conditions. In dynamic prioritization, less important alarms are presented to operators but distinguished from those that are more important, such as by using a different color or a different location from other alarms. There are tradeoffs between the two approaches. Since designers cannot anticipate all possible plant disturbances, some of the processed alarms may be important to an operator's decision making in a specific context. Thus, dynamic prioritization does not conceal any information from operators. However, the operator must perceptually filter alarms and may be distracted by the less important ones. Suppression removes potentially distracting alarms; however, since they are accessible on auxiliary displays, additional workload imposed by requiring the operator to retrieve them.

The results of this study supported the suppression of alarms. Nearly all the operators preferred suppression over dynamic prioritization. The operators thought that although prioritization had the advantage of making all information immediately available, there was often little useful information in the low priority list, and they were concerned that an operator could distracted by the list or might read the wrong list. Instead, they preferred to look at a list of suppressed alarms.

These findings may be inconsistent with the preference for dynamic prioritization found in earlier research (Fujita, 1989). The difference may be due to numerous factors including the comparison conditions and the method of implementing dynamic prioritization. However, since the reasons are unknown, no specific guidance was developed on dynamic prioritization, and it remains an open issue.

The study did not explicitly examine alarm filtering, wherein alarms determined by processing techniques to be unimportant are eliminated and unavailable to the operators. However, operators commented that they would not favor having alarms completely removed for several reasons. First, there was concern that the processing logic may not be 100 percent correct, and under some circumstances may remove important alarms. Second, operators sometimes use such alarms for other purposes, such as status information, to check that events occurred as expected. Thus, the study confirmed Guideline 4.4-4, Filtered Alarms.

In Roth and O'Hara's (1998) study, the alarm system's design retained a degree of spatial dedication while taking advantage of the flexibility afforded by using computer-generated text. The primary alarm display panel had 254 message windows. The messages were grouped and assigned to windows based on the plant's functional organization. Although only one alarm message could be displayed in an alarm window at a time, more than one alarm message associated with that window could be active at the same time. In that case, a prioritization scheme determined which message was displayed in the window. Prioritization of messages only occurred within narrowly defined queues of alarms all relating to the same plant function; there was no prioritization across functions. This contrasts with many other computerized alarm systems that predefine each alarm with an urgency level for operator

action, with some alarms always coded as “high” urgency and others always coded as “low” urgency. In this system, operators did not have to consciously consider the relative priority. The alarms that appeared in the windows at any time were expected to be addressed by the operators. Those not displayed were stored in a queue of active alarm messages associated with a given alarm window. If there were messages in the queue, a symbol appeared in the alarm message window to alert the operators. The lower priority alarm messages then could be accessed from a VDU console.

Crews were observed during their initial training with the new system using full-scope simulations of plant disturbances, and operators and other utility and vendor personnel were interviewed. In some cases, when there were many messages in a queue, the operators said that they did not have time to go back and look at them. Thus, during a dynamically evolving event, the board operators directly involved may not have time to consult secondary displays to review overflow (lower priority) alarms. They may do so in special cases, or later in the event when their workload is lower, but, in general, they rely on the alarm prioritization scheme to make them aware of the most important alarms. This increases the importance of having a robust alarm prioritization scheme that is broadly applicable across contexts.

General HFE Literature

On the issue of alarm filtering, Beattie and Vicente (1996) observed that operators tend to be uncomfortable with a reduction in alarms and, instead, prefer to “...deal with the additional quantity rather than missing a message which could be important in a particular situation, even though judged to be globally minor” (p. 13).

4.2.4.2 Modifications to Guidelines on Alarm Prioritization and Availability

Based on the foregoing discussion, the following changes to the guidance on alarm prioritization and availability have been made:

- The section name was changed to “Alarm Prioritization and Message Availability” to more clearly indicate what the term “availability” refers to.

- Guideline 4.4-1 Prioritization Criteria – the Criterion, Additional Information, and Discussion was modified to incorporate the findings of Roth and O’Hara (1998).

- Guideline 4.4-3, Access to Suppressed Alarms – a reference to the findings from the NRC alarm study and those of Roth and O’Hara (1998) was added to the Discussion.

- Guideline 4.4-4, Filtered Alarms – the Discussion was modified to include the NRC alarm study and the findings of Beattie and Vicente (1996).

4.2.5 Display

Alarm display addresses the ways in which alarm information is presented to the operating crew. NUREG-0700, Part 2, Section 4.5, has seven main subsections with general guidelines on displays and on displaying importance and urgency, alarm status, shared alarms, alarm message content and format, coding methods, and organization of the alarms. Alarm display was among the topics explicitly examined in the NRC alarm study. The following findings primarily apply to general alarm presentation.

4.2.5.1 Visual Displays

4.2.5.1.1 Evaluation of Recent Research

NRC Research

In the NRC alarm study, three primary types of displays were compared: (1) a dedicated tile format, (2) a mixed tile and message list format, and (3) a format in which alarm information is integrated into the process displays. These formats enabled two aspects of alarm display design to be examined: spatial dedication, and the degree of integration with process information.

The operator's comments gave significant insights into differences between the three types of displays. They strongly supported the availability of spatially dedicated displays. The benefits included the fact that important alarms were easy to find and interpret, and that all important ones were directly observable. One operator commented that he used both the list and the tile display, but in difficult scenarios with many alarms he looked only at the tile display.

However, even though spatial dedication was preferred, its benefits declined when the number of alarms was very large. This was reflected in the operators' preference for the mixed display condition where the number of tiles was relatively small. When all alarms were presented in tiles, operators said that it was sometimes hard to find new alarms and that it was difficult to get an overview of the situation when many alarms were coming in. Due to these considerations, the operators stated that the key alarms should be on the alarm tiles.

Another problem with the tiles was that they did not give the detailed information that operators believe is necessary to understand a disturbance, i.e., time, alarm sequence information, alarm setpoints, and parameter values. Many operators indicated that the sequence of alarms was important to understanding what initiated an event and how it progressed. The alarm message lists were most useful for obtaining this detailed information. However, alarm lists were time consuming to read and, as a result, operators could not effectively use them there were many alarms. A significant problem was identified when the alarms exceeded one page (one VDU display). The operators then did not like the fact that there were alarms on pages they could not see. Further, operators were reluctant to scroll to unseen alarm pages and sometimes abandoned scrolling when the workload became high.

Integrating alarms into the process overview displays and process mimics was effective and had many positive aspects similar to the tiles: it was good for rapidly assessing a disturbance, and when the number of alarms was high these displays were used more than the message lists. Including alarms in the process displays made the task of understanding the relationship between the alarms and the related plant equipment easier. A problem with the integrated display was that some alarms were in process formats not on the current displays. In addition, because of the way the alarms were implemented in this study, it was unclear if an alarm parameter was high or low relative to its setpoint, and in which direction it was trending.

The results of the study suggest that the most effective alarm display would be one that included tiles (SDCV displays), message lists, and alarms integrated into process monitoring displays. The tiles provide the main alerting and overview functions, and are reserved for a small set of important alarms. Their advantage is that they are continually present at a single location for operators observing the status of key parameters, equipment, systems, and functions. Alarms integrated into the process formats give a similar high-level status indication and also may be used in situation assessment, since the alarms are embedded in the displays depicting the relationships between the plant's equipment, systems, and functions. However, integrated alarms do not offer the same broad overview as the tile display because many alarms cannot be seen immediately. Neither the tiles nor the integrated displays supply the detailed alarm information; this may be provided by alarm message lists. The lists can give operators information, such as time, sequence, setpoint, and parameter values, which they need to analyze disturbances, mainly in their early and late stages. An important issue for such a system would be the coordination of alarm information across all three types of displays so that operators can make easy and rapid transitions between them.

A message list only format was not included in the study because it was considered unacceptable under the types of alarm processing conditions being evaluated. Earlier research determined that unless there was an extensive reduction in alarms (such that even significant process disturbances produced only a few) a message list is difficult for operators to manage. Such extensive processing is not typical of near-term applications. This decision was supported by the results of the study. Operators clearly indicated that the list was not useful under high alarm conditions, and abandoned it in favor of the primary alarm displays.

In Roth and O'Hara's (1998) study, a key feature of the advanced alarm system was that the display was organized functionally, based on a goal-means decomposition of the plant (Rasmussen, 1986). Operators found that the functional organization of system was very helpful and enhanced their understanding of the plant's state. One commented that while operators deal with disturbances in terms of goals, their old tile-based alarm system was not organized in that way, but instead reflected the equipment's physical location.

In addition to the advanced system, two other alarm systems were available to operators. One was the original tile-based system established when the plant was built. The tiles are typical of conventional alarm tiles that are organized into matrices by plant functions and systems. The other was an existing, chronologically organized VDU message list display which contained alarm setpoints associated with every plant parameter on the plant's data highway.

During normal operations, operators were observed to rely on the chronological-list alarm system because it was useful for picking up early signs of minor equipment malfunctions. In an emergency, when a large number of alarms were generated, the chronological list organization became ineffective. The advanced system was preferred, it organized information functionally and showed the alarms in parallel on physically distributed panels. This does not imply that chronological lists are the most appropriate means displaying information for normal operations; it is likely that this preference was due to the fact that the advanced alarm system did not include as many specific alarms relevant to normal operations. Rather, it illustrates that the information required by operators, and, therefore, the uses of alarm systems, are very different in normal and emergency conditions, and that these differences should be explicitly considered in evaluating these systems.

The findings of both studies suggest that multiple types of alarm displays may be needed to satisfy the operator's varied use of the system.

General HFE Literature

Beattie and Vicente (1996) noted that alarm systems did not provide all the information necessary for operators to make full use of the system:

> There are still classes of information not currently accessible to operators which they believe would be helpful. Some are specific to operating needs, such as access to the alarm limits within control programs, and extension of the Point Data display to points other than AIs; others are more general, such as the information in the engineering database (GSIO) which is used to manage and control all changes in the DCC-based annunciation system. This desire on the part of operators to have access to more information is by no means restricted to annunciation systems; analogous desires can be found throughout the control room. No-one has yet assessed the cost-benefit trade-offs associated with making such information available.
>
> Operators have also suggested that there should be more states associated with some points, rather than just single alarm limits (for example, greater use of "margin" alarms). This stems partly from the fact that Operating Policies and Principles (OP&Ps), which must be observed, set fairly conservative limits on many parameters. (p. 15).

These findings reinforce those discussed above that operators have multiple uses for alarms and that the information needs vary based upon those uses.

4.2.5.1.2 Modifications to Visual Display Guidelines

Based on the foregoing results, the following changes to the guidance on alarm prioritization and availability have been made:

- Guideline 4.5.1-1, Display Functions – Additional Information on the potential need to use multiple display formats to achieve alarm system objectives was added, as well as a Discussion of recent NRC research supporting this information.

- Guideline 4.5.1-2, Coordination of Alarm Alerting and Informing Functions – a Discussion of the NRC alarm study findings about the ease of accessing detailed information was added.

- Guideline 4.5.1-3, Presentation of Alarm Priority with Detailed Alarm Information – a Discussion of the NRC alarm study on priority coding was added.

- Guideline 4.5.1-4, Use of Spatially-Dedicated, Continuously-Visible Displays – a Discussion of the NRC alarm study findings on SDCV displays was added.

- Guideline 4.5.2-1, Importance/Significance – the criteria was reworded and an Additional Information section was added for clarity to address peer reviewer comments.

- Guideline 4.5.2-2, Simultaneous Display of High-Priority Alarms – a Discussion of the results of the NRC alarm study about alarm lists and the lack of a display area was added.

- Guideline 4.5.2-3, Coding of Alarm Priority – Additional Information on a caution about the potential confusion of alarm lists was added, as well as a Discussion of the NRC alarm study findings.

- Guideline 4.5.3-2, New Alarms – a reference to Guideline 1.3.10-10, Flash Coding for Text was added to Additional Information, as well as a Discussion of the NRC alarm study findings on flashing text.

- Guideline 4.5.3-6, Cleared Alarms That Re-Enter the Abnormal Range – this new guideline was added to address an issue raised by a peer reviewer. The criterion and Additional Information describe how an alarm system should respond when a variable deviates from the normal range after the alarm has cleared. A Discussion of relevant high-level design review principles is provided.

- Guideline 4.5.4-1, Minimize Shared Alarms – a Discussion was added which refers to Woods' (1995) remarks on shared alarms (discussed in Section 4.2.1.1 above). Table 1 was modified to address peer reviewer comments. In the upper portion (i.e., alarms that may be considered for combination), the text for the second bullet was modified for clarity. In the lower portion (i.e., conditions under which alarms should not be combined), the text for the second bullet was modified for clarity.

- Guideline 4.5.5.1-1, Alarms Information Content - additional information items were added to the criterion based on reviewer comments.

- Guideline 4.5.5.2-2, Format of VDU and Printer Messages - an Additional Information section was added for clarity to address reviewer comments.

- Guideline 4.5.6.2-1, Visual Signal for Important Alarms – the title, criterion, and Additional Information were revised for clarity based on peer reviewer comments. A reference to Guideline 1.3.10-10, Flash Coding for Text was added to Additional Information.

- Guideline 4.5.6.2-5, Brightness Levels for VDU Displays – the Additional Information was revised for clarity based on peer reviewer comments.

- Guideline 4.5.6.2-7, Spatial Coding – a qualification based on the NRC alarm study about the spatial segregation of dynamically prioritized alarms was added to Additional Information .

- Guideline 4.5.7.1-1 Functional Grouping of Alarms – a Discussion of Roth and O'Hara's (1998) findings on the functional organization of an alarm display was added.

- Guideline 4.5.7.1-2, Separation of Function Groups – Additional Information on application to alarm lists was added, as well as a Discussion of the NRC alarm study findings on separating primary and secondary alarms; reference to the description of designs in which alarms separated by system was made.

- Guideline 4.5.7.1-4, Coordinate Designation Identifiers – Additional Information was modified for clarity based on peer reviewer comments.

- Guideline 4.5.7.2-2, Message Listing Options – a Discussion of the reference to Roth and O'Hara's (1998) findings on chronological list display was added.

4.2.5.2 Auditory Signals

Much of the guidance on coding in Section 4.5.6 of NUREG-0700 pertains to auditory signals associated with alarms. In recent years, there has been a growing interest among researchers in designing more effective auditory signals for alarm systems (see the discussions of auditory masking and perceived urgency in NUREG/CR-6105). Literature on the topic is summarized below. Audio signals are not typically treated in any detail in descriptions of alarm systems. However, a few discussions are available, including some that mention the possibility of using speech output in alarm system. The NRC study did not examine audio aspects of alarms.

4.2.5.2.1 Evaluation of Recent Research

System Descriptions and Evaluations

More complex and meaningful auditory alarm signals have begun to be used in control rooms. The alarm system of the Sizewell 'B' (UK) plant uses auditory codes to indicate the 'ownership' (by either operators or the supervisor) of an alarm so as to avoid unnecessarily distracting those for whom an alarm is not task-relevant (Hickling, 1994). In addition, the relative importance or urgency of the alarms is coded rhythmically and harmonically, i.e., by varying the temporal patterns and frequency (pitch) composition of the alarm sounds. Hickling does not give examples; the research bases for such coding techniques are described in detail below. The coding of alarm signals is among the improvements included in the main control board for advanced Japanese pressurized water reactors (Shimada, Yamamoto, Tani, and Kobashi, 1996). Frequency and repetition period are varied according to the systems concerned and the category of the alarm (e.g., first out). Details of the coding scheme were not given, and the system evaluation reported by Shimada et al. did not specifically discuss the effectiveness of the audio coding.

Using speech for mediating alarm related interactions is also being considered. Ohga, Seki, and Arita (1996) describe the development of alarm handing methods for boiling water reactors. They evaluated both alarm selection and alarm presentation. The prototype interface includes speech input and output devices, which are used in conjunction with touch screens and VDU display, respectively. Their evaluation test of the prototype did not include measures of the operator's performance. Gutiérrez, Jelinek, and O'Neil (1996) describe the development of HSI concepts for the ABWR (generally described in Section 4.1). They used operating personnel and part-task simulation in evaluating iterative designs. One concept was to use verbal communication, rather than conventional audio signals, to notify operators of plant-level alarms, and a voice to notify operators that an action contrary to the current automatic action was being taken. The use of verbal prompts in place of audio alarm signals was implemented in the simulations; Gutiérrez et al. do not report the outcome.

4 RESULTS

General HFE Literature

When the guidance in NUREG/CR-6105 was being compiled, techniques for designing more effective auditory alarms had been described, and a limited amount of experimental work had been done. Since then several exploratory studies have appeared in the general human factors literature. Noteworthy developments have occurred in the following areas. First, the audibility of alarm sounds has been examined, and also the acoustical features leading to difficulty in identifying such sounds. Second, research into coding alarm urgency using acoustical parameters has greatly expanded. Finally, researchers have begun to explore the design of monitoring sounds, i.e., sounds that might provide operators with feedback about the changes in process parameters. Each of these areas is reviewed below. In addition, studies on using speech displays in the context of alarms display are reviewed.

Audibility

Patterson (1982) suggested a method for estimating the signal level required to insure that alarms were audible. His approach was based on the fact that signals are masked only by energy in a critical band of frequencies close to the signal's frequency. More recently, a method for predicting alarm audibility was described by LaRoche, Tran Quoc, Hétu, and McDuff (1991); this method, referred to as the Detectsound model, is also based on the critical-band concept, although the specific assumptions about the critical band are slightly different. The model, which is implemented in software, allows the effects of age and of wearing hearing protection to be taken into account in estimating the audibility of warning signals.

Momtahan, Hétu, and Tansley (1993) used the Detectsound model to analyze audio signals produced by medical monitoring equipment. They measured the ambient noise in operating rooms and intensive-care units, the noise produced by the equipment used in the rooms, and the alarm sounds produced by the equipment. They found that many alarm sounds would be completely masked (i.e., rendered inaudible) by ambient noise, equipment noise, or the sounds of other alarms. Many others were not sufficiently above threshold to be considered reliably detectable.

Momtahan et al. point out that the audio alarms also were deficient based on other psychoacoustical considerations, which they summarized as follows:

> ...[A]uditory alarms that are continuous are difficult to remember, they are more likely to mask other signals, and they disrupt speech communication. Auditory alarms that contain mainly high frequency components are unpleasant. Sound localization is best for frequencies below about 1500 Hz and above 3500 Hz, although the greatest difficulty in localizing sound occurs at 1500 Hz... For alarm sounds that need to wrap themselves around obstacles, such as other equipment, frequencies below 1500 Hz are best. Additionally, alarms should be composed of more than one frequency in order to decrease the chance that they will be masked by other signals or noise; if these frequency components have a harmonic relationship to one another, the alarm is more likely to sound more pleasant and due to a phenomenon called residue pitch, harmonic components strengthen the perception of the fundamental frequency, even if the fundamental frequency itself cannot be heard...(p. 1162).

Confusibility

Meredith and Edworthy (1994) examined the learning of, and confusions among, a set of alarm sounds used in hospitals' intensive therapy units. Previous laboratory research suggested that only five or six sounds are easily learned, and that learning more difficult. They hypothesized that in operating environments, where the warnings are meaningful and more varied, a larger set of warnings might be learned. They recorded the warnings used in an intensive care unit and trained subjects to identify them. In separate experiments, the warnings were presented either in the same form in which they were recorded, or standardized for level and duration. In a third experiment, the standardized sounds were given 'neutral' names (rather than the names of equipment in the other experiments). Subjects learned a set of 12 warning sounds within a short time; training was most rapid for non-standardized warnings.

The warnings most often confused consisted of continuous, high-pitched tones. The difference in their frequencies was large enough to be easily discriminated when the tones were directly compared, but when longer intervals passed between the presentation of the two tones, identification became difficult. Sounds with the same temporal pattern, including signals with similar duty cycles (on-off times), also were consistently confused, despite having very different pulse speeds (i.e., periods).

Meredith and Edworthy suggest that confusions might be based on similarities in the semantic labels that subjects attached to the sounds; i.e., sounds that are very different acoustically may be confused because the hearer labels them similarly. If true, this would allow possible confusions to be anticipated without undertaking formal studies.

Urgency

Edworthy (1994) summarized a series of studies which demonstrated that the perceived urgency of audio signals could be reliably measured, that relative urgency could be predicted based on their acoustical properties, and that psychophysical techniques could identify the parameters that are most effective in producing changes in urgency. Edworthy noted that these results can not only be used to create sets of warning signals that differ in perceived urgency, but also to design signals with similar perceived urgencies that nevertheless are readily distinguishable from one another.

Haas and Casali (1995) studied the perceived urgency of, and response time to, auditory warning signals. To approximate operational conditions, they used a monitoring task to induce workload, and had a continuous broadband noise in the background. The signals were trains of pulses consisting of four components (pure tones at .5, 1, 2, 4 kHz) which were presented either simultaneously or sequentially; a frequency-modulated signal which increased in frequency from .5 to 3 kHz over one pulse duration was also used. The inter-pulse interval (0, 100, 300 ms) and pulse level (5 and 19dB above threshold) were also varied. Direct magnitude estimation ratings and paired comparisons were used to scale the perceived urgency of the signals. The subjects' time to respond to the signals was also recorded.

The rated urgency of the sequential presentation was less than that of a simultaneous or frequency-modulated presentation. The rated urgency was higher for more intense signals; this effect was more pronounced for the sequential pulse than for the others. The paired comparison data showed the same effect. Rated urgency was inversely related to inter-pulse interval; i.e., urgency was perceived to be higher when pulses occurred faster. A similar effect was evident in the paired comparison data.

Response times were roughly 40 ms longer for the sequential pulse presentation than for simultaneous or frequency-modulated signals; responses were roughly 60 ms faster for the more intense signals. The perceived urgency was inversely related to response time; i.e., signals perceived as more urgent were responded to more rapidly.

Monitoring Sounds

Edworthy, Hellier, and Hards (1995) investigated the semantic associations of audio signals that differed in pitch, speed, inharmonicity, and rhythm. In one experiment, subjects rated individual sounds on 42 operationally relevant adjectives. The analysis identified instances in which the parameter's values were reliably related to changes in the ratings assigned to the adjectives. In a second experiment, the sounds to be judged consisted of individual parameter values played in succession; the sounds were rated as in the first experiment. Again, reliable associations emerged between changes in the parameters and the adjectival ratings. For example, the increasing pitch sequence was most associated with the adjectives 'rising' and 'controlled'; increasing speed was related to 'starting up' and 'urgent'.

Edworthy et al. used these semantic associations in designing monitoring sounds or *trendsons*. These sounds, which provide immediate feedback about the changes in physical parameters, would be programmed to play when predetermined levels of a parameter are reached; the number of levels used would be based on the typical time history of the development of a malfunction.

Speech

Stanton (1994b) points out that presenting alarm information by speech displays has several potential benefits in process control contexts. These include the ability to capture attention regardless of operators' location or direction of gaze, the lack of any requirement to learn the meanings of codes, and the possibility of reducing the load on the visual channel. Stanton and Baber (1997) compared the effects of presenting alarm information by means of synthesized speech, a message list, or using the two combined. Subjects were required to respond to alarms and diagnose failures in a simulated industrial process while also undertaking a spatial secondary task. Performance measures included process output, time taken to acknowledge and investigate alarms, number of inappropriate actions taken, and number of alarms correctly recalled in an unanticipated test after the experiment. Their performance for the speech-and-text and the text-alone presentations did not differ; performance with speech-alone was significantly worse by several measures. Stanton and Baber suggest a number of problematic characteristics of speech signals under certain circumstances. For example, a speech message demands attention during its entire duration, and the signal is transitory – once it is given, it is gone. Accordingly, there is a memory requirement for information that must be kept available; the study showed that this memory was poor. Stanton points out that these characteristics conflict with aspects of the process control setting; e.g., operators sometimes do not or cannot respond immediately to alarm information, multiple alarms may be present simultaneously, and it is necessary to respond to information from more than one source.

Edworthy and Adams (1996) considered the use of voice warnings in noisy environments, where intelligibility is a major issue. Maintaining intelligibility when speech is amplified requires proper adjustment of the relative intensity of the low and high frequency portions of the signal. Simply making normal speech louder can reduce intelligibility owing to the increased masking of some components of the speech signal by others; the situation is complicated when environmental noise masks portions of the signal.

Using synthesized speech in noisy environments may be useful when its frequency spectrum can be tailored to the ambient noise more easily than that of natural speech, whether recorded or digitized. However, there is also evidence to suggest that processing synthesized speech imposes greater cognitive demands. Technological advances in generating synthesized speech may have mitigated this problem, but until this issue is explored further, it may not be advisable to use synthesized speech in high workload settings. Edworthy and Adams also point out that comparisons of the efficacy of speech and non-speech warnings tend to involve traditional signals (such as sirens or bells), not the richer audio signals that represent the current state of the art.

Speech messages can be presented at faster-than-normal rates, thereby mitigating potential problems associated with the length of warnings. Edworthy and Adams reviewed recent literature which shows that high rates of speech result in faster reaction times. They point out that this might be due simply to the information being conveyed faster, or to the perception of increased urgency in quickly spoken messages. More importantly however, as might be expected, they note that very high rates, such as 250 words/minute, degrade intelligibility.

Despite some potential advantages of speech over other means of presenting information, it has not been shown that speech is an appropriate alarm medium for process control contexts. Stanton and Baber conclude that "...speech alone as a medium for alarm displays cannot be recommended for tasks where there is a memory component, there is likely to be some delay before the fault is attended to, there is likely to be more than one alarm presented at a time, and the operator is required to assimilate information from a variety of sources using spatial reference. If speech is to be incorporated into the alarm system for 'process control' tasks, it is recommended that it be paired with other media such as a scrolling text display."

4.2.5.2.2 Modifications to Guidelines for Auditory Signals

Descriptions of current alarm systems or system concepts indicate that recent techniques for designing auditory alarm signals will be applied in the control rooms nuclear power plants. Continuing research has resulted in findings pertaining to the audibility and distinctiveness of auditory signals and the effectiveness of various coding

techniques. Likewise, using speech for presenting alarm information has been considered and investigated. Based on the foregoing findings, the following changes to the guidance on auditory coding of alarms were made:

- Guideline 4.5.6.3-1, Audio Signal for Important Alarms – the title was edited for clarity and an explanatory statement was added to the Additional Information to address peer reviewer comments.
- Guideline 4.5.6.3-4, Audible Signals for Alarm States – the criterion was edited for clarity based on peer reviewer comments.
- Guideline 4.5.6.3-5, Reminder Audible Signals – the Additional Information was modified for clarity based on peer reviewer comments.
- Guideline 4.5.6.3-7, Interference Among Signals – a Discussion was added based on the review of material on the audibility of alarm signals.
- Guideline 4.5.6.3-8, Readily Identifiable Source – a Discussion of localization and signal frequency was added.
- Guideline 4.5.6.3-13, Auditory Signal Discriminability – a summary of the confusibility material was added to Additional Information.
- Guideline 4.5.6.3-14 Number of Tonal Signals – a reference to Guideline 4.5.6.3-13 was added to Additional Information.
- Guideline 4.5.6.3-16, Pulse Codes – a statement about the confusibility of signals with similar temporal patterns was added to Additional Information.
- Guideline 4.5.6.3-20, Compound Codes – a statement emphasizing explicit consideration of confusibility was added to Additional Information; a summary of the findings on confusibility was added to a Discussion.
- Guideline 4.5.6.3-22 – a new guideline was added cautioning against the use of speech alone for presenting alarm information.

4.2.6 Control

Functional requirements refers to the specification of control functions that the system prossesses for the operator's interaction with the alarm system. The typical control functions used in the nuclear industry are silence, acknowledge, reset, and test (SART). In conventional plants, these functions are supported by dedicated controls, such as pushbuttons. The SART philosophy also is applied to advanced alarm systems, where control functions for the operators' interaction may be more sophisticated and require greater flexibility than conventional alarm systems. For example, the operator may be able to define temporary alarms, adjust setpoints, and control filtering options. Some of these capabilities may require more sophisticated methods of communication with the system than is possible with traditional dedicated switches, or pushbuttons.

The guidance on alarm control in NUREG-0700, Part 2, Section 4.6 has four main subsections: general guidelines, silence controls, acknowledge controls, and reset controls.

4.2.6.1 Evaluation of Recent Research

Among the improvements in the alarm system in the current annunciation strategy for CANDU plants are changes to the alarm control interaction (Davey, Feher, and Guo, 1995). CAMLS alarms are indicated by a momentary tone, which eliminates the need for a silence response from the operators. Alarm acknowledge and reset functions are accomplished through a single button. Upon acknowledging an alarm, detailed information and alarm response

procedures are automatically presented. No acknowledgment is required for low-priority alarms when higher-priority ones are acknowledged. In addition, status messages are not acknowledged.

As discussed in Section 4.1 in the context of alarm system functions, Roth et al. (1997) observed that operators sought to modify the alarm system to provide better support for a broad range of functions under normal operating conditions that were not necessarily designed into the system. While operators find these functions helpful, the additional operator-defined alarms and indications present the same paradox as does alarm generation – they create additional alarm processing demands for operators. The ways in which the existence and status of these alarms and indications should be presented has not been explicitly addressed. Hickling (1994) considers using sounds to denote conditions which are not alarms, e.g., an operator-defined, unique audible signal to indicate that a process is complete. He notes that due to advances in audio displays, it is conceivable that the number of 'alarms' may be increased since signals conveying the expected completion of a process can be differentiated from those indicating an unexpected deviation.

The 'ownership' of Sizewell B alarms is allocated to specific personnel, either operators or their supervisors. Although alarms can be viewed at any workstation, they can only be acknowledged or reset at the station used by that particular person (Hickling, 1994). While this might be expected to ease the operator's interaction with the alarm system, there is no confirmatory research data or operating experience.

Beattie and Vicente (1996) found that although the functional capabilities of alarm systems have increased, additional features are still needed: "Another area where operators see a need for annunciation system improvements is in the support it provides for post-event analysis, reporting, review with supervisors, etc. The engineers responsible for configuration management of the annunciation system see a need for more online utilities for managing and verifying major updates." (p. 15).

4.2.6.2 Modifications to Guidelines for Alarm Control

To better address the added functionality of alarm management, the original section was divided into two sections: 4.6, User-System Interaction and 4.7, Control Devices. The new section 4.6 contains the guidance for silence, acknowledge, and reset controls. However, since the guidance addresses their functional characteristics, the term "controls" was replaced with "functions" in both of the sections. Two new subsections were added. Subsection 4.6.5 addresses Alarm Management. It includes several guidelines previously set out in Section 4.7. The guidelines covering the operators' management of alarms were moved into this new section. The following guidelines are affected:

[Note: The prior sections provided the gl numbers and TITLES. This section is inconsistent.]

- Guideline 4.6.2-1 had its Additional Information section modified for clarity to address reviewer comments.
- Guideline 4.6.3-1 had its criterion modified for clarity to address reviewer comments. A reference to guideline 4.5.3-4 was also provided.
- Guideline 4.7-2 was renumbered 4.6.5-1 and a Discussion section was included to address the studies by Roth and O'Hara (1998) and Beattie and Vicente (1996) on operator modification of the interface with the alarm system.
- Guideline 4.7-3 was renumbered 4.6.5-2 and was modified to address operator selected configuration changes instead of both operator and automatic changes. Guideline 4.6.6-2 now addresses only automatic changes.
- Guideline 4.7-4 was renumbered 4.6.5-3.
- Guideline 4.7-5 was renumbered 4.6.5-4 and a Discussion was added to reference Guideline 4.6.5-1 (see above).

- Guideline 4.7-6 was renumbered 4.6.5-5 and a Discussion was added to address the indications associated with operator-defined alarms.

The second new subsection is 4.6.6, Automatic Features. It consists of three guidelines that were in the old Section 4.7, Automated, Dynamic and Modifiable Characteristics. The three guidelines were 4.7-1, Automated Alarm System Configuration; 4.7-3, Acknowledgment of Alarm System Configuration Change; and 4.7-7, Automatic Move-Defined Setpoints. The guidelines are now numbered 4.6.6-1, 4.6.6-2, and 4.6.6-3, respectively. A change was made to Guideline 4.6.6-1. The title includes the term "Automatic" to refer to the source of the configuration change; the reference to operators changing the configuration in the guideline have been deleted (this is now addressed in Guideline 4.6.5-2). Finally a discussion of dynamic thresholding was added to Guideline 6.6.6-3.

The new Section 4.7, Control Devices, addresses the physical controls and their characteristics. It contains the guidelines that were previously in Section 4.6.1, General Alarm Control Guidelines, with the single exception of Guideline 4.6.1-6, Access to New Undisplayed Alarms, which is now Guideline 4.6.1-1. The guidelines in the new Section 4.7, have been renumbered from their 4.6.1-X designations to 4.7-X designations. A change was made in the title of the old Guideline 4.6.1-1, Provision of Control Functions, which is now 4.7-1, Separate Controls for Alarm Functions. For the new guideline 4.7-1, Separate Controls for Alarm Functions, a statement was added to the Additional Information section for clarity to address reviewer comments. For the new guideline 4.7-4, Separate Controls for Tile and VDU Alarms, the Additional Information section was modified for clarity based on peer reviewer comments.

4.2.7 Automated, Dynamic, and Modifiable Features

In certain situations, such as during major process disturbances, it may be desirable to reduce the workload by automating some alarm system functions, such as silencing lower priority alarms or temporarily shutting down unacknowledged alarm flashing. Similarly, automated controls may be included to trigger appropriate displays, such as alarm graphics, data windows, or display pages. Other dynamic aspects of the alarm system may allow operators to introduce operator-defined characteristics, such as parameters and setpoints. These dynamic aspects of the interface should be reviewed to avoid excessive workload demands while preserving the overall functional characteristics of the alarm system. These dynamic aspects of the alarm system should not be disruptive or confusing to operators, especially when the alarm system changes its modes of operation.

NUREG-0700, Part 2, Section 4.7, discusses the implementation of operator-defined alarms and setpoints, and other features of the alarm system that may be modified by the operating crew. The guidelines from this section have been integrated into other sections, 4.6.5 and 4.6.6, as discussed above. Therefore, the section no longer exists.

4.2.8 Reliability, Test, Maintenance, and Failure Indications

The alarm system must reliably provide information to the operator. Important considerations include the reliability of alarm system's hardware and software, the manner in which the system conveys information to the operator about alarm system failures or malfunctions, the ease with which test and maintenance can be performed upon the alarm system with minimal interruption to the operators, and the provisions made for backup systems, devices, and functions to support personnel if the system malfunctions. NUREG-0700, Part 2, Section 4.8, addresses these aspects of alarm system design. To reflect the importance of redundancy and diversity in the alarm system, the title of this section has been changed to Backup, Test, Maintenance, and Failure Indication Features.

Recent research has not explored this aspect of designing alarm systems, beyond the discussion of the reliability of individual alarms in Section 4.2.2; thus no modifications to guidance were made in that basis. Based on reviewers' comments, the titles of two ~~a~~ guidelines were ~~was~~ modified for clarity and to be more generally applicable to current technology:

- The title of Guideline 4.8.2-1 was changed to "Testing Capabilities,"

- The title of Guideline 4.8.3-7 was changed to "Aids for Alarm System Maintenance," and the criterion and Additional Information were worded more generally.

4.2.9 Alarm Response Procedures

Alarm response procedures (ARPs) provide more detailed information about the alarm condition than is typically provided in the alarm message. Generally, such information includes the source of the alarm (sensor), setpoint, causes, automatic actions, and operators' actions. These details are especially important to operators when an unfamiliar alarm is activated or when an alarm seems inconsistent with the operator's understanding of the plant's state. ARPs may be hard copy or computer based. NUREG-0700, Part 2, Section 4.9 discusses ARPs.

4.2.9.1 Evaluation of Recent Research

Several of the systems described in Section 4.1, such as the EdF N4 alarm system and the AECL CAMLS, illustrate that alarm response procedures are being incorporated into plant computer systems for ready access from the alarm management system. However, the utility of this approach has not been explored.

The topics to be covered by ARPs are identified in Guideline 4.9-3, Alarm Response Procedure Content. They are generally consistent with those identified in new systems. However, the EdF system gives operators verifying information so they can confirm alarms. In light of the discussion on the complexity of monitoring in Section 4.2.1, General Guidelines, and of alarm reliability in Section 4.2.2, Alarm Definition, displaying information to support operators to verify that an alarm is authentic is important in a noisy, complex environment.

4.2.9.2 Modifications to Guidelines for Alarm Response Procedures

- Guideline 4.9-2, ARP Access – a Discussion of the basis for providing easy access to alarm-related information was added.

- Guideline 4.9-3, ARP~~Alarm Response Procedure~~ Content – Additional Information was added emphasizing the importance of providing confirmatory information and referring to a Discussion of alarm verification. The third bullet was edited for clarity based on reviewer comments. Also, an additional bullet was added indicating that explanations should be provided for alarm processing capabilities that are relevant to the alarm.

4.2.10 Control-Display Integration and Layout

Control-display relationships and general layout significantly affect the operators' performance with alarm systems, as they do for other aspects of the HSI. NUREG-0700, Part 2, Section 4.10 describes these aspects of alarm system design.

4.2.10.1 Evaluation of Recent Research

Recent research has not specifically addressed this aspect of alarm system design. Guideline 4.10-7, Location of Access to Process Controls and Displays, recommends that alarm panels should be located close to related controls and displays. In VDU-based systems, such as the AECL and EdF systems, there is direct access to these supporting HSIs from the alarm system.

4.2.10.2 Modifications to Guidelines for Control-Display Integration and Layout

Guideline 4.10-7, Location for Access to Process Controls and Displays – a Discussion of the need to minimize the effort associated with accessing alarm-related information was added.

4.3 Human Performance Issues

Recent research was reviewed to identify whether there were human performance issues not previously identified (O'Hara and Brown, 1991a; O'Hara and Brown, 1991b) or which suggested new interpretations of existing issues. Appendix C describes those previously-identified issues. The implications of the new research reviewed for those issues is discussed below.

Role of the Alarm System

One objective of the IAEA Specialists' Meeting on Alarm Systems (IAEA, 1996) was to define the role of the alarm system. However, its design as an integrated system has increased its functionality and made it more difficult to precisely define the alarm system's role independently from other HSI resources. Within the alarm system, operators can obtain procedures, P&IDs and related displays, and controls.

This trend is evident in the design of other HSI resources, such as computer-based procedures (O'Hara, Higgins, Stubler, and Kramer, 1998). In general, as control room resources (alarms, displays, controls, and procedures) evolve further, their functionality increases to incorporate functions typically associated with the other resources. The net result can be multiple overlapping systems having the same functions.

The effect of this expanding and overlapping functionality must be considered, especially for backfit or upgrade applications where it may lead to inconsistencies across control room resources.

Alarm Management Functions

Alarm systems now have many new capabilities, such as sorting alarms and establishing temporary setpoints. The benefits or drawbacks to these management features have not been researched, and there is insufficient operating experience to develop guidance.

Interface Management Workload and Alarm System Use

Operators often are reluctant to engage in interface management tasks in general (O'Hara, Stubler, and Nasta, 1998), and, in particular, when they involve alarm systems (O'Hara et al., 2000; Roth and O'Hara, 1998). The impact of this reluctance on the increased workload associated with alarm systems and alarm management functions needs to be examined, as does its implications for displaying alarms.

5 DISCUSSION

The objectives of this study were to review the technical bases in recent literature, including the NRC's recent studies, and then to propose changes to the alarm system characterization (objective 1), the HFE guidelines (objective 2), and the list of human performance issues (objective 3). Each is briefly discussed below.

Alarm System Characterization

While the characterization of alarm systems in NUREG/CR-6105 reasonably represented the functional characteristics of alarm systems, it did not adequately address all aspects that are important to an HFE design review. Thus, the characterization was expanded to (1) better illustrate the relationship of the alarm system to the processes and systems of the plant, and (2) more clearly indicate the relationships between the HSI aspects of the alarm system and the guidance. Appendix A contains this revised characterization.

HFE Design Review Guidelines

Recent research has addressed many aspects of alarm system design, and as a result, modifications have been made to most of the ten elements of the alarm system characterization. In general, the research yielded confirmatory data which could be used to further clarify the intent of the guidelines. In these cases, the Additional Information and Discussion sections of the guidelines were either newly created or modified. The guideline criteria also were modified or supplemented. In addition, where warranted, several new guidelines were developed. Appendix B contains the revised guidelines.

Human Performance Issues

Several human performance issues were identified in recent literature. In most cases, they reflect ones already identified in earlier phases of this NRC project (O'Hara and Brown, 1991a; O'Hara and Brown, 1991b); these are summarized in Appendix C.

The studies reviewed have strengthened the technical basis of information on the human performance issues identified earlier – especially for alarm processing and alarm availability. Three areas were especially reinforced. The first is the desirability of alarm processing and its operational acceptability. The second is the importance of providing access to suppressed alarms. The third is the need to provide information on the alarm's reliability and information to enable operators to confirm the validity of alarms in the extremely complex and noisy control room.

The changes to the characterization and HFE guidelines described in this document will be incorporated into NUREG-0700, Revision 2.

6 REFERENCES

Beattie, J. and Vicente, K. (1996). *Human factors review of annunciation systems in Canada and of the latest in human factors annunciation worldwide*, (Report prepared for the AECB). Toronto: University of Toronto.

Bliss, J., Dunn, M., and Fuller, B. (1995). Reversal of the cry-wolf effect: An investigation of two methods to increase alarm response rates. *Perceptual and Motor Skills*, *80*, 1231-1242.

Bliss, J., Gilson, R., and Deaton, J. (1995). Human probability matching behaviour in response to alarms of varying reliability. *Ergonomics*, *38*, 2300-2312.

Bliss, J., Jeans, S., and Piroux, H. (1996). Dual-task performance as a function of individual alarm validity and alarm system reliability information. In *Proceedings of the Human Factors and Ergonomics Society 40th Annual Meeting.* Santa Monica, CA: Human Factors and Ergonomics Society.

Bliss, J. and McAbee, P. (1995). Alarm responses in a dual-task paradigm as a function of primary task criticality. In *Proceedings of the Human Factors and Ergonomics Society 39th Annual Meeting.* Santa Monica, CA: Human Factors and Ergonomics Society.

Bryan, R. and Fuld, R. (1995). An objective approach to advanced control room alarm management. In *Proceedings of the Topical Meeting on Computer-Based Human Support Systems: Technology, Methods, and Future*. La Grange Park, IL: American Nuclear Society.

Carrera, J and Easter, J (1991). *Advanced alarm management in the aware system*. Pittsburgh, PA: Westinghouse Electric Corporation.

Davey, E., Feher, M., and Guo, K. (1995). An improved annunciation strategy for CANDU plants. In *Proceedings of the Topical Meeting on Computer-Based Human Support Systems: Technology, Methods, Future.* La Grange Park, IL: American Nuclear Society.

Easter, J. and Lott, L. (1992). Backfitting a fully computerized alarm system into an operating Wesinghouse PWR: A progress Report. In *Proceedings of the IEEE Conference on Human Factors and Power Plants*. Monterey, CA: IEEE.

Edworthy, J (1994). Urgency mapping in auditory warning signals. In N. Stanton (Ed.) *Human factors in alarm design*. London: Taylor and Francis.

Edworthy, J. and Adams, A. (1996). *Warning design: A research prospective*. London: Taylor and Francis.

Edworthy, J., Hellier, E., and Hards, R. (1995). The semantic associations of acoustic parameters commonly used in the design of auditory information and warning signals. *Ergonomics*, *38*, 2341-2361.

Feher, M., Davey, E., and Lupton, L. (1996). Validation of the computerized annunciation message list system (CAMLS). In *Proceedings of the Specialists' Meeting on Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants*. Vienna: International Atomic Energy Agency.

Førdestrømmen, N., Moum, B., and Torralba, B. (1994). *Alarm system CASH: Main design characteristics* (HWR-398). Halden, Norway: OECD Halden Reactor Project.

Førdestrømmen, N., Moum, B., Torralba, B., and Decurnex, C. (1995). CASH: An advanced computerized alarm system. In *Proceedings of the Topical Meeting on Computer-Based Human Support Systems: Technology, Methods, and Future*. La Grange Park, IL: American Nuclear Society.

Fujita, Y. (1989). Improved annunciator system for Japanese pressurized-water reactors. *Nuclear Safety*, *30*, 209-221.

6 REFERENCES

Gutierrez, R., Jelinek, J., and O'Neil, T. (1996). Human-machine interface concepts for the ABWR. In *Proceedings of the International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies.* La Grange Park, IL: American Nuclear Society.

Haas, E. and Casali, J. (1995). Perceived urgency of and response time to multi-tone and frequency modulated warning signals in broadband noise. *Ergonomics, 38*, 2313-2326.

Hickling, E. (1994). Ergonomics and engineering aspects of designing an alarm system for a modern nuclear power plant. In N. Stanton (Ed.), *Human factors in alarm system design*. London: Taylor and Francis.

IAEA (1996). *Proceedings of the International Atomic Energy Agency Specialists' Meeting on Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants*. Vienna: International Atomic Energy Agency.

Kim, I. et al. (1996). An integrated approach to alarm processing. In *Proceedings of the International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies.* La Grange Park, IL: American Nuclear Society.

LaRoche, C., Tran Quoc, H., Hétu, R., and McDuff, S. (1991). 'Detectsound': a computerized model for predicting the detectability of warning signals in noisy workplaces. *Applied Acoustics, 32*, 193-214.

Lee, C., Hur, S., Shin, H., Park, H., and Koo, I. (1996). Development of a new indicator and alarm system in NPPs. In *Proceedings of the International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies.* La Grange Park, IL: American Nuclear Society.

Long, T. and Davey E. (1996). Darlington annunciation: User information needs, current experience, and improvement priorities. *Experience and improvements in advanced alarm annunciation systems* (IAEA-IWG-NPPCI-97/1). Vienna: International Atomic Energy Agency.

McDonald, D., Gilson, R., and Mouloua, M. (1996). Spatial proximity of multiple alarms and the cry-wolf phenomenon. In *Proceedings of the Human Factors and Ergonomics Society 40th Annual Meeting.* Santa Monica, CA: Human Factors and Ergonomics Society.

McDonald, D., Gilson, R., Mouloua, M., and Deaton, J. (1995). The effect of collateral alarms on primary response behavior. In *Proceedings of the Human Factors and Ergonomics Society 39th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

Meredith, C and Edworthy, J. (1994). Confusion in intensive therapy unit alarms. In N. Stanton (Ed.) *Human factors in alarm design*. London: Taylor and Francis.

Miazza, P., Torralba, B., Karstad, T., Moum, B., and Follesø, K. (1994). *CASH: Computerized alarm system for HAMMLAB* (HWR-362). Halden, Norway: OECD Halden Reactor Project.

Momtahan, K., Hétu, R., and Tansley, B. (1993). Audibility and identification of auditory alarms in the operating room and intensive care unit. *Ergonomics, 36*, 1159-1176.

Mumaw, R., Roth, E., Vicente, K., and Burns, C. (1996). *A model of operator cognition performance during monitoring in normal operations.* Pittsburgh, PA: Westinghouse Science and Technology Center (prepared for the Atomic Energy Control Board).

O'Hara, J. and Brown, W. (1991a). Nuclear power plant alarm systems: Problems and issues. In *Proceedings of the Human Factors Society 35th Annual Meeting.* Santa Monica, CA: Human Factors Society.

6 REFERENCES

O'Hara, J. and Brown. W. (1991b). *Compilation of alarm system guidelines and evaluation of their applicability to hybrid and advanced control rooms* (BNL Technical Report No. A3697-2-10/91). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., Brown, W., Hallbert, B., Skråning, G., Wachtel. J., and Persensky, J. (2000). *The effects of alarm display, processing, and availability on crew performance* (NUREG/CR-xxxx). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Brown, W., and Higgins, J. and Stubler, W. (1994). *Human factors engineering guidance for the review of advanced alarm systems* (NUREG/CR-6105). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Brown, W., and Nasta, K. (1996). *Development of NUREG, 0700, Revision 1* (BNL Technical Report L-1317-2-12/96). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., Higgins, J., Stubler, W., and Kramer, J. (1999). *Computer-based procedure systems: Technical basis and human factors review guidance* (NUREG/CR-6634). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Stubler, W., and Higgins, J. (1996). *Hybrid human system interfaces: Human factors considerations* (BNL Report J6012-T1-4/96). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., Stubler, W. and Nasta, K. (1998). *Human-system interface management: Effects on operator performance and issue identification* (BNL Report W6546-1-1-7/97). Upton, NY: Brookhaven National Laboratory.

Ohga, Y., Seki, H., and Arita, S. (1996). Development of alarm handling methods for boiling water reactors. In *Proceedings of the Specialists' Meeting on Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants*. Vienna: International Atomic Energy Agency.

Patterson (1982). *Guidelines for auditory warning systems on civil aircraft* (CAA 82017). London: Civil Aviation Authority.

Pirus, D (1996). Alarm processing - ways to the future. In *Proceedings of the International Atomic Energy Agency Specialists' Meeting on Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants.* Vienna: International Atomic Energy Agency.

Rasmussen, J. (1986). *Information processing and human-machine interaction*. New York: North Holland.

Roth, E. and O'Hara, J. (1998). *Integrating digital and conventional human-system interface technology: Lessons learned from a control room modernization program*. (BNL Report J6012-3-4-7/98). Upton, New York: Brookhaven National Laboratory.

Roth, E., Mumaw, R., Vicente, K., and Burns, C. (1997). Operator monitoring during normal operations: Vigilance or problem-solving? In *Proceedings of the Human Factors and Ergonomics Society 41st Annual Meeting.* Santa Monica, CA: Human Factors and Ergonomics Society.

Shaw, J. (1993). Distributed control systems: Cause or cure of operator errors. *Reliability Engineering and System Safety*, *29*, 263-271.

Shimada, M., Yamamoto, Y., Tani, M., and Kobashi, S. (1996). Development of the newly advanced alarm system for APWR plant. In *Proceedings of the Specialists' Meeting on Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants.* Vienna: International Atomic Energy Agency.

Stanton, N. (1994a). *Human factors in alarm system design*. London: Taylor and Francis.

Stanton, N. (1994b). The utility of speech-based alarm displays for human supervisory control tasks. In *Proceedings of the 12th Triennial Congress of the International Ergonomics Association, Volume 4: Ergonomics and Design*. Ontario, Canada: Human Factors Association of Canada.

Stanton, N. and Baber, C. (1997). Comparing speech versus test displays for alarm handling. *Ergonomics, 40*, 1240-1254.

Suh, Y., Jang, G., Lee, T., Koo, I., and Park, J. (1996). Plant information processing system for Korean future nuclear power plants. In *Proceedings of the International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*. La Grange Park, IL: American Nuclear Society.

Vicente, K., Burns, C., Mumaw, R., and Roth, E. (1996). How do operators monitor a nuclear power plant?: A field study. In *Proceedings of the International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies.* La Grange Park, IL: American Nuclear Society.

Woods, D. (1995). The alarm problem and directed attention in dynamic fault management. *Ergonomics, 38*, 2371-2393.

Appendix A

Alarm System Characterization

A.1 Introduction

This section provides a framework for identifying and describing characteristics of alarm systems that are important to personnel performance and, therefore, should be addressed by HFE design reviews. The characteristics of advanced alarm systems often are described through comparisons with a typical, conventional NPP alarm system.

Figure A.1 shows a block diagram of a conventional alarm system.

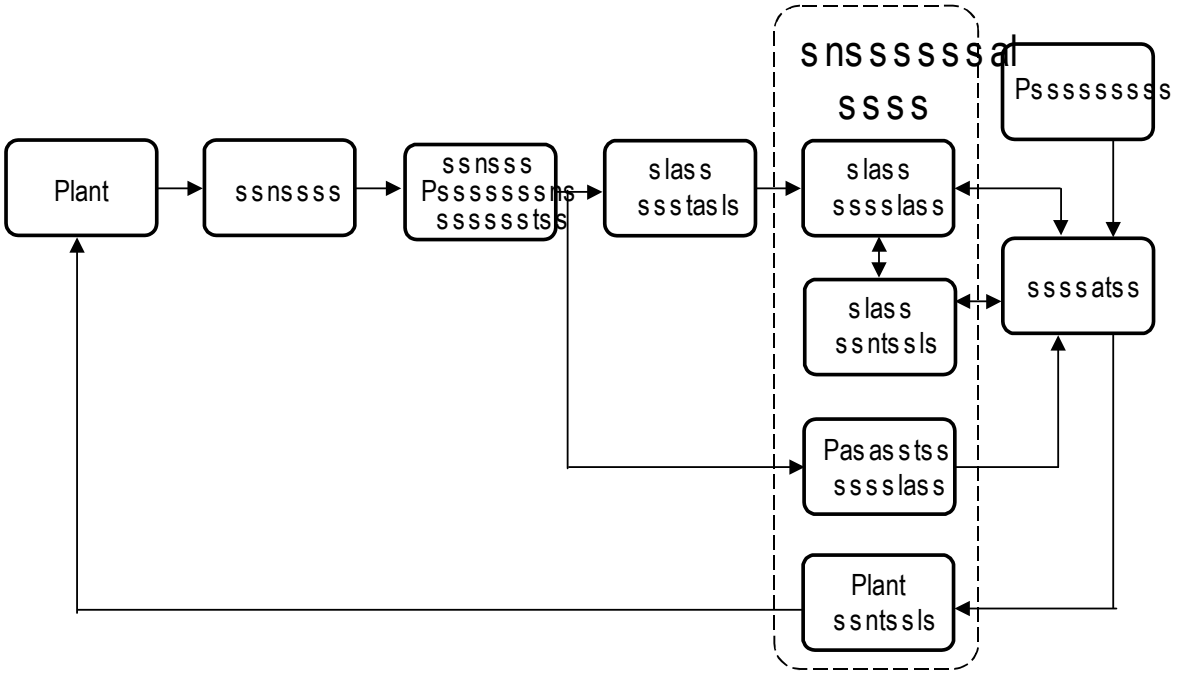

Figure A.1 Conventional alarm system and the operator

Various plant parameters, such as temperatures and pressures, are monitored by sensors, such as resistance temperature detectors (RTDs) and bellows pressure detectors. The output of the sensors is processed electronically to send the signals to various circuits that serve as controls, displays, and alarms. Figure A.1 shows the inputs to a parameter display and to an alarm bistable (B/S). Each alarm circuit for a parameter has a setpoint value at which the alarm is triggered; the bistable is the element that senses when the parameter exceeds the setpoint and actuates the alarm display. The control room operators then can make judgments about the plant state and what actions to take, based upon the parameter displays and procedures. The operators would also review other information sources (e.g., access other displays, contact plant personnel), and make adjustments to the plant systems and components through the plant controls. These adjustments would affect plant processes and the results would be detected by the sensors and transmitted back to the alarms and displays of the HSI.

Figure A.2 presents a similar block diagram for an advanced alarm system. The plant, the sensors, and the signal processing circuitry are similar to that in a conventional alarm system. However, the advanced alarm system (depicted in the dotted box) typically contains more extensive information processing capabilities. The functioning of this circuitry will be discussed later in Section A.2.3. The outputs from the advanced alarm system are typically input to some integrated HSI network that may use VDUs or other versatile display devices to present alarm information to the operators. In addition, individual parameter displays and controls may also be integrated; e.g., a computer-based display may include a representation of a plant system, plant parameter information, alarm information, and controls for adjusting plant systems. The operators would use their procedures and the HSI to assess the situation, plan responses, and take any necessary actions to control the plant. These actions would be reflected in a feedback loop to the plant, the sensors, and back to the HSI.

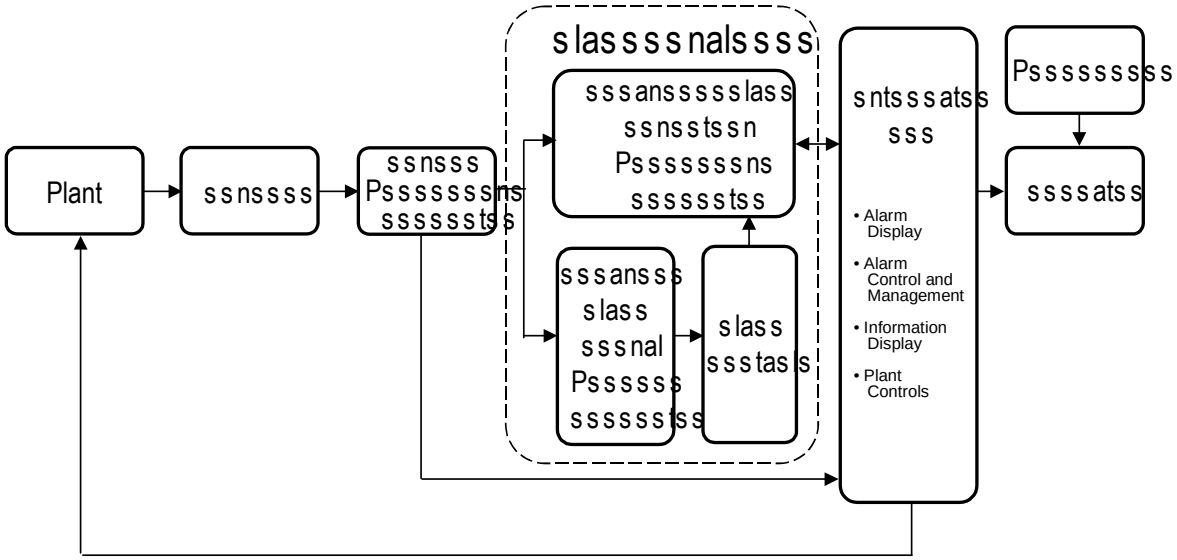

Figure A.2 Advanced alarm system and the operator

Figure A.3 depicts the major functional elements of an alarm system related to the role of the operator: Alarm Definition, Alarm Processing, Alarm Prioritization, Alarm Display, Alarm Response Procedures, and Alarm Control and Management. These elements are described in detail in the following sections and subsections and are reflected in the organization of the guidelines in Appendix B. In the following sections and subsections, three types of information are given: an introduction to the functional element, an identification of the types of information a reviewer should address, and a reference to the section in Appendix B that contains the guidelines for reviewing the topic. The functional elements are addressed as follows:

- Section A.2, Functional Capabilities, addresses alarm definition, alarm processing, and alarm prioritization.
- Section A.3, Alarm Information Representation covers alarm display characteristics related to formats for organizing and presenting alarm information.
- Section A.4, Alarm Display Devices includes alarm display characteristics related to display devices used for presenting alarm information.
- Section A.5, User-System Interaction, addresses alarm control and management characteristics that relate to the means (e.g., types of dialog) through which users interact with the alarm system.
- Section A.6, Alarm Controls, addresses input devices used for alarm control and management functions.
- Section A.8, Alarm Response Procedures, covers the procedures that personnel follow when responding to particular alarms.

Not depicted are considerations of general alarm system characteristics (described in section A.2.1), backup, test, maintenance, and failure indication capabilities (described in Section A.7), and integrating the alarm system with other components of the HSI (described in Section A.9).

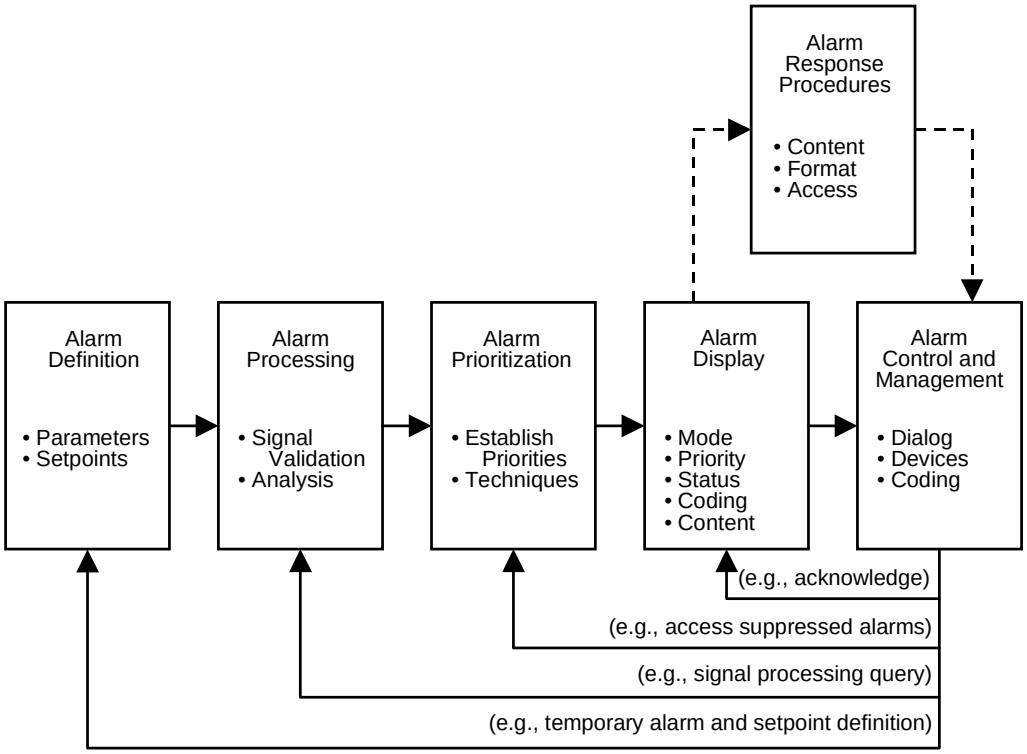

Figure A.3 Alarm system functional elements

A.2 Functional Capabilities of Alarm Systems

Functional capabilities refers to the information processing functions performed by an alarm system. The important characteristics and concerns associated with each of the major elements are discussed below.

A.2.1 General Alarm System Characteristics

General characteristics include the basic functions associated with alarm systems (i.e., to alert the operator, to present information to facilitate the operator's response, to assist in monitoring of events, to facilitate the operator's interaction with the plant) and the relationship between the alarm system and the rest of the HSI. The following general alarm system characteristics are important:

- Functional characteristics (e.g., alert, inform, feedback) of the alarm system.
- The methods by which consistency is established between the alarm system and (1) non-alarm HSI standards and conventions, and (2) general HFE principles, standards, and guidelines. A design guideline or system specification, which describes the design features and their technical basis, may be available from the designer or utility to meet this requirement.
- Development tests, evaluations, and validation tests of the system.

Guidelines for reviewing general characteristics of alarm systems are given in Section 4.1 of Appendix B.

A.2.2 Alarm Definition

Alarm definition is the specification of the process parameters monitored and displayed by the alarm system and the setpoints used to define alarm conditions. The following are important considerations for alarm definition:

- Alarm conditions (events or situations that represent challenges to plant safety):
  - challenges to critical safety functions
  - deviations in key plant parameters
  - conditions representing hazards to personnel
  - challenges to equipment having a safety function
  - deviations from technical specifications
  - deviations from emergency procedure decision points
  - safety considerations related to plant modes (i.e., from full power to shutdown)
- The criteria used for selecting alarm parameters related to alarm conditions
- The criteria for determining alarm setpoints
- The verification process (for task appropriateness):
  - process by which inclusion of alarms was checked
  - process for assuring that non-alarms are not presented by the alarm system
- Alarm states (new, acknowledged, cleared, and reset)

Section 4.2 of Appendix B has guidelines for the review of characteristics related to alarm definition.

A.2.3 Alarm Processing

Alarms in conventional plants tend to be stand-alone systems that alert operators to off-normal conditions and to the status of systems and components, and, by inference, the functions they support. After being alerted, the operators consult other indicators for specific information (e.g., they may determine the actual value of a parameter for which a low-level alarm has been activated). Such systems may confuse operators during certain transients because of the many nearly simultaneous annunciator activations with varying relevance to operator tasks. Thus, alarm processing techniques were developed to support operators in coping with the volume of alarms, to identify which alarms are most significant, and to increase the operator's understanding of plant conditions. Alarm processing addresses a fundamental aspect of system design, namely, which alarms are displayed to the operating crew.

<u>Alarm Signal Processing</u>

Alarm signal processing refers to the process by which signals from plant sensors are automatically evaluated to determine whether any of the monitored parameters have exceeded their setpoints, and to determine whether these deviations represent true alarm conditions. Alarm signal processing includes techniques for analyzing normal signal drift and noise signals. They are used to eliminate signals from parameters that momentarily exceed the setpoint limits but do not indicate a true alarm. Figure A.2 illustrates the incorporation of signal processing into the circuitry of an advanced alarm system.

Signal Validation Processing

Signal validation is a group of techniques by which signals from redundant or functionally related sensors are analyzed to identify and eliminate false signals resulting from malfunctioning instrumentation, such as a failed sensor. Alarm conditions that are not eliminated by the alarm signal processing may be evaluated further by alarm condition processing and other analyses before alarm messages are presented to the operator.

Alarm Condition Processing

Alarm condition processing refers to the rules or algorithms that are used to determine the operational importance and relevance of alarm conditions. This process determines whether the alarm messages associated with these alarm conditions should be presented to the operator. Figure A.2 illustrates alarm condition processing. Alarms screened by the alarm condition processing circuitry may or may not have already been screened by the alarm signal processing and validation circuitry. Also, the alarm condition processing circuitry receives inputs directly from the sensor processing circuitry to set the various values of logic that automatically determine how alarms are screened.

There are a wide variety of processing techniques. Advanced alarm processing systems often employ combinations of them. Each processing technique changes the resulting information provided to operators. For this discussion, four classes of processing techniques will be defined: Nuisance Alarm Processing, Redundant Alarm Processing, Significance Processing, and Alarm Generation Processing. The classes of processing techniques are described below, Table A.3.1 gives examples of each.

Nuisance Alarm Processing – This class of processing includes techniques that eliminate alarms having no operational safety importance. For example, mode-dependent processing eliminates alarms that are irrelevant to the current mode of the plant, e.g., the signal for a low-pressure condition may be eliminated during modes when this condition is expected, such as startup and cold shutdown, but be maintained during modes such as normal operation when this condition is not expected.

Redundant Alarm Processing – This class of processing includes techniques that analyze alarm conditions are true or valid but are considered to be less important because the information they provide is redundant with other alarms and theoretically supplies no new or unique information. For example, in causal-relationship processing, only causes are alarmed and consequence alarms are eliminated or their priority lowered. However, such techniques may minimize information that the operator uses to confirm that the situation represented by the true alarm has occurred, for situation assessment, and for decision making. Thus, in addition to quantitatively reducing alarms, processing methods may qualitatively affect the information given to the operating crew.

Significance Processing – This class of processing includes techniques that analyze for alarm conditions that are true or valid but are considered to be less significant than other alarm conditions. For example, in an anticipated transient without scram, alarms associated with minor disturbances on the secondary side of the plant could be eliminated or their priority lowered.

Alarm Generation Processing – This class of processing includes techniques that evaluate the existing alarm conditions and then generate alarm messages which (1) give the operator higher level or aggregate information, (2) notify the operator when unexpected alarm conditions occur, and (3) notify the operator when expected alarm conditions do not occur. These processing techniques, in effect, generate new (e.g., higher-level) alarm conditions. This processing presents an interesting paradox. Alarm systems should reduce errors, which often reflect the overloaded operator's incomplete processing of information. Alarm generation features may help mitigate these problems by calling the operator's attention to plant conditions that are likely to be missed. However, the single most significant problem with alarms systems, as reported in the literature, is the many alarm messages presented to the operator at once. Since alarm generation creates additional messages, it may exacerbate the problem.

Guidelines for reviewing alarm processing and reduction are given in Section 4.3 of Appendix B.

Table A.2.1 Alarm Processing Approaches

Category	Approach	Functional Description[1,2]
Nuisance	Status-alarm Separation	Separating status annunciators from alarms that require operator action.
Nuisance	Plant Mode Relationship	Alarms which are irrelevant to the current operational mode, such as start-up, are suppressed.
Redundant	Multi-setpoint Relationship	The relationship between multi-setpoints of a process variable is used to suppress lower priority alarms, e.g., when the level in the steam generator exceeds the high-high level setpoint, the high-level alarm is suppressed.
Redundant	State Relationship	Alarms associated with a well-defined situation, e.g., pump trip, are suppressed.
Redundant	Causal Relationship	The cause-effect relationship is used to identify alarms associated with causes while suppressing alarms associated with effects.
Significance	Relative Significance	Alarms associated with relatively minor disturbances are suppressed during more significant events.
Generation	Hierarchical Relationship	Using an alarms relationship with components, trains, systems, and functions, hierarchical alarms can be generated to provide operators with higher-level information.
Generation	Event Relationship	The unique pattern of alarms typically activated following the occurrence of an event is recognized and the potential initiating event is identified.
Generation	Alarm Generation	Alarms are generated when (1) conditions or events are expected to occur but do not occur (for example, when all control rods do not reach their fully inserted limits within a prescribed time after a scram) or (2) an alarm is expected but does not occur.

[1] For illustration purposes, the descriptions refer to alarm *suppression*, but filtering and prioritization can be also used.
[2] Functional descriptions are not intended to imply how the software accomplishes the processing.

A.2.4 Alarm Condition Priority and Message Availability

Alarm condition priority (or alarm prioritization) refers to a determination of the relative importance of all present alarm conditions to the operating crew. This determination is made by applying alarm condition processing in an advanced alarm system. The dimensions for evaluating the priority of alarm conditions should include the required immediacy of operator action, and the significance of the alarm condition to plant safety.

Alarm message availability refers to the process by which alarm messages are selected for presentation to the operators based on the priority of their alarm conditions. Thus, while two alarm messages may be valid for current plant conditions, one may be very important to the operator's role and should be emphasized, while the other message may be of less importance and should be de-emphasized. Techniques for alarm message availability highlight important alarm messages and play down less important ones. This differentiation supports the operator in focusing attention on those messages with the greatest operational significance.

Three alarm availability techniques are: filtering, suppression, and dynamic priority coding. They are defined below. The terms filtering and suppression sometimes are used interchangeably in the literature.

Filtering – alarms determined by processing to be less important, irrelevant, or otherwise unnecessary are eliminated and are *not available* to the operators.

Suppression – alarms determined by processing to be less important, irrelevant, or otherwise unnecessary are not presented to the operators, but can be accessed at their request (Figure A.4).

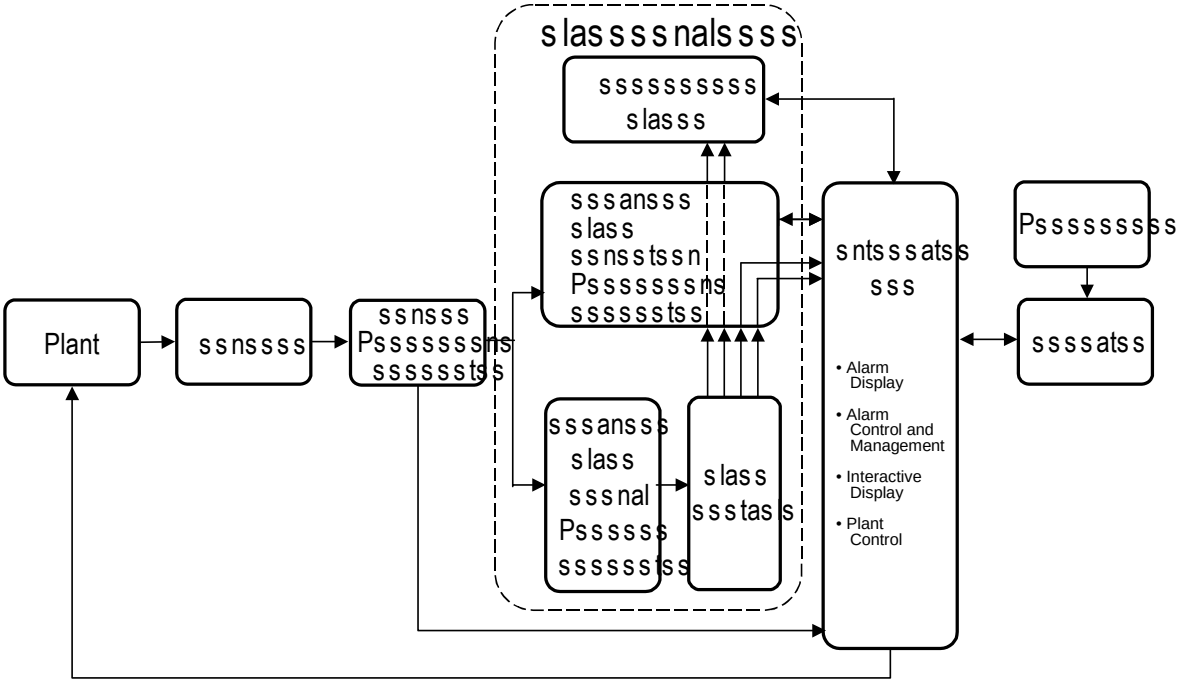

Figure A.4 Alarm suppression

Dynamic priority coding – the results of alarm processing are provided by segregating them into priority groupings (e.g., low and high priority) in contrast to filtering or suppressing alarms determined to be of lower priority.

A specific alarm system may employ a combination of these approaches. There are tradeoffs between them, and thus, an issue remains as to which method should be used or in what contexts the various options should be exercised. Filtering eliminates the possibility of less important alarms distracting the operators. However, the designer may be removing information useful for other purposes. Thus, the alarm system characterization should include a technical basis, such as the results of validation tests, that provide a basis for determining whether the processing method will function appropriately in all plant conditions. Suppression offers the potential benefits of filtering by removing distracting alarms. However, since such alarms are still accessible on auxiliary displays, they may impose an additional secondary task workload to retrieve them. Dynamic priority coding does not conceal any information from operators. However, the method requires operators to perceptually filter alarms, using the priority codes, to identify the higher priority messages. This method may be distracting because it displays messages of all levels of importance. The effect of these alternatives on the operator's performance needs to be considered in the HFE design review.

The reviewer should obtain information on the following:

- Dimensions used to prioritize alarms,
  - Need for operator action
  - Safety system challenge
  - Threat to critical safety function

- Number of levels of priority for each dimension
- Method for assigning priority:
  - Static prioritization (i.e., predetermined level of priority is assigned to each alarm condition)
  - Dynamic prioritization (i.e., level of priority assigned to each alarm condition is assigned from an analysis of current conditions, such as the plant's operating mode and the presence of other alarm conditions)
- Method used to remove low priority alarms from view:
  - Filtering (i.e., complete removal)
  - Suppression (i.e., available to operators upon request).

Guidelines for the review of alarm prioritization and availability are set out in Section 4.4 of Appendix B.

A.3 Alarm Information Display

Information display refers to the way that information is organized and displayed to control room personnel, in terms of elements, formats, and networks, as described in Section 1.0 of NUREG-0700. The following describes considerations specific to presenting alarm information. The various roles that NPP alarm systems serve are complex, e.g., showing a first alert to an anomaly or status and also additional information to aid operators in decision making. Alarm information may be auditory or visual. The auditory components of alarms capture the operator's attention to a change in the plant. The visual components guide attention to the appropriate alarm (by using techniques such as flashing) and show detailed information.

To support the different functions of the alarm system, multiple visual display formats may be required, such as a combination of separate displays (e.g., alarm tiles) and integrated displays (i.e., alarms integrated into process displays). Thus, the display format of alarm information and the degree to which it is presented separately or is integrated with other process information are important safety considerations.

Approaches to displaying alarms can first be characterized into three basic types:

1. Spatially dedicated, continuously visible (SDCV) alarm displays (i.e., alarms represented by individual display devices that are spatially dedicated and always visible, such as alarm tiles).
2. Alarm message lists (e.g., alarms are shown in the form of a temporary list, often based on the chronology of their occurrence).
3. Alarms integrated into process displays (e.g., displays representing plant processes include existing alarm conditions).

Other types of display are possible by combining the features of more than one of these.

For each of the different types, the following characteristics are important:

- General characteristics
  - Display functions (e.g., supporting the operator's monitoring and decision making)
  - Degree of independence of alerting and informing functions

- Degree of independence of priority and detailed information
- Principles and criteria for allocating alarms to major display types
- Graphics
- Consistency of alarm coding

- Display of high-priority alarms (e.g., methods used to distinguish the priority of alarms)
- Display of alarm status (e.g., methods used to represent new, acknowledged, and cleared states)
- Display of shared alarms (e.g., a single alarm that represents a change in more than one parameter)
- Alarm messages (e.g., content and format of alarm messages)
- Coding methods (e.g., visual and audible codes representing alarm information)
- Layout and organization of displays
  - SDCV alarm displays
  - Alarm message lists

If alarms are integrated into process displays, the reviewer should obtain information about the display's characteristics from NUREG-0700, Revision 1. The detailed arrangement of alarm information in these displays should be consistent with the guidelines for process displays (as per Guideline 4.1-4, Conformance to HSI Design Review Guidelines).

It is also important to consider whether the alarm display's elements (symbols, acronyms, labels, measurement units, and coding) are consistent with the ones in the rest of the HSI and procedures (as per Guideline 4.1-3, Consistency with the Main HSI).

Guidelines for reviewing alarm displays are given in Section 4.5 of Appendix B

A.4 Alarm Display Devices

The characteristics of the display devices used in the alarm system should be described, as discussed in Section 1.0. This should include the number, type, and placement of devices, and the characteristics of the individual devices, such as their quality and update rate.

A.5 User-System Interaction

User-system interaction refers to the types of interaction allowed between the user and the alarm system, and includes input formats, cursor characteristics, system response, interface management, the management of information, and error response. Alarm control and management refers to the capabilities for interacting with, and controlling, the alarm system. The control functions typically used in the nuclear industry are silence, acknowledge, reset, and test (SART) controls. The SART philosophy also applies to advanced alarm systems, where the control for operators' interaction may be more sophisticated and require greater flexibility than conventional systems.

In addition to the basic SART controls, newer alarm systems have many varied alarm-management functions. For example, the operator may be able to define temporary alarms, adjust setpoints, control filtering options, and sort

alarms according to many separate dimensions such as time, priority, and system. These dynamic aspects of the interface should be reviewed to avoid excessive workload demands, while preserving the overall functional characteristics of the alarm system. It is important to consider these dynamic aspects because they may be disruptive or confusing to operators, especially when the alarm system changes modes of operation.

Some of these capabilities may use more sophisticated methods of communication with the alarm system than is possible with traditional dedicated switches, or pushbuttons. The general method of communication between the operator and the alarm system, also called the dialog format, can include menu selection, command language, and special function keys (NUREG-0700, Revision 1 discusses various options for dialog design).

In certain situations, such as major process disturbances, it may be desirable to reduce the operator's workload by automating some alarm system functions, such as silencing lower priority alarms or temporarily stopping of unacknowledged alarm flashing. Similarly, automated controls may be implemented to trigger appropriate displays, such as alarm graphics, data windows, or display pages. These dynamic aspects of the alarm system may be disruptive or confusing to operators, especially when the alarm system changes modes of operation.

Therefore, the important considerations to be included in a characterization of alarm control and management capabilities include the following:

- General characteristics (e.g., defeating controls, access to new alarms)
- Alarm silencing capabilities (e.g., global and manual silencing)
- Alarm acknowledge capabilities (e.g., operation and effects of acknowledge action)
- Alarm reset capabilities (e.g., appropriate use and effects)
- Alarm management capabilities (e.g., operators' selection and control of alarm system configuration, and operator-defined setpoints)
- Automatic features (e.g., automatic alarm system configurations and mode-defined setpoints)

Section 4.6 of Appendix B has guidelines for reviewing the user-system interaction capabilities of alarm system functions.

A.6 Controls

The types of devices used to operate the computer-based communication system should be identified, including input devices and conventional controls, as described in NUREG-0700, Rev. 1. In conventional plants, the alarm silence, acknowledge, reset, and test functions are supported by dedicated, hardwired controls, such as pushbuttons. In advanced control rooms, the operator may interact with the alarm system through interfaces that are also used for other purposes. That is, the operator may use the same input or control devices (e.g., keyboard or mouse) to interact with the alarm system and with other controls or displays. Thus, the characterization of the controls used in an alarm system should identify the types of control device (e.g., pushbutton, switch, or touch screen) and the coding and demarcations which identify the control and its functions. In addition, the characterization should identify the following:

- where these controls are located
- how these controls are organized relative to each other
- how these controls are organized relative to other controls and displays that are used with them.

Section 4.7 has guidelines on this area.

A.7 Backup, Test, Maintenance, and Failure Indication

The alarm system must provide alarm information to the operator reliably. Important considerations include backup systems or capabilities that may be used if an alarm system fails or malfunctions, the means by which such information is communicated to the operator, and design features that support testing and maintenance of the alarm system. Each of these points is discussed below.

Backup Systems and Capabilities

The hardware and software components of the alarm system should have sufficient redundancy and diversity that their anticipated failures do not cause significant loss of functions or information. For example, the alarm system should allow the operators to obtain alarm information from an alternate display device if the primary device fails. Therefore, the alarm system characterization should include alternative display and control devices and methods of interaction with the alarm system. For example, in advanced alarm systems, indications associated with critical plant parameters may appear in multiple locations including dedicated alarm indicators, display pages depicting plant processes, alarm message displays, and an alarm printer. In addition, the individual devices used to interact with the alarm system should have redundancy and diversity features to protect against component failures (e.g., VDU reliability; dual light bulbs for annunciators).

Alarm System Test and Failure Indication Features

When the alarm system malfunctions, it should make this apparent to operators. NPP events have emphasized the importance of giving operators an active method of verifying the status of the alarm system itself (see, for example, Information Notice 93-47, U.S. NRC, 1993). Test controls provided in conventional control rooms traditionally have allowed operators to check the operation of the alarm display (e.g., detect burnt-out annunciator lamps), but not other portions of the alarm system, such as signal processing components. In addition, these test controls only tested the alarm system upon demand; they did not continuously monitor for anomalies. Since operators rely on the alarm system as the first indication of a process disturbance, it is important that advanced systems notify the operator of any loss of functioning. The characterization of alarm system testing and indication capabilities should include built-in test and continual test capabilities. These features allow testing with minimal interference of the operators' activities and provide prompt indications to personnel.

Maintenance Features

Maintenance features of the alarm system, like the test features, should be designed so that maintenance can be performed with minimal interference with the operators' activities. These features include modular components that can be rapidly removed and replaced, rear access panels which prevent maintenance work from obstructing the operator's view of controls and displays, tagged-out features, and maintenance aids.

Guidelines for the review of these characteristics are set out in Section 4.8 of Appendix B.

A.8 Alarm Response Procedures

Alarm Response Procedures (ARPs) provide more detailed information about the type of alarm condition than is given in the alarm message; typically, the source of the alarm (sensor), setpoint, causes, automatic actions, and operator actions. ARPs are especially important to operators when an unfamiliar alarm is activated or when an alarm seems inconsistent with the operator's understanding of the plant's state. ARPs may be hard copy or computer based.

The following characteristics of ARPs are important:

- ARP information content (e.g., descriptions of the alarms, operators' actions, and support material)
- ARP format (e.g., the way in which information is arranged)
- APR location (e.g., the accessibility of the APRs to control room personnel)
- Methods of user access to, and interaction with, ARPs (especially computer-based ARPs)

Guidelines for reviewing ARPs are given in Section 4.9 of Appendix B.

A.9 Integration with Other HSI Components

Control-display relationships and general layout significantly affect the operator's performance with alarm systems, as they do for other aspects of the HSI. The following considerations are important:

- Control console layout of alarm display devices and controls
- Alarm display layouts for VDUs
- Relationship between alarm controls and displays and the associated process indicators and controls
- Physical relationship between the operators and the alarm controls and displays, and the associated process indicators and controls

Guidelines for the review of control-display integration are provided in Section 4.10 of Appendix B.

Appendix B

Alarm System Guidelines

4.1-1 Alarm System Functional Criteria

The alarm system should:

- Alert the operator to the fact that a system or process deviation exists;
- Inform the operator about the priority and the nature of the deviation;
- Guide the operator's initial response to the deviation; and
- Confirm, in a timely manner, whether the operator's response corrected the deviation.

ADDITIONAL INFORMATION: . While the functional requirements for the alarm system assume the existence of a process deviation, it is found that operators actively use features of alarm system in the course of monitoring the plant during normal operations. Accordingly, if explicit HSI support for routine monitoring is not part of the overall information system design, the alarm system may serve this function as well. It should also be recognized that the alarm system must be effective in the context of ongoing fault management, and that the information it provides must not only meet the operators' requirements but must also be made available in ways that will not unnecessarily disrupt operators' response to deviations.[6105]

4.1-2 Operator Verification of Alarms

Operators should be able to rapidly confirm the authenticity of alarms.

ADDITIONAL INFORMATION: Operators need to be able to verify that alarms are true indications of the conditions they are intended to monitor and not the result of nuisance conditions, such as improperly calibrated equipment or maintenance activities.

Discussion: Operators concluding that alarms are spurious or nuisance alarms, such as the result of maintenance activities or improperly calibrated equipment, is a significant problem undermining the ability of the systems to achieve their functional purpose. Thus it is important for operators to be ascertain that alarms are real indications of the process conditions they are intended to represent. Further, the research reviewed in Section 4.2.2.1 of Brown, O'Hara, and Higgins (1998) , particularly the results reported by Bliss, Jeans, and Piroux (1996), suggest that operators should be made aware of sources of confirmatory information that they can use to judge the validity of alarms. Such material might be presented as part of alarm response procedures. The current guidance on alarm response procedures calls for operators to be provided with information about the sensor and validating logic associated with alarms, and to be advised of actions that operators can take to confirm the existence of an alarmed condition.

4.1-3 Alarm System Upgrade Functionality

A new alarm system that is installed into an existing control room should support all of the operator functions that the old system supported, in addition to satisfying the functional requirements of the SAR and various other functional criteria (such as those listed in Section 4.2).

ADDITIONAL INFORMATION: Operators use alarm systems in ways not always envisioned by the designers. Further, as discussed in Guideline 4.1-1 above, the function of an alarm system may change from control room to control room depending on the design of other control room HSI resources such as the information system. When an alarm system is replaced, an analysis of the functional use of the old system should be conducted in conjunction with operations personnel to assure that safe operation is not compromised by removing an information source and not replacing it in the new alarm system. For example, operators frequently use alarm systems to determine overall plant status. It should be noted that the specific roles that an alarm system plays in a plant depend on the overall design of the HSI of which the alarm system is only a part. Thus, for example, the use of alarm systems to determine overall plant and system status may not be necessary in advanced plants where large plant and system overview displays are available to the operating staff.[6105]

Discussion: The importance of the multiple purposes for which operators use alarm systems has been noted by many researchers (e.g., Fink et al., 1992; Kragt et al., 1983; MPR Associates, 1985; O'Hara et al., 2000; Sheehy et al., 1993). For example, MPR Associates (1985) evaluated the role of alarm systems in the operator's decision making during off-normal conditions. Several specific uses were identified:

- Support for the determination of the status of various systems or components (an aspect of the alarm system that may be lost when a conventional system is replaced with a advanced system).
- Alert to a simple malfunction where simple "rule-based" action is used.
- Facilitate the operator's recognition of the need to branch to alternate sections of the procedures during use of emergency operating procedures (EOPs).
- Provide both high-level and system/component level information to the operator to support more abstract, knowledge-based responses to plant upsets in situations where appropriate immediate actions/strategies are not clear.
- Provide feedback functions such as the return to normal status.
- Indicate the need for Site Emergency Plan activation.

Thus, the alarm system supports the operator's goal-directed information processing which has been found to play a role at all levels of abstraction.

In addition, this guideline is consistent with the high-level design review principles of Task Compatibility and User Model Compatibility.

4.1-4 Consistency with the Main HSI

The alarm system HSI should be consistent with the standards and conventions used for the HSIs for other displays and controls in the control room.

ADDITIONAL INFORMATION: The alarm system should use the same conventions such as symbols, icons, acronyms, coding, and measurement units that are used in the main HSI displays and procedures. While some minor differences may exist, the alarm system should never use a display feature, such as coding, in a way that is different from or conflicts with other HSIs. For example, if color is used to code priority, it should have the same meaning in the alarm system as in the process displays.[6105]

Discussion: This guideline is consistent with the high-level design review principle of Consistency.

4.1-5 Consistency with Emergency Operating Procedures

The alarm system HSI should be consistent with the standards, conventions, and terminology used in the plant emergency operating procedures.

ADDITIONAL INFORMATION: The alarm system should use the same conventions, such as terminology for plant systems and equipments, identification codes for plant components and parameters, and measurement units, that are used in the main HSI displays and procedures. Defined values, such as alarm setpoints, should be consistent. In addition, if the procedures use coding to present information, such as in graphical displays of a computer-based procedure system, then the alarm system should use the same conventions, such as symbols, icons and coding. For example, if color is used to code priority, it should have the same meaning in the alarm system as in the displays of a computer-based emergency operating procedure.[6105]

Discussion: This guideline is consistent with the high-level design review principle of Consistency.

4.1-6 Conformance to HSI Design Review Guidelines

Alarm system elements (e.g., displays and controls) should conform to general HSI guidance as well as alarm system guidelines.

ADDITIONAL INFORMATION: While alarm system guidance takes precedence over other more general HFE guidance, it should be kept in mind that the alarm system is a part of the overall HSI. As such, it should conform to the same guidelines for general display and control design. For example, if the alarm system uses a touch screen interface for operator input and query of the system, the review guidance for touchscreens (Section 3.2.4) should be used to evaluate that aspect of the interface. As another example, if the alarm displays are integrated into P&ID VDU displays, the P&ID aspect to the display, such as icons and symbols, should be evaluated using Sections 1.2.8 and 1.3.4. *In the event of overlap or conflict in guidance, the guidance for alarm systems takes precedence when reviewing the alarm system.*[6105]

4.1-7 Alarm System Validation

The effectiveness of the alarm system should be validated through real-time, dynamic simulation.

ADDITIONAL INFORMATION: Alarm system design has historically been a problem in complex process control systems in general and NPPs in particular. While HFE guidance addresses many design issues, there remain aspects of alarm system design review that are not adequately addressed by HFE guidelines. Thus, the functionality of the system should be assessed through dynamic performance evaluation that addresses both (1) the HSIs associated with operation of the alarm system, and (2) the quality, accuracy, timing, and usefulness of the information provided by the alarm system to plant personnel.[6105]

4.2-1 Alarm Selection

The following criteria should be included in the basis for selecting alarm conditions:

- Monitoring critical safety functions and key parameters,
- Preventing personnel hazards,
- Avoiding significant damage to equipment having a safety function,
- Assuring that technical specifications are met,
- Monitoring emergency procedure decision points, and
- Monitoring plant conditions appropriate to plant modes ranging from full power to shutdown.

ADDITIONAL INFORMATION: One of the key aspects of an alarm system is to support operators in ensuring that the plant remains within the safe operating envelope as defined by the Safety Analysis Report (SAR) and technical specifications. This includes ensuring that automatic systems can still perform their intended functions to protect the plant and personnel. This assurance can be provided in a number of ways by the alarm system with the monitoring of critical safety functions and key parameters being a typical choice. Selection of alarms should consider all operational modes including shutdown. After a scheme for selecting alarm conditions has been developed and applied, the selected alarm conditions should be reviewed to verify that important aspects of all of the above categories are addressed within the main control room alarm system.[0700, 6105]

Discussion: Several researchers, such as Beattie and Vicente (1996) found that the alarm systems may be deficient in their support for plant conditions that are representative of full power, e.g., during maintenance outages.

4.2-2 Timely Warning

Alarm set points should be determined to ensure that the operating crew can monitor and take appropriate action for each category of alarms, e.g., respond to out-of-tolerance conditions, in a timely manner.

ADDITIONAL INFORMATION: Alarms are established to help ensure that the plant remains within SAR and technical specification limits. In order to achieve this, the setpoints may be specified at conservative levels that are well before the actual limits to allow sufficient response time for operators and plant systems. Thus, where practical, alarm setpoints should be determined such that the operator is alerted before a major system or component problem results in a condition which causes a loss of availability (e.g., plant trip), equipment damage, violation of SAR and technical specification requirements, or other serious consequences. Other criteria are acceptable if they do not compromise these factors.[6105, 0700]

Discussion: This guideline is consistent with the high-level design review principle of Timeliness.

4.2-3 Setpoint Determination and Nuisance Alarm Avoidance

The determination of alarm setpoints should consider the trade-off between the timely alerting of an operator to off-normal conditions and the creation of nuisance alarms caused by establishing setpoints so close to the "normal" operating values that occasional excursions of no real consequence are to be expected.

ADDITIONAL INFORMATION: When determining setpoints, consideration should be given to the performance of the overall human-machine system (i.e., operator and alarm system acting together to detect process disturbances). If setpoints are established such that many false alarms occur, operators become less likely to respond to the alarm, especially when their tasks become cognitively demanding.
Processing techniques (see Guideline 4.3-4) are applied to prevent normal variation from producing alarms. Under some circumstances, however, preventing such alarms may deprive operators of needed information. In cases where raising an alarm's setpoint or delaying its presentation is not acceptable, more sophisticated techniques (e.g., alarms based on rate of change of the parameter or the time at which the parameter is projected to exceed a setpoint) should be considered. [6105, 0700]

Discussion: Process control operators are in a monitoring environment that has been described in signal detection terms as an "alerted-monitor system" (Sorkin et al., 1985 and 1988). This is a two-stage monitoring system with an automated monitor and a human monitor. The automated monitor in a NPP is the alarm system which monitors the system to detect off-normal conditions. When a plant parameter exceeds the alarm criterion, the human monitor is alerted and must then detect, analyze, and interpret the signal as a false alarm or a true indication of a plant disturbance. Both the human and automated monitors have their own specific signal detection parameter values for sensitivity and response criterion. For the human monitor, both parameters are strongly affected by alarm system characteristics including set points, the presence of nuisance and false alarms, and alarm density. A significant issue associated with alerted-monitor systems is that optimal overall performance of the alerted-monitor system is a function of the interaction of both components. Optimizing the signal detection parameters for one component of the system may not optimize performance of the entire two-stage system. An alarm setpoint philosophy frequently employed is to attempt to optimize the detection of signals by

the automated monitor subsystem. The response criterion is set to minimize missed signals. This, however, increases the false alarm rate, thus increasing the noise and lowering the operators' confidence in the alarm system.

Bliss and co-workers have conducted a series of laboratory studies of mistrust of alarms. Bliss, Gilson and Deaton (1995) developed a procedure which demonstrated mistrust of alarm in a laboratory context. They examined subjects' responses to alarms of varying reliability in a dual-task paradigm, measuring the accuracy and speed of responses to alarms which occurred as the subjects performed a cognitively demanding primary task. Different groups of subjects responded to alarms of different reliability. Most subjects' rate of responding to alarms roughly matched the expected probability of a true alarm. Subjects responded more often to high-urgency alarms than to low-urgency alarms, regardless of alarm reliability condition. Response time, however, did not differ as a function of alarm reliability or urgency. The authors suggest that, because of the sensitivity of subjects' responses to the reliability of the alarms, avoiding false alarms is critical in designing alarm systems.

Bliss and McAbee (1995) considered whether differences in the criticality of the primary task would affect subjects' responses to alarms under circumstances similar to those described above. The criticality of the primary task was manipulated by adjusting the penalties (points lost) for marginal performance on the task. Subjects responded to a greater proportion of alarms when the primary task criticality was low than when it was moderate or high. The results are interpreted as indicating that the effects of operator mistrust of alarm systems may be exacerbated when the operators' tasks are most demanding. The authors suggest that redundant alarm systems might be used to increase reliability, or that during critical periods the task of alarm response might be performed by a second operator who does not have primary responsibility for the critical task.

In another study using procedures similar to those described above, Bliss, Dunn, and Fuller (1995) investigated methods of increasing the frequency of responding to alarms. The experiment indicated that providing information that alarms would be more reliable than they had been in a previous session increased the subjects' rate of responding to the alarms. The authors conclude that since response rate was sensitive information provided to the subjects, appropriate alarm responding by operators of complex processes might be encouraged through training.

Bliss, Jeans, and Piroux (1996) examined the effects of providing information about the overall reliability of an alarm system and about the validity of individual alarms. Two types of information about the reliability of the alarm signals were defined: information about the validity of individual alarm signals and information about the overall reliability of the alarms consisted of verbal instructions to the subject, as in experiments previously described. Different groups of subjects received one or the other type of information, both types of information, or no information regarding reliability. Subjects who received information about overall reliability responded more frequently than the other groups. Those receiving information about the validity of individual alarms responded to fewer alarms, but were correct more often. Based on the results, the authors recommend that, to the extent possible, redundant sources of information be made available to operators for every alarmed condition.

In addition, this guideline is consistent with the high-level design review principles of Cognitive Compatibility and Timeliness.

4.2-4 Darkboard Configuration

Candidate alarms and setpoints should be chosen so that no alarms are active for the normal operating conditions of the plant.

ADDITIONAL INFORMATION: This has traditionally been referred to as the dark board (or blackboard) concept. Typically, this condition will be full power operation, with all systems lined up in their most typical configuration for full power operation. This concept has implications for the plant's operating philosophy as well, including issues such as (1) repairing failed equipment expeditiously, (2) taking corrective actions for instrument drifts that cause alarms, and (3) correcting conditions that frequently lead to repeat alarms.[0700,6105]

4.3-1 Assured Functionality Under High Alarm Conditions

The alarm processing system should ensure that alarms which require immediate operator action or indicate a threat to plant critical safety functions are presented in a manner that supports rapid detection and understanding by the operator under all alarm loading conditions.

ADDITIONAL INFORMATION: Alarm processing should be provided to ensure that alarm functional criteria (see 4.1-1, Alarm System Functional Criteria) are not lost under any operational or accident conditions. The alarm system should provide the capability to reduce the number of concurrent alarm messages so that during off-normal conditions, the alarm system does not overload of the operator's cognitive processes. Special attention should be given to the problem of "secondary disturbance detection," i.e., detection of a second malfunction following the presentation of alarms related to an initial disturbance.[6105]

Discussion: While guidance documents generally agree that alarm processing and reduction are features necessary to achieve an effective alarm system, especially under high alarm conditions, there is conflicting evidence regarding how these objectives can be met and what the specific effects are on human performance. The major conclusion from key research in this area (summarized below) is that alarm processing effects are complex and need to be carefully reviewed for each specific application. However, comprehensive HFE guidance is not yet available.

The HALO (Handling Alarms with Logic) alarm system was developed by the Halden Reactor Project in Norway and tested to determine its effects on operator performance. In an initial study, inexperienced students were trained with the system and were asked to identify disturbances in a simulated pressurized water reactor (Marshall, 1982). Alarm information was presented as (1) unfiltered message lists, (2) filtered message lists, or (3) filtered message lists with an overview display. Alarm information was presented in static displays rather than dynamic simulation. Diagnosis time and accuracy were the primary dependent variables. The results indicated that accuracy was improved with filtering, but the benefit was specific with respect to the plant transient. No significant difference was found for operator response times. Also no differences were observed between the filtered message list used alone and the filtered list used with the overview display.

More recent studies evaluated the alarm processing and display characteristics of HALO (Baker et al., 1985a and 1985b; Marshall and Owre, 1986). Three alarm systems were compared: (1) an unfiltered text-based version of conventional alarms presented on a CRT, (2) a filtered text-based version of alarms presented on a CRT, and (3) a filtered text/symbolic-based version of alarms presented on a CRT. In the latter condition, top-level alarm schematic overview displays of the plant were presented on a CRT. When an alarm activated, symbols representing the appropriate subsystems would blink (red if high priority and yellow if not). The operator could then move to a second-level display which was an enlarged schematic presented on a separate CRT. Flashing symbols indicated the problem system. Text-based alarm messages were provided. An alarm keyboard was used to interface with the alarm system. The filtering system reduced the alarms by approximately fifty percent; the filtered alarms were not available to the operator. The principal dependent variables were detection time and percentage, diagnosis time and percentage, percentage of checks, and percentage action. Process variables and subjective evaluations were also measured. Seven crews of two operators each used the three systems in 12 simulated scenarios. Filtering of alarms had little effect on observed performance. It was observed that the detection of events decreased from 81 percent to 51 percent when the event occurred late in a scenario rather than early in a scenario. This statistically significant result demonstrated the failure of the alarm system to achieve its primary function of alerting the operator to off-normal conditions when high alarm conditions exist. None of the systems tested helped to mitigate the problem. One potential problem with interpreting the results of this study is that the display type and use of alarm filtering were experimentally confounded. Thus, no conclusions with respect to the *independent* effects of display mode or filtering can be made.

These results conflict with previous findings (reported above) that alarm filtering improves diagnostic accuracy (Marshall, 1982). In part, the difference may be explained by the fact that the earlier tests were performed using inexperienced subjects viewing static displays rather than dynamic simulations.

Fujita and Sanquist (1988) used a simulator to investigate the effects of alarm filtering on the operator's information processing. Verbal protocol analysis was used to measure the operator's cognitive processes. The protocols were taken in real time from three operators during simulated malfunctions. The investigators found the method to be weak and not very successful for revealing decision-making strategies. None the less, they found that although the operators expressed support for the alarm filtering system, no evidence was found that it had a positive effect on their performance.

As part of research conducted by Mitsubishi in support of development of the Dynamic Priorities Alarm System (DPAS), Fujita and Kawanago (1987) found that operators preferred to have status alarm information presented to them rather than to have status information filtered out. Color was used to support the operators in distinguishing between status and alarm information.

In another more rigorous test (Fujita, 1988 and 1989), DPAS reduced the number of high-priority alarms through mode, multi-setpoint, and cause-consequence alarm processing. Alarms were displayed on a combination of tiles and CRTs. The tiles were the primary display mode. Each tile was capable of being lit in three colors. The CRT displays used the same color coding conventions. Performance with and without the new system was compared. Nine crews of three experienced operators used the systems during simulated scenarios involving single and multiple failure events. Operator performance measures included time to identify initiating event, time to identify second malfunction, time to take control action, and alarm utilization frequency. No difference between the two systems was found for initiating event identification; however, detection time for second malfunctions was significantly reduced in three of the four scenarios when the alarm handling system was available. Thus, it was concluded that the alarm handling system helped reduce the operator's "mental fixation" on the initiating event. Scenario effects were again observed. DPAS

significantly reduced the time required to take a control action in two of the four test scenarios. The finding that second malfunction detection time was reduced with the alarm handling system is not consistent with the findings from the HALO research reported earlier where secondary event detection was not enhanced. There are several possible reasons for the discrepancy, i.e., scenario differences, the implementation of the alarm handling logic, and the alarm system's integration with the control room controls and displays.

Finally, in a study conducted for comparing conventional and CRT-based alarm presentations (Fink et al., 1992), one of the experimental conditions included a CRT presentation of alarms where the typical alarms associated with reactor and turbine trip were suppressed. This presentation reduced the number of "maverick" alarms (those not typically occurring during a plant trip) that were missed by the operators by approximately 50 percent in comparison to a typical tile display. However, it was noted that one operator objected to such suppression because he believed that the timing of some of the normal trip-related alarms facilitated the crew's understanding of transients.

In summary, the results of the research discussed above on the effects of alarm processing on operator performance do not provide a technical basis on which to develop more definitive review guidance. While no negative performance effects were observed, two studies (Baker, 1985a and 1985b, and Fujita and Sanquist, 1988) found little effect due to alarm filtering. One study (Fujita, 1988 and 1989) found no effect for the detection of initial disturbances, but found improved performance in the detection of secondary malfunctions (which is a significant problem). Another study (Fink et al., 1992) found a positive effect on detection of unusual alarms, but raised a question regarding possible trade-offs with the loss of information making the operator's understanding of events more difficult. Finally, interaction effects with scenarios seems to be an important consideration.

In addition, this guideline is consistent with the high-level design review principles of Cognitive Compatibility, Situation Awareness, Task Compatibility, and Timeliness.

4.3-2 Alarm Reduction

The number of alarm messages presented to the crew during off-normal conditions should be reduced by alarm processing techniques (from a no-processing baseline) to support the crew's ability to detect, understand, and act upon all alarms that are important to the plant condition within the necessary time.

ADDITIONAL INFORMATION: Since there is no specific guidance on the degree of alarm reduction required to support operator performance, the designer should evaluate the system with operators to assess the effectiveness of the alarm reduction process. This assessment should include evaluations that simulate the operation of the alarm system under situations that activate multiple alarm conditions and/or generate increased operator workload. The use of dynamic mockups and prototypes of the alarm system and dynamic control room simulators should be considered when developing these assessments.[6105]

Discussion: While it is clear that the number of unprocessed alarms is overwhelming to operators and that processing techniques can reduce the number of alarms (Cory et al., 1993; Gertman et al., 1986), little research exists that provides more specific guidance on what number of alarms is an appropriate target. Hollywell and Marshall (1994) found that operators preferred CRT alarm message rates of not more than 15 messages per minute and that when the rate increased the number of missed alarms increased. This of course depends on the alarm display and types of message design implemented. It has also been found that reducing the number of alarms by 50% has little effect on operator performance (Baker, 1985a). O'Hara et al. (2000) compared a condition in which there was no alarm processing to a condition in which nuisance alarms were identified and a condition in which both nuisance and redundant alarms were identified. Operators generally favored the maximum amount of alarm reduction, noting that it was difficult to find new alarms when the number of active alarms was high. However, no specific guidance can be offered based on this study or other research as to how much reduction is effective in aiding performance. In terms of operator processing of alarm information, it is probably inappropriate to specify alarm reduction in terms of absolute numbers of alarms (a metric often used to assess alarm reduction schemes). The demands placed on operators' information processing resources depend not only on the absolute number of alarms, but on their rate, their recognizability as familiar patterns, their predictability, and the complexity of the operator's ongoing task. The compatibility of the alarms' manner of presentation with the operator's tasks will also influence the burden associated with the alarms. Woods (1995) argues for alarms being designed so that each incoming alarm does not unconditionally demand a shift in the operator's attention and an interruption of ongoing activities. If alarm information is conveyed using techniques designed to minimize the attentional resources required to process each indication, the number of alarms presented to operators would be less important. This guideline is consistent with the high-level design review principles of Cognitive Compatibility, Situation Awareness, Task Compatibility, and Timeliness.

4.3-3 Alarm Signal Validation

Sensor and other input signals should be validated to ensure that spurious alarms are not presented to plant personnel, due to sensor or processing system failure.

ADDITIONAL INFORMATION: Instrumentation failure is not a common problem in NPPs. However, when such failures occur such as a failed sensor, biased or false signals are generated. The use of these signals by the alarm system may result in the presentation of either false or nuisance alarm messages. Such alarm messages are misleading and may interfere with the crew's situation assessment or reduce the crew's confidence in future alarm messages. Signal validation is a set of alarm processing techniques by which signals from redundant or functionally related sensors are

compared and analyzed to determine whether a true alarm condition exists. The purpose of these techniques is to prevent the presentation of false alarms to the operator due to malfunctioning plant instrumentation. Hence, signal validation should be included in an advanced alarm system.[6105]

Discussion: This guideline is consistent with the high-level design review principles of Cognitive Compatibility, Situation Awareness, and Task Compatibility.

4.3-4 Parameter Stability Processing

The alarm system should incorporate the capability to apply time filtering, time delay, or deadbanding to the alarm inputs to allow filtering of noise signals and to eliminate unneeded momentary alarms.

ADDITIONAL INFORMATION: Noise from plant instrumentation may result in signals that momentarily exceed the limit for alarm message activation for a plant parameter. Time delay processing prevents this signal from generating a spurious alarm message to the crew. In some cases, these applying these techniques may reduce the timeliness of the information provided to operators. When this tradeoff is not acceptable, other processing methods can be used (see additional information for Guideline 4.2-3). [6105]

Discussion: Using a high-fidelity simulation of an advanced control room, O'Hara et al. (2000) compared a condition in which there was no alarm processing to a condition in which nuisance alarms were identified and a condition in which both nuisance and redundant alarms were identified. Time delay processing was part of the nuisance alarm processing. Operators commented that when alarms identified as nuisance alarms were segregated on a separate VDU list, they did not see any alarms on that list that were important to their handling of the situation. Thus the application of this technique reduced the number of alarms without interfering with operator performance.

4.3-5 Alarm-Status Separation

Status indications, messages that indicate the status of plant systems but are not intended to alert the operator to the need to take action, generally should not be presented via the alarm system display because they increase the demands on the operators for reading and evaluating alarm system messages.

ADDITIONAL INFORMATION: While status information is important to operators, status indications which do not meet the functional definition of an alarm condition should be presented to operators via a non-alarm display, e.g., on process displays. If the presentation in the alarm display of status indications is justified on the basis of the unique aspects of the design, such status messages should be designed so that operators may readily distinguish them from true alarm messages.[6105]

Discussion: Many studies have found that operators use the alarm system to obtain status information and that under some conditions they prefer to have status alarm information presented to them rather than to have status information eliminated (Kragt and Bonton, 1983, Fujita and Kawanago, 1987, MPR Associates, 1985, Sheehy et al., 1993). In a study of alarm processing using a high-fidelity simulation of an advanced control room, O'Hara et al. (2000) examined a condition in which nuisance alarms were (including status indications) were presented on a separate VDU list. Operators indicated that they did not see any alarms on that list that were important to their handling of the situation. Thus the application of the technique in this case reduced the number of alarms without interfering with operator performance. The issue as to whether to include status indications in an alarm system is mainly a question of how the criteria for alarm selection are defined and what capabilities are provided by other portions of the HSI for displaying plant status indications in a manner that rapidly informs the operator but does not interfere with the operator's ability to handle alarm messages. In addition, this guideline is consistent with the high-level design review principles of Cognitive Compatibility, Situation Awareness, and Task Compatibility.

4.3-6 First-Out Processing

As an aid to diagnostic procedures and root cause analysis, provision should be made for identifying the initiating event associated with automatic plant trips through the use of first-out alarms.

ADDITIONAL INFORMATION: In conventional alarm systems, first-out alarms, which identified the parameter within an interrelated group which first exceeded its setpoint, were provided to support operators in determining the initiating cause of a reactor or turbine trip. Advanced alarm systems should include this first-out capability along with the results of any additional processing that could improve the identification of the initiating event.[0700, 6105]

4.3-7 Mode Dependence Processing

If a component's status or parameter value represents a fault in some plant modes and not others, it should be alarmed only in the appropriate modes.

ADDITIONAL INFORMATION: The following is an example of mode dependent processing. The fact that a particular pump has shutdown may only have operational significance to the crew when the plant is operating in the power range. Mode dependent processing would allow this alarm message to be presented when the plant is in the power range but not when it is in other modes (e.g., hot standby). Strategies have also been described in which different alarm setpoints are in effect for some parameters depending on plant mode. When there may be mode-dependent changes in the alarm system's responses the cautions contained in Guideline 4.7-7, Automatic Mode-Defined Setpoints should be considered.[6105]

Discussion: Using a high-fidelity simulation of an advanced control room, O'Hara et al. (2000) compared a condition in which there was no alarm processing to a condition in which nuisance alarms were identified and a condition in which both nuisance and redundant alarms were identified. Mode dependence processing was part of the nuisance alarm processing. Operators commented that when alarms identified as nuisance alarms were segregated on a separate VDU list, they did not see any alarms on that list that were important to their handling of the situation. Thus the application of this technique reduced the number of alarms without interfering with operator performance.

The improved annunciation strategy for CANDU plants developed by AECL (Davey et al., 1995) uses 'dynamic thresholding' of setpoints for a limited number of parameters; i.e., alarm thresholds depend on operating context (e.g., reactor power). Similarly, a description of the PIPS (Plant Information Processing System) being developed for future Korean nuclear power plants by KAERI (Suh et al., 1996) mentions that "any alarm has variable alarm setpoints assigned which are a function of plant operating mode."

4.3-8 System Configuration Processing

If a component's status or parameter value represents a fault in some system configurations and not others, it should be alarmed only in the appropriate configurations.

ADDITIONAL INFORMATION: The following is an example of system configuration processing. The fact that a particular pump has a low discharge pressure may only indicate a fault when the associated fluid system is configured to perform a particular function. Other discharge pressures may be appropriate when the fluid system is configured to perform a different function. In addition, a low pump discharge pressure may not be relevant when the fluid system is taken out of service. System configuration processing would allow the alarm message for pump discharge pressure to be presented when the fluid system is in the proper configuration and prevent its presentation when the system is in an alternate configuration.[6105]

Discussion: Using a high-fidelity simulation of an advanced control room, O'Hara et al. (2000) compared a condition in which there was no alarm processing to a condition in which nuisance alarms were identified and a condition in which both nuisance and redundant alarms were identified. System configuration processing was part of the nuisance alarm processing. Operators commented that when alarms identified as nuisance alarms were segregated on a separate VDU list, they did not see any alarms on that list that were important to their handling of the situation. Thus the application of this technique reduced the number of alarms without interfering with operator performance.

4.3-9 Logical Consequences Processing

If a single event invariably leads to subsequent alarmed events that are the direct consequence of this event, only the alarm message associated with the main event may be presented and the other alarm messages suppressed, so long as this does not interfere with the operators' use of alarm information.

ADDITIONAL INFORMATION: For example, logical sequences processing may be used to suppress alarms that follow as a logical consequence of trip or isolation conditions. When implementing logical consequences processing, the designer should ensure that messages associated with the "consequence" alarm conditions are not needed by the operators for other operational tasks, and that operators are aware that the associated "consequence" alarm conditions were generated but not presented. This guideline only suggests suppression of these alarms, not their complete elimination (i.e., filtering).[6105]

Discussion: The suppression of alarms, such as the typical alarms associated with reactor and turbine trip, has been shown to reduce the number of "maverick" alarms (those not typically occurring during a plant trip) missed by the operators by 50 percent (Fink et al., 1992). However, it should be noted that some operators may object to such suppression since the timing of some of the normal trip-related alarms facilitates the crew's understanding of transients. In a study of alarm processing using a high-fidelity simulation of an advanced control room, O'Hara et al. (2000) compared a condition in which there was no alarm processing to a condition in which nuisance alarms were identified and a condition in which both nuisance and redundant alarms were identified. Logical consequences processing was part of the redundant alarm processing. Operators commented that when alarms identified as nuisance alarms were segregated on a separate VDU list, they did not see any alarms on that list that were important

to their handling of the situation. Thus the application of the technique in this case reduced the number of alarms without interfering with operator performance.

4.3-10 Exceptions to Expected Alarm Patterns

The system should notify the operator when "unexpected" alarms occur, if the alarm processing logic can support such an analysis.

ADDITIONAL INFORMATION: Such an analysis may apply, for example, during certain transients (e.g., reactor scram) where the expected alarm pattern is well known.[6105]

Discussion: EPRI research (Fink et al., 1992) has found that CRT presentations were superior to tiles for highlighting alarms that were "unusual" for a given transient. In addition, this guideline is consistent with the high-level design review principle of Situation Awareness.

4.3-11 Absence of Expected Alarm Patterns

The system should notify the operator when "expected" alarms do not occur, if the alarm processing logic can support such an analysis.

ADDITIONAL INFORMATION: Such an analysis may apply, for example, during certain transients (e.g., reactor scram) where the expected alarm pattern is well known.[6105]

Discussion: Processing techniques which generate new alarms present a paradox. Alarm systems should facilitate the reduction of heuristics-initiated errors which often reflect the overloaded operator's incomplete processing of information (Norman, 1988; Reason, 1987, 1988, 1990). Alarm generation features may help mitigate these problems by calling the operator's attention to plant conditions that are likely to be missed due to the operator's bias toward "capture" errors. However, this type of alarm processing should be used judiciously because the generation of new alarms has the potential of increasing demands on operators, thus potentially exacerbating the original problem. Roth and O'Hara (1998) conducted a study of the integration of advanced interfaces, including an advanced alarm system, into a control room. Among the features of the alarm system was the provision of alerts when automatic safety system did not actuate as expected or when an event was not proceeding as expected. Crews were observed during their initial training with the new system on a full-scope simulator, and interviews were conducted with operators and other utility and vendor personnel. The training included full-scope simulations of plant disturbances. Operators repeatedly remarked that support for detecting unexpected events was a particular strength of the advanced system, since aid was most useful in circumstances that were ‘out of the ordinary.' In addition, this guideline is consistent with the high-level design review principle of Situation Awareness.

4.3-12 Intelligibility of Processed Alarm Information

Processing methods should not be so complex that operators have difficulty evaluating the meaning or validity of the resulting alarm messages.

ADDITIONAL INFORMATION: Complexity of the processing impacts the operator's ability, as the system supervisor, to understand the results of alarm processing and to understand its constraints and limitations. Since the alarm system is the operator's first indication of process disturbances and operators will confirm the validity of alarm signals prior to taking action, it is essential that operators easily comprehend the meaning of alarm data, how they are processed and the bounds and limitations of the system. An alarm system that combines multiple processing methods should not be so complex that it cannot be readily understood and interpreted by the operators who must rely on the system's information. If operators are unaware of the relationships among displayed alarms and how those relationships might depend on the processing being applied, they may draw incorrect conclusions about the state of the system or the reliability of the alarms. [6105]

Discussion: In a study of alarm processing using a high-fidelity simulation of an advanced control room, O’Hara et al. (2000) compared a condition in which there was no alarm processing to a condition in which nuisance alarms were identified and a condition in which both nuisance and redundant alarms were identified. When commenting on conditions in which a high degree of processing was applied, operators expressed concern over processing complexity, stating that the alarm system should not be so advanced that operators do not understand what it is doing functionally and logically; they were also concerned about the loss of potentially important information. Operators generally expressed the idea that alarm processing needs to be performed with caution. McDonald and colleagues have extended the ‘cry-wolf’ research to situations in which multiple alarms are presented simultaneously. Using methods similar to those of Bliss et al., they examine subjects’ responses to small arrays of simulated alarms. McDonald, Gilson, Mouloua, and Deaton (1995) examined whether subjects' confidence in the validity of alarms is influenced by the number of other alarms present in a display. Subjects recorded their confidence that a 'test' alarm was valid. There was a roughly linear relationship between the number of other alarms present and subjects' confidence in the 'test' alarm - this in spite of the fact that the actual probability was known to the subjects. The results are interpreted to indicate a natural tendency for subjects to consider additional indications as confirmatory evidence. The authors suggest that if alarms are systematically grouped (as is the often the case in actual alarm systems) this tendency might lead to faster and more

accurate response. However, they point out, there are circumstances (e.g., multiple unrelated failures) in which the assumption of relatedness is not appropriate.

In a similar experiment, McDonald, Gilson, and Mouloua (1996) demonstrated that confidence of an alarm's validity was influenced by the number and proximity of other active alarms. The results showed simple linear relationships between both number and proximity of other alarms and subjects' reported confidence in the 'test' alarm. The authors interpret the results as demonstrating natural tendencies to attribute common causes to event, depending on the way in which they manifest themselves.

The tendencies of subjects in these studies to respond in a way contrary to what they 'knew' about the probability of a valid alarm may to some extent reflect experimental demand characteristics. However, to the extent their responses might reflect strong, perceptually-based effects, some implications for alarm presentation can be cautiously considered. In a well-designed spatially-dedicated alarm display, alarms in proximity to one another are often related; they may provide independent evidence of an underlying fault and thus increase the operators' confidence that an actual problem exists. This would be augmented by the effects demonstrated in these studies. However, if the multiple alarms were related to the same signal (i.e., if the information was not independent) the phenomenon demonstrated in the study would predispose the operators to false confidence. The effects of alarm suppression, then, would be expected to depend on the relationships among the alarms and the operators' training. If operators are uncertain about the degree of independence of alarm indications, or do not have a full understanding of the processing logic underlying the alarm displays, they may default to response tendencies similar to those demonstrated by McDonald et al.

The concept of information "decomposition" used in the expert-system domain is particularly relevant here. This concept states that users should be able to access progressively greater levels of detail, including processing rules, and sensor values in order to understand the basis upon which the system is providing recommendations. In addition, this guideline is consistent with the high-level design review principles of Logical/Explicit Structure and Simplicity of Design.

4.3-13 Access to Inputs

Operators should have the capability of viewing inputs to the alarm processing system (e.g., sensor data).

ADDITIONAL INFORMATION: Operators may need to view sensor data and values that result from alarm system processing under certain circumstances, such as if the pattern of alarm messages appears to be contradictory, or if operators suspect that there is a problem with the processing system such that the results of alarm processing are incorrect.[6105]

Discussion: This guideline is consistent with the high-level design review principles of Logical/Explicit Structure User Guidance and Support, and Flexibility.

4.4-1 Prioritization Criteria

Alarm messages should be presented to the operators in prioritized form based on prioritization dimensions that include urgency (immediacy of required operator action) and challenges to plant safety.

ADDITIONAL INFORMATION: Additional alarm priority dimensions, such as challenges to plant productivity or investment protection, may also be implemented. The selected prioritization scheme should be logical such that those alarms of the highest safety significance receive the highest priority and such that the prioritization appears reasonable to operators.[0700, 6105]

Discussion: Roth and O'Hara (1998) conducted a study of the integration of advanced interfaces, including an advanced alarm system, into a control room. The primary alarm display panel was composed of 254 alarm message windows. The alarm messages were grouped and assigned to alarm windows based on a plant function organization scheme. Although only one alarm message could be displayed in an alarm window at a time, it was possible for more than one alarm message associated with a given alarm window to be active at the same time. A prioritization scheme determined which alarm message was displayed in the window when more than one alarm message is active. Prioritization among alarm messages is only performed within narrowly-defined queues of alarms that all relate to the same plant function. No attempt was made to prioritize alarms across functions. This contrasts with many other computerized alarm systems that assign each alarm a predefined indication of urgency for operator action, with some alarms always coded as "high" urgency for action and other alarms always coded as "low" urgency. In this alarm system, operators did not have to consciously consider relative alarm priority. The alarms that appeared in the alarm windows at any given point in time were expected to be addressed by the operators. The alarms not displayed in the windows were stored in a queue of active alarm messages associated with a given alarm window. If there were alarm messages in the queue, a symbol appeared in the alarm message window to alert the operators that queued messages existed. The lower-priority alarm messages in the queue could be accessed from a VDU console.

Crews were observed during their initial training with the new system on a full-scope simulator, and interviews were conducted with operators and other utility and vendor personnel. The training included full-scope simulations of plant disturbances. In some cases, when there were many messages in a queue, the operators indicated that they did not have time to go back and look at the queued messages. Thus, during a dynamically evolving event, directly involved board operators may not have time to consult secondary displays to review ‘overflow' (lower priority) alarms. They may do so in special cases, or later in the event during low tempo periods, but in general they rely on the alarm prioritization scheme to present them with the most important alarms they should be aware of. This increases the importance of having a robust alarm prioritization scheme that is broadly applicable across contexts.

Alarm prioritization has been determined to be required in order for an alarm system to meet alarm system functional criteria as described in NUREG/CR-3217. In addition, this guideline is consistent with the high-level design review principles of Situation Awareness and Task Compatibility.

4.4-2 Number of Priority Levels

The number of priority levels within a dimension should be no greater than four.

ADDITIONAL INFORMATION: Prioritization schemes with many levels may require operators to devote excessive attention to the priority level and thus reduce the benefits of prioritization.[0700, 6105]

4.4-3 Access to Suppressed Alarms

When alarm suppression is used, the operator should be able to access the alarm information that is not displayed.

ADDITIONAL INFORMATION: Suppressed alarms are not presented to the operators, but they can be accessed by operators upon request. The method for accessing suppressed alarms and the scheme for their presentation to the operators should not be excessively complex.[6105]

Discussion: In a study of alarm system design using a high-fidelity simulation, O’Hara et al. (2000) presented alternative methods of making available information about low-priority alarms. Operators generally did not favor the complete removal (i.e., filtering) of alarm information. Operators preferred a condition in which such information was suppressed (not presented but available on request) to one in which it was prioritized (presented on a separate display).

Roth and O'Hara (1998) conducted a study of the integration of advanced interfaces, including an advanced alarm system, into a control room. The primary alarm display panel was composed of 254 alarm message windows. Only one alarm message could be displayed in an alarm window at a time, it was possible for more than one alarm message associated with a given alarm window to be active at the same time. The lower-priority alarm messages in the queue could be accessed from a VDU console. Crews were observed during their initial training with the new system on a full-scope simulator, and interviews were conducted with operators and other utility and vendor personnel. In some cases, when there were many messages in a queue, the operators indicated that they did not have time to go back and look at the queued messages. Thus, during a dynamically evolving event, directly involved board operators may not have time to consult secondary displays to review ‘overflow' (lower priority) alarms. They may do so in

special cases, or later in the event during low tempo periods, but in general they rely on the alarm prioritization scheme to present them with the most important alarms they should be aware of. This demonstrates the importance of minimizing the demands associated with accessing potentially useful information on secondary displays.

This guideline is consistent with the high-level design review principles of Logical/Explicit Structure User Guidance and Support, and Flexibility.

4.4-4 Filtered Alarms

Alarm filtering should only be employed where alarm messages have no current operational significance to the crew's monitoring, diagnosis, decision making, procedure execution, and alarm response activities.

ADDITIONAL INFORMATION: As the term is used here, filtered (as contrasted with suppressed) alarm messages are eliminated are not available to the operators. Research has indicated that operators prefer to have information available to them to support verification and decision-making activities. Thus, only alarms that can be demonstrated to have no operational significance to operators should be filtered. This includes alarm messages that are irrelevant within the context of the current plant mode or the configuration of the associated plant system. For example, alarm messages that indicate that a pump discharge pressure is low after the fluid system has been removed from service should be filtered. Alarms that are considered redundant or lower priority should be suppressed (where operators can retrieve them) rather than filtered.[6105]

Discussion: In a study of the presentation of alarm information, O'Hara et al. (2000) simulated alternative methods of making available information about low-priority alarms. Operators generally did not favor the complete removal (i.e., filtering) of alarm information. This is consistent with the findings from other investigations (e.g., see Beattie and Vicente, 1996). They noted that it was necessary to check alarms following events such as a trip in order to verify that the event is proceeding as expected, and emphasized that extreme care must be taken not to filter alarms that are needed for such purposes. Operators preferred a condition in which such information was suppressed (not presented but available on request) to one in which it was prioritized (presented on a separate display). This guideline is consistent with the high-level design review principle of Task Compatibility.

4.5.1-1 Display Functions

The alarm display should support the operator's ability to rapidly discern:

- Priority (e.g., urgency for operator action and importance to plant safety);
- Distinct alarm states: new, acknowledged, and cleared;
- The first-out alarms for reactor trip;
- The need to access other displays to verify or clarify the alarm state; and
- The difference between alarms which can be canceled through ongoing corrective actions (i.e., by operations personnel) and alarms that require significant maintenance intervention.[0700,6105]

ADDITIONAL INFORMATION: Multiple alarm display formats, such as dedicated tile-like display and message lists, may be necessary to satisfy all operator alarm information needs.[0700,6105]

Discussion: Rather than showing the overall superiority of specific display options, such as SDCV, message lists, and integrated alarms and process displays, the results of O'Hara et al. (2000) and Roth and O'Hara (1998) both indicate the multiple display formats may be necessary to satisfy the operator's information needs. That is, each option has its unique advantages and is useful under different circumstances.

4.5.1-2 Coordination of Alarm Alerting and Informing Functions

When alarm alerts are displayed separately from detailed alarm information, the design should support the operator in making rapid transitions between alerts and detailed information.

ADDITIONAL INFORMATION: In conventional annunciator tile-based alarm systems, the annunciator tile performs both the alerting function (i.e., providing a salient indication of the presence of an alarm condition) and the informing function (i.e., providing information that describes the nature of the alarm condition). In advanced alarm systems, the alerting and informing functions may be separated. For example, an alarm tile display may alert the operator to the presence of an alarm condition while an alarm message list display may provide detailed information such as the alarm parameter name and setpoint value. The presentation of the alerting and informing information should be coordinated so the operator can rapidly access detailed alarm information associated with the alarm condition alerts.[6105]

Discussion: Using a high-fidelity simulation of an advanced control room, O'Hara et al. (2000) compared different alarm display approaches. One approach combined tile-like SDCV displays with message lists. Operators in this condition indicated that when the number of alarms was high, it was sometimes difficult to go from the tile alarm to its corresponding alarm message, emphasizing the importance of easy access to detailed information. By contrast, operators found it relatively easy to go from the SDCV displays to the process formats (because of the way tiles were spatially organized). This guideline is consistent with the high-level design review principles of Task Compatibility and Response Workload.

4.5.1-3 Presentation of Alarm Priority with Detailed Alarm Information

When alarm alerts are displayed separately from detailed alarm information, the detailed alarm information display should provide an indication of the priority and status of the alarm condition.

ADDITIONAL INFORMATION: The operational significance of the detailed alarm information, such as the parameter name and the exceeded setpoint value, may be more readily apparent to the operator when accompanied by an indication of alarm condition priority and status (e.g., new and acknowledged).[6105]

Discussion: The simulation study of alarm display designs conducted by O'Hara et al. (2000) used color coding to indicate the (static) priority of messages in alarm lists. Operator opinion of the approach was favorable. This guideline is consistent with the high-level design review principles of Task Compatibility and Response Workload.

4.5.1-4 Use of Spatially-Dedicated, Continuously-Visible Displays

Spatially-dedicated, continuously-visible (SDCV) alarm displays should be considered for:

- Regulatory Guide 1.97 Category 1 parameters,
- Alarms that require short-term response by the operators,
- Main alarms used by operators in diagnosing and responding to plant upsets, and
- Main alarms used by operators to maintain an overview of plant and system status.

ADDITIONAL INFORMATION: Spatial dedication means that the alarm messages always appear in the same position. Continuously visible means a parallel presentation method is used, i.e., the alarm information is always available to the operator, as opposed to serial presentation methods in which the operator must select the information to be seen. A SDCV alarm display (such as is provided by conventional tiles) generally has been found during high-density alarm conditions to be superior to a spatially focused, variable location, serial display (as has been typical of some computer-based presentations, such as on CRT or flat-panel displays). SDCV displays provide perceptual advantages of rapid detection and enhanced pattern recognition. Note that VDU displays can be used as SDCV alarm displays, but the space required for this type of alarm display can make their use impractical when a large number of alarms is to be presented.[6105]

Discussion: Direct comparisons of operator performance under spatially distributed but fixed alarm display (conventional boards) versus focused but variable alarm display (computer-based system) are of significant interest. EPRI performed a series of tests examining the role of conventional and CRT-based alarm presentations (Fink et al., 1992). The study investigated alternative systems for alarm presentation including (1) alarm tile display alone, (2) CRT display alone, and (3) combined tile and CRT alarms (additional display conditions were also evaluated). Fifteen licensed operators participated in the tests using an alarm system (not a full-mission) simulator. Performance measures included the speed and accuracy with which operators could extract information from the alarm system and operators' opinions on ease of use and other subjective parameters. The results indicated that the grouping of alarms by system and function improves performance. This was consistent with the finding of an earlier EPRI study (Fink, 1984). Interestingly, the conventional alarm system allowed the operators to obtain information more quickly and easily than did the CRT presentation.

Matsushita (1988) requested experienced operators to evaluate an advanced control room design after using the design in simulated scenarios. The alarm display system was CRT-based. The operators indicated that the CRT displays were sufficient when few alarms were presented. However, during accident or transient conditions, the CRT system made problem identification harder than it was when using the conventional alarm system. The advanced control room design was modified to include both a conventional alarm system and the CRT-based system.

Kragt (1984) compared three types of alarm systems in terms of their effects on human performance. The main objective of the comparison was to evaluate the parallel versus sequential presentation of alarms. The three systems were (1) the conventional lighted window arrangement, (2) a CRT-based model similar to the conventional system, and (3) a CRT-based sequential textual alarm presentation. A laboratory simulation was set up to make the comparison, and 24 chemical plant trainees served as test subjects. Operator errors and difficulty ratings were the main dependent variables. The results indicated that the sequential presentation of alarms was inferior both in terms of operator performance and subjective ratings. The differences between presentation modes was even greater during high alarm density conditions. The lack of operator ability to recognize a pattern of alarms was offered as an explanation for the advantages of parallel alarm presentation.

Operator preference for conventional systems has been found in other studies as well (e.g., Kragt, 1982; Rankin, 1985; and Wickens, 1987). Wickens (1987) found increased memory load for computer-based display presented information and a loss of spatial organization of information which facilitates information processing.

Using a high-fidelity simulation of an advanced control room, O'Hara et al. (2000) compared alarm displays differing in the degree of spatial dedication. In one condition all alarms were presented in a tile-like format while another condition used SDCV displays for important alarms (such as those identified in the guideline) and message lists for other alarms. Operators expressed a preference for the condition which combined SDCV and list displays. Operators commented that they could immediately detect the disturbed system with this display and liked the fact that no important alarms were "hidden." In contrast, when all alarms were SDCV and operators indicated that it was sometimes hard to find new alarms in the display. It was recommended that if all alarms were to be presented using a SDCV display, a high degree of alarm reduction should be applied. This result would be functionally the same as the mixed condition, i.e., a relatively small set of SDCV alarms.

Data obtained via survey and/or anecdote provide similar results. MPR (1985) surveyed utilities in North America to identify potential alarm improvements. In plants having both conventional and VDU alarm displays, operators reported a preference for the VDU alarms during normal power operations when the number of alarms is small but a preference for the conventional systems during plant upsets when the number of alarms was large. In the Canadian plants surveyed, while VDU-based displays are the primary method of alarm presentation, an increasing trend toward conventional alarm presentations had been observed. One of the major problematic issues was the method of alarm presentation. When alarm data are presented as message lists on a CRT, the display becomes difficult to manage during plant upsets. In fact, the authors state that "there is clear evidence that CRT message lists are a poorer method of presenting alarms that the conventional alarms that they 'supplement'." More recently, CRT alarm message flooding has been identified as a significant problem in some Canadian plants (Sheehy et al., 1993; Moore et al., 1993). Operator problems with VDU-based message displays in high density situations have been noted in other field observations (Corsberg, 1988).

The EPRI ALWR document requires the use of spatially dedicated, continuous, and parallel display (such as a tile-based system) for (1) main process alarms used by operators in diagnosing and responding to plant disturbances, (2) alarms used to maintain an overview of plant and system status, and (3) alarms that require short-term response by operators. NUREG/CR-3987 recommends such a display for "most critical warning information." EPRI NP-3659 recommends the use of tile displays for indicating deviant plant conditions that require immediate access to displays to verify alarms. NUREG/CR-3987 indicates that alarm systems should include both variable (e.g., VDU-displayed) warnings and permanent, spatially dedicated (e.g., tile-displayed) alarms.

In addition, this guideline is consistent with the high-level design review principles of Situation Awareness and Cognitive Workload.

4.5.1-5 Alarm Graphics

The graphics related to alarm presentation should be designed such that the display is fully contained in one VDU screen.

ADDITIONAL INFORMATION: For example, the operators should not have to scroll the graphic of the overall reactor system, a major subsystem such as the primary system, or a portion of the subsystems, such as the pressurizer, to access a complete set of related alarm messages.[6105]

4.5.1-6 Alarm Coding Consistency

Coding (e.g., flash-rate, intensity, and color coding) conventions should be consistently applied throughout alarm displays (e.g., on tiles and on VDUs).[6105]

4.5.1-7 Multi-Unit Alarms

Alarms for any shared systems in multiple-unit plants should be duplicated in all control rooms.

ADDITIONAL INFORMATION: Multiple-unit NPPs may contain systems that are shared by two or more units. The status of any such equipment should be provided in all control rooms. When an item of shared equipment is being operated from one control room, a status display or signal should be provided in all other control rooms which could potentially control this equipment.[0700]

4.5.2-1 Importance/Significance

~~The display of important alarms should override the display of alarms of lower importance.~~[6105]

Alarms that have higher importance or greater safety significance should be given greater priority in their presentation than less important or significant alarms.

ADDITIONAL INFORMATION: The priority of presentation should be part of an overall process for alarm management, which may include coding for the level of importance or priority, and alarm processing, filtering, and suppression.[6105]

4.5.2-2 Simultaneous Display of High-Priority Alarms

For non-spatially dedicated alarm presentations such as VDU message lists, sufficient display area should be provided for the simultaneous viewing of all high-priority alarms.

ADDITIONAL INFORMATION: Non-spatially dedicated alarm displays, such as message lists, should generally not be used as the primary method of presenting high-priority alarm messages. If non-spatially dedicated alarm displays are used, they should have sufficient display space available for simultaneous presentation of all high-priority alarms under the worst credible conditions. Operators should never have to page or scroll a display to view high-priority alarms.[6105]

Discussion: O'Hara et al. (2000) compared different alarm display approaches in a high-fidelity control room simulation. Message lists were among the approaches examined. Many operators participating in the study indicated that lack of alarm display area was a problem. In addition, operators did not want to engage in the secondary task activities associated with alarm list scrolling when the alarms required more than one VDU. Such reluctance emphasizes the importance of sufficient VDU space for simultaneous presentation of all high-priority alarms, even when the number of alarms is high. This guideline is consistent with the high-level design review principle of Response Workload.

4.5.2-3 Coding of Alarm Priority

A method of coding the visual signals for the various priority levels should be employed.

ADDITIONAL INFORMATION: Acceptable methods for priority coding include color, position, shape, and symbolic coding. Color and position (top to bottom) are especially effective visual coding methods. However, coding priority by alarm element position can disrupt the functional grouping of elements and should not be used when the loss of functional grouping may affect the operator's ability to effectively use alarm information. In this case, another dimension, such as color, should be used for priority coding. Dynamically segregating alarms differing in priority on adjacent lists or displays is also potentially confusing.[6105]

Discussion: In the O'Hara et al. (2000) study of alarm processing and display, operators favored spatial coding for indicating which alarms of a group of valid alarms are higher priority. However, operators indicated that the use of spatial coding for dynamically prioritized alarms (display of alarms that have been processed out) was distracting and a potential source of error.

4.5.3-1 Indication of Alarm Status

New, acknowledged, and cleared alarm states should have unique presentations to support the operators' ability to rapidly distinguish them.[6105]

4.5.3-2 New Alarms

New alarms should be indicated both by visual (e.g., flashing) and audible means.[6105]

ADDITIONAL INFORMATION: When new alarm messages are presented on a VDU, the message text itself should not flash. Rather, an adjacent flashing symbol should be used to indicate the new message (see Guideline 1.3.10-10, Flash Coding for Text).

Discussion: Operators who participated in the O'Hara et al. (2000) simulation study indicated that in the plant in which they actually work, the text of new alarm messages blinks. When they are busy and quickly glance at the alarm list, they can sometimes miss the blinking alarm message. The alarm messages in the study did not blink. Instead, an asterisk next the message blinked. The operators indicated that this approach was a better than having the entire message blink.

4.5.3-3 Notice of Undisplayed New Alarms

If the operator is not currently viewing the VDU display where new, unacknowledged alarm messages appear, the alarm system should notify the operator that a new alarm message is available, the priority of the alarm message, and the location where the alarm message can be found.[6105]

4.5.3-4 Acknowledged Alarms

After the operator has acknowledged an alarm (e.g., pressed the acknowledge button), the alarm display should change to a visually distinct acknowledged state and the alerting function (e.g., audible tone) should cease.[6105]

4.5.3-5 Clearing Alarms/Ringback

If the operator is required to take action when an alarm clears (i.e., the parameter returns to the normal range from an abnormal range), the return to normal conditions should be indicated by visual and audible means.

ADDITIONAL INFORMATION: Ringback, alerting the operator when a parameter returns to normal, should not be required for all alarms but should be required when it is important that the operator know immediately when the deviation has cleared, or when the deviation is not expected to clear for some time. Such cleared alarms should provide a positive indication by initiating audible and visual signals. Techniques that may be employed include: a special flash rate (one-half the normal flash rate is preferred, to allow discrimination); reduced brightness; or a special color that is consistent with the overall control room color coding scheme. Cleared alarms should have a dedicated, distinctive audible signal which should be of finite and relatively short duration.[0700, 6105]

4.5.3-6 Cleared Alarms That Re-Enter the Abnormal Range

If an alarm has cleared but was not reset and the variable re-enters the abnormal range, then the condition should be presented as a new alarm.

ADDITIONAL INFORMATION: When an alarm clears, the operator is informed via the ringback feature that the value is now in its normal range. Since the operator might expect the parameter to remain in the normal range, the alarm system should alert the operator when the parameter deviates from the normal range. If the variable again enters the abnormal range, the alarm system should behave as it does for new alarms, by producing visual and auditory signals to alert the operator. For cases in which a variable might move (e.g., oscillate) in and out of the normal range, alarm processing should be used to prevent the frequent reoccurrence of the alarm from becoming distracting to the operator. One technique might be to require the parameter to move further into the normal range before the alarm clears. Another techniques might be to require the parameter to remain within the normal ranch for particular amount of time before allowing the alarm to clear.

Discussion: This guideline is consistent with the high-level design review principle from Appendix A.2 of NUREG-0700, Rev. 1 of Feedback, which states that the HSI should provide useful information on system status. It is also consistent with the high-level design review principle of Task Compatibility, which states that the system should meet the requirements of users to perform their tasks.

4.5.4-1 Minimize Shared Alarms

Alarms with inputs from more than one plant parameter (shared alarms) should be minimized.

ADDITIONAL INFORMATION: Shared alarms are those formed from the combination of different process deviation conditions through "or" logic. For example, a "trouble" message may combine several potential problems associated with a single plant system or component, or it may address the same problem for a group of similar components (e.g., a bearing temperature alarm may address bearings from more than one component). When shared alarms are used, an inquiry capability should be provided to allow the operator to obtain specific information about which of the ganged parameters exceeded its setpoint. Criteria for the use/avoidance of shared alarms are given in Table 4.1. In traditional (i.e., tile-based annunciator) alarm systems, shared alarms imposed additional workload on the operator compared to single alarms because the operator had to identify the deviant parameter(s). This type of shared alarm should be minimized in advanced alarm systems. Some advanced alarm systems automatically present information related to the deviant parameter when the shared alarm is initiated. This reduces the operator workload associated with retrieving alarm information and minimizes the negative effects of shared alarms.[0700, 6105]

Discussion: Woods (1995) contrasts the "mentally economical" evaluation of incoming information allowed by, e.g., well designed auditory displays or spatially-dedicated alarm panels with the forced attention shift associated with shared alarms. He points out that the operator cannot evaluate an aggregated indication without interrupting ongoing activity and investigating the content of the alarm.

4.5.4-2 Shared Alarm Identification

Operators should have the capability to access the individual alarm information when a shared alarm activates.

ADDITIONAL INFORMATION: The information could be provided by means of alarm messages on a VDU, an alarm list on an alarm printer, or by other means. This information may be provided automatically or by operator action.[0700]

4.5.4-3 Shared Alarm Reflash

If a new parameter deviation has occurred before a preceding alarm has cleared, the shared alarm should return to the new alarm state (e.g., flashing).

ADDITIONAL INFORMATION: The alarm logic system should provide the capability to "reflash" (i.e., reactivate the visual and audible alert indications for the alarm) when subsequent alarm conditions occur after the initial alarm condition has been acknowledged.[6105, 0700]

Table 1 Shared alarm considerations

TYPES OF ALARMS THAT MAY BE CONSIDERED FOR COMBINATION (SUBJECT TO THE RESTRICTIONS LISTED BELOW)

- Alarms for the same condition on redundant components, or logic trains, when each has a separate indicator and the indicators are placed in close proximity on the console (e.g., pump A or B trip, logic train A or B actuation)
- Alarms for several conditions relating to one component or several redundant components, which require the operator to obtain further diagnostic information either by sending an auxiliary operator out to the component(s) or checking a~~the~~ computer system (e.g., pump A or B trouble) *[Note the point here is to make a distinction between the alarm system and other computer systems. If the information already resides in the Alarm system's computer, then a shared alarm should not be used. However, a shared alarm may be acceptable if individual alarms are not feasible because the info is not available to the alarm system.]*
- Alarms for several conditions that call for the same corrective action
- Alarms that summarize single-input alarms elsewhere in the control room

CONDITIONS UNDER WHICH ALARMS SHOULD NOT BE COMBINED

- Different actions are to be taken depending on which alarm condition exists and information is not readily available to the operator to identify which constituent is alarming
- The required response must be initiated ~~immediately~~ relatively quickly, so that taking time to consult ~~the control panel or the computer~~ a local panel to determine which constituent is alarming would risk an inadequate operator response
- Information or protection for other alarm constituents is not available to the operator after any one alarm constituent has activated the combined alarm (reflash can provide such protection as discussed in Guideline 4.5.4-3)
- Operator understanding is improved by alarming the conditions separately because of similarity to the layout of associated controls
- The constituent conditions are not of a similar nature, or are not of the same order of importance, such that the action to be taken is very different depending on which condition is alarming

4 ALARMS
4.5 Display
4.5.5 Alarm Messages
4.5.5.1 Content

4.5.5.1-1 Alarm Information Content

The alarm should provide the following information:

- Alarm title or legend;
- Plant system or component involved (e.g., reactors coolant pump A);
- Parameter involved (e.g., temperature, pressure, voltage);
- Status of parameter (e.g., high, low, or inadequate);
- Alarm source, i.e., the particular sensor or group of sensors supplying the signal;
- Alarm priority;
- Setpoint and parameter values;
- Required immediate operator actions; and
- Reference to procedure for more detailed follow-up actions.

ADDITIONAL INFORMATION: This information should be presented whenever possible, so long as it does not result in a confusing display or overload the operator with information. It should be noted that conventional alarm systems generally cannot effectively supply most of this information, but advanced systems can by providing it on alarm display screens or on operator-selectable displays upon receipt of a given alarm. The system should not provide excessive information in a single display and should not employ excessive levels and/or dimensions for coding information. More detail on each of these individual information requirements is specified by subsequent guidance in this section.[0700, 6105]

4.5.5.1-2 Alarm Text/Legend

Alarm text should be clearly understandable, use standard terminology, and address conditions specifically.

ADDITIONAL INFORMATION: For example, specifically identify the parameter and state (e.g., HIGH PRESSURE) instead of using one legend for multiple parameters or multiple states (e.g., TEMPERATURE-PRESSURE or HIGH-LOW).[0700]

4.5.5.1-3 Alarm Source

The content of each message should provide information that identifies the alarm source.

ADDITIONAL INFORMATION: Information should be available as to which specific sensor (or group of sensors) supplied the alarm signal.[6105]

4.5.5.1-4 Alarm Priority

An alarm message should indicate its priority.[6105]

4.5.5.1-5 Setpoint Values

If an alarm condition requires verification before action is taken, the relevant setpoint limits should be included in the alarm message.

ADDITIONAL INFORMATION: There are circumstances in which setpoints should not be included in alarm displays. However, these apply to conventional, not advanced alarm systems. First, the setpoint values may change and temporary labels will have to be used, thus violating the human factors principle that states that labels should be as permanent as the equipment to which it is attached. While this may be a concern in conventional tile-like displays, computer-driven displays characteristic of advanced control rooms would not be subject to this limitation since the label is "soft." Second, the setpoint information only gives partial information (i.e., condition is above or below some setpoint), and the operator could assume that the condition is near the setpoint when, in fact, it is well above it or below it. However, parameter values should be given in alarm messages provided in VDU and printer displays (see Guideline 4.5.5.1-6); thus, this objection is overcome. Third, adding this type of information goes against the principle that the alarm system should not encourage undue reliance. However, advanced control rooms should provide enhanced data integration and minimize the requirements for operators to integrate information from different sources, e.g., alarms and indicators. Thus, while these concerns may apply to a conventional alarm system, setpoint values should be provided in an advanced system.[6105]

4.5.5.1-6 Parameter Values

Deviant parameter values should be included in the alarm message when alarm information is presented on VDU or printer displays.[6105]

4.5.5.1-7 Required Immediate Operator Actions

Immediate operator actions should be presented or made available directly upon operator request when alarm information is presented on VDU or printer displays.

ADDITIONAL INFORMATION: To meet the general alarm system principle of guiding the operator's response to an alarm (see Guideline 4.1-1, Alarm System Functional Criteria), the immediate actions should be provided to the operator. For conventional alarm systems, the immediate operator actions should be available in Alarm Response Procedures that are clearly and simply keyed to an alarm tile and located nearby for easy and quick reference. In this case, the procedure would contain those items noted in Guideline 4.5.5.1-1, Alarm Information, that could not be incorporated into the alarm display itself (e.g., alarm source, setpoint value, immediate actions, and follow-up actions). Advanced alarm systems may present the relevant alarm response procedure (e.g., via a nearby VDU).[6105]

4.5.5.1-8 Reference to Procedures

When alarm information is presented on VDU or printer displays, references to alarm response procedures should be provided.
ADDITIONAL INFORMATION: The document title, major section, and page number should be included in such references.[6105]

Discussion: In NUREG/CR-3217, keying procedures to alarms was considered an alarm system requirement to meet alarm system functional criteria.

4.5.5.1-9 Reference to Other Panels

Alarms which refer the operator to another, more detailed display located outside the primary operating area should be minimized.

ADDITIONAL INFORMATION: Advanced alarm systems should be designed such that required information is readily accessible from within the primary operating area.[0700]

4 ALARMS
4.5 Display
4.5.5 Alarm Messages
4.5.5.2 Format

4.5.5.2-1 Format for Tile Displays

The format of messages on alarm tiles or tile-like displays should be consistent for all alarms.

ADDITIONAL INFORMATION: Information on a tile might be organized as follows: top line, name of alarmed parameter; middle line, alarm setpoint value; bottom line, indication of severity.[6105]

4.5.5.2-2 Format of VDU and Printer Messages

The alarm message format should be consistent for VDU and printer message displays.
ADDITIONAL INFORMATION: The format of alarm message lists should be consistent with the format of the SDCV displays [6105]

4.5.6.1-1 Coding Effectiveness

The coding scheme used by the alarm system should assure rapid detection and interpretation by the operators under all control room operating conditions.[0700]

4.5.6.1-2 Coding Dimension Discriminability

Each level of a coding dimension should be easily and readily distinguishable from the other levels.

ADDITIONAL INFORMATION: For example, if color is used, the different colors should be easily discriminated. Each color should have a single, precise meaning consistent with its use in the rest of the HSI. In addition, color should not be used in a manner that is counter to cultural stereotypes. A formal coding scheme that encompasses all coding dimensions (e.g., color, shape, brightness, textures/pattern, and flashing) and specifies a hierarchical order of salience should be established and formally documented before any coding is applied to the displays. Alarm information should be organized into categories according to a scheme for priority. Coding dimensions should be systematically applied to these categories such that alarm information with the highest priority is also most salient.[6105]

4.5.6.1-3 Unique Coding Dimensions

For coding techniques being used to support detection and recognition of status within an alarm dimension, each coding technique should represent one dimension of alarm classification.

ADDITIONAL INFORMATION: If flash rate is being used to indicate alarm state (e.g., new, acknowledged, or cleared), it should not also be used to indicate need for operator action (e.g., immediate action required, action required within 15 minutes, or no near-term action needed).[6105]

4.5.6.1-4 Coding Complexity

The number of different coding techniques should be kept to a minimum, so that the overall coding system does not become difficult to understand.[6105]

4.5.6.2-1 Visual Coding~~Signal~~ for ~~Important~~ Alarms

~~A flashing visual signal should be included for all important alarms.~~
Visual coding should be used to direct operator attention to alarms and to indicate their status.

ADDITIONAL INFORMATION: To be ~~An~~ effective, an alarm system should-attract the operator's attention and help the operator focus attention on more-important rather than less-important alarms. ~~will capture and direct the operator's awareness under any and all conditions~~. A flashing visual signal is a preferred means for directing attention and indicating alarm status (e.g., unacknowledged, acknowledged, and cleared-not reset) on SDCV and computer-based displays. Under high alarm volume conditions, the designer may consider suppressing or delaying the alerting indications (e.g., visual flashing) for those alarm conditions that (1) do not require immediate response, and (2) do not indicate a challenge to plant safety and technical specifications. This will assist operators in detecting the more significant alarm messages and reduce distraction from less important ones.[6105]

Discussion: This guideline is consistent with the high-level design review principles of Situation Awareness and Cognitive Workload.

4.5.6.2-2 Redundant Coding Dimensions

Redundant codes (e.g., fast flashing or brightness) should be used for alarms that require rapid operator action.[6105]

4.5.6.2-3 Flash Rate

Flash rates should be from three to five flashes per second with approximately equal on and off times.[0700]

4.5.6.2-4 Brightness Levels for Transilluminated Displays

For transilluminated displays, such as lighted alarm tiles, the brightest state should be no more than 300 percent brighter than the inactivated state, and the dim state should be at least 10 percent brighter than the inactivated state.

ADDITIONAL INFORMATION: Brightness of "on" alarms should not annoy or distract operators.[6105]

4.5.6.2-5 Brightness Levels for VDU Displays

For VDU displays, the bright state should be at least 100 percent brighter than the inactivated state.

ADDITIONAL INFORMATION: While transilluminated alarms may display up to three~~more than two~~ levels of brightness, VDU displays should be limited to only two levels.[6105]

4.5.6.2-6 Color Detectability

Low-intensity indications (e.g., dark red) in the periphery of the visual field should be avoided where color coding is used, since they may not be readily detected.

ADDITIONAL INFORMATION: If the display system has an area that is a specific focus of attention, then displays located in adjacent areas may be frequently in the periphery of the operator's field of vision.[6105]

4.5.6.2-7 Spatial Coding

Spatial coding may be used to indicate alarm importance.

ADDITIONAL INFORMATION: Spatial coding can be effective especially in VDU types of alarm presentation. In an otherwise variable alarm display, having a dedicated or consistent location for presentation of important alarms will enhance operators' ability to detect them. However, a similar approach applied to alarms dynamically assigned a low priority is not recommended. Spatial coding is related to alarm organization which is addressed in Section 4.5.7.[6105]

Discussion: In the O'Hara et al. (2000) study of alarm processing and display, operators favored spatial coding for indicating which alarms of a group of valid alarms are higher priority. However, operators indicated that the use of spatial coding for dynamically prioritized alarms (display of alarms that have been processed out) was distracting and a potential source of error. This guideline is consistent with the high-level design review principle of Cognitive Workload.

4.5.6.2-8 Suppressed Visual Codes

If the visual coding used to indicate alarm status is automatically suppressed or delayed during high alarm volume conditions or the presence of more important alarms, they should be automatically presented after the more important alarms have been addressed.

ADDITIONAL INFORMATION: Plant personnel should not be required to remember to request alarms to have been automatically suppressed.[6105]

Discussion: This guideline is consistent with the high-level design review principles of Situation Awareness, Cognitive Workload, and Error Tolerance and Control.

4.5.6.3-1 Audio Signal for ~~Important~~ Alarms

An auditory signal should be used to alert the operator to the existence of a new alarm, or any other condition of which the operator must be made immediately aware.

ADDITIONAL INFORMATION: Auditory cues should be provided for all new alarms under normal operating conditions. However, under off-normal conditions where high alarm density exists, the designer should consider suppressing the auditory signal for those alarmed conditions that (1) do not require immediate response and (2) do not indicate a challenge to plant safety and technical specifications. For example, audio signals associated with clearing alarms might be omitted under certain circumstances. This will prevent operators from being distracted by less important alarms while attending to more significant ones. Some designs may have a timed audible signal rather than one that is continuous until acknowledged. In this case, see the guideline for reminder audible signals, below.[6105]

Discussion: This guideline is consistent with the high-level design review principles of Situation Awareness, Cognitive Workload, and Response Workload.

4.5.6.3-2 Auditory Coding of Remote Alarms

Auditory coding techniques should be used when the operator workstation associated with the alarm is not in the primary operating area.

ADDITIONAL INFORMATION: During off-normal conditions, the designer should consider the suppression of the auditory code for those alarms that (1) do not require immediate response and (2) do not indicate a challenge to plant safety and technical specifications. This will prevent operators from being distracted by less important alarms while attending to more significant ones.[0700]

4.5.6.3-3 Distinguishable Auditory Signals

The auditory signal associated with a SDCV alarm should be easily distinguishable from the auditory signal associated with an alarm message displayed by other means (e.g., on a VDU message display).[6105]

4.5.6.3-4 Audible Signals for Alarm States

The tones used for incoming alarms should be separate and distinct from tones used to signify "clearing" alarms.~~, which should be momentary or "self-silencing."~~[6105]

4.5.6.3-5 Reminder Audible Signals

If the tone to indicate an unacknowledged alarm automatically turns off after an interval of time, a reminder tone should be presented to alert the operator to the continued presence of an unacknowledged alarm.

ADDITIONAL INFORMATION: The same principle holds for alarms which may have had the auditory code suppressed because of high alarm conditions or the presence of more important alarms. When the more important alarms have been addressed, the alarm system should remind the operator, via visual or auditory signals, of the presence of the unacknowledged alarms.[6105]

Discussion: This guideline is consistent with the high-level design review principles of Situation Awareness, Cognitive Workload, and Error Tolerance and Control.

4.5.6.3-6 Reset of Auditory Alert

The auditory alert mechanism should automatically reset when it has been silenced.[0700]

4.5.6.3-7 Interference Among Signals

Audio alarm signals should not conflict with other auditory codes or signals.

ADDITIONAL INFORMATION: If continuous, relatively loud signals are used, they may render other codes and signals less audible. Thus, it may be necessary to consider the audibility of a signal not just in the presence of ambient control room noise, but also in combination with other signals that might plausibly occur at the same time. To avoid mutual masking, the frequencies of tonal signals associated with alarms that may be active at the same time should be separated by at least 20 percent of the center frequency. Interference among alarm signals is less of a concern if the signals consist of a number of widely separated frequency components or of brief groups of pulses presented at intervals. Techniques are available that allow the audibility of signals in noise to be predicted.[0700, 6105]

Discussion: Patterson (1982) described a method for estimating the signal level required to insure that audio alarms were audible. His approach was based on the fact that signals are masked only by energy in a 'critical band' of frequencies close to the frequency of the signal. More recently, a method for predicting alarm audibility has been developed by LaRoche et al. (1991); this method, referred to as the Detectsound model, is also based on the critical band concept, although the specific assumptions about the nature of the critical band are slightly different. The model, which is implemented in software, allows the effects of age and of wearing hearing protection to be taken into account in estimating the audibility of warning signals. The Detectsound model was used by Momtahan, Hetu, and Tansley (1993) in a study of audio signals produced by medical monitoring equipment. They measured the ambient noise levels in operating rooms and intensive care units, the noise produced by the equipment used in the rooms, and the alarm sounds produced by equipment. Using the Detectsound analysis they found that many alarm sounds would be completely masked (i.e., rendered inaudible) by ambient noise, equipment noise, or the sounding of other alarms. Many others were not sufficiently above threshold to be considered reliably detectable. This guideline is consistent with the high-level design review principle of Physiological Compatibility.

4.5.6.3-8 Readily Identifiable Source

The operator should be able to quickly determine where to direct attention (e.g., which functional area of the plant or which station) from the characteristics of the auditory alert and/or the source from which the auditory alert originated.

ADDITIONAL INFORMATION: This guideline pertains to the use of auditory tones to direct the operator to the location of a spatially-fixed alarm display device in order to expedite the operator's response to the alarm condition. The use of sound to indicate the location of the alarm display may be of less value if the advanced alarm system allows the same alarm message to be retrieved from multiple locations (e.g., from redundant VDUs) in the control room. It should also be noted that in advanced control rooms that feature compact control consoles, the alarm display devices may not be physically separated enough to use sound localization as a cue. In this case, coded audio signals (possibly from a single source) would be used to direct the operators' attention. Thus, this guidance is most appropriate for advanced alarm systems that feature spatially-fixed alarm display devices. It has been recommended that coded signals from a single audio source should not be used to identify individual workstations within the primary operating area, and that each major console should be equipped with a separate sound generator capable of producing a distinctive sound. If the direction of a source sound is to be used as a cue, the signal should not be a high-frequency pure tone, since such signals can be difficult to localize.[0700, 6105]

Discussion: Edworthy and Adams (1996) point out that localization of continuous pure tone signals in the region of 1 kHz is poor. Unfortunately this frequency region is often used for warnings because auditory sensitivity is high. If it is necessary for the operator to immediately locate the source of the signal, it should be intermittent rather than continuous and should be acoustically complex rather than a pure tone. Momtahan, Hetu, and Tansley (1993) note that the greatest difficulty in localizing sound occurs at 1500 Hz so that frequencies well above or below this value are preferred when localization is important. They also note that, for alarm sounds that need to wrap themselves around obstacles, such as other equipment, frequencies below 1500 Hz are best.

4.5.6.3-9 Signal Level

The signal intensity should be such that operators can reliably discern the signal above the ambient control room noise.

ADDITIONAL INFORMATION: The intensity of an audio signal should be such that operators are alerted aurally to an alarm occurrence under the most adverse anticipated background noise conditions. A signal level 10 dB(A) above average ambient noise is generally considered adequate. It has also been recommended that sound intensity should be limited to a maximum of 95 dB(A), but that signal levels of 115 dB(A) may be used if considered absolutely necessary to achieve required attention-getting reliability for alarms indicating extreme danger. The tendency for designers to err on the side of conservatism results in many audio signals being more intense than is necessary to ensure reliable detection (see Guideline 4.5.6.3-10, Avoid Startle).[0700, 6105]

Discussion: Only that portion of a background sound within a narrow frequency range of the signal affects its detection. Accordingly, the levels of tonal signals should be specified relative to the masked threshold of the signals in the presence of the ambient noise, i.e., relative to the level at which the signal is just audible. A signal presented 15 dB above its masked threshold will be clearly audible; signals 25 dB or more above threshold are likely to be aversive. Masked thresholds can be determined by experiment in the control room, or estimated using the methods described by

Patterson (1982). Assuming the frequency spectrum of background noise is fairly uniform, the threshold for a signal with frequency *f* is equal to the spectrum level of the background noise at *f* plus 10log(0.15*f*). Note that the spectrum level is the noise power *per cycle* at the signal frequency, not the overall noise level. If the frequency spectrum of background noise varies more than 6 dB in the vicinity of the signal (.i.e., within 0.15*f*), a more complex estimation procedure can be used (Patterson, 1982).

4.5.6.3-10 Avoid Startle

The signal should capture the operator's attention but should not cause irritation or a startle reaction.

ADDITIONAL INFORMATION: Irritation and startle resulting from the audible alarm signals should be minimized through the design of audio signals, the selection of signal intensity, and the overall design of the audible alarm scheme.[0700, 6105]

Discussion: When a high-intensity sound is switched on instantaneously (i.e., when the level of the sound rises more than 10 dB/msec) it is likely to produce a startle reaction. The onsets of audio signals should be shaped so that the signals reach maximum level over a period of 20 to 30 msec. This "rise time" is long enough to avoid startle, but not so long that the onset of the signal becomes less attention-getting. Signal shaping is easily done with digital sound generation equipment. Patterson (1982) recommends increasing intensity from zero to maximum using the first quarter cycle of a sine function with a frequency of about 10 Hz. This results in a steep initial rise (typically masked by ambient noise) followed by a more gradual increase at higher levels.

4.5.6.3-11 Manual Disable/Adjustment of Signal Intensity

Manual disable or adjustment of auditory signal intensity (loudness) should be avoided.

ADDITIONAL INFORMATION: The need to adjust auditory signal level can be alleviated by improved signal design and level selection. If signal level is adjustable, it should be controlled by administrative procedure. Under no circumstances should operators be able to disable audio alarm signals or reduce their level so as to render them inaudible.[0700, 6105]

Discussion: Kragt and Bonton (1983) conducted an observational assessment of operator use of the alarm system at a chemical plant. During a process upset, the operators found the auditory alarm characteristics irritating and would typically silence the alarms as soon as possible without necessarily identifying the alarms that came in. This indicates that the audio characteristics of the alarms were poorly designed, e.g., causing distraction as a result of being unnecessarily loud or preventing communication by sounding continuously once activated. There are numerous reports in the human factors literature of operators defeating auditory alerts and silencing alarm systems (see Sorkin, 1989). In addition, this guideline is consistent with the high-level design review principle of Error Tolerance and Control.

4.5.6.3-12 Sound Sources

The number and placement of loudspeakers should be such that auditory signals are free of distortion and are equally audible at any operator work station in the ~~primary~~ operating area.

ADDITIONAL INFORMATION: Speakers should be oriented away from surfaces that could scatter or diffuse the acoustic wave. Speakers should not be located behind structures that could cause distortion, echoes, or sound shadows. When sound localization is used to direct the operator to particular alarm display devices, the loudspeakers should be oriented such that their location can be quickly discerned and corresponds to the location of the intended alarm display device. Loudspeakers for adjacent alarm display devices should have adequate separation to allow their individual locations to be discerned.[0700, 6105]

4.5.6.3-13 Auditory Signal Discriminability

Each audio signal should be unambiguous and easily distinguishable from every other tone in the control room.

ADDITIONAL INFORMATION: Current sound generation technology allows the design of alarm signals that make better use of the operator's ability to process audio information. It is possible to design signals that are not only more discriminable from one another than are conventional signals, but have the potential to carry more information. Signals should be composed of unique combinations of tone pattern and frequency. In addition, the location of the sound source should be unique if sound localization is to be used to direct the operator to a particular alarm display device. If the direction of a source sound is to be used as a cue, the signal should not be a high-frequency tone, since such signals can be difficult to localize.[0700, 6105]

Discussion: Meredith and Edworthy (1994) examined the learning of and confusions among a set of alarm sounds used in intensive therapy (i.e., hospital) units. Previous laboratory research had suggested that only five or six sounds are easily learned and that learning new sounds beyond that number becomes difficult. Meredith and Edworthy hypothesized that in operating environments, where the warnings are meaningful and more varied,

the set of warnings that could be learned might be larger. They recorded actual warnings used in an intensive care unit and trained subjects to identify them. Subjects were able to learn a set of 12 warning sounds within a short time. The warnings most often confused were both continuous, high-pitched tones. The difference in their frequencies was large enough to be easily discriminated when the tones were directly compared, but when longer intervals of time passed between presentation of the two tones, identification became difficult. Sounds with the same temporal pattern, including signals with similar duty cycles (on-off times), were also consistently confused, despite having very different pulse speeds (i.e., periods).

Meredith and Edworthy suggest that confusions might be based on similarities in the semantic labels that subjects attached to the sounds; i.e., sounds that are very different acoustically may be confused because the hearer labels them similarly. If true this would allow possible confusions to be anticipated without undertaking formal confusibility studies. This guideline is consistent with the high-level design review principle of Physiological Compatibility.

4.5.6.3-14 Number of Tonal Signals

When information is coded by the pitch of narrow-band signals (i.e., tones), no more than three frequencies should be used.

ADDITIONAL INFORMATION: The frequencies should not be in a ratio of 2:1 with one another, since it can be difficult to identify pitches an octave apart. Although some sources recommend that no more than 5 separate frequencies should be used, operators may not reliably distinguish among more than three pitch codes. For critical alarms with differing response requirements, the more conservative guidance should be followed. If more than three critical alarms are to be coded, it is preferable to combine pitch with another dimension to create more distinctive signals. See Guideline 4.5.6.3-13, Auditory Signal Discriminability.[6105]

4.5.6.3-15 Frequency of Tonal Signals

Center frequencies should be widely spaced within a range of from 500 to 3,000 Hz, although a wider range of from 200 to 5,000 Hz may be acceptable.

ADDITIONAL INFORMATION: It is recommended that tonal signals be broad band and widely spaced within the 200 to 5000 Hz range.[6105]

4.5.6.3-16 Pulse Codes

No more than three pulse repetition rates should be used for coding purposes.

ADDITIONAL INFORMATION: Repetition rates should be between 1 and 8 pulses per second, since faster rates may not be perceived as pulses. Repetition rates should be sufficiently separated (e.g., differ by a factor of 2) to ensure operator discrimination. Sounds with the same temporal pattern, including signals with similar duty cycles (on-off times), may be confused, despite having very different pulse speeds (i.e., periods). Such signals are therefore more appropriate for coding the level of urgency of a condition than for indicating different types of conditions.[0700, 6105]

Discussion: Meredith and Edworthy (1994) examined the learning of and confusions among a set of alarm sounds used in intensive therapy (i.e., hospital) units. They recorded actual warnings used in an intensive care unit and trained subjects to identify them. Subjects were able to learn a set of 12 warning sounds within a short time. Sounds with the same temporal pattern, including signals with similar duty cycles (on-off times), were consistently confused, despite having very different pulse speeds (i.e., periods).

4.5.6.3-17 Number of Frequency Modulated Signals

No more than three modulated frequency codes for audible alarms should be used.

ADDITIONAL INFORMATION: Warbling sounds, with frequencies modulating from 1 to 3 times per second, are attention-getting as well as easily recognized, whereas slower modulation rates do not develop distinguishable characteristics rapidly enough to be appropriate for alerting applications.[6105]

4.5.6.3-18 Center Frequency of Frequency Modulated Signals

If modulation of frequency (Hz) of a signal is used to denote information, the center frequencies should be between 500 and 1000 Hz.[0700]

4.5.6.3-19 Audio Pattern Codes

If sequences of tones are used to represent information, the patterns should be easily recognizable.

ADDITIONAL INFORMATION: Warning sounds consisting of "bursts" composed of five or more brief pulses (about 0.1 second in duration) with inter-pulse intervals of .15 to .3 seconds have been recommended. The pulses may be designed to be distinctive with respect to their onset and offset shaping, fundamental frequency, and harmonic structure. The bursts may vary as to the number of pulses, the tempo at which they are presented, and the rhythmic and pitch contours.[6105]

Discussion: The resulting signals might be described as brief syncopated melodies. These bursts are not presented continuously, but are repeated at appropriate intervals. For example, an incoming alarm might be accompanied by a burst, repeated 1-2 seconds later to give a busy operator, alerted by the first presentation, an opportunity to grasp the message. The signal might then remain off for several seconds, allowing operators to communicate if necessary. If the alarm were urgent and remained unacknowledged, the burst might then be repeated at greater volume and/or at a faster tempo. A less critical alarm might repeat less frequently at a slower tempo.

Edworthy (1994) summarizes a series in studies which demonstrated that the perceived urgency of audio signals could be reliably measured, that relative urgency could be predicted based on the acoustical properties of the signals, and that psychophysical techniques could be used to identify the parameters that are most effective in producing changes in urgency. Edworthy notes that these results can be used not only to create sets of warning signals that differ in perceived urgency, but also to design signals with similar perceived urgencies that are nevertheless readily distinguishable from one another.

4.5.6.3-20 Compound Codes

A maximum of nine auditory signals should be used when coded in two or more dimensions.

ADDITIONAL INFORMATION: When signals differ in two or more dimensions (e.g., pitch and temporal pattern), a greater number of signals can be reliably distinguished. This maximum includes auditory signals used outside of the control room (e.g., fire alarm or site emergency alarm). The number of conditions for which reliably recognizable audio codes can be used can be maximized by taking advantage of differences in the perceived urgency of warning sounds. The potential confusibility of signals should be considered in the design of these more complex signals (see Guideline 4.5.6.3-13, Auditory Signal Discriminability).[6105]

Discussion: Meredith and Edworthy (1994) demonstrated that in operating environments, where the warnings are meaningful and more varied, the number of warnings that could be learned might be larger than five or six, as had been previously suggested based on laboratory research. Their subjects were able to learn a set of 12 warning sounds within a short time. The warnings most often confused were both continuous, high-pitched tones. The difference in their frequencies was large enough to be easily discriminated when the tones were directly compared, but when longer intervals of time passed between presentation of the two tones, identification became difficult. Sounds with the same temporal pattern, including signals with similar duty cycles (on-off times), were also consistently confused, despite having very different pulse speeds (i.e., periods). Meredith and Edworthy suggest that confusions might be based on similarities in the semantic labels that subjects attached to the sounds; i.e., sounds that are very different acoustically may be confused because the hearer labels them similarly. If true this would allow possible confusions to be anticipated without undertaking formal confusibility studies.

4.5.6.3-21 Intensity Coding

Coding of auditory signals by intensity (loudness) should not be used.

ADDITIONAL INFORMATION: The range of intensities between the level required to ensure audibility and the level at which signals become aversive can be relatively narrow; the usefulness of this dimension for coding is therefore limited. If such coding must be used, no more than two levels should be defined. The signals should differ from each other by a minimum of 6 dB(A). The lower intensity should be about 10 dB(A) above the ambient noise level, and the maximum signal-to-noise ratio should be 10 dB(A) for most applications of sound intensity coding. It is recommended that sound intensity should be limited to a maximum of 95 dB(A), but that signal levels of 115 dB(A) may be used if considered absolutely necessary to achieve required attention-getting reliability for alarms indicating extreme danger. Whether this coding would be effective would depend on the frequency spectrum of the ambient control room noise and the frequency of the signal.[0700, 6105]

4.5.6.3-22 Speech Presentation of Alarm Information

Using speech alone for presenting alarm information is not recommended.

ADDITIONAL INFORMATION: Speech is an acceptable medium for presenting interface-related information (see Section 1.2.11, Speech Displays), and there may be advantages associated with using speech for presenting alarm information as well. However, its appropriateness has been questioned

for tasks where there is a memory component, there is likely to be some delay before the fault is attended to, there is likely to be more than one alarm presented at a time, and the operator is required to assimilate information from a variety of sources using spatial reference. Therefore, it has not yet been shown that it is an appropriate method for presenting alarm information in process control contexts. Speech should only be used in conjunction with other methods of presenting alarm information.

Discussion: Stanton
1994b) points out that presenting alarm information by means of speech displays has a number of potential benefits in process control contexts. These include the ability to capture attention regardless of operator's location or direction of gaze, the lack of any requirement to learn the meanings of codes, and the possibility of reducing the load on the visual channel. Stanton and Baber (1997) compared presentation of alarm information by means of synthesized speech, message list, or using the two combined. Subjects were required to respond to alarms and diagnose failures in a simulated industrial process while also performing a spatial secondary task. Performance measures included process output, time taken to acknowledge and investigate alarms, number of inappropriate actions taken, and number of alarms correctly recalled (in an unanticipated test after the experiment). Performance for the speech-and-text and the text-alone presentations did not differ; performance with speech-alone was significantly worse on a number of measures. Stanton and Baber suggests a number of characteristics of speech signals that may can be problematic in certain circumstances. For example, a speech message demands attention during its entire duration, and the signal is transitory - once it is presented, it is gone. Accordingly there is a memory requirement for information that needs to be kept available, and the study showed that memory for information presented using speech was poor.

Stanton points out that these characteristics conflict with aspects of the process control setting; e.g., operators sometimes do not (or can not) respond immediately to alarm information, multiple alarms may be present simultaneously, and it is necessary to respond to information from more than one source.

Edworthy and Adams (1996) consider the use of voice warnings in noisy environments, where intelligibility is a major issue. They note that maintaining intelligibility when speech is amplified requires the relative intensity of the low and high frequency portions of the signal to be adjusted appropriately. Simply making normal speech louder can reduce intelligibility owing to increased masking of some components of the speech signal by others; the situation is complicated when noise in the environment masks portions of the signal.

The use of synthesized speech in noisy environments has been recommended because the frequency spectrum of synthesized speech can be tailored to the ambient noise more easily than that of natural (recorded or digitized) speech. However, there is also evidence to suggest that processing of synthesized speech imposes greater cognitive demands. Technological advances in synthesized speech production may have mitigated this problem, but until this issue is explored further, the use of synthesized speech in high workload settings may not be advisable. Edworthy and Adams also point out that available research comparing the efficacy of speech and non-speech warnings tends to involve traditional signals (such as sirens or bells), not the better-designed audio signals that represent the current state of the art.

Speech messages can be presented at faster-than-normal rates, thereby mitigating potential problems associated with the length of warnings presented in this way. Edworthy and Adams review recent literature which shows that high speech rates result in faster reaction times. They point out that this might be due simply to the information being conveyed in a shorter time, or to the increased perceived urgency of quickly spoken messages. More importantly however, as might be expected, they note that very high rates (e.g., 250 words/minute) can degrade intelligibility.

Despite some potential advantages of speech over other means of presenting information, it has not yet been shown (based on the above discussion) that speech is an appropriate alarm medium for process control contexts. Stanton and Baber conclude that "speech alone as a medium for alarm displays cannot be recommended for tasks where there is a memory component, there is likely to be some delay before the fault is attended to, there is likely to be more than one alarm presented at a time, and the operator is required to assimilate information from a variety of sources using spatial reference. If speech is to be incorporated into the alarm system for ‘process control' tasks, it is recommended that it be paired with other media such as a scrolling text display."

4 ALARMS
4.5 Display
4.5.7 Display Layout and Organization
4.5.7.1 Spatially Dedicated, Continuously Visible Alarm Displays

4.5.7.1-1 Functional Grouping of Alarms

Alarms within a display should be grouped by function, system, or other logical organization.

ADDITIONAL INFORMATION: Alarm elements should be grouped so that system functional relationships are readily apparent. For example, area radiation alarms should be grouped on one display, not spread throughout the control room. As much as possible, the alarms should be grouped with controls and displays of the same system.[0700, 6105]

Discussion: Roth and O'Hara (1998) conducted a study of the integration of advanced interfaces, including an advanced alarm system, into a control room. A key feature of the alarm system was that the alarm display was organized functionally, based on a goal-means decomposition of the plant (Rasmussen, 1986). Crews were observed during their initial training with the new system on a full-scope simulator, and interviews were conducted with operators and other utility and vendor personnel. The training included full-scope simulations of plant disturbances. Operators indicated that the functional organization of system was helpful. One commented while operators deal with disturbances in terms of goals, the old tile-based alarm system was not organized in that way (it instead reflected the physical location of equipment). The operators indicated that the system's organization was very helpful and enhanced their understanding of plant state.

4.5.7.1-2 Separation of Functional Groups

Alarm functional groups should be visually distinct from one another.[6105]

ADDITIONAL INFORMATION: Although the concept of functional grouping is typically applied in the context of spatially-dedicated, continuously-visible displays, it can be applied to alarm lists as well. Segregating alarm messages by plant system may allow operators to direct their attention more effectively, especially when individual members of a crew are assigned principal responsibility for different plant systems.

Discussion: The simulation study of alarm display designs conducted by O'Hara et al. (2000) included an SDCV display consisting of tile-like elements presented on VDUs and alarm lists. The organization of SDCV alarms by functions and systems was favorably commented on by the operators who participated in the study. In addition, operators noted that the organization of the alarm message lists by primary and secondary side of the plant reduced the number of alarms presented to any one operator and enabled operators to better understand the disturbances in the side of the plant they were responsible for. The design of the Advanced Main Control Board being developed for advanced Japanese PWR plants (Shimada et al., 1996) combines a large overview display with CRT displays. For easier recognition, alarms displayed on the console are categorized according to plant system as well as priority. Although the validation test described by Shimada et al. did not address this display feature *per se*, performance using the new design (as compared with the conventional alarm system) was reported to be improved (with respect to user acceptance, secondary failure detection, and workload reduction).

4.5.7.1-3 Group Labels

System/functional groups should be clearly delineated and labeled such that the operating crew can easily determine which systems have alarms that have not yet cleared and which system is affected by a particular incoming alarm.[6105]

4.5.7.1-4 Coordinate Designation Identifiers

If alarm displays are organized in matrices, the vertical and horizontal axes of the displays should be labeled with alphanumerics for ready coordinate designation of a particular visual element.

ADDITIONAL INFORMATION: Coordinate designation is preferred on the left side of rows to support left-to-right reading and the ends (e.g., tops or bottoms) of columns ~~top sides~~ of the display.[0700]

4.5.7.1-5 Density of Alarm Elements

An alarm tile display matrix should contain a maximum of 50 alarms per matrix.

ADDITIONAL INFORMATION: Matrices smaller than 50 alarms are preferred.[0700]

4.5.7.1-6 Logical Arrangement of Alarms

Alarms should be ordered to depict naturally occurring relationships.

ADDITIONAL INFORMATION: Naturally occurring relationships (e.g., those derived from the physical process) include the following:

- pressure, flow, level, and temperature alarms in fluid systems;
- alarms for a given thermodynamic parameter at different points within the system which indicate a progression (e.g., within a fluid system, a series of pressure alarms starting with the source tank and ending with the system discharge);
- several alarms for the same variable indicating levels of severity (e.g., tank level low and tank level low-low); and
- alarms related by cause and effect.

For example, pressure, flow, level, and temperature could be arranged left-to-right.[6105]

4.5.7.1-7 Consistent Ordering

Alarm parameters (e.g., level, flow, pressure, and temperature) arranged in one order on one panel should be arranged in the same order on other panels.

ADDITIONAL INFORMATION: Once an arrangement has been chosen, the arrangement should be used consistently within similar systems or alarm groups. Redundant components identified as A, B, and C that are placed left-to-right for one alarm display should be placed consistently for all displays; elements arranged in left-to-right order to represent how fluid flows through one system should be in the same order for other systems.[6105]

4.5.7.1-8 Alarm Display Identification Label

Each group of alarm displays should be identified by a label above the display.

ADDITIONAL INFORMATION: A group of displays could be a panel of tiles or a group of VDU-type alarm displays.[0700,6105]

4.5.7.2-1 Listing by Priority

Lists of alarm messages should be segregated by alarm priority with highest priority alarms being listed first.[6105]

4.5.7.2-2 Message Listing Options

In addition to priority grouping, operators should have the capability to group alarm messages according to operationally relevant categories, such as function, chronological order, and status (unacknowledged, acknowledged/active, cleared).

ADDITIONAL INFORMATION: For example, the alarm messages should be capable of being listed in chronological order with the most recent messages placed at the top of the stack (i.e., alarm messages entered in a pushdown stack mode). Grouping alternatives should not interfere with the operator's detection of high-priority alarms.[6105]

Discussion: Among the alternatives simulated in the O'Hara et al. (2000) study was a condition in which alarms assigned a lower priority were presented on a separate display unit from alarms with higher priorities. Operators in the study indicated the need for time and priority considerations. They expressed a desire not to have too many separate lists (such as separate lists for different priorities) because it would make it difficult to see overall timing and sequence of all alarms, which they felt was important for situation assessment. Thus it is important to provide operators with methods of using lists in various ways based on their information needs.

Roth and O'Hara (1998) conducted a study of the integration of advanced interfaces, including an advanced alarm system, into a control room. In addition to the advanced system, there were two other alarm systems available to operators. One was the original tile-based alarm system that was implemented at the time the plant was built. The tiles are typical of conventional alarm tiles that are organized into matrices by plant functions and systems. The other was an existing, chronologically-organized VDU message list display which contained alarm setpoints associated with every plant parameter on the plant data highway. It was observed that, during normal operations, operators relied on the chronological-list alarm system because it was useful for picking up early signs of minor malfunctions (e.g., equipment problems). In an emergency, the large number of alarms generated and chronological list organization made this system ineffective. This illustrates that the information required by operators, and therefore the preferred organization of alarm lists, may be different in normal and emergency conditions.

4.5.7.2-3 Blank Lines

Alphanumeric alarm lists should have a separation (blank row) every four or five alphanumeric messages.[6105]

4.5.7.2-4 Scrolling of Message List

The method of adding alarm messages to the list should preclude message scrolling.

ADDITIONAL INFORMATION: Scrolling makes it difficult to read alarm messages, especially when many alarms are coming in. An alternative method of viewing alarm lists, such as paging, is preferred.[6105]

4.5.7.2-5 Message Overflow

Alphanumeric alarm messages that overflow the first page of alarm messages should be kept on subsequent alarm pages.

ADDITIONAL INFORMATION: Important alarm information should not be truncated solely because the immediate display space is exceeded. In addition, the alarm system should clearly indicate that additional information is available in subsequent pages.[6105]

4.6.1-1 Access to New Undisplayed Alarms

A VDU-based alarm system should provide rapid access to any new alarm messages that are not shown on the current display.

ADDITIONAL INFORMATION: When a new alarm has been indicated, e.g., by an auditory indication, plant personnel should have rapid access to the alarm information that describes the nature of the alarm condition.[6105]

Discussion: The results of the simulation study by O'Hara et al. (2000) of alarm display designs emphasize the importance ready access to incoming information. Operators were reluctant to scroll to unseen alarm pages (older alarms). Rather than do so they indicated they would use SDCV displays instead (when available) and expressed a desire for additional alarm VDUs. Some operators just abandoned scrolling the alarm lists when workload became high. It is important to provide easy and efficient methods for operators to cope with alarms that are not displayed.

4.6.2-1 Global Silence Capability

It should be possible to silence an auditory alert signal from any set of alarm system controls in the primary operating area.

ADDITIONAL INFORMATION: A global silence capability together with separate silence and acknowledge capabilities can be useful during high alarm situations. It can allow the operator to silence many distracting alarms and then acknowledge these alarms at their respective panels. It is not necessary that silence capability be provided only where the specific alarm can be read, so long as the operator is made aware of all alarms that are being silenced. That is, the operator should not be able to silence alarms that cannot be visually detected from the global silence control. The primary purpose of the auditory signal is to alert the operator to a new alarm. Once alerted, the operator refers to visual indications of the specific alarm and its message. The auditory signal can rapidly become distracting and irritating to the operators. It should be possible to silence an audible cue from either a VDU or a tile panel control station (see also Guideline 4.6.1-4).[0700,6105]

4.6.2-2 Manual Silencing

Auditory signals should be silenced manually by the operators unless this interferes with other more critical operator actions.

ADDITIONAL INFORMATION: While manual silence is a generally desirable feature to get the operator's attention, it may become distracting to manually silence all alarms under high-alarm conditions. Guidelines 4.7-1 and 4.7-2 address alarm system configuration changes made either automatically or by operator-selection, such as automatic silence of auditory alerts for lower priority alarms under high-alarm conditions.[6105]

4.6.3-1 Effect of Acknowledge Function

An alarm acknowledgment function should cause the alarm to change to a visually distinct acknowledged state and the alerting function (e.g., flashing and audible tone) should cease. (Also see guideline 4.5.3-4.)
~~terminate the flashing of an alarm and have it continue at steady illumination until the alarm is cleared.~~[0700]

4.6.3-2 Acknowledgment Locations

Acknowledgment should be possible only from locations where the alarm message can be read.

ADDITIONAL INFORMATION: If alarm information is available at multiple VDUs, then operators should be capable of acknowledging the alarm from the VDU at which they are working. If alarm information is presented on a large control room overview display, operators should be able to acknowledge it from alarm control locations where it can be seen. This flexibility will minimize disruption caused by the alarm system interactions. It should not be possible to acknowledge alarms from locations where they cannot be read. If alarms can be acknowledged from multiple locations, then a means should be provided for ensuring that all operators for whom the alarm is important are aware that the alarm occurred. These means may include spoken, telephone, or computer-based communications between personnel.[6105]

Discussion: This guideline is consistent with the high-level design review principle of Error Tolerance and Control.

4.6.3-3 Acknowledgment of Alarm Messages

Non-SDCV alarms should only be acknowledged when the alarm message is on the screen.

ADDITIONAL INFORMATION: Alternatively, the acknowledgment action may display the alarm message.[6105]

Discussion: This guideline is consistent with the high-level design review principle of Error Tolerance and Control.

4.6.4-1 Effect of Reset Function

The reset function should place the alarm system in an unalarmed state after an alarm has cleared.

ADDITIONAL INFORMATION: The reset function should silence any audible signal indicating clearance and should extinguish the light and return the alarm to an inactive state. Note that some alarms may have automatic reset, when it is not necessary that the operators specifically know the reset condition.[0700]

4.6.4-2 Appropriate Use of Manual Reset

A manual reset sequence should be used where it is important to explicitly inform operators of a cleared condition that had once been deviant.

ADDITIONAL INFORMATION: An automatic reset sequence should not be used in this situation.[6105]

4.6.4-3 Appropriate Use of Automatic Reset

An automatic reset sequence should be available where operators have to respond to numerous alarms or where it is essential to quickly reset the system.

ADDITIONAL INFORMATION: A manual reset sequence should not be used in high-workload situations in which the time and attention required to reset the alarms may detract from other, more-critical tasks .[6105]

4.6.4-4 Reset Function Location

The reset function should be effective only from locations at which plant personnel know which alarm they are resetting.[0700,6105]

Discussion: This guideline is consistent with the high-level design review principle of Error Tolerance and Control.

4.6.5-1 Operator-Selectable Alarm System Configuration

If the alarm system provides operator-selectable operational configurations, then these configuration changes should be coupled with an indication of the present configuration.

ADDITIONAL INFORMATION: Alarm systems may provide the capability for operators to select alternative functional configurations of the alarm system under some alarm situations, such as automatic silence of auditory alerts for lower priority alarms under high-alarm conditions. Another example may be operator selection of an alarm message suppression mode in which low priority messages are not presented via the alarm displays but may be accessed through operator action. It is important that the alarm system informs the operators that a requested change in system configuration has been successfully achieved. In addition, a prominent display of the present configuration should be available.[6105]

Discussion: Roth, Mumaw, Vicente, and Burns (1997) conducted extensive observations and interviews of nuclear power plant operators with the aim of understanding the nature of operators' cognitive activity during normal operations. They concluded that, rather than being a vigilance task, monitoring during normal operations is an active process involving selective attention. According to Roth et al., monitoring activities include confirming expectations about plant state, pursuing unexpected findings, checking for problems considered to be likely, validating initial indications, and interpreting specific indications. Roth et al. also describe changes that operators make to the alarm interface in order to enhance the information available and reduce cognitive demands during these activities. Among these are attempting to enhance the salience of selected signals and reduce "noise" or clutter, establishing bases for monitoring parameter trends, creating new alarms or reminder indications, and creating external cues concerning the configuration of the interface. Whenever the alarm system behavior is changed, mode errors are possible; see the discussion of in Guideline 4.7-1.

4.6.5-2 Acknowledgment of Operator Alarm System Configuration Changes

Operator acknowledgment (or confirmation) should be required if a significant alarm system configuration change is to be made by operator selection.

ADDITIONAL INFORMATION: Alarm systems may provide the capability for operators to select alternative functional configurations of the alarm system under some alarm situations. An example may be operator selection of an alarm message suppression mode in which low priority messages are not presented via the alarm displays but may be accessed through operator action. It is important that the alarm system informs the operators that a requested change in system configuration has been successfully achieved. In addition, a prominent display of the present configuration should be available.[6105]

Discussion: See discussion of mode error in Guideline 4.7-1.

4.6.5-3 Operator-Defined Alarms/Setpoints

The alarm system may provide temporary, operator-defined alarms and operator-defined set points for specific conditions where such alarms are determined to be of assistance to the operators in selected evolutions (e.g., temporary alarms to support increased monitoring of a problem component, or at other times when the operator wants to know of a parameter trend that is approaching a limit).

ADDITIONAL INFORMATION: In addition, administrative controls should control the definition and removal of operator-defined alarm system characteristics.[6105]

Discussion: Operators have suggested that there should be more states associated with some alarms, rather than just single alarm limits, for example, greater use of “margin” alarms (Beattie and Vicente, 1996). See discussion of operator initiated changes to the alarm system interface in Guideline 4.6.5-1; see also the discussion of mode error in Guideline 4.7-1.

4.6.5-4 Interference of Operator-Defined Alarms/Setpoints with Existing Alarms

Operator-defined alarms and setpoints should not override or interfere with the existing alarms and setpoints.

ADDITIONAL INFORMATION: In addition, administrative controls should control the definition and removal of operator-defined alarm system characteristics.[6105]

Discussion: This guideline is consistent with the high-level design review principle of Error Tolerance and Control.

4.6.5-5 Control of Operator-Defined Alarms/Setpoints

The alarm system should provide clear indication of operator defined alarms and setpoints as distinct from the alarm/setpoints designed into the system.

ADDITIONAL INFORMATION: In addition, administrative controls should control the definition and removal of operator-defined alarm system characteristics.[6105]

Discussion: The ways in which the existence and status of operator-defined alarms should be indicated to operators has not been explicitly addressed. Hickling (1994) considers the use of audible signals to indicate conditions which are not alarms, e.g., an operator-defined unique audible signal to indicate completion of a process. He notes that advances in the design of audio displays make it conceivable add to the number of 'alarms' since it is now possible to effectively differentiate signals associated with the (excepted) completion of a process from those that indicate an unexpected fault or deviation. See discussion of mode error in Guideline 4.7-1.

4.6.6-1 Automated Alarm System Configuration

If the alarm system automatically changes operational configurations under some alarm situations, then these configuration changes should be coupled with an alert to the operator and an indication that the configuration has changed.

ADDITIONAL INFORMATION: Alarm systems may provide automated functions under some alarm situations, such as automatic silence of auditory alerts for lower priority alarms under high-alarm conditions. It is important that operators be notified of the change in system functioning. In addition, a prominent display of the present configuration should be available to remind operators of the current configuration of the system.[6105]

Discussion: The configurable aspects of the alarm system can give rise to operator error due to confusion over changing modes of operation. A common human error, called "mode error," in digital, reconfigurable systems is failure to recognize the current operating mode of the system in use and, as a result, improperly interpret and use the information provided (Cook, Woods, and Howie, 1990; Sarter and Woods, 1992). In addition, this guideline is consistent with the high-level design review principles of Situation Awareness, Feedback, and Error Tolerance and Control.

4.6.6-2 Acknowledgment of Automatic Alarm System Configuration Changes

Operator acknowledgment (or confirmation) should be required if a significant alarm system configuration change is to be made automatically.

ADDITIONAL INFORMATION: Alarm systems may provide the capability for operators to select alternative functional configurations of the alarm system under some alarm situations, such as automatic silence of auditory alerts for lower priority alarms under high-alarm conditions. It is important that the alarm system informs the operators that a requested change in system configuration has been successfully achieved. In addition, a prominent display of the present configuration should be available.[6105]

Discussion: See discussion of mode error in Guideline 4.6.6-1.

4.6.6-3 Automatic Mode-Defined Setpoints

If an alarm system provides automatic adjustment of setpoints for different plant modes or conditions, it should be evaluated whether operator acknowledgment/confirmation of the significant changes is necessary.

ADDITIONAL INFORMATION: Alarm systems may alter setpoints in a effort to minimize nuisance alarms. While, such changes may be associated with well-understood, easily recognizable plant conditions, others may be less familiar and not readily understood by plant personnel. In the latter situation, plant personnel may misunderstand the alarm information because they do not realize the setpoints have changed. When this situation is of concern, operator confirmation of the change should be considered.[6105]

Discussion: ‘Dynamic thresholding' of setpoints for a limited number of parameters (i.e., alarm thresholds that depend on operating context, e.g., reactor power) is among the processing techniques used in the improved annunciation strategy for CANDU plants developed by AECL (Davey et al., 1995)

4.7-1 Separate Controls for Alarm Functions

Separate controls should be provided for silence, acknowledgment, reset (acknowledging an alarm that has cleared and returning it to normal), and testing.

ADDITIONAL INFORMATION: A global silence capability together with separate silence and acknowledge capabilities can be useful during high alarm situations by allowing the operator to silence many distracting alarms and then acknowledge these alarms at their respective panels. A variety of controls is possible, such as pushbuttons, function keys, and on-screen controls.[0700, 6105]

4.7-2 Distinct Coding of Control Functions

Alarm system controls should be distinctively coded for easy recognition.

ADDITIONAL INFORMATION: The controls should be distinguishable from each other, by touch and sight, to prevent accidental operation of the wrong control. Such techniques as color coding, color shading the group of alarm controls, demarcating the group of alarm controls, or shape coding should be used.[0700, 6105]

4.7-3 Consistent Layout of Control Group

Each set of alarm system controls should have the functions in the same relative locations.

ADDITIONAL INFORMATION: Consistent locations should be established for silence, acknowledge, reset, and test operating sequence controls.[0700, 6105]

4.7-4 Separate Controls for Tile and VDU Alarms

If the alarm system contains both alarm tiles and VDU alarm displays, each should have its own set of operator controls.

ADDITIONAL INFORMATION: If alarm information is presented redundantly on tile and VDU displays, then alarm acknowledgment via one device (i.e., either the VDU or tile panel control station) should cause the redundant alarm to be automatically acknowledged on the other device. ~~The user should be able to *silence* audible cues from either the VDU or tile panel control station~~. All other control actions (acknowledge, reset and test) should be specific to the workstation associated with the alarm (see also Guideline 4.6.2-1).[6105]

4.7-5 Defeating Controls

Alarm system control designs should not allow the operator to defeat the control.

ADDITIONAL INFORMATION: For example, some pushbuttons used for alarm silencing and acknowledgment can be held down by inserting an object in the ring around the pushbutton. Some soft controls may be easily defeated in software. The alarm system should be designed to prevent the controls from being defeated.[0700, 6105]

Discussion: This guideline is consistent with the high-level design review principle of Error Tolerance and Control.

4.8.1-1 Design for Reliability

The alarm system should be designed so that no single failure will result in the loss of a large number of alarms.[6105]

ADDITIONAL INFORMATION: Also, the failure of a single alarm system component should not result in the loss of an individual alarm important to plant safety.

Discussion: This guideline is consistent with the high-level design review principle of Error Tolerance and Control.

4.8.1-2 VDU Reliability

Where alarms are presented on a VDU as the primary display, operators should be able to access the alarms from more than one VDU.

ADDITIONAL INFORMATION: Failure of a single VDU should not remove the operator's access to VDU-based alarm presentations at their primary workstation. Alarm printer displays should not be the only back-up to a VDU display.[6105]

Discussion: This guideline is consistent with the high-level design review principle of Error Tolerance and Control.

4.8.1-3 Dual Light Bulbs

Annunciator tile-type displays should be designed with dual light bulbs so that a single bulb failure will not interfere with the operator's detection of the alarm condition.

ADDITIONAL INFORMATION: Alarm system displays should be designed with a high level of reliability. In the case of annunciator tile displays, each tile should be lit by two or more light bulbs to protect against loss of indication due to failure of a light bulb.[6105]

4.8.1-4 Flasher Failure Mode

In case of flasher failure of an active alarm element, the element should assume a highly salient state such as a high flash rate or a steady on (e.g., illuminated) state rather than a less salient state such as off.

ADDITIONAL INFORMATION: While it is preferable in the case of a flasher failure for the active alarm element to remain on (e.g., illuminated) rather than off, a unique and highly salient code is best. The code should be unique to prevent confusion between new and acknowledged alarms. It should be salient to alert the operator to the malfunction of the alarm display system. In addition, other alerting mechanisms such as warning messages may be used to inform the operator of a malfunction in the alarm display system.[0700,6105]

Discussion: This guideline is consistent with the high-level design review principles of Situation Awareness and Error Tolerance and Control.

4.8.2-1 Testing Capabilities ~~Availability~~

Test controls should be available to initiate operability tests for all essential aspects of the alarm system (including processing logic, audible alarms, and visual alarm indications).[0700,6105]

ADDITIONAL INFORMATION: Test controls may not be necessary for advanced alarm systems that feature capabilities for continuous, self-testing.

4.8.2-2 Testing Requirement

Periodic testing of the alarm system should be required and controlled by administrative procedure.

ADDITIONAL INFORMATION: Simple functional tests are normally required once per operating shift. Reliability analyses of the alarm system may be used to determine appropriate intervals and degree of testing to be performed on the alarm system.[0700]

4.8.3-1 Design for Maintainability

The alarm system should be designed so that maintenance activities can be performed with minimal interference with the activities of the operators.

ADDITIONAL INFORMATION: Desirable design features may include built-in test capabilities, modular components that can be rapidly removed and replaced, and rear access panels which prevent maintenance activities for obstructing the operator's view of controls and displays.[6105]

4.8.3-2 Tagged-Out Alarms

Tagging out an alarm (taking it out of service) should require disabling of the associated visual and audio signals.

ADDITIONAL INFORMATION: A tagged-out alarm should never be lit or flashing, and should never cause any audible device to sound.[6105]

4.8.3-3 Out-of-Service Alarm Indication

Cues for prompt recognition of an out-of-service alarm should be designed into the system.

ADDITIONAL INFORMATION: Tagging out an alarm should not prevent its identification and should not obscure any other alarm or interfere with operations.[0700, 6105]

4.8.3-4 Extended Duration Illumination

If an alarm tile must be "ON" for an extended period during normal operations because of equipment repair or replacement, it should be (1) distinctively coded for positive recognition during this period, and (2) controlled by administrative procedures.[0700]

4.8.3-5 Tile Cover Replacement

If a lamp replacement requires legend tile removal, there should be a way to ensure that the tile is replaced in the correct location.

ADDITIONAL INFORMATION: The alarm element and/or the replacement task should be designed to prevent incorrect positioning of the cover, legend, or tile. For example, annunciator tiles might be permanently marked with a unique identifier specifying their position in the alarm window matrix.[0700, 6105]

4.8.3-6 Hazard Avoidance

Lamp replacement should not pose an electrical shock hazard.[0700]

4.8.3-7 Aids for Alarm System Maintenance

Aids should be provided, if needed, to assist operators or other personnel in performing alarm system maintenance.

ADDITIONAL INFORMATION: Operator aids include instructions and specialized tools. For example, aids may be needed to support operators in changing light bulbs in the alarm system.[0700]

4.8.4-1 Alarm System Failure Indication

Operators should be given prompt indication of a failure of the alarm system or its major subcomponents.[6105]

Discussion: NRC Information Notice 93-47 describes incidents where the operators were unaware of alarms that were inoperable for long periods of time. Since operators rely on the alarm system as the first indication of a process disturbance, it is important that the alarm system notify the operator of any loss of functioning when it occurs. In general, the alarm system should have a fail-safe design in which the alarm system assumes a configuration that is more consistent (rather than less consistent) with safety when a malfunction occurs (e.g., loss of the flash capability results in salient indication rather than a steady off state). Alarm system functional criteria including failure indication are addressed in NUREG/CR-3217. In addition, this guideline is consistent with the high-level design review principles of Situation Awareness, Feedback, and Error Tolerance and Control.

4.9-1 ARP Scope

ARPs should be available for alarm conditions that require an operator response which affects the plant process control system or plant equipment.

ADDITIONAL INFORMATION: Minor alarms associated with data input errors or computer space navigation errors may not require ARPs. In addition, other alarms such as those in alarm systems that are separate from the main process alarm systems and require simple operator responses, may not need ARPs. In this latter case, the lack of ARPs should be specifically considered and justified.[5908]

4.9-2 ARP Access

Operators should have immediate access to ARPs from the location at which the alarm messages are read.

ADDITIONAL INFORMATION: An operator should not be required to leave the location at which the alarm message is displayed in order to access ARP information. In a tile system, the identification and indexing of ARPs should be consistent with the method of identifying the alarm. The means used for identifying row and column locations of alarms should be distinct so that possible confusion of these identifiers is avoided. A computerized system may display the appropriate procedure for a given alarm on a VDU when the operator "selects" the alarm message.[6105]

Discussion: Recent research on operators' interaction with alarm systems (O'Hara et al., 2000; Roth and O'Hara, 1998) and current characterizations of the cognitive aspects of fault management (Woods, 1995) emphasize the importance of minimizing the 'costs' of accessing alarm-related information. Operators' reluctance to engage in interface management tasks to access alarm information when workload is high (see, for example, the discussion in Guideline 4.6.1-61) can be assumed to apply to alarm response information as well.

4.9-3 ARP Content

ARPs should contain the following information:

- The system/functional group to which the alarm belongs,
- The exact alarm text or legend,
- The alarm source [i.e., the sensor(s) sending the signal, processors and ~~including processing or~~ signal validation logic, and the actuating device(s) for the alarm with a reference to a schematic diagram on which such devices can be found],
- Alarm setpoints,
- Priority,
- Potential underlying causes for the alarm (e.g., low water level -- feed flow deficient in the long term),
- Required immediate operator actions, including actions the operator can take to confirm the existence of the alarm condition,
- Actions which occur automatically when the alarm occurs (and which the operator should verify as having taken place),
- Followup actions,
- Explanations of relevant alarm processing (e.g., comparisons and combinations of plant parameters; alarm filtering and suppression; alarm setpoints that are conditional, such as setpoint values and time delays used to prevent the occurrence of nuisance alarms when a parameter oscillates in an out of the alarm range), and

- Pertinent references.[6105]

ADDITIONAL INFORMATION: Operators should be given information (such as that associated with 'alarm source' in the guideline) that they can use to confirm the existence of alarmed conditions. (See the discussion in Guideline 4.1-2, Operator Verification of Alarms.)

4.9-4 Information Consistency with the HSI

Information contained in the ARPs should be consistent with information on control boards, in the alarm system, in I&C procedures used to calibrate alarm setpoints, in controlling documents that determine setpoints (e.g., Technical Specifications and accident analyses), in P&IDs, in emergency operating procedures, and in other plant procedures.[6105]

Discussion: This guideline is consistent with the high-level design review principles of Consistency and Error Tolerance and Control.

4.9-5 Presentation Consistency with the HSI

The terminology, conventions, standards, and codes used in the presentation of the ARPs should be consistent with the rest of the HSI.

ADDITIONAL INFORMATION: The ARPs should use the same conventions, such as terminology for plant systems and equipments, identification codes for plant components and parameters, and measurement units, that are used in the main HSI displays and procedures. Defined values, such as alarm setpoints, should be consistent. In addition, information coding schemes used in the ARPs should be consistent with the rest of the HSI. For example, if graphical displays are used in the presentation of the ARPs , then coding conventions, such as symbols, icons and color, should be consistent with the rest of the HSI, such as information presented via plant displays and computer-based systems for emergency operating procedures. For example, if color codes are used to indicate priority, it should have the same meaning across all displays of the HSI.

Discussion: This guideline is consistent with the high-level design review principle of Consistency.

4.9-6 ARP Format

The ARP format should:

- Highlight the ARP identifier on each page of the procedure,
- Highlight important items,
- Locate information categories in the same position on each page,
- Consistently present information throughout the ARP, and
- Minimize the need for operators to page back and forth to obtain the information.[6105]

4.10-1 Display and Line of Sight

Visible alarm indications should be located within about 60 degrees on either side of the direct line of sight of the operator's normal work position.[6105]

4.10-2 Interference from Nearby Indicators

Indicator lights used to present information about the state of equipment should not be located near unilluminated display elements used to represent acceptable plant conditions.[6105]

4.10-3 Location of Alarm System Displays and Controls

Alarm displays and controls should be located in close proximity so that the display can be read while operating the controls.

ADDITIONAL INFORMATION: The design should not require an operator to leave the workstation to acknowledge or reset an alarm.[6105]

4.10-4 Location of First-Out Alarms

First-out displays should be located at the main workstation for the system and/or at a plant overview display visible to the crew.[0700]

4.10-5 Consistent Ordering

The ordering (e.g., left-to-right positioning) of displayed alarm groups should be consistent with the ordering of displays and controls of related plant systems and components.[6105]

4.10-6 Location for Prompt Response

Alarm displays and controls should be arranged and located such that the operating crew member(s) who must respond to an alarm can access the alarm information in sufficient time to respond adequately.

ADDITIONAL INFORMATION: The design should never require one operator to read an alarm message only to recite it to another person. Consideration should be given to the need for the senior reactor operator to hear the control room alarms from all parts of the control room vital area.[6105]

4.10-7 Location for Access to Process Controls and Displays

Visual alarm panels should be located near the controls and displays which are required for corrective or diagnostic action in response to the alarm.

ADDITIONAL INFORMATION: If displays and controls associated with an alarm are on different panel segments, ensure that the alarm displays are located near the process display segment. If they are presented on a VDU, easy access to supporting controls and displays should be provided in the display.[0700, 6105]

Discussion: Recent research on operators' interaction with alarm systems
O'Hara et al., 2000; Roth and O'Hara, 1998) and current characterizations of the cognitive aspects of fault management (Woods, 1995) emphasize the importance of minimizing the 'costs' of accessing alarm-related information. Operators' reluctance to engage in interface management tasks to access alarm information when workload is high (see, for example, the discussion in Guideline 4.6.1-61) can be assumed to apply to the physical proximity of information as well.

Appendix C

Alarm System Human Performance Issues

Appendix C

Alarm System Human Performance Issues

The literature reviewed in over the course of this research has led to the identification of a number of human performance issues related to alarm system design. These issues are summarized below. An issue was defined as an aspect of alarm system design for which (1) specific problems were identified, (2) conflicting findings were found in the literature, or (3) a lack of data was evident. They are organized below into four topic area: general issues, processing methods and related issues, display of alarm data, and alarm system controls. The issues are listed in Table C1.

Table C.1 Alarm System HFE Issues

TOPIC	ISSUE
1 General Issues	1.1 Operator-Centered Alarm System Design 1.2 Role and Definition of Alarm Systems 1.3 AWS Lessons Learned and Advanced Alarm Systems 1.4 Context-Specific Alarm Response Characteristics 1.5 Hybrid Systems 1.6 Alarm Setpoints and the Alerted Monitor 1.7 Second Event Detection
2 Processing Methods and Related Issues	2.1 Effects of Processing Methods 2.2 Design Goals of Alarm Processing Systems 2.3 Alarm Information Availability 2.4 Criteria for Prioritization 2.5 Alarm Generation 2.6 Processing Complexity
3 Display of Alarm Data	3.1 Alarm Allocation to Display Types 3.2 Design of VDU Alarm Displays 3.3 Information Content of Alarm Displays 3.4 Hierarchical Displays, Alarm Integration, and Data Layers 3.5 Use of Auditory Cues 3.6 Speech Displays
4 Alarm System Controls	4.1 Increased Complexity with Advanced Alarm Systems 4.2 Role of Automation 4.3. Implementation of Controls in Advanced Alarm Systems

C.1 General Issues

C.1.1 Operator-Centered Alarm System Design

The large number of alarms occurring during a NPP transient overloads the operator's information processing ability. Since fault detection performance decreases as cognitive workload increases, the operator will have a great deal of difficulty handling the flood of alarms associated with process disturbances. The main problems are associated with the limitations of working memory (limited capacity and short duration) and the limited availability of attentional processing resources. As a result, under high workload situations such as NPP transients, signal detection and recognition capability is reduced. The operator samples rather than completely scans alarm information. The operator's information processing system attempts to handle high workload situations through the application of heuristics. These heuristics reduce overall load on the information processing system but can also lead to human error. In light of these aspects of human information processing and the large amount of alarm information presented in a NPP, the operator-centered objectives of the alarm system should include the following parameters:

- support accurate situation awareness,
- minimize the time required to take appropriate action by providing the cues required to activate the operator's mental model which is appropriate to the situation (thus minimizing the higher-level processing and the information processing burden),
- minimize cognitive workload,
- minimize operator error, and
- support operator scanning patterns which may change as workload increases.

Guidance for reviewing alarm system designs for accomplishing these objectives is needed.

C.1.2 Role and Definition of Alarm Systems

The alarm system is the principle source of information for the detection of a specific off-normal condition. However, in conventional NPPs, it is also used for the indication of system/function status and in this role also supports a feedback function on the success of actions taken by the operator. Observations of operators have shown that the status indication function of the alarm system is important to operators. However, the combining of status indication and alarm functions in a single system has contributed to the difficulty operators have with the system under high alarm density conditions. The number of alarms the operator must deal with can be significantly reduced by separation between these functions. In advanced control rooms, such a separation can be easily accommodated. In a conventional control room, replacement of the AWS by an advanced alarm system requires consideration of how to handle the status indication functions of the system. Some of the problems encountered with early attempts to utilize advanced alarm systems possibly stem from the loss of the status indication function. The relationship between alarm and status indication functions needs further research.

C.1.3 AWS Lessons Learned and Advanced Alarm Systems

Analytical studies evaluating the alarm characteristics required to meet the functional requirements of alarm systems have identified a number of features which are generally considered important and if included, can reduce human error-related plant risk. These include, for example, prioritization, alarm inhibit features, first-out alarms (for reactor and turbine trip), reflash, message legibility/intelligibility, and keying alarms to alarm procedures. While these studies were directed to characteristics of conventional alarm systems, the features represent generic alarm system characteristics. However, in spite of the above, there is a limited empirical basis to recommend specific alarm system design features. Thus, the lessons learned from investigations of conventional alarm systems should be carefully examined for their applicability to the design of advanced alarm systems.

C.1.4 Context-Specific Alarm Response Characteristics

The response of the alarm system can be made context specific to assist operators. For example, during a significant process disturbance, some operator tasks, such as silencing the auditory warning of lower priority alarms, may be automated. This possibility can be considered in an effort to make the alarm system more effective under accident conditions. However, such changes to the alarm system operating mode must be accomplished with operator awareness or mode errors may result. One way to accomplish this would be to have no change occur without operator request or acknowledgment. The candidate alarm functions for context specific variation and their implementation need additional research.

C.1.5 Hybrid Systems

The role of alarm systems in hybrid control rooms (i.e., retrofits of advanced alarm systems into existing conventional control rooms) may be different from that in advanced control rooms. In conventional plants, the alarm system exists as an independent system from a safety parameter display system (SPDS) and other plant data displays. Advanced control rooms will have superior data display, integration, and operator aids. This difference could suggest that more should be expected of advanced alarm systems in hybrid plants than needs to be expected of alarm systems in advanced plants.

C.1.6 Alarm Setpoints and the Alerted Monitor

Process control operators are in a monitoring environment that has been described in signal detection theory terms as an "alerted-monitor system." This is a two-stage monitoring system with an automated monitor and a human monitor. The automated monitor in a NPP is the alarm system which monitors the system to detect off-normal conditions. When conditions exceeding the criterion of the automated monitor exist, the human monitor is alerted and must then detect, analyze, and interpret the signal as a false alarm or a true indication of a plant disturbance. Both the human and automated monitors have their own specific signal detection parameter values for sensitivity and response criterion. Sensitivity for the human monitor is strongly affected by alarm system characteristics including set points, the presence of nuisance and false alarms, and alarm density. A significant issue associated with alerted-monitor systems is that optimal overall performance of the alerted-monitor system is a function of the interaction of both components. Optimizing the signal detection parameters for one component of the system may not optimize performance of the entire two-stage system. An alarm setpoint philosophy frequently employed is to attempt to optimize the detection of signals by the automated monitor subsystem. The response criterion is set to maximize the number of disturbances detected. However, this increases the false alarm rate for the automated monitor, which may, in turn, cause the operator to lose confidence in the system and adopt a more conservative criterion and can result in poor overall performance. Further research is needed to understand the optimal integration of the automated and human components of the overall alarm system.

C.1.7 Second Event Detection

Crew awareness of second failures is especially problematic and the alarm processing techniques had mixed success at improving this aspect of performance. Second event detection limitations may be the result of the typical human problem solving strategies: (1) scanning is initiated by signals from the alarm system and the operator’s attention is split between a variety of data gathering activities, (2) the operator "homes in" on a specific group of indicators and makes an initial diagnosis, (3) the operator’s attentional resources seek data confirming the hypothesis, and (4) the operator becomes fixated on the hypothesis and can fail to notice changes in the plant’s state or subsequent new developments. The operator’s awareness of subsequent failures is hampered by limited information processing resources. Since a primary purpose of an alarm system is alerting operators to failure conditions, this problem needs to be addressed further.

C.2 Processing Methods and Related Issues

C.2.1 Effects of Processing Methods

A variety of processing methods (such as mode dependency, state dependency, etc.) were described. However, the relative merits of the individual methods have not generally been evaluated for their effects on operator performance. Of the studies of combined processing methods, the results of the research on the effect of alarm processing on operator performance were equivocal and no clear conclusion emerges. The observed differences in results could be due to many factors such as type of processing used, degree of filtering achieved, method of data display, and familiarization of the subjects with the system. Or the results could be transient dependent, e.g., dependent on the specific scenario or on the operators ability to recognize a familiar pattern. Guidance about processing methods and operator control over the implementation of these methods is needed.

C.2.2 Design Goals of Alarm Processing Systems

Many designers of advanced alarm systems set design goals on the basis of achieving some percentage of alarm filtering, e.g., to reduce by a factor of two the number of alarms during major transients. While this might be reasonable for the application of specific processing approaches, the resulting alarm system might not noticeably improve crew performance. To the human information processing system, reducing incoming alarms by a factor of two may not help at all. The design goal for alarm filtering should be stated in terms of the degree of alarm filtering required to improve human performance. However, present research does not support the development of guidance for this objective.

C.2.3 Alarm Information Availability

Three alarm availability techniques were identified: filtering, suppression, and priority coding. There are trade-offs among these approaches. Filtering completely eliminates the possibility of less important alarms distracting the operators. However, the designer may be removing information useful for other purposes. In addition, the designer must be certain that the processing method is adequately validated and will function appropriately in all plant conditions. Suppression provides the potential benefits of filtering by removing distracting alarms. However, since such alarms are still accessible on auxiliary displays, retrieving them may impose additional secondary task workload. Alarm priority coding does not conceal any information from operators. For example, the DPAS identified above utilizes color coding to distinguish the importance of the alarm messages. Three different colors are used: red, yellow, and green. The red alarms indicate alarm information that the operator needs to know in order to take corrective action or diagnose a problem. The yellow alarms indicate caution information, telling the operator that some automatic feature has actuated and the equipment should be checked. The color green is used for the alarms which do not fall into either of the above two categories and do not require operator attention. However, the method requires operators to perceptually "filter" alarms, using the priority codes, to identify the higher priority alarm messages. This creates the potential for distraction because it presents alarm messages of all levels of importance. Thus an issue remains as to which method should be used or in what contexts the various options should be exercised.

C.2.4 Criteria for Prioritization

Alarm prioritization schemes can be based on several dimensions such as the overall importance to plant safety or the urgency of operator action. The selection of one or more of these dimensions will impact the alarm systems characteristics and operator performance. This issue is also related to the functional basis of the alarm system to provide warnings and status indication of conditions.

C.2.5 Alarm Generation

Alarm generation techniques create new alarms. The generation of alarm conditions and their resulting alarm messages presents an interesting paradox. Alarm systems should facilitate the reduction of errors which often reflect the overloaded operator’s incomplete processing of information (Norman, 1988; Reason, 1987, 1988, 1990). Alarm generation features may mitigate these problems by calling the operator’s attention to plant conditions that are likely to be missed. However, the single most significant problem with alarm systems, as reported in the literature, is the high number of alarm messages presented to the operator at one time. Since alarm generation creates additional alarm messages, it may potentially exacerbate the problem.

C.2.6 Processing Complexity

Many significant NPP events, such as the TMI accident, have resulted from complex combinations of problems occurring. The behavior of alarm filtering systems in such complex situations needs to be addressed when any sophisticated dynamic processing system is utilized. Since the alarm system is the operator's first indication of process disturbances and operators will confirm the validity of alarm signals prior to taking action, it is essential that operators understand what alarm data means and how it is processed. In addition, operators must understand the bounds and limitations of the system.

C.3 Display of Alarm Data

C.3.1 Alarm Allocation to Display Types

A SDCV display (such as is provided by conventional tiles) has been generally found to be superior to a variable message display (as has been typical of some computer-based text message presentations) during high-density alarm conditions. SDCV displays are often thought to provide perceptual advantages of rapid detection and enhanced pattern recognition. The role of integration of alarm information into process displays and other graphic display forms has not received much research and there is little operating experience upon which to draw. While operators appear to prefer graphic displays which integrate alarm and process information, they have not generally been shown to significantly improve performance beyond message lists. Another consideration is that in advanced control rooms, alarm data will be primarily available to the operator at workstation VDUs, thus alarm information may not be readily available to the entire operating crew. Issues concerning the proper allocation of alarm functions to displays need to be addressed.

C.3.2 Design of VDU Alarm Displays

The major attraction of computer-based displays is the flexibility to present alarm information in a wide variety of ways. The research on VDU alarm displays has focused primarily on alarm messages. However, given the problems associated with message lists in high alarm density conditions and operator preference for spatially dedicated displays, further work is needed to explore the appropriate use of graphic displays of alarm information (possibly in combination with message lists). The organization of alarms by system and function has been shown to be preferred by operators and to improve their performance. Approaches to preserve this display approach in VDU alarm displays should be considered. In general, the design of VDU displays for presentation of alarms needs further consideration.

C.3.3 Information Content of Alarm Displays

When alarms occur, operators must determine whether the signal represents an actual or spurious event. The low probability of significant off-normal events in NPPs, and therefore, low expectancy, can make operator acceptance of certain alarms difficult or slow. Upon verification of several consistent indicators, the operator will take appropriate action. In broader terms, alarms are sometimes used in groups to diagnose faults. The specific information needed in alarms to accomplish alarm functions and how that information should be presented needs additional research. Too little information makes the alarm system less useful. Too much information will make it cumbersome to use.

C.3.4 Hierarchical Displays, Alarm Integration, and Data Layers

Related to Issue 3 above, is the issue of how the alarm information is presented to operators, e.g., as single messages, data layers, integrated into other displays, etc. One way of reducing the flood of alarms which operators must deal with in process disturbances is to provide alarm information in hierarchical displays such as integrating lower level alarm information into higher-order alarms. If such a system is to be effective, it must integrate alarms into units that are meaningful to operators and represent units that the operator would have developed without the system. Another method is to present the data in layers, with more detailed alarm information presented in supplemental displays. Such an approach may lower operator alarm processing workload, however, it can also increase the operator's interface management workload. (This type of problem was evident in the Baker (1985) study.) Thus while data layering, organization into display hierarchies, and alarm integration should facilitate operator information processing, their

display characteristics may limit the usefulness of these approaches. More advanced display techniques for alarm data require further investigation.

C.3.5 Use of Auditory Cues

The auditory characteristics of alarms have often been found to be problematic, i.e., startling and distracting. More appropriate and acceptable methods of using tonal cues need to be identified. While the visual features of alarm systems are often overwhelming, the operator's ability to extract information from auditory cues has probably not been fully exploited. For example, zonal auditory cuing (which is used in many plants already) can facilitate the operator's location of alarms. Auditory cues in advanced alarm systems may not have to provide spatial cues, but may be used to convey other information, such as alarm priority or alarm system/function.

C.3.6 Speech Displays

Whether speech displays can be effectively used in the acoustically crowded NPP control room must be investigated. The advantage of speech-based alarms in supervisory control tasks is presumed to be its attention capturing potential, reduction in demands on the visual information channel, ease of understanding the importance and meaning of the message, lack of training required, and public nature of the message. However, studies of its effects have been inconclusive.

C.4 Alarm System Controls

Control interfaces for advanced alarm systems have not been systematically investigated. However, several issues are associated with the application of computer technology to alarm systems.

C.4.1 Increased Complexity with Advanced Alarm Systems

The NPP industry has recommended separate SART controls for conventional alarm systems. The controls associated with advanced systems will likely become much more complicated and will require investigation. While the separate SART philosophy may also apply to advanced systems, additional controls may be required for features such as operator defined alarms, operator adjustment of limits, and operator control of filtering. These control options need to be identified and may require specific guidelines to control their use and assure plant safety.

C.4.2 Role of Automation

In certain situations, such as accident conditions, some operator controls may be automated, such as the silencing of lower priority alarms. However, these changes of alarm system operating mode must be accomplished with operator awareness or mode errors may result. One way to accomplish this would be to have no change occur without operator request or acknowledgment. In general, the most appropriate control functions for automation need to be determined along with their implementation methods. (This issue is related to the Context Specific Alarm Response Characteristics issue identified above.)

C.4.3 Implementation of Controls in Advanced Alarm Systems

In advanced control rooms, alarm systems will be integrated with other interfaces and will, therefore, share control interfaces for some functions, such as, for example, keyboard entry of temporary setpoints. Some control functions may have dedicated control devices, such as SART controls. The mixture of "soft" and hard controls and dedicated vs. shared interfaces needs to be addressed.