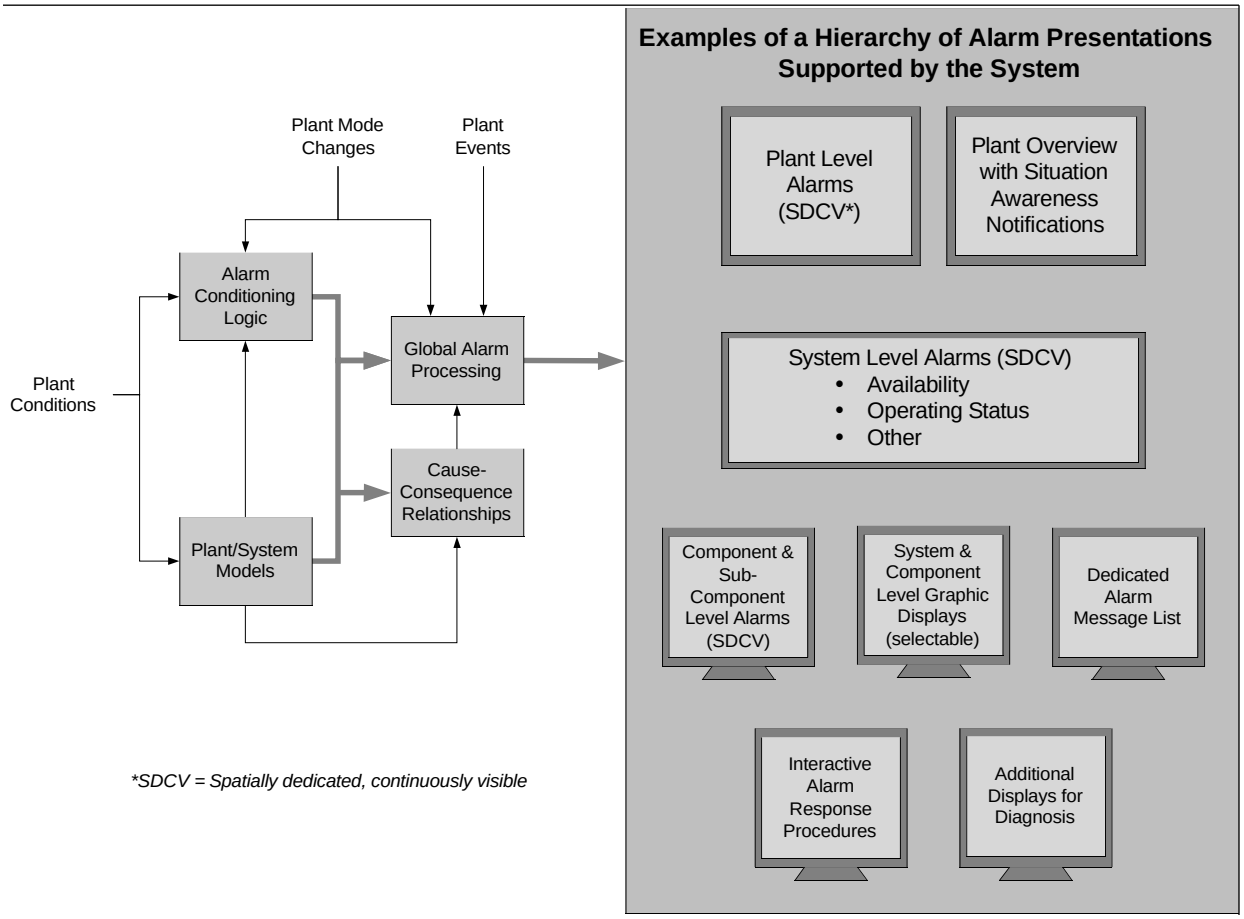
EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Advanced Control Room Alarm System: Requirements and Implementation Guidance

Technical Report



Effective December 6, 2006, this report has been made publicly available in accordance with Section 734.3(b)(3) and published in accordance with Section 734.7 of the U.S. Export Administration Regulations. As a result of this publication, this report is subject to only copyright protection and does not require any license agreement from EPRI. This notice supersedes the export control restrictions and any proprietary licensed material notices embedded in the document prior to publication.

Advanced Control Room Alarm System: Requirements and Implementation Guidance

1010076

Final Report, December 2005

EPRI Project Manager
J. Naser

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1395 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

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

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

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

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

MPR Associates, Inc.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

CITATIONS

This report was prepared by

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

Principal Investigators
R. Fink
D. Herrell
V. Doumtchenko

This report describes research sponsored by the Electric Power Research Institute (EPRI).

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

Advanced Control Room Alarm System: Requirements and Implementation Guidance. EPRI, Palo Alto, CA: 2005. 1010076.

REPORT SUMMARY

Alarms play an important role in helping nuclear power plant control room operators monitor plant systems and equipment and detect off-normal conditions that require their attention. However, conventional alarm systems installed in most operating plants are severely limited in their ability to build intelligence into the alarms and associated displays. As a result, many alarms occur during plant transients and mode changes that are not meaningful and can mask alarms that are important and require operator action. This report defines requirements for an advanced control room alarm system for new or existing nuclear plants that incorporates capabilities that go well beyond current systems and should provide much more effective support for operators under all operating conditions.

Background
As existing plants undergo modernization and new plants are designed, modern control and information system technologies are being employed in instrumentation, control systems, and control rooms. Commercially available systems provide some improved capabilities for alarm handling as compared to conventional systems. However, it is widely recognized in power and other process industries that further improvement is needed to provide effective support to users of alarm information. Considerable research has been conducted on alarm systems, identifying a variety of features and capabilities that show promise for improving system performance. No single system is available that supports these more advanced capabilities.

Objectives
To provide a set of requirements for plant owners and designers in specifying an advanced alarm system for an existing or new nuclear power plant.

Approach
The project team reviewed results of recent research and development related to alarm systems and features provided in commercially available systems and in the alarm systems of new nuclear plants. Recently developed human factors engineering guidelines for alarm systems were used, as well as experience gained in applying those guidelines to define improved alarm system capabilities for plants undergoing control room modernization. The team then identified features and capabilities that are expected to provide significantly improved performance.

Results
Implementing the requirements in this report should lead to an alarm system with a number of important advancements compared to conventional systems. The alarm system will provide a hierarchy of alarm information, allowing operators to quickly determine the impact of alarms on the plant and its major systems. Particularly significant, the system allows operators to drill down

to lower levels of detail to determine the cause of the alarm conditions and take appropriate actions. Alarms that are presented are generated and processed with knowledge of the current operating states of the plant and the relevant systems, so all alarms are "context aware." Alarm information needed by engineering and maintenance personnel is distinguished from information needed by operators. Alarm system reliability and availability requirements are described to help ensure that needed alarm functionality is always available, including limited capability that continues under accident conditions.

EPRI Perspective

EPRI has long identified the need for defining what is required to make an alarm system truly effective for its users. This report pulls together results of several related EPRI projects—plus research and operating experience reported by others—to define what an advanced alarm system should be. The document specifies important functional, design, and performance requirements that can be used as desired by plant owners or designers, depending on the specific needs of each plant. Related EPRI reports are *Information Display Considerations for Designing Modern Computer-Based Display Systems* (1002830), *Alarm Processing Methods: Improving Alarm Management in Nuclear Power Plant Control Rooms* (1003662), and *Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance*" (1010042).

Keywords

Advanced alarm requirements
Alarm systems
Annunciators
Alarm processing
Instrumentation and control systems
Control room
Human-system interface
Operator aids

ABSTRACT

Alarm systems continuously and automatically monitor plant conditions, detect any abnormal conditions, and alert operators when situations occur that require operator action. While they play an important role in plant operation, they also have posed some significant challenges to the users of alarm information. Common problems include too many alarms occurring at too high a rate during upsets, spurious or nuisance alarms, and poor distinction between alarms and status changes. This document defines requirements for an advanced control room alarm system for nuclear power plants. The requirements define a system that overcomes the shortcomings of present alarm systems, takes advantage of the capabilities of newer technologies, and integrates into one system those features that have been shown or are expected to provide significantly enhanced performance and usability for the control room operators and other users of the alarm system.

The requirements can be used in designing an alarm system for a new plant, a new control room for an existing plant, or modernization of the control room for an operating plant. A broad range of capabilities is specified, with the ability for a plant owner, designer or system integrator to enable the features that are desired and to configure the alarm presentations to meet their needs. In addition, it is intended that the requirements will be used in a modular fashion. Plant owners/designers can choose which of the requirements they wish to use to define and procure an alarm system meeting their particular needs.

As it is described here, the "alarm system" need not be a separate, physical system. Rather, the requirements given in this document specify the full range of alarm handling capabilities that should be provided in the control room, regardless of what physical systems provide that functionality. In fact, the most effective implementation is likely one that integrates alarm functionality with other functions of the control and information systems.

The alarm system requirements provided in this document are not specific to any particular instrumentation and control or information system architecture. However, they do assume that modern computer-based systems will be used for monitoring and controlling the plant. This document does not provide all the requirements needed to specify an alarm system completely. The requirements focus primarily on those features and capabilities that are needed to achieve the specific advancements as compared to current systems, and to avoid additional problems that can arise when using computer-based systems to implement an alarm system.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the valuable contributions and insights provided by the following individuals during the development of this report: François Cheriaux and Pierre-Etienne Delon of Electricité de France, Doug Hill of MPR Associates, John O'Hara of Brookhaven National Laboratory, Les Ward of Omaha Public Power District, and Dave Whitsitt of TXU Power.

EXECUTIVE SUMMARY

This document defines requirements for an advanced control room alarm system for nuclear power plants. The requirements can be used in designing an alarm system for a new plant, a new control room for an existing plant, or modernization of the control room for an operating plant. A broad range of capabilities is specified, with the ability for a plant owner, designer, or system integrator to enable the features that are desired and to configure the alarm presentations to meet their needs. In addition, the requirements can be used in a modular fashion. Plant owners and designers can choose which of the requirements they wish to use to define and procure an alarm system to meet their particular needs.

Advanced Alarm System Features

Alarm systems play an important role in plant operation, but they also have posed some significant challenges to the users of alarm information. Common problems include too many alarms occurring at too high a rate during upsets, spurious or nuisance alarms, and poor distinction between alarms and status changes. The requirements given in this document should provide an alarm system with a number of important advancements that directly address the problems experienced with conventional systems. Refer to the figure below, which illustrates some of the key features of the advanced alarm system.

Support for a Hierarchy of Alarms and Alarm Presentations

One of the shortcomings of conventional systems is that alarms typically are generated based on low-level conditions such as pressures, temperatures, and flows. The advanced alarm system specified here generates and displays alarms at multiple levels in a hierarchy, matching the hierarchy of plant information displays presented to the operators. This includes generating plant-level alarms, alarms at the system or function level indicating availability and operating status of major plant systems and critical functions, and more detailed alarms at the component or individual parameter level. This approach supports the operators' need to determine quickly the impact of alarms on the systems and the plant, and to drill down to the more detailed information needed to determine an appropriate response.

Generation of Alarms that are "Context-Aware"

Alarm conditioning logic, supplemented where possible by simple models of the plant systems and processes, makes the alarms more intelligent and aware of plant and system states. Additional processing based on plant mode and major events provides further assurance that alarms will not become nuisances, contribute to alarm overload during upsets, or cause large numbers of standing alarms during non-power operating modes.

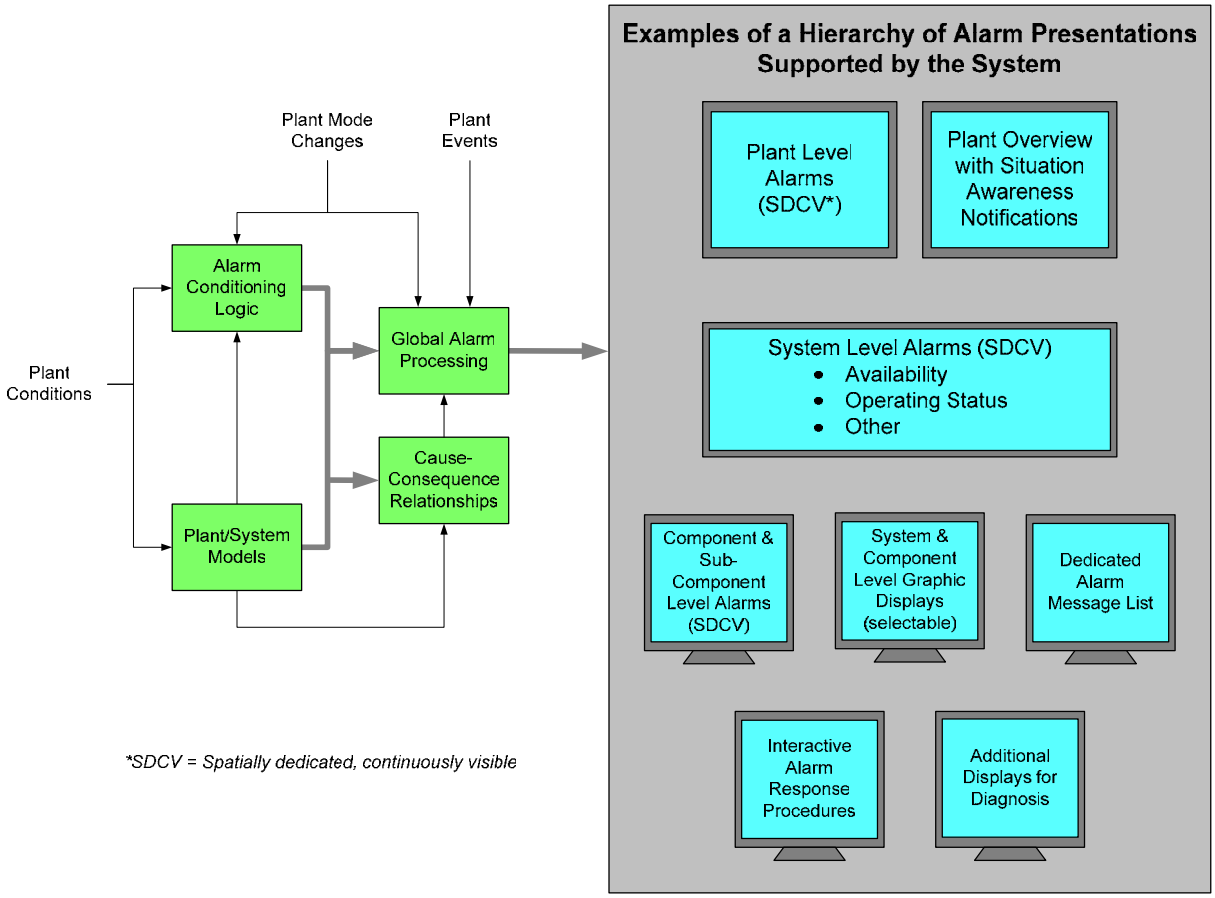


Figure 1
Advanced Alarm System Features

Separation of Status information from Alarms

Alarm systems are often used to present status changes that do not require any operator action, and thus contribute to the overall number of alarm indications and reduce the effectiveness of the alarm system. In the advanced alarm system, status changes that are important to the operators' ability to maintain situation awareness are processed and routed to a separate display specifically designed to promote situation awareness. Operators are alerted to the new status information, but they are not required to take any action. This allows them to focus on alarms or other important tasks until they have time to examine the changes in plant or equipment status.

Separation of Maintenance Notifications from Alarms Needing Operation Action

Some alarms require action primarily by maintenance personnel. Operators may need to be alerted to these conditions, but the information needs of the operator and the maintenance technician are likely to be quite different. The advanced alarm system provides information to the operator on the operational impact and the operator action needed to respond to the detected fault or failure. The maintenance staff gets their detailed information on the fault at a maintenance workstation, helping them focus on locating and repairing the faulty equipment.

Better Support for Responding to Plant Transients and Events

The advanced alarm system provides alarm presentations and aids that help the operator determine quickly what short-term actions need to be taken in response to plant upsets, diagnose the cause of the event, and determine appropriate longer-term corrective actions. Alarm response procedures are presented directly by the system, to facilitate confirming and responding to individual alarms. Built-in cause-consequence relationships among alarms are used to either automatically diagnose the cause of an event, or provide information to the operator to assist in diagnosing the cause. Alarms or events that are unusual for a given transient are highlighted, and events that were expected but did not occur are identified.

High Reliability and Availability under both Normal and Accident Conditions

Total failures of some computer-based alarm systems have occurred in the past, resulting in loss of updated alarm data for some time until the staff could restore the system to operation. This document provides requirements for redundancy and fault tolerance, with appropriate failure analyses demonstrating protection against single failures and common cause failures such that large-scale loss of alarm functionality should not occur during the lifetime of the plant. In addition, features are provided to allow the operators to regularly confirm proper alarm system operation and exercise it from end to end, building confidence, and demonstrating that no "silent" failures have occurred. In addition, the requirements call for a portion of the alarm system to be implemented using qualified equipment, so that at least a minimum level of alarm functionality needed during accidents will be available to the operators.

Ability to Create and Manage User-Defined Alarms

The advanced alarm system allows the operator to define and manage temporary alarms for special situations in which enhanced monitoring of equipment is required, or special system configurations are used that require temporary alarms.

Additional Guidance for Implementation of the Requirements

In addition to requirements for the alarm system, this report also provides high-level requirements for the plant's overall alarm management program. Even the best alarm system will not meet expectations if the plant does not design, maintain, and operate the alarm system within the context of an appropriate alarm management program.

The report also provides implementation guidance that can be used when applying the advanced alarm system requirements. Guidance is provided for applying the requirements to new designs and to modernization of existing control rooms, defining the system architecture, and employing human factors engineering principles and methods in the design and evaluation of the alarm system. The guidance emphasizes the importance of simplicity in the design, and ensuring that there is adequate user participation from the beginning to the end of the design and implementation process.

CONTENTS

1 **INTRODUCTION 1-1**

1.1 Objective 1-1

1.2 Applicability 1-1

1.3 Contents of This Document 1-2

2 **ALARM SYSTEM IN THE OVERALL CONTEXT OF ALARM MANAGEMENT 2-1**

2.1 Alarm Management 2-1

2.2 Alarm System 2-3

Inputs 2-3

Alarm Generation 2-4

Alarm Processing 2-4

Alarm/Event Routing 2-4

Alarm Presentation and User Interaction 2-5

ARP Presentation 2-5

Alarm Controls 2-6

User-Definable Alarm Features 2-6

System Configuration and Maintenance 2-6

Alarm System Performance Monitoring 2-6

3 **BACKGROUND AND BASIS FOR THE REQUIREMENTS 3-1**

3.1 Background 3-1

3.2 Basis and Objectives of the Requirements 3-3

Full Hierarchy of Alarms 3-4

Alarms Generated are Context-Aware 3-5

Status Changes Separated from Alarms 3-5

Maintenance Alarms Separated from Operator Alarms 3-6

Better Support for Responding to Plant Transients and Events 3-6

High Reliability and Availability in Normal and Accident Conditions 3-8

User-Defined Alarms 3-8
3.3 Limitations of the Requirements 3-9

***4* ADVANCED ALARM SYSTEM REQUIREMENTS 4-1**
4.1 Objectives of the Alarm System 4-1
4.1.1 Aid Initiation of Prompt Operator Action 4-1
4.1.2 Aid in Determining Plant and System Status 4-2
4.1.3 Aid in Diagnosing and Responding to Plant Transients and Events 4-3
4.1.4 Facilitate Maintenance 4-4
4.1.5 Avoid Distracting or Overloading the Users 4-5
4.1.6 Exhibit High Reliability and Availability 4-5
4.1.7 Support Alarm System Performance Monitoring 4-6
4.1.8 Provide Alarm Information to Other Systems and Users 4-6
4.2 Functional Requirements 4-6
4.2.1 Alarm Generation 4-6
4.2.2 User-Defined Alarms 4-18
4.2.3 Alarm Processing 4-19
4.2.4 Alarm Routing to Users/Locations 4-23
4.2.5 Alarm Recording 4-24
4.2.6 Alarm Information Display 4-25
4.2.7 Alarm Controls (SART) 4-32
4.2.8 Alarm Response Procedures 4-33
4.2.9 Alarm System Performance Monitoring 4-35
4.2.10 Alarm System Support for Maintenance 4-38
4.3 System Design and Performance Requirements 4-39
4.3.1 Time-Related Requirements 4-39
4.3.2 Hardwired Input and Output Requirements 4-44
4.3.3 Data Communication Requirements 4-45
4.3.4 System Configuration and Configuration Management 4-46
4.3.5 Alarm Archiving/Recording Requirements 4-47
4.3.6 Availability Under Accident Conditions 4-48
4.3.7 System Integrity 4-50
4.3.8 Reliability and Diagnostics 4-50
4.3.9 Maintainability 4-52
4.3.10 Testability 4-52

5 PLANT ALARM MANAGEMENT REQUIREMENTS 5-1

6 IMPLEMENTATION GUIDANCE 6-1

6.1 Applying the Requirements 6-1

6.1.1 Designing a New Alarm System 6-1

6.1.2 Defining an Endpoint Concept for Modernization 6-1

6.1.3 Alarm System Procurement 6-2

6.1.4 Defining a Plant Alarm Management Strategy 6-2

6.2 Defining the System Architecture 6-2

6.3 Keeping it Simple 6-3

6.4 Applying Human Factors Engineering (HFE) 6-4

6.5 User Participation in System Design and Evaluation 6-4

7 DEFINITIONS 7-1

8 REFERENCES 8-1

LIST OF FIGURES

Figure 2-1 Alarm Management Overview 2-2
Figure 2-2 The Alarm System 2-7
Figure 3-1 Advanced Alarm System Features 3-4

1
INTRODUCTION

1.1 Objective

The objective of this document is to define requirements for an advanced control room alarm system for nuclear power plants. In this context, advanced means that the system defined here has capabilities that go beyond current systems. It is not expected that any single system available today will necessarily meet all of the requirements specified here. Rather, the purpose of specifying these requirements is to define a system that:

- Overcomes the shortcomings of present alarm systems
- Takes advantage of the capabilities of the latest technologies available, and
- Integrates into one system those features that have been shown or are expected to provide significantly enhanced performance and usability for the control room operators and other users of the alarm system

Each plant typically has its own operating philosophy and desires with respect to alarms and how they are presented. In addition, the operating philosophy or concept of operations may change over time, particularly for existing plants that undergo successive stages of modernization. Therefore, to an extent, the "best" alarm system is one that allows each plant to configure the system to meet their needs at a given time. This is reflected in the alarm requirements. A broad range of capabilities is specified, with the ability for a plant owner, designer or system integrator to enable the features that are desired and to configure the alarm presentations to meet their needs.

Finally, the requirements are intended to be modular. Plant owners/designers can choose which of the requirements they wish to use to define and procure an alarm system meeting their particular needs.

1.2 Applicability

The alarm system requirements provided in this document are not specific to any particular instrumentation and control (I&C) or information system architecture. However, they do assume that modern computer-based systems will be used for monitoring and controlling the plant. The intent is that the requirements can be used by existing plants that are modernizing their I&C systems and control room human-system interfaces (HSIs), or by designers of new control rooms for existing or new nuclear plants.

1.3 Contents of This Document

In order to be effective in providing support to the operators and other users, the alarm system must operate within an overall alarm management program. Section 2 provides an overview of alarm management, identifying activities the plant staff should undertake to establish alarm management policies, and define how alarms will be selected and alarm configurations will be managed as changes are made over time. The alarm system is then discussed in the context of alarm management, and the main functional elements of an advanced alarm system are introduced.

Section 3 provides background on the problems with previous alarm systems, describes the basis for the requirements provided in this document, and summarizes the advancements offered by an alarm system that is designed to meet the requirements.

Section 4 specifies the requirements for an advanced alarm system. Included are high-level objectives and detailed functional, design and performance requirements for the alarm system.

Section 5 provides high-level requirements for alarm management activities that take place outside the alarm system.

Section 6 provides additional information on how the requirements can be used in different situations, including new plant designs and modernization of existing plants. Section 7 gives definitions of terms used in this document, and Section 8 provides the list of references.

2
ALARM SYSTEM IN THE OVERALL CONTEXT OF ALARM MANAGEMENT

Making effective use of alarm information requires not only an effective alarm system, but also an overall approach to alarm management that ensures alarms are properly defined and configured, and that changes to the alarms and the alarm system are managed properly over time. The section gives a brief overview of alarm management, and how the alarm system fits into an alarm management framework. It then describes the alarm system and introduces the various functions that should be performed by the system.

2.1 Alarm Management

Figure 2-1 illustrates the process of alarm management. First, alarm management policies must be defined. This includes defining rules for alarm definition and configuration management and how these will be applied initially and over the plant's lifetime. Appropriate design criteria, performance objectives, administrative procedures and policies should be established including assignment of responsibilities within the plant organization.

The alarm management policies should be consistent with the plant's "concept of operations" and "concept of maintenance." Concept of operations refers to how the plant is operated and how the operating crew is organized, including what functional responsibilities reside in the control room, operating crew size and makeup, roles and responsibilities of the crewmembers, and how normal and emergency operations are conducted. Concept of maintenance refers to how maintenance activities are performed, including the relative roles of the operating crew and the maintenance staff in maintenance activities, how the two will work together to support testing and maintenance, and how maintenance activities and information will be managed.

The items shown in green in Figure 2-1 relate to defining requirements and a conceptual design for the alarm system, detailed design and system procurement, alarm system configuration (configuring alarm settings such as setpoints and priorities, determining where alarms will be routed for display, display configurations, etc.), and alarm system operation. This document is focused primarily on the first of these activities, definition of alarm system requirements.

The items shown in light blue in the figure are very important elements of alarm management: alarm selection, definition and prioritization, alarm configuration management, and system performance monitoring. Even with the very best alarm system, if the alarms are not properly selected, configured and managed, the system likely will not meet its performance objectives. Alarms that are improperly chosen or poorly defined and configured can create nuisances, over-burden the operators with non-meaningful information, and greatly reduce the effectiveness of the alarm system in alerting operators to conditions that need their attention.

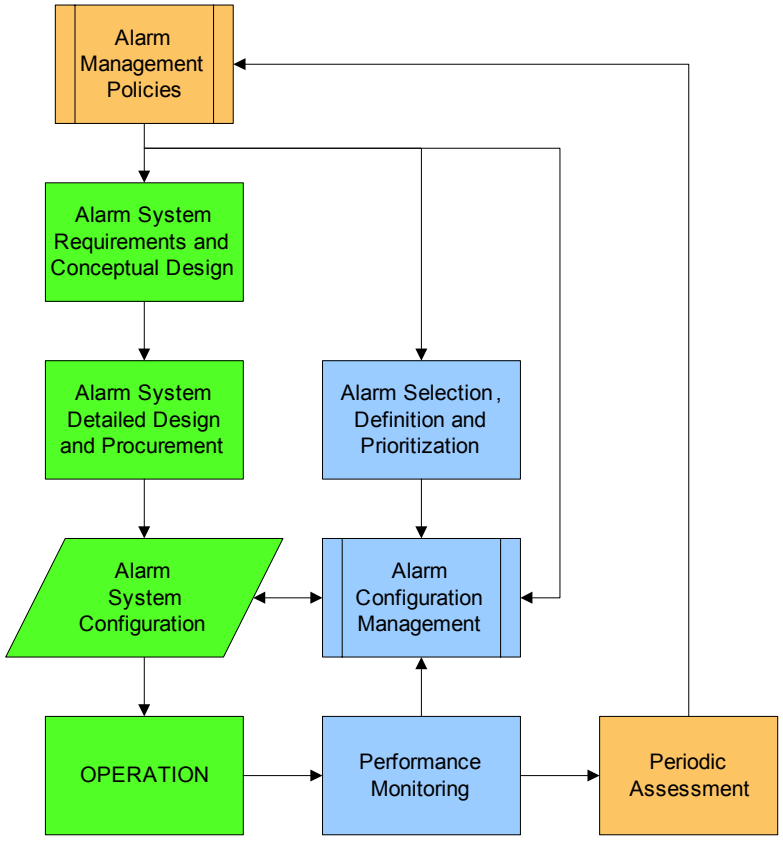


Figure 2-1
Alarm Management Overview

Performance monitoring is important to ensure the performance objectives are met initially, and to continue monitoring performance to identify problems that occur during operation (e.g., instrumentation problems that cause nuisance alarms, changes made to the alarms or the system that degrade performance, etc.). In addition, potential improvements to the alarms or alarm system may be identified through regular performance monitoring (e.g., relationships among alarms may be identified that can lead to improved logic in the alarm system to make the alarms more effective with less redundant information presented).

Finally, periodic assessments of performance should be made to re-examine the overall alarm management approach and determine whether policies and procedures should be modified to improve performance in the long term.

The primary focus of this report is on the alarm system. However, again, the system will not be effective if does not operate within an effective alarm management framework. Section 5 provides a set of high-level requirements related to alarm management, to aid plant owners or designers in developing a suitable alarm management approach.

2.2 Alarm System

Figure 2-2 shows a functional block diagram of the alarm system. As used in this document, the "alarm system" includes all of the alarm-related functionality provided in the control room. This functionality is not necessarily contained in any one physical system, but may be provided by a number of systems including plant control and monitoring systems, protection systems, and other information display systems. All of this functionality is described here as being part of an "alarm system" because it is important for the alarm functionality to be integrated as much as possible. Although alarms may be generated by different physical systems, and alarm information may be displayed by various information display systems, the divisions between systems should be transparent to the users. It is important that alarms be defined and generated on a consistent basis, and that alarm presentations work together to provide effective support for the operating crew and other users to perform their tasks.

In operating plants, alarms are used for more than just alerting operators to off-normal conditions. They are used to help maintain awareness of the operating status of the plant and its major systems and components, and the availability of systems. However, in a modern control room the plant information systems also should play an important, or even a leading role in these functions. In fact, the most effective interface is likely achieved when alarm and information displays are integrated together. Some of the functionality specified in this document may be implemented by a system dedicated to alarms, some is likely to be provided within the plant information systems or integrated alarm and information systems, and some may be provided by separate systems or software applications that communicate with the alarm and information systems. What is important here is that the functional requirements for alarm and information display are met, regardless of which physical "system" hosts the required capabilities.

The main functional elements of the alarm system, as shown in Figure 2-2, are discussed below. Section 3 provides more detail on the advanced functionality that is provided by these features, as compared to conventional alarm and annunciator systems. Section 4 provides detailed functional and design requirements for the system.

Inputs

The primary inputs to the alarm system are plant process, system and equipment parameters that are automatically monitored to detect off-normal conditions. The alarm system also needs the current values of these parameters, both for display purposes and for generating "smart" or high-level alarms that combine a number of conditions using logic or calculations. Plant parameters or conditions may be input directly to the alarm system, or the system may obtain this data from other monitoring, control or protection systems.

As plants make greater use of equipment condition monitoring and diagnostic systems, these will be an increasingly important source of information for the alarm system. Advanced monitoring and diagnostics can provide early warnings of degradation of equipment and processes, and the information they provide may be used in diagnosing and responding to plant events.

Alarm Generation

Alarms are likely to be generated by multiple systems, and alarm generation may be distributed among multiple input sections or units of a distributed system. It is important that consistent capabilities for alarm generation be provided as specified in Section 4 of this document. Alarm configuration settings are used in generating the alarms. These include items such as setpoints, alarm priorities, and alarm message text.

Alarm conditioning logic should be applied at the point of alarm generation to reflect the operating modes or states of the associated components and systems, and prevent nuisance alarms.

Alarm Processing

As noted above, alarms may be generated at various locations within the instrumentation, control and protection systems. The alarms are then brought together for further processing and application of global (plant-wide) alarm processing techniques. An example of these techniques is suppression of a pre-defined group of alarms based on plant mode changes or occurrence of a major plant event in which the alarms are expected and do not provide additional information that is useful to the operators in the near term (however, the operators can still access the alarms for review when needed).

The distinction made here between alarm generation and alarm processing is not in itself important, as the dividing line between the two functions is not necessarily distinct. The main point is that alarms may be generated "locally" by a number of different systems at different locations, covering different areas of the plant. This information is then combined and processed plant-wide, applying such techniques as mode and event-based suppression or other modifications to groups of alarms.

Alarm/Event Routing

Alarms and events (e.g., status changes important for situation awareness) need to be "routed" to appropriate destinations based on their intended use. Alarms that require operator action are routed to operator displays or workstations. The system provides the capability to route only a subset of the alarms to one or more workstations if the operator(s) using those workstations have responsibility only for a portion of the plant. Alternatively, all operator alarms can be routed to all operator workstations.

Alarms also may be routed to one or more maintenance workstations. These would present alarm information tailored to the tasks performed by maintenance personnel. For example, detailed information on a fault in the instrumentation and control systems or the alarm system itself would be provided to maintenance technicians for troubleshooting and repair. At the same time, the operators may be provided information on the fault alarm if there is action that they should take (for example, switching to alternate instrumentation if the fault indicates certain sensors or measurements are failed or suspect). In that case, the information routed to the

operators would be tailored to their needs, telling them what the operational impact of the condition is and how they should respond.

All alarms and events are routed to the alarm history archive or database for permanent record keeping. This historical information also can be accessed by all users of the system for purposes such as diagnosing an event or condition, analyzing a transient, performing post-event reviews and analyses, or monitoring alarm system performance. Alarm history information is integrated with other plant data records to help support these functions. In fact, the alarm recording function could be implemented as part of an overall plant data historian, as long as it meets the requirements specified in this document.

Alarm Presentation and User Interaction

Alarms are presented to the operators using both visual and audible means. With the advanced alarm system specified here, a hierarchy of alarm presentations is provided, displaying alarms at the plant level, the level of major systems and functions, and the component and sub-component levels. Spatially dedicated, continuously visible (SDCV) displays are provided so that operators can quickly determine what parts of the plants are affected by incoming alarms, and they can determine the status of plant systems, functions and components. SDCV displays include computer-generated "tile replica" type displays (similar to conventional annunciator tiles) and alarm indications integrated with other graphical displays such as a plant or system mimic diagram. The alarm system provides, for each major plant system or function, alarms indicating the availability of the system/function and its operating status. The system-level alarms indicate the severity of off-normal conditions in the systems/functions (e.g., a minor problem not needing immediate attention, serious problem requiring short-term action prior to system failure, or the system or function has failed).

Alarm message lists also are provided giving detailed information on the alarms and providing the chronology of alarms and events. Sorting and filtering capabilities are provided, allowing the operators to display different views of the information to support their tasks in monitoring, diagnosing and responding to plant events.

Alarm information also is presented to other users of the alarm system. Alarms routed to a maintenance workstation are displayed in a form suitable for use by maintenance technicians. Alarm displays also can be presented that assist engineers and other users in using alarm systems for equipment monitoring, plant performance monitoring, and related functions.

The alarm presentations provide means for interacting with the system that allow easy access to the various levels and types of displays, and provide a path for operators to drill down to more detailed alarm information including alarm response procedures (see below).

ARP Presentation

The alarm system displays electronic or computer-generated alarm response procedures (ARPs) to the operators. These can be selected from any of the appropriate alarm presentations (e.g., alarm message list, tile replica or other SDCV display of an alarm). The procedures not only

provide written instructions for confirming and responding to the alarm, but also display directly to the operator the data needed to support these tasks (e.g., values of plant variables that need to be checked, status of components, etc.). Other aids also are provided, such as current parameter trends, information on cause-consequence relationships among related alarms and events, and historical data related to the alarm. Paper copies of the ARPs are provided as a backup.

Alarm Controls

Controls are provided to silence, acknowledge, reset and test the alarms. These are referred to as SART controls. The controls are arranged to ensure convenience access and to avoid having to actuate multiple controls to silence or acknowledge alarms.

User-Definable Alarm Features

The system provides the capability for operators to define temporary alarms for special circumstances. For example, alarms may be needed temporarily while testing or performing maintenance on plant equipment. A temporary alarm might be established to provide closer monitoring and early warning of problems on a component that has exhibited problems and warrants special scrutiny. The plant should provide administrative procedures that control the definition, tracking and removal of these temporary alarms.

System Configuration and Maintenance

The system is designed for ease of configuration and maintenance. Features are provided that allow coordinated use of an off-line engineering database (created and maintained by the plant) and the on-line alarm system configuration database, which contains alarm configuration, processing and presentation settings. The human-system interface provided for configuring and maintaining the system is designed for ease of use, provides features that support configuration management (e.g., tracking and identifying sources of changes to the configuration), and aids in keeping the off-line and on-line databases in synchronism.

Alarm System Performance Monitoring

The system provides features for monitoring the performance of the alarm system, including automatic collection of statistics on key performance indicators such as alarm rates and number of standing alarms. Performance monitoring also can identify nuisances, chattering alarms, and relationships among alarms based on their behavior over time. This information can be fed back to make improvements in the alarm configurations and alarm processing.

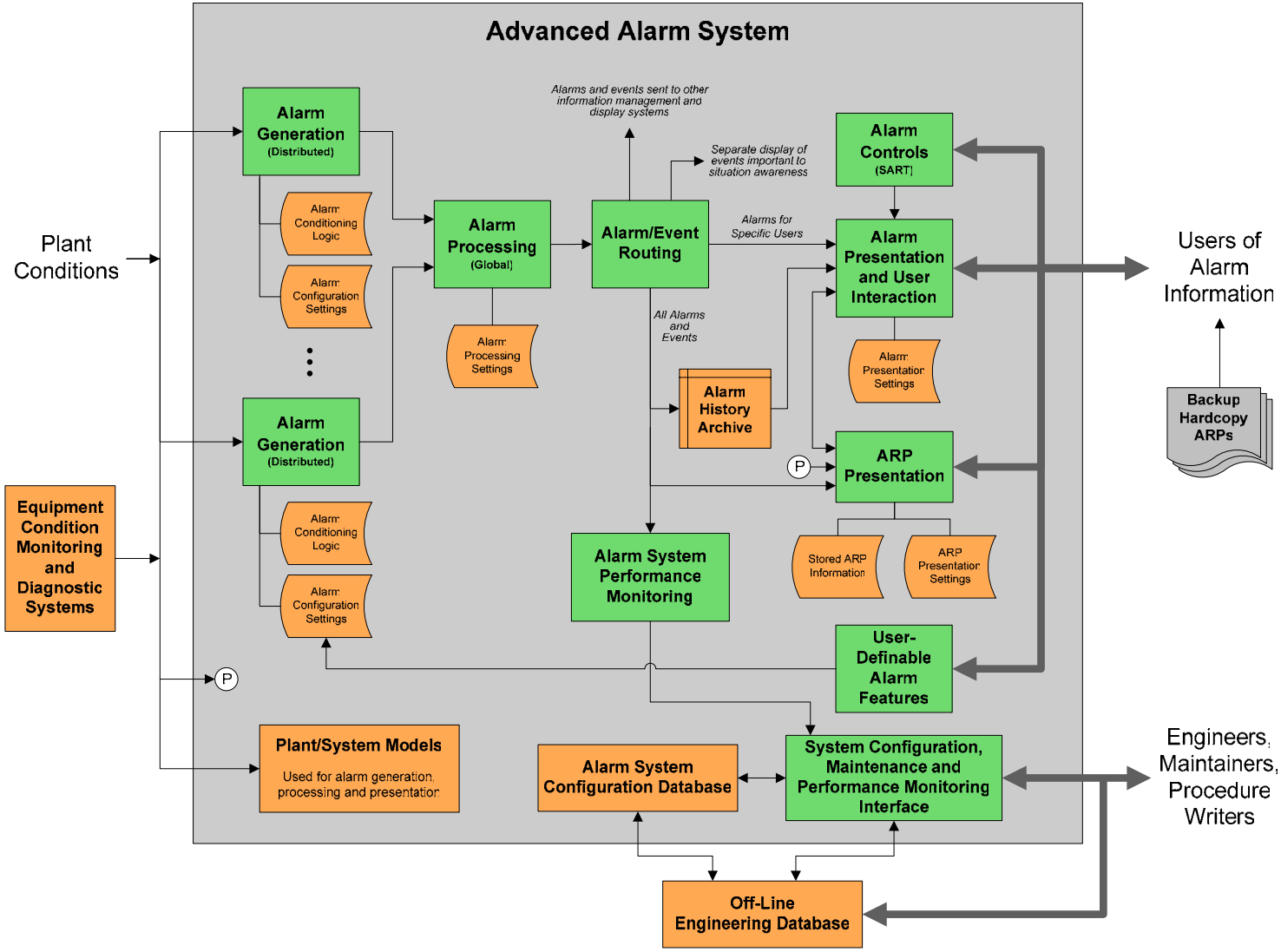


Figure 2-2
The Alarm System

3
BACKGROUND AND BASIS FOR THE REQUIREMENTS

This section provides some background information and describes the basis and objectives of the requirements provided in this document.

3.1 Background

Alarm systems are designed to continuously and automatically monitor plant conditions, detect any abnormal conditions, and provide both visual and auditory alerts when a situation occurs that requires operator action. In addition to the primary purpose of monitoring and detection, in most plants alarms are also used for other purposes, such as providing an overall assessment of plant status, determining the availability of systems and components, diagnosing transients and events, and supporting testing and maintenance.

While alarms play an important role in plant operation, they have also posed challenges to the users. Common problems include:

- Too many alarms (this creates alarm overload, important alarms cannot be distinguished from those that are of lesser importance, and operators cannot process the flood of alarm information)
- Too many spurious or nuisance alarms (this causes distractions, contributes to alarm overload, and may cause users to discount alarm information)
- Poor distinction between alarms and status changes (this can make it difficult to distinguish normal from abnormal conditions).

Previous alarm systems have been reasonably effective in alerting operators to off-normal conditions while the plant is operating at power and only minor malfunctions occur, generating one or only a few alarms. Operators can attend to the limited number of alarm indications without being distracted, interpret the meaning of the alarms, collect additional information if needed, and take appropriate actions. However, when the plant experiences a major transient, hundreds of alarms may occur in the first few minutes of the event. Operators typically are forced to ignore the alarms during this time, because it is almost impossible to distinguish between alarms that provide useful information that the operator needs now and the other alarms that also occur. Thus, the alarms act primarily as a distraction, and they increase workload when the operators turn their attention back to the alarms to acknowledge them, silence the auditory warnings, and review the alarm information presented.

Research and practical experience have shown that operators prefer alarm systems that reduce the number of alarms occurring in upsets, or which provide views of alarm information that allow them to focus on the most important alarms, as long as the alarm system does not take

important information away from them. In addition, there is evidence that reducing the alarm overload can increase operator performance and enhance the value of the alarm information [1, 2].

Newer technology can improve other aspects of the alarm system as well. For example, with conventional systems the operator uses paper-based alarm response procedures (ARPs) with a fixed set of information, directing the operators to gather additional information needed to confirm and respond to the alarm. Modern systems can present the ARPs on screens at the operator's workstation and provide the current values of important parameters needed when responding to an alarm without the operator having to go and find that information. Links can be provided to give easy access to related system displays or detailed information useful in diagnosing the problem.

In addition, an advanced alarm system meeting the requirements given in this document can separate maintenance-related notifications from alarms requiring operator action. It can provide information to both the maintainer and the operator such that each receives information only on the events important to that user, tailored to their specific information needs. Information needed by system engineers and other users also can be provided specific to their needs.

Considerable research has been performed and a number of documents have been published that provide information on the problems commonly found in alarm systems and guidance for addressing them. Some examples are listed below (see Section 8 for a complete list of references):

- Section 4.4 of EPRI 1010042 [3] provides human factors engineering guidelines for design and evaluation of alarm systems. It also addresses implementation of new alarm capabilities as part of modernizing an existing control room.
- EPRI 1003662 [1] provides results of a study examining the effectiveness of alarm reduction techniques for addressing the alarm overload problem. The emphasis in that study was on taking advantage of the alarm processing capabilities of modern systems and the use of relatively simple techniques for alarm overload reduction. The report also includes guidance for developing an overall alarm management strategy for the plant and for specifying and implementing new digital systems to implement this strategy.
- NUREG/CR-6684 [4] provides the results of a study of the effects of alarm system design characteristics on operator performance and the introduction of computer-based human system interface systems into conventional nuclear power plants.
- NUREG/CR-6691 [2] presents the results of research that evaluated the impact of alarm display, processing, and availability on crew performance. The research included an experimental study with test trials of several combinations of alarm display design features, processing capabilities, and alarm availability, covering a wide range of operating scenarios.
- NUREG/CR-6105 [5] presents the results of a comprehensive literature review and considerable research in the area of control room alarm systems.

3.2 Basis and Objectives of the Requirements

The advanced alarm system requirements provided in this document are based on:

Research and Development Related to Alarm Systems

- Research and development of updated human factors engineering guidelines for modern control rooms, including alarm systems (EPRI 1010042 [3])
- Recent EPRI research on alarm systems and alarm reduction techniques (EPRI 1003662 [1])
- Review of other research on advanced alarm system techniques in nuclear power plants
- Review of recent developments in other process industries related to improving alarm management

Alarm Features Provided with Commercial Systems and New Plant Installations

- Review of alarm features of commercially available control and information systems
- Review of alarm features provided in new nuclear plants recently built or under development

Experience in Operating Plants

- Operating experience with alarm systems installed in current plants
- Experience in defining and implementing improvements to alarm systems at plants that have embarked on control room and alarm system modernization

The requirements are intended to provide an alarm system with a number of important advancements when compared to conventional systems used in many plants today:

- Support for a hierarchy of alarms and alarm presentations
- Generation of alarms that are "context-aware"
- Separation of status information from alarms
- Separation of maintenance notifications from alarms needing operation action
- Better support for responding to plant transients and events
- High reliability and availability under both normal and accident conditions
- Ability to create and manage user-defined alarms

Each of these advancements is discussed briefly below. Refer to Figure 3-1, which illustrates some of the key features of the advanced alarm system that enable these advancements.

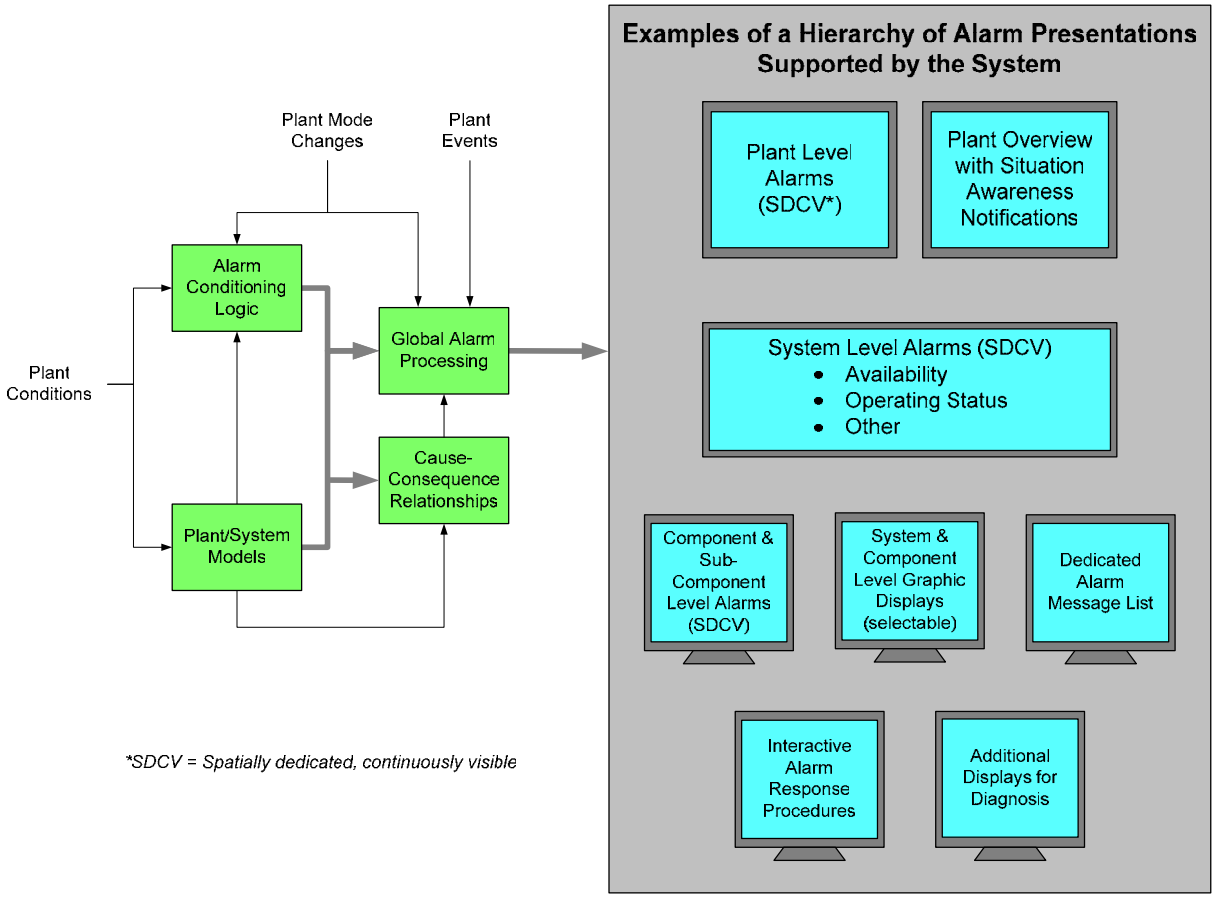


Figure 3-1
Advanced Alarm System Features

Full Hierarchy of Alarms

Conventional systems generate alarms based on individual parameters such as pressures, temperatures, flows and levels. Operators must determine from these low-level conditions what event has occurred, what the impact is on plant operations, and how to respond. Alarm response procedures support the operators in this task, but often require them to gather additional information.

The advanced alarm system generates alarms at multiple levels, supporting a hierarchy of alarms including:

- Plant level alarms (e.g., major plant events such as reactor trip and safety injection actuation)
- Alarms at the system or function level (e.g., availability and operating status of major plant systems, critical safety and availability functions, etc.)
- Component level alarms (e.g., pumps, tanks)
- Sub-component and component support level (e.g., lube oil for a pump)

For each major system or function, alarms are generated indicating the availability of the system/function, and its operating status. Alarms on operating status can be graded in severity, indicating for example whether the system has a minor problem that does not need immediate attention, the system is degraded and requires action to prevent failure, or the system has failed. Displays showing these alarms can provide at-a-glance determination of which systems have problems and the degree of degradation of systems and functions.

By generating alarms at all levels of the hierarchy, the alarm information can be more readily integrated into information system displays that follow the same hierarchy. In addition, these alarms can help the operator drill down to lower levels of detail when responding to an alarm.

Alarms Generated are Context-Aware

Conventional systems typically have had little capability to apply logic or other processing techniques when generating alarms. As a result, a decision must be made as to what is "off-normal" when defining alarms. Typically, normal is defined with respect to full power operation, with all systems configured in their most typical lineup for that mode. Thus, when the plant goes through mode changes, or systems are operated in different configurations, many alarms can occur for conditions that are not abnormal for the new mode/configuration but are expected for those situations. These become nuisances, contribute to alarm overload during upsets, and contribute to the number of standing alarms during operating modes other than full power operation.

In the advanced alarm system, alarms are generated in context, with logic and processing that reflect the plant, system and equipment operating modes so that alarms occur only when conditions are truly off-normal, or unexpected for the current operating state. Alarm conditioning logic is used to reflect relationships between systems, components and sub-components and the associated operating conditions for different states. For example, an alarm on low discharge pressure for a pump can be conditioned to occur only when the pump is running, and only after a preset time delay after starting the pump.

When generating alarms, the alarm system can also make use of models of the plant and its systems to properly reflect system and component states or functional relationships among components and process parameters. At the plant level, more "global" alarm processing techniques can be applied, such as plant mode and event-based alarm processing. For example, on occurrence of a particular event, the alarm processor may suppress alarms that are a direct consequence of that event and thus do not provide any additional information useful to the operator in the short term. The suppressed information can still be accessed by the operator on demand. In addition, conditions or status changes that were expected to occur during the event, but did not, can be highlighted by the system.

Status Changes Separated from Alarms

Alarm systems often present conditions that represent status changes in the plant, along with off-normal conditions requiring operator action. Some status changes are important, and the operators should be made aware of them so they can maintain overall awareness of the state of

the plant and its systems. However, in many cases these status changes require no action, yet they are mixed in with conditions that do require an operator response. This contributes to alarm overload and makes it difficult for operators to distinguish between status changes and conditions requiring operator action.

The advanced alarm system recommended here distinguishes between events that represent important status changes, and off-normal conditions requiring operator action. The latter are processed and presented as alarms. The status change events are processed and routed to a separate display designed to provide operators an overview of the plant and help them maintain situation awareness. This might be a large plant overview display visible to the entire operating crew, or a display available at each workstation that provides the status information, or both. Operators are alerted to the status change events by a momentary auditory tone (such as a chime) and their attention is drawn to the display, but they are not required to take any action. This allows them to focus on alarms or on other important tasks, and then check the overview display when they have time.

Maintenance Alarms Separated from Operator Alarms

Some alarms require action primarily by maintenance personnel, and not by operators. This is particularly true of *system alarms* that occur when a fault occurs within the alarm system or other control or monitoring system. If all of these alarms are presented to the operators, this contributes to overload and burdens the operators with the task of communicating the information to maintenance personnel for action.

In the advanced alarm system, alarms that require action by maintenance personnel are routed to a maintenance workstation. Operators also may need to be alerted to the condition, but the information needs of the operator and the maintenance technician are likely to be different. The system provides information to the operator on the operational impact of the fault or failure and what action the operator needs to take in response. This can be very different from the detailed information on the condition that is provided to the maintenance technician to facilitate locating and repairing the fault. The alarm system incorporates knowledge of the relationships between the sensed faults and the operational status of the system, and creates messages appropriate to each user of the information. As an example, consider an intelligent valve positioner. When the positioner detects increased friction but is still able to perform its function, the maintenance staff should be notified. However, the operators may not need to be alerted to this condition. When the positioner is no longer able to perform its design function, then both the operators and maintenance personnel need to be informed, as both now have tasks to perform in response.

In a similar fashion, the system can provide information needed by system engineers separately from that provided to operators and maintenance technicians.

Better Support for Responding to Plant Transients and Events

Because conventional alarm systems produce large numbers of alarms at a high rate during plant upsets and transients, it is difficult for the operators to use alarm information to support their near-term response to the transient. Once they have stabilized plant conditions and can spend

time digesting the alarms, there is a lot of low-level information to go through and they must discern the connections or relationships among the alarms in order to diagnose the cause of the event and determine what corrective actions are needed to recover from it.

The advanced alarm system provides alarm presentations and aids that give better support to the operators in this task. First, the system provides the information needed to prompt near-term actions, and prioritizes the information to help the operators focus on what is most important at that time. The operators use the plant-level and system-level alarms to focus quickly on the affected parts of the plant and determine the status of major systems, including how seriously the event has degraded the systems and critical functions. In addition, individual alarms are prioritized based on time to respond and severity of the consequences of not responding. These features allow the operators to order their response based on taking actions that are most important in the short term.

The alarm system provides a path for the operators to drill down to lower levels of information in responding to the alarms, starting at the plant level, then system/function level, and then selecting displays that provide more detailed information about the systems and components. Alarm conditions can be seen on graphical displays showing components and their inter-relationships, along with values of key variables and status of components. Cause-consequence relationships among alarms can be shown on the graphic, helping the operators relate alarms and determine possible causes of an event. The operators also can select displays showing all of the active alarms associated with a given system or component.

Links are provided to give rapid access to alarm response procedures associated with the alarms. The procedures not only provide instructions for confirming and responding to an alarm, but also retrieve and display the additional data needed by the operators. For example, if the procedure calls for checking the level in a tank associated with a pumping system alarm, the procedure provides the current value of the tank level and shows whether it is normal or in an alarm state. In addition, cause-consequence relationships are built into the system logic and the ARPs, and these are used to provide automatic diagnosis wherever possible. For example, cause-consequence relationships among alarms in the electrical distribution system might be used to indicate automatically the likely cause of a loss of power to a component, identifying the upstream feeder breaker that opened or the highest-level bus that first lost voltage, resulting in a cascade of alarms in downstream power panels and subsequent equipment power losses.

Equipment condition monitoring and diagnosis capabilities that are becoming more widely available will also assist the alarm system in providing diagnostic information. Consider the digital valve positioner mentioned above, which has built-in diagnostics that can detect an increase in friction. Alarms from these diagnostics might be linked with alarms on improper valve position or other related alarm conditions so that ARPs can quickly identify potential causes of those conditions.

If the operator concurs with the diagnosis, then appropriate corrective actions can be taken. When an automatic diagnosis is not possible or the operator questions the diagnosis, the electronically presented ARP aids the operator or other personnel in diagnosing the condition.

Additional displays are available to the operator, giving the chronology of alarms and events and integrating this information with plant process data and trends. Different sorts and filters can be

applied to the data to aid in understanding the event and determining the cause. For each alarm, a detailed information display can be accessed that pulls together related information from maintenance and engineering systems. For example, the operator can view alarm performance statistics such as how often it has occurred in the past and how long it typically remains active, open work orders related to the alarm or the affected equipment, any related engineering or design changes that are planned or in progress, and notes from operators, maintainers and engineers related to past history with the alarm and the associated equipment.

For common or anticipated events, the system maintains pre-stored event histories that can be automatically compared to the actual event data. The presentation can highlight differences from the "normal" event sequence to help identify the cause of the event, and to identify any unusual deviations (including events that were expected but did *not* occur) or secondary failures that may have occurred.

All alarms and events are captured in the historical record and are available to all users for post-event review and analysis.

High Reliability and Availability in Normal and Accident Conditions

Total failures of some computer-based alarm systems have occurred in the past, resulting in loss of updated alarm data for some time until the staff could restore the system to operation. "Silent failures" have made it difficult for operators to recognize that the alarm system is not updating information, which lengthens the amount of time the system is out of service. In addition, most alarm systems are not qualified to survive during accidents and, as a result, operators cannot count on alarms to support them during and following an accident, nor can they be credited in the licensing basis.

The advanced alarm system described here is required to have sufficient redundancy and fault tolerance such that single failures will not cause loss of any significant amount of alarm functionality. Evaluations are required to demonstrate that common cause failures that could produce a large-scale loss of functionality will not occur during the lifetime of the plant. In addition, features are provided that allow the operators to regularly confirm proper operation of the alarm system, including a "heartbeat" indicator on each alarm display indicating whether the system is continuing to process and display updated alarm information. In addition, the system includes a manual test capability that exercises the entire system from end to end.

The advanced system recommended here also includes a portion that uses qualified equipment (hardware and software) on a qualified power source, so that a minimum level of alarm functionality will be available to the operators during and following accidents, including loss of offsite power.

User-Defined Alarms

Conventional systems have not provided the capability for the operators to define temporary alarms when needed. Such alarms may be useful in situations in which enhanced monitoring of

a piece of equipment is required, or when special system configurations are used or maintenance activities are being performed that require temporary alarms.

The advanced alarm system allows the operator to define and manage temporary alarms for special situations. Appropriate administrative controls should be provided to ensure that these alarms are documented, tracked and removed when they are no longer needed.

3.3 Limitations of the Requirements

This document does not provide all the requirements needed to specify an alarm system completely. The requirements given here focus primarily on those features and capabilities that are needed to achieve the advancements indicated above, and to avoid additional problems that can arise when using computer-based systems to implement an alarm system. Examples of requirements that would typically be included in a complete alarm system specification, but are not addressed here, include detailed input requirements (current and voltage input signal ranges, types of contact inputs accepted, etc.), cabinet ventilation requirements, power requirements, and system documentation requirements. These and other typical specification details are important, but are not directly relevant to the types of functional and performance advancements that are the focus of this report.

4
ADVANCED ALARM SYSTEM REQUIREMENTS

This section provides a set of requirements for an effective, advanced control room alarm system. In most cases, the requirements are stated using "should" rather than "shall." This is because it is up to the plant owner or designer to determine which of these requirements will be imposed as mandatory and which ones will be considered desirable but not mandatory. There is no single, "best" way to process and present alarms. The intent is that the owner/designer will be able to choose among the requirements provided here, applying only those that fit with the particular design constraints, control room design concept, I&C and data communications architecture, and operating philosophy of the plant.

The requirements are written from the perspective of the plant owner and user of the alarm system. They do not specify details of the design. The requirements identify functional and design characteristics or capabilities that should result in an alarm system meeting key objectives, stated in Section 4.1.

Each requirement is numbered and is distinguished by a special character (➢) in front of the requirement number. In some cases, additional information is provided related to a requirement. This information is intended to help explain the basis for the requirement, and discuss how it can be applied. The discussion appears as indented text located below the requirement. If the discussion applies to several requirements, it appears after the last requirement in that group.

4.1 Objectives of the Alarm System

This section provides objectives or high-level requirements for the alarm system. Section 4.2 (functional requirements) and Section 4.3 (design and performance requirements) provide more detailed requirements for alarm system characteristics and features needed to meet these objectives.

4.1.1 Aid Initiation of Prompt Operator Action

➢ 4.1.1.1 The alarm system should alert the operators to off-normal plant conditions that require action.

The primary purpose of the alarm system is to notify the operators of a process deviation or other off-normal condition that requires operator action. Part of the plant's alarm management strategy should be to define as alarms only those conditions that require a defined action. See Section 5 for requirements related to the plant's alarm management program.

➢ 4.1.1.2 The system should inform the operators about the nature of the off-normal condition.

When plant conditions deviate from normal, the alarm system should help the operators determine the nature of the off-normal condition, and which systems or components are potentially affected.

➢ 4.1.1.3 The system should inform the operators about the priority of the off-normal condition.

When plant conditions deviate from normal, the alarm system should help the operators determine the priority of responding to the alarm. Prioritization helps determine what to respond to first. The severity of the condition (consequences of not responding) and urgency (time available to respond) should dictate the priority of the operators' response. Alarms should be prioritized as part of alarm definition (see Section 5).

➢ 4.1.1.4 The system should guide the operators' initial response to the off-normal condition.

The information provided by the alarm system should aid the operator in determining an appropriate response. Alarm Response Procedures (ARPs) provide instructions on confirming the alarm and taking the appropriate actions in response. The alarm system should provide the operator with access to the ARP for the particular alarm condition. In addition, the alarm system should provide or guide the operator to other process or system information needed in order to confirm and respond to the alarm.

4.1.2 Aid in Determining Plant and System Status

➢ 4.1.2.1 The system should facilitate assessment of the operating status of the plant, and its major systems and components.

Alarms should alert the operator to situations in which a plant system or function is not operating properly or not fulfilling its operational goals. Alarm presentations should facilitate rapid determination of the operating status of major plant systems and components.

➢ 4.1.2.2 The alarm system should provide information that operators can use to determine the availability of plant systems and components.

When a system, train, or significant component goes to a condition where it is not available to perform its normal functions, the alarm system should bring this change to the operator's attention. Alarm presentations should facilitate rapid determination of the availability and operability of major plant systems and components.

➢ 4.1.2.3 The system should assist the operators in identifying degrading conditions before they reach a point at which they begin to affect plant operation.

Providing operators and maintenance staff with early warning of an impending problem can help prevent plant trips and damage to equipment, and thus have a positive impact on plant economics and safety. Early warning alarms may be generated based on process conditions input to the alarm system, data from equipment condition monitoring systems, or other sources of data.

- 4.1.2.4 The system should indicate changes in plant and system status and early-warning indications in a way that does not over-burden the operators or distract them from responding to alarms requiring action.

  It is important for the operators to be notified of changes in the status of the plant and its major systems and components, and indication of impending problems, as this supports their ability to maintain overall situation awareness. However, this information needs to be processed and displayed in a way that does not over-burden the operators or affect their ability to respond to current alarms needing their attention.

4.1.3 Aid in Diagnosing and Responding to Plant Transients and Events

- 4.1.3.1 The alarm system should support diagnosis of plant transients and events.

  When a plant transient or other event occurs, the alarm system's first objective is to prompt short-term actions that are required in response to the event. This is discussed in Section 4.1.1 above. In addition, the alarm system should provide the operators with information that either directly identifies the cause of the event or, at a minimum, assists the operators in determining the root cause and identifying appropriate corrective actions.

- 4.1.3.2 The system should support the use of abnormal and emergency operating procedures.

  Alarms should be chosen and presented such that they prompt the operators when conditions occur that require entry into the plant's abnormal or emergency operating procedures, or require changing paths or branching within the procedures.

- 4.1.3.3 The alarm system should aid the operator in confirming that actions taken in response to an alarm have been successful.

  Once the operator has taken action in response to an alarm, the alarm system should help the operator determine whether the action has been successful. At a minimum, the system should allow the operator to determine whether the alarm condition has returned to normal and when this occurred.

- 4.1.3.4 The alarm system should provide an historical record of alarms and events, the times at which they occurred and when they returned to normal. The times at which alarms are acknowledged also should be recorded. This information should be easily accessible by the operators and other users.

  This historical record should be preserved in electronic format so that it is searchable for similar types of events. This historical data should be made available for statistical and other analyses such as post-event reviews and development of historical profiles of similar events.

- 4.1.3.5 The alarm and event information should be integrated with recorded data on behavior of plant variables so that all of this information can be used together to support post-event review and diagnosis, plant and alarm system performance monitoring, and other needs for historical data analysis.

4.1.4 Facilitate Maintenance

- 4.1.4.1 The alarm system should alert maintenance personnel to off-normal conditions in the plant requiring their attention.

  Alarm conditions that require maintenance action should be presented separately to plant maintenance personnel (e.g., via a maintenance workstation).

- 4.1.4.2 The system should support cooperative work between operations and maintenance personnel in responding to off-normal conditions.

  In addition to action by maintenance personnel, some conditions may need operator action as well, or are significant enough that operators need to be alerted to the state of the affected system or equipment. However, in these circumstances, the information needs of operators and maintenance personnel may differ. Maintenance personnel should be able to access the same historical records that are available to the operators, plus other maintenance-related historical records as appropriate.

- 4.1.4.3 Alarm system features and support provided for maintenance personnel should allow for ready integration with other maintenance management systems and capabilities, such as equipment condition monitoring and maintenance work order management.

  The alarm system should accept inputs from condition monitoring systems implementing automated equipment monitoring and diagnostics. The alarm system also should provide information to maintenance and engineering personnel that supports their use of those systems along with the alarm and event information available from the alarm system. Integration with maintenance management systems also should be supported, including for example the ability to generate maintenance work orders automatically from the alarm system, or assist personnel in entering work orders in response to alarms.

- 4.1.4.4 Features should be provided to facilitate configuration, maintenance and testing of the alarm system.

  The alarm system should include features that continuously indicate to users that the system is working properly. In addition, it should provide manual test capabilities that allow users to confirm proper operation on demand. The system should be easy to maintain, and should provide features that automatically detect internal failures and facilitate troubleshooting and repair of the system. The system should be easy to configure and provide features and tools that support configuration management.

- 4.1.4.5 The alarm system should support maintenance and surveillance testing of plant systems and equipment that interface with the alarm system, helping to ensure adequate overlap between plant system testing and alarm system testing.

  Overlap between alarm system tests and plant equipment surveillance tests ensures that the interfaces between plant equipment and the alarm system are adequately tested without operators having to respond to alarms during the surveillance testing. The system can block presentation of the alarms to the operator, but provide the information needed by personnel who are running the tests to confirm that the alarm system has received or detected the expected signals or conditions.

4.1.5 Avoid Distracting or Overloading the Users

- 4.1.5.1 The alarm system should minimize unnecessary distractions.

  The system should avoid distracting the operator or other users unnecessarily, such as might result from occurrence of nuisance alarms not requiring any action.

- 4.1.5.2 The system should minimize the workload required to interact with the system.

  The alarm system should be designed such that the difficulty and time required by the operator to interact with the system is minimized (e.g., to silence auditory outputs, acknowledge alarms, select particular displays, interrogate the alarm system for more information, or access an alarm response procedure) and the system is easy to use. Similarly, other users such as maintenance personnel should find the system easy to use with a minimum of burden associated with user interaction.

- 4.1.5.3 The alarm system should integrate alarm information from multiple sources to provide a consistent, easy to use interface for assimilating and responding to alarms.

  Alarms may be generated by a number of different systems. Bringing alarm information together and integrating it with other control room information can ease operator burden in assimilating and responding to alarms. The alarm system should consolidate silence, acknowledge, and reset controls so that the operators are not burdened by having to use multiple controls at different locations.

- 4.1.5.4 The alarm system should be predictable and understandable.

  It is important that the alarm system not appear to users as unpredictable or performing actions that they do not understand. The system should support users in understanding its operation, and the basis for its actions and the information it provides.

- 4.1.5.5 The alarm system should not overload users with information.

  The alarm system design, combined with careful selection of alarms and definition of alarm conditioning logic and processing, should minimize the likelihood of presenting too many alarms, or presenting alarms at too high a rate for users to assimilate them.

4.1.6 Exhibit High Reliability and Availability

- 4.1.6.1 The alarm system should employ redundancy and other fault tolerance features which, combined with use of very reliable hardware and software, ensure that the system will not suffer any large-scale loss of alarm functionality or data during the lifetime of the plant.

  The alarm system is very important to the operators' ability to maintain safe and economic operation of the plant. Each individual alarm and alarm function should be highly reliable, and the overall system should not suffer any large-scale loss of functionality during plant operation (e.g., loss of or failure to update a significant number of alarms, loss of important alarm processing functionality, loss of multiple alarm displays).

➢ 4.1.6.2 At least a minimum level of alarm functionality needed during and following accidents should remain available under accident conditions.

Alarms can continue to play an important role under accident conditions. By implementing a portion of the system using equipment that has been qualified to continue operating under accident conditions, including seismic events, at least a minimum level of alarm functionality important to emergency operation can remain available to the operators. There is no regulatory requirement that the alarm system be qualified or credited for accident mitigation. The intent here is to ensure that the system will have some capability to continue supporting the operator during and following accidents. The plant owner can decide whether the equipment will be treated as safety-related within its quality management program and whether it will be credited in any way in licensing.

4.1.7 Support Alarm System Performance Monitoring

➢ 4.1.7.1 The alarm system should provide features that support continuous monitoring of alarm system performance.

Monitoring the performance of the alarm system is an important part of overall alarm management. The alarm system should automatically collect data needed to support alarm system performance monitoring and analysis.

4.1.8 Provide Alarm Information to Other Systems and Users

➢ 4.1.8.1 The alarm system should make alarm and event information available to other information systems.

Alarm and event information may be used to support various engineering and management functions such as equipment condition monitoring, and plant performance monitoring. The system should provide means for transmitting alarm and event information in real time, as well as making available the historical record of alarms and events.

4.2 Functional Requirements

This section provides requirements related to alarm system functionality. Section 4.3 addresses other design and performance related requirements. However, the requirements in the two sections tend to overlap and interact with each other, so it is important to consider both sets of requirements together when specifying, designing, or modifying an alarm system.

4.2.1 Alarm Generation

This section provides requirements related to *alarm generation.* This is the activity or function that monitors plant conditions and, based on pre-defined *alarm configuration* settings and *alarm conditioning logic*, generates alarms and other notifications. Alarms and notification events may be generated by various distributed control and monitoring systems, or generated within the alarm system. The alarm system may then combine alarms and events with other conditions for more global or higher-level *alarm processing* and route the alarms to displays or workstations for

presentation to the intended users. See the glossary in Section 7 for further explanation of these terms.

Identification of off-normal conditions that require action, and definition of alarm configuration settings to implement these in the alarm system, is an engineering activity performed outside the alarm system. This document refers to that activity as *alarm definition*. The alarm generation requirements given below should provide the features and capabilities needed in the alarm system to allow for configuration of alarms that are sufficiently intelligent that they occur only when needed and always provide meaningful information to the users when they do occur.

4.2.1.1 Alarm Sources and Types of Alarms

- 4.2.1.1.1 The alarm system should be able to process alarms and events generated in other systems and communicated to the alarm system, as well as alarms and events generated within the alarm system itself.

- 4.2.1.1.2 The alarm system should be capable of generating alarms and events based on conditions that are directly input to the system (i.e., field inputs to the alarm system), from data or signals received from other systems, and from calculated or synthesized parameters derived from multiple inputs to the alarm system (direct or received from other systems).

  Alarms may be generated from any of a number of different information sources, including direct inputs and data received from other instrumentation and control and monitoring systems. However, when receiving inputs from other systems, it is preferable that those systems generate and time stamp the alarms, and then communicate them to the alarm system for further processing and display. This helps minimize inaccuracy in the time stamps. See Section 4.3.1.1 for further discussion and additional requirements.

  The alarm system should accept inputs from equipment condition monitoring and diagnostic systems. Advanced monitoring and diagnostic systems can provide improved detection and early warning of degraded conditions, which are useful to maintenance and engineering personnel as well as operators.

- 4.2.1.1.3 The alarm system should distinguish between alarms and events, including as a minimum:
  - Alarms indicating conditions that require a defined action
  - Events that do not require a specific action, but should be alerted to personnel due to their importance in maintaining adequate situation awareness
  - Other events that do not require action and are not considered important to maintaining situation awareness, but which should be recorded as part of the historical record

  Existing alarm systems often present conditions that represent status changes in the plant, along with off-normal conditions requiring operator action. Some status changes are important, and the operators should be made aware of them so they can maintain overall awareness of the state of the plant and its systems. In many cases, these status changes require no action, yet they are mixed in with conditions that do require an operator response. This contributes to alarm overload and makes

it difficult for operators to distinguish between status changes and conditions requiring operator action.

The advanced alarm system should distinguish between events that represent important status changes, and off-normal conditions requiring operator action. The latter should be processed and presented as alarms. The status change events should be processed and routed to a separate display designed to provide operators an overview of the plant and help them maintain situation awareness. Other events should simply be logged as part of the historical record of alarms and events.

➢ 4.2.1.1.4 The alarm system should distinguish instrumentation failures from actual process alarm conditions.

In the plant information systems and the alarm system, signal validation techniques should be used to distinguish between instrumentation failures and process alarm conditions. *Process alarms* should be generated from validated values wherever possible to prevent nuisance alarms due to sensor or signal failures. Failures of sensors or signals should generate *system alarms* for action by maintenance personnel. When alarm information is obtained from other systems for processing and display, this information should distinguish between sensor/signal failures and actual process alarm conditions.

For safety systems, where validation could introduce undesirable complexity and where signals from multiple divisions may not be available, a system outside the safety systems should perform the signal validation and generate the validation-related alarms.

➢ 4.2.1.1.5 For discrete (digital or binary) parameters (e.g., on/off, open/closed, tripped/un-tripped), either of the two possible states should be configurable as the alarmed state.

➢ 4.2.1.1.6 For analog variables, the alarm system should provide the capability to generate at least the following types of alarms:

- Alarms or events indicating the variable value has exceeded a high or low limit (setpoint). It should be possible to configure up to four limits above the normal operating range (high alarm limits) and up to four limits below the normal operating range (low alarm limits) for each variable
- Alarms on high rate of change of the value, where positive and negative rate limits are separately configurable
- Alarms indicating deviation from another variable or parameter, with separately configurable high and low deviation limits

Most analog variables (e.g., pressures and temperatures) will be configured with only one or two alarm limits, and some may have no limits set. However, for critical variables tied to various automatic protective actions, up to four limits may be needed in one or both directions (high or low). For example, these might be used to implement:

- An early-warning alarm indicating deviation from the normal range, well before any automatic actions are taken
- An alarm indicating approach to a trip setpoint, allowing the operator to take manual corrective action prior to a trip

- An alarm indicating that the variable has gone beyond the trip setpoint and further automatic safety actions may occur if corrective action is not taken
- An alarm indicating the variable has exceeded safety limits.

➢ 4.2.1.1.7 The system should provide the capability for alarm limits on analog variables to be calculated in real time from other variables or parameters.

Calculated alarm limits allow for alarm setpoints that depend on other conditions. For example, if reactor coolant system (RCS) temperature is below a certain threshold, reactor power may be limited to a small percentage of nominal. Reactor power alarm limits might be calculated accordingly. In addition, a steam table function may be applied to RCS pressure in order to calculate an alarm setpoint for sub-cooling margin based on a dynamic comparison to RCS temperature.

➢ 4.2.1.1.8 The system should have the capability to assign alarms to groups, which can be used for display purposes or other uses. The configuration for each alarm should include at least five group designators or tags.

The intent here is to provide flexibility to accommodate different views of the alarm information, assist with analysis of alarm information, or facilitate grouping of alarms for other purposes. For example, groups might be used for different areas of the plant (e.g., primary, secondary, electrical distribution, etc.). One of the group tags would be filled in with the number or designator for the area to which that alarm applies. Other group tags could be used for other purposes. The maximum number of tags given in this requirement should be modified as necessary to meet the plant's needs regarding grouping of alarms.

4.2.1.2 Preventing Chattering Alarms

➢ 4.2.1.2.1 A deadband should be configurable for each alarm on an analog variable, where the deadband is the difference between the alarm limit setpoint and the value at which the alarm clears.

The deadband provides hysteresis, which can prevent the alarm from chattering when the variable value oscillates above and below the alarm setpoint.

➢ 4.2.1.2.2 Discrete inputs should have contact debounce filters or other means to prevent alarm "chattering" due to contact bounce. The contact debounce filter delay or time constant, expressed in milliseconds, should be configurable.

For alarms generated from physical contacts, the system must have some means to prevent contact bounce from causing the alarm to chatter. For discrete alarms generated from computed values, the system should have a means to prevent chattering due to rapid changes of state of the computed discrete parameter cause by oscillating inputs. Contact debounce filtering needs to be applied at the source where the alarm condition is detected.

➢ 4.2.1.2.3 Time filtering should be provided for all alarms, so that momentary excursions beyond the setpoint or oscillations around the setpoint will not cause momentary or chattering alarms. The filter delay or time constant (expressed in seconds) should be configurable.

In addition to contact bounce, another cause of chattering alarms is an analog variable that oscillates around the setpoint (beyond the configured deadband). This may be caused, for example, by fluid turbulence or "sloshing" of a liquid level in a vessel. For some conditions, any excursion beyond the setpoint (including repeated excursions) should be captured and recorded, but for others a momentary excursion or repeated oscillations around the setpoint do not provide meaningful information. Time filtering can be used to address this. The filter delay or time constant needs to be adjustable so that an appropriate value can be chosen for each alarm such that the expected oscillations are filtered out while still ensuring that the alarm is not delayed so much that the operator has insufficient time to respond to valid alarms.

- 4.2.1.2.4 The system should allow individual alarms to be configured for chattering alarm detection and suppression, based on exceeding a preset number of alarm events in a preset time. Once chattering is detected, alarm generation for that condition should be suspended until: (1) the alarm behavior falls within a second set of predefined limits (less than a preset, configurable number of alarm events occurring within a preset, configurable time), or (2) for an alarm on an analog variable, the value exceeds the alarm setpoint by more than a preset, configurable amount. The times at which alarm suppression begins and ends should be recorded in the alarm history. Any alarm lists that display this alarm should include messages indicating the beginning and end of chatter suppression. During the time that the alarm is suppressed, any SDCV displays or other displays showing the status of the alarm should indicate clearly that the alarm is under chatter suppression.

Even after application of contact debounce or other time filtering at the input, an alarm still may occur repeatedly under some circumstances, and thus create a large number of alarm events. This can be an annoyance to the operators, over-burden communication pathways, and add many records to the alarm history database. The system should monitor for this behavior and suppress generation of additional alarms until the chattering has fallen below preset limits. For an analog variable, chatter suppression also should be released if the variable value significantly exceeds the alarm setpoint.

It is very important that any display of information related to an alarm configured for chatter suppression provide clear indication of when suppression is in effect and when it has been released. Chatter detection and suppression are best performed at the source, where the alarm is first generated, as this minimizes loading on processors and communication links downstream of this point.

4.2.1.3 Alarm Prioritization

- 4.2.1.3.1 The system should support alarm prioritization. At least six priority levels should be provided, so that each alarm can be configured with a priority of from 1 to 6, where 1 is the highest priority and 6 is the lowest priority.

Prioritization allows operators to determine which alarms need to be dealt with first when multiple alarms are occurring, or to decide how quickly a response may be needed to an alarm that occurs while other tasks are ongoing. Typically, at most three or four priority levels should be used for alarms intended for the control room operators. However, availability of additional priority levels can allow use of these priority assignments to accomplish other related objectives. For example, one priority level might be used to segregate early-warning alarms from other alarms. The maximum number of priority levels specified can be adjusted based on the plant's expected needs.

Priority levels can be used, if desired, to separate events from alarms (e.g., events important to situation awareness, and other events that should be logged). However, it is preferable that these be categorized separately rather than identified through a priority assignment. Priority normally should be reserved for indicating urgency of response for alarms requiring action by the user.

The priority assigned to an alarm can be based on the time available to respond to the alarm and the consequences of not responding. Consequences should consider the impact on nuclear safety, personnel safety, plant operation, and investment protection. Priority assignments should be such that a target distribution of alarms across priorities is achieved based on actual performance in plant transients and upsets. The number of Priority 1 alarms occurring should be limited to ensure that the prioritization is effective in drawing the operator's attention to those requiring the most urgent attention.

It is important to note that prioritization should not be relied upon as the sole means to deal with alarm overload. Alarms should be generated and processed with logic that is aware of system and plant operating modes, and system-level alarms should be provided indicating the operating status and level of degradation of systems. These intelligent alarm techniques should be incorporated first, placing less burden on global prioritization as a means to address alarm overload.

The chosen prioritization scheme should be reviewed and validated carefully, preferably based on simulation prior to use in the plant.

- 4.2.1.3.2 The system should support priority escalation. When an alarm is configured for priority escalation, a timer is started when the alarm initially occurs. If the condition is still in the alarm state (acknowledged or unacknowledged) when the timer times out, the condition is re-alarmed at a higher priority level. The old alarm is removed or replaced (see the next requirement below). The time delay and the new priority level should be configurable for each alarm.

An alarm may be given a relatively low priority because there is a significant amount of time available to respond to the alarm. However, if the alarm has serious consequences and it is left standing for some time without any action being taken, then response to the alarm may become much more urgent. Escalation can help in this situation by re-alarming the condition with a higher priority consistent with the increased urgency of the required response.

Note, however, that priority escalation may not be the best approach for addressing this. Typically, response to the alarm becomes more urgent because conditions degrade further over time. The best approach in this situation is to generate additional alarms that alert the operator to the more serious conditions occurring in the plant, assigning them a priority appropriate to the urgency of responding to those conditions. For example, an alarm on an analog variable (e.g., pressure) can have multiple alarm limits that signal increasing severity of a high or low pressure condition (e.g., pressure high and high-high alarm limits). If the pressure high alarm gets no response and the pressure continues to rise, the high-high alarm will occur at a higher priority level, alerting the operator to the continued degradation of the pressure condition. For some alarms, there may be other plant or process conditions signal increasing degradation of the process, system, or component, ensuring that the operators are made aware of the increasing urgency of response. Alarm logic or processing may be needed to suppress earlier alarms when a new, higher-priority alarm occurs due to the degrading conditions.

Typically, use of a fixed time delay for escalation provides a less direct indication of degrading conditions or increased urgency. Therefore, this method should be used only if it is not practical to

provide an additional alarm or alarms directly tied to the degrading conditions that require a more urgent response.

- 4.2.1.3.3 When a condition is re-alarmed due to priority escalation, the new higher-priority alarm should replace the older, lower-priority alarm. This should be done in a way that the older alarm does not appear to have "cleared" (returned to normal), or that the operator is presented with multiple indications of the same alarm but at different priorities.

  It is important that priority escalation not confuse users into believing the old condition has returned to normal. The system should not require the user to take any action regarding the old alarm. The user should only have to acknowledge the new higher-priority alarm.

4.2.1.4 Dynamic Setpoints and Dynamic Prioritization

Use of dynamic setpoints and dynamic priorities can help make alarms more aware of the operating context in which they occur – operating states or modes of the plant and the associated systems. Note that alarm presentations should always make clear what mode is currently being used to determine the setpoints and priorities, so that users are not confused about how the alarm system is generating and processing alarms. See Section 4.2.6 for requirements on alarm presentation.

- 4.2.1.4.1 Dynamic setpoint capability should be provided so that setpoints (for analog variables and discrete parameters) and deadbands (for analog variables) can change automatically based on the current plant or system operating mode, or on the occurrence of other conditions or events.

  The normal or expected operating range for a plant variable may depend on the operating mode of the system or the plant. The alarm state for a discrete parameter also may depend on the current operating condition. Mode or condition dependent alarm setpoints can be set to ensure that alarms are meaningful in each operating condition.

- 4.2.1.4.2 Dynamic prioritization should be provided so that alarm priorities can change based on the current plant or system operating mode, or on the occurrence of other conditions or events.

  The priority of an alarm may depend on the operating mode of the system or the plant. The ability to change priority dynamically based on these conditions will help ensure that the operators can continue to rely on prioritization to help determine which alarms to respond to first as systems and the plant go through mode changes.

- 4.2.1.4.3 For each alarm, the capability should be provided to configure individual setpoints, deadbands, and priorities for up to eight different plant modes.

  This feature facilitates the use of dynamic setpoints and dynamic prioritization based on plant mode. Nuclear plants typically have five or six operating modes as defined by the plant technical specifications and operating procedures. However, if not already included, it may be beneficial to define additional "transitional" modes, such as a post-trip mode that applies after a reactor/turbine trip, or a de-fueled mode.

Including the ability to configure the full set of priorities and setpoints for all plant modes as part of the alarm configuration simplifies the management of these settings.

- 4.2.1.4.4 Dynamic setpoints, deadbands, and priorities should change automatically upon entering a new plant mode or condition, regardless of whether the mode/condition change is initiated automatically or manually.

  Plant mode changes may be made automatically by the control and monitoring system or the system may prompt the operator when the conditions for a mode change appear to be met, letting the operator decide when to declare entry to the new mode. In either case, the system generating the alarm should make the corresponding adjustments to setpoints and priorities automatically when the mode has been changed, without requiring any explicit operator action to change these values.

- 4.2.1.4.5 The system should provide the capability for an operator to determine, prior to a plant mode change, what impact this change will have on the current alarms and any new alarms that will result. This should be done in a way that does not alter the primary alarm displays being used by the operators or other users (e.g., the information can be brought up on a separate screen upon request).

  With dynamic setpoints based on plant mode, and alarm conditioning logic that makes alarms mode-aware, a change in plant mode may cause new alarms to appear automatically. In addition, some existing alarms may clear, and other alarms may change their priority. As an aid to the operator, the system can provide a "preview" of these changes, upon operator demand. For example, this would allow the operator to determine beforehand what new alarms would be brought in by the mode change, indicating a condition that would be off normal for that mode. This could prompt action to correct these conditions prior to entering the new mode, avoiding the alarms, and more importantly, avoiding any potential consequences the alarms are designed to protect against.

  Ideally, all pre-conditions for entering a new mode would be met through actions taken in accordance with plant operating procedures prior to the mode change, and thus no alarms would occur on entering the new mode. However, it is best to provide the operator with an aid to confirm this, and identify any potential off-normal conditions for the new mode if they do exist. This can also aid in examining the effects of the mode change on existing alarms, and in a general sense, it can help reinforce the operators' training and understanding of the mode-based relationships built into the alarm system.

  It is important that the preview of new alarm states not cause confusion for any members of the operating crew or other users of the alarm information regarding what the current alarm states are. Therefore, the aid should be provided on a separate display from those normally used to monitor alarm status.

4.2.1.5 Time Stamping

- 4.2.1.5.1 All alarms and events should be tagged or "stamped" with the time of occurrence. This information should be carried with the alarm/event information as it is processed for display and recording in the historical record. Similarly, the time at which the condition clears (returns to normal) also should be tagged and recorded. These are referred to as *time stamps*.

➢ 4.2.1.5.2 Time stamping should be done as close as possible to the source of the alarm, so that the time stamp represents as closely as possible the actual time of detection in the plant.

See Section 4.3.1 for additional requirements related to time tagging of alarms and events.

4.2.1.6 Alarm Hierarchy

➢ 4.2.1.6.1 The alarm system should support generation and display of *process alarms* and events in a hierarchy, corresponding to the hierarchy of plant systems and functions, components, and sub-components. At a minimum, the following levels should be supported:

- Plant level
- System or function level (e.g., auxiliary feedwater system, component cooling)
- Component level (e.g., pump or tank)
- Sub-component or component support level (e.g., lube oil, or individual sensors)

The alarm hierarchy should correspond to the hierarchy of information display in the rest of the plant information systems. See Section 4.1.3.1 of EPRI 1010042 [3] for guidance on establishing an information display hierarchy.

➢ 4.2.1.6.2 Alarms and events should be provided with configurable tags indicating the level in the hierarchy and, for each level below the plant level, the particular system/function, component, or sub-component. Tagging or coding the alarm and event records with this information will facilitate sorting and filtering based on these tags, constructing alarm displays that depict the hierarchy, and integrating alarms into process graphics and other displays that reflect the hierarchy.

➢ 4.2.1.6.3 The alarm system should provide alarms at the system/function level indicating problems with the availability of any system or function that is not currently operating, but which should be operable when needed. These alarms should be conditioned based on plant mode such that the alarm will not occur when the plant is in a mode for which the system or function will not be needed. However, an event still should be generated under these conditions, so that the system availability indicator can properly reflect the availability or unavailability of the system/function.

When a system or function is not currently operating, the alarm system should alert the operators to any conditions indicating that the system has become unavailable, i.e., it will not operate properly if called into action. When presented on a spatially dedicated, continuously visible (SDCV) display, the absence of the alarm serves as an indication that the system is available. This capability to indicate availability/unavailability of major plant systems and functions is an important aid in helping the operators to maintain situation awareness. The display can be implemented as an SDCV alarm display, or it can be integrated with a plant information display, adding alarm functionality to a system availability indicator. This feature may be most effective when implemented as part of an overall information display or set of displays specifically designed to support situation awareness. See Section 4.1.3.1 of EPRI 1010042 [3] for further guidance.

There are several ways to generate these alarms. Any one or a combination of techniques may be used, including:

- Combine individual alarms and events, any one of which would indicate unavailability of the system or function, thus creating a grouped or *shared alarm*
- Use logic to create the system/function-level alarm based on lower-level conditions (process variables, equipment status indications, etc.) used as inputs
- Construct models of the plant systems and functions that provide, as outputs, indication of system/function availability or unavailability

Alarm engineers should ensure that these alarms reflect all of the conditions that could cause the system/function to be unavailable, within the limits of available instrumentation. It is important that the system availability/unavailability indicators be as complete and accurate as possible.

A number of modeling techniques have been proposed for use in nuclear plant information and alarm systems, and some have seen limited use. Recent examples are the use of state models [6] and multi-level flow modeling [7]. Modeling capability may be built into the alarm system, or the models may be run as separate software applications. If they are run separately, they need to be well integrated with the alarm system, and they should not introduce unacceptable delays in generating and processing alarms.

➢ 4.2.1.6.4 The alarm system should provide alarms at the system/function level indicating problems with the operational status of the system or function that require operator action. These alarms should reflect awareness of the current mode of operation of the system or function so that they are relevant in all operating modes. The alarms should indicate whether the detected condition(s) have caused the system or function to fail to perform properly. If the system/function has not failed, the alarms should indicate the seriousness of the problem(s) that were detected, based on their potential impact on the system or function and the time available to respond to the condition(s).

While a system or function is in operation, conditions may be detected that have varying levels of impact on the operational status of the system/function. Some conditions may have no effect on current operation, but indicate a need for maintenance (e.g., low level in an oil reservoir on a pump indicating a need to replenish the oil). These should be routed to maintenance personnel for action. Operators may need to be notified of the condition and the fact that maintenance has been alerted, but if there is no action for them to take, it is not an operator alarm.

Other conditions may indicate more serious problems that require operator action, but leave the system operational. An example might be loss of one pump in a redundant pair, where the second pump is running and allows the system to continue to fulfill its function. Other conditions may occur that indicate the system has failed to operate, or is not fulfilling its function.

As part of the alarm hierarchy, one or more alarms should be generated at the system level to indicate the operational status of the system or function. When presented on a spatially dedicated, continuously visible (SDCV) display that shows both the alarm and normal (non-alarm) states, the system-level operational status alarms provide positive indication of each system's health. Like the availability indication discussed above, the capability to indicate operational status of major plant systems and functions is an important aid in helping the operators to maintain situation awareness. It can be implemented as an SDCV alarm display, or it can be integrated with a plant information display, adding alarm functionality to a system's operational status indicator. Again, this feature may be most effective when implemented as part of an overall information display or set of displays specifically designed to support situation awareness. See EPRI 1010042 [3] Section 4.1.3.1.

As with alarms on system availability, there are several ways to generate alarms on operational status of a system, including use of system models. Any one or a combination of the techniques discussed above for system availability alarms may be used. Alarms intended to indicate whether a system is or is not operating correctly should reflect all of the conditions that could cause the system to fail or not fulfill its function, within the limits of available instrumentation.

➢ 4.2.1.6.5 Plant or system models used by the alarm system in generating or processing alarms should exhibit the following characteristics:

- Simplicity – it is important that any models used be sufficiently simple that they can be easily understood by the engineers who configure them, and by operators and other users of the resulting alarms
- Transparency – the alarm system should provide, on demand, information that explains the basis for the model outputs (e.g., an operator can query the alarm system for information explaining the basis for a system availability alarm driven by a model of the associated system)
- Accuracy and reliability – it is very important that outputs from models used in generating or processing alarms be correct; if there is uncertainty regarding correctness or completeness of the model outputs, then other options for generating the alarms should be considered

4.2.1.7 Alarm Conditioning Logic

➢ 4.2.1.7.1 The system should provide the capability to generate alarms based on calculations and logical combinations of inputs, referred to as *alarm conditioning logic*. It should be possible to apply this logic to the following:

- Analog variables, received as system inputs or derived or calculated within the system
- Discrete inputs or derived logical variables
- Operating modes or states of the plant, the associated systems and components, and
- Other alarms and events

The conditioning logic capabilities should include the ability to apply timers with configurable time intervals.

Use of conditioning logic when generating alarms can make alarms smarter in the sense that they are more aware of the states of the related components and systems, and less likely to cause nuisance alarming. All alarms should be "context aware," or "state aware." As a simple example, an alarm on low discharge pressure for a pump can be conditioned to occur only when the pump is operating, and on startup only after a preset time delay to allow the pump to come up to speed. Simple Boolean logic functions should be provided, along with time delay functions. In addition, calculations may be needed to derive alarms for some conditions (e.g., summing two or more flow rates to create an alarm on total flow, or subtracting two temperatures to derive an alarm on differential temperature). Finally, alarms themselves may need to be combined using logic to create higher-level alarms, such as those needed to support the alarm hierarchy (e.g., a system-level alarm created based on a combination of component-level alarms).

➢ 4.2.1.7.2 In a manner similar to *process alarms*, the alarm system should generate *system alarms* in a hierarchy that provides information to operators and maintenance technicians that is appropriate to their needs. This should include system-level information indicating the operational impact of faults and failures, as well as detailed information on detected faults or failures, as appropriate for each user.

System alarms are alarms on off-normal conditions detected within the instrumentation and control, information, and alarm systems based on self-diagnostics. Maintenance personnel need to be alerted to all faults and failures detected within these systems. Detailed information on these faults and failures should be provided to maintenance personnel to support troubleshooting and repair of the systems. However, operators have a different need for information. They need to understand the operational impact of the detected conditions so that they can take appropriate actions in response. To support them in their tasks, the alarm system should generate higher-level information that meets their needs. For example, the operators should be provided with alarms that indicate:

- An automatic control system is not operating properly or has failed, requiring operator intervention
- An automatic control system is still functioning but its performance is degraded (e.g., a fault automatically results in a change in control mode that retains automatic control but provides less functionality or performance)
- Manual control capability has been lost (e.g., failure of an I/O unit that sends manual control signals to field equipment, potentially resulting in the need to use local manual control of the equipment)
- The system (including both automatic and manual control capabilities) is operating properly, but maintenance is required on some portion of the system (e.g., a fault in a redundant module not affecting operation or information flow)
- A supporting feature as been lost or is degraded, potentially affecting operational capability (e.g., loss of a calculational capability such as leak rate calculations due to failure of a server or pair of servers, or loss of historian or data recording capability)
- An individual data input or subset of the input signals has been lost or is suspect (e.g., due to instrument failures, or loss of a local instrument bus or multiplexer), causing these values, plus any calculated values derived from the affected signals, to be suspect
- A portion of the alarm system is degraded or not functioning properly (e.g., loss of a central alarm server or pair of servers, resulting in loss of global alarm processing capabilities)
- A portion of the operator's overall human-system interface has been lost or is degraded (e.g., failure of one or more workstations, or failure of a data network providing information to the workstations)

4.2.1.8 Inhibiting or Disabling Alarms

➢ 4.2.1.8.1 The alarm system should provide the capability to inhibit or disable individual alarms temporarily when this is necessary to prevent nuisance alarms (for example, when the associated equipment is undergoing maintenance or repair). This feature should be implemented in a way that does not require that the setpoint be modified or removed, or that any other configuration settings be altered. The date and time at which an alarm is inhibited, and the date and time at which it is released, should be recorded in the alarm history.

In order to avoid alarms occurring as nuisances or becoming "standing alarms" during planned equipment maintenance or repair, it is important for users to be able to inhibit alarm generation for the affected conditions. This should not require altering the normal configuration settings for the alarms, as this would make configuration management more difficult and could lead to configuration errors. A separate "inhibit" or "disable" function should be provided. Alarm inhibits and their release should be recorded in the alarm history to ensure that the historical record of alarms properly reflects the time interval during which any alarm was disabled.

The alarm inhibit function should not be used as a way to address improperly designed or configured alarms. It should be used only for temporary situations during which a properly designed alarm would occur unnecessarily due to activities ongoing in the plant. If an alarm proves to be a nuisance due to having an improper setpoint or alarm conditioning logic that is incorrect or incomplete, then a design change should be made to correct the setpoint or logic, or some other permanent change should be made to address the problem.

If an alarm has already occurred and it is concluded that the alarm will remain active for a long time (e.g., repairs must be made that will take time to complete), then alarm "shelving" should be considered as a way to address the alarm. See Section 4.2.3.2.

- 4.2.1.8.2 When an alarm is inhibited, all detailed alarm displays showing information about the alarm should clearly indicate that the alarm is inhibited. In addition, users should be able to display and print a list of all inhibited or disabled alarms to assist in tracking and managing these.

The plant should have appropriate procedures in place to control use of the inhibit function, ensuring that alarms are inhibited or disabled only with appropriate approvals, and that inhibits are released prior to returning the equipment to service. The system should support the plant staff in this effort by clearly indicating on any detailed alarm display or list that the alarm is inhibited, and providing the capability to obtain a listing of all currently inhibited or disabled alarms.

- 4.2.1.8.3 Any spatially dedicated, continuously visible (SDCV) display of an alarm that is inhibited or disabled should indicate that the alarm is inhibited. For grouped or shared alarms on SDCV displays, the display should indicate when one or more of the inputs to a shared alarm are inhibited.

SDCV display of an alarm that is fully or partially out of service due to an alarm inhibit should indicate this to the users of the information. Then, when the indication is inactive (e.g., a tile is unlit or "dark"), users are not confused as to whether the condition is truly normal or the alarm is out of service.

See Section 4.2.6 for additional requirements related to alarm information display.

4.2.2 User-Defined Alarms

- 4.2.2.1 The alarm system should provide the capability for authorized users to create temporary user-defined alarms. For analog variables, it should be possible to set one temporary high alarm limit and/or one low alarm limit, regardless of what alarm limits are already set for that variable. For any discrete variable that has no existing alarm defined, either of the possible states should be configurable as an alarmed state to create a temporary alarm for that variable.

Temporary user-defined alarms can be very useful in situations in which enhanced monitoring of a piece of equipment is required, when special system configurations are used, or maintenance activities are being performed that require additional alarms to properly monitor and detect problems during these activities. It should be possible for the user to establish a temporary alarm for any variable available within the alarm system including calculated or derived values (except discrete variables for which an alarmed state has already been defined).

User-defined alarms should be routed for display to those users who established the alarms. See Section 4.2.4 for requirements on alarm routing.

User-defined alarms should be presented separately from the permanently configured alarms and in a way that does not interfere with the user's ability to assimilate and respond to the permanently configured alarms that may be more critical. See Section 4.2.6 for requirements on alarm presentation.

- 4.2.2.2 User-defined alarms should not interfere with the proper functioning of any other alarms or events.

Establishing, modifying, and removing temporary user-defined alarms will be at the users' discretion, and will not be subject to the plant's design control procedures. The alarm system must prevent these alarms from interfering with any of the designed-in functionality of the alarm system (e.g., by ensuring that users who are authorized only for entering and changing user-defined alarm settings cannot change the normal alarm configuration settings, ensuring that no user-defined settings can over-write existing alarm settings, etc.).

- 4.2.2.3 The system should record the date and time any time a user-defined alarm is established, modified, or deleted. The system also should record the identity of the person making the change. This information should be archived with the alarm and event history.

The plant should establish appropriate administrative procedures to control the creation, tracking, and removal of user-defined alarms. These features will support the plant in managing these alarms.

- 4.2.2.4 The interface provided for users to establish, track and remove user-defined alarms should be simple and easy to use. The alarm system should provide the capability to list all currently active user-defined alarms, the date and time when they were created, and who created them.

The human-system interface provided for establishing and managing these alarms should be simple, intuitive, and easy to use so that it is suitable for the alarm system users. It should not require the level of knowledge and experience of the personnel who maintain the configuration of the overall alarm system.

4.2.3 Alarm Processing

This section addresses additional processing of alarms performed by the system after the alarms have been generated. It is preferred that intelligence be built into the alarms as they are generated, so that all alarms that are generated are meaningful and no unnecessary or redundant alarms are generated. However, alarms are likely to be generated in different systems or sub-systems, which may be limited in their access to plant-wide information, or limited in their

processing capabilities. Therefore, the alarm system should be capable of applying additional processing functions based on plant-level information (e.g., plant mode and plant-wide events) or relationships among alarms that have been generated at multiple locations.

Distinguishing between what is an "alarm generation" function and what is an "alarm processing" function is not important. What is important is that all alarms have sufficient intelligence built in to ensure that they are meaningful to the users, and the alarm system does not overload users with information, regardless of where in the system the intelligence is applied.

4.2.3.1 Cause-Consequence and Event-Based Processing

- 4.2.3.1.1 The alarm system should be able to recognize when alarms and events occur that have defined cause-consequence relationships. These relationships can be identified through use of models of plant processes and systems, or through pre-configured groupings of alarms that have such relationships. The system should identify and tag the alarm or event that represents the "cause" or initial alarm in the cause-consequence grouping, and separately tag the consequential alarms.

  A major contributor to alarm overload with existing alarm systems is the occurrence of multiple alarms caused by a single event. By identifying when such groups of alarms occur, and which ones are potential "causes" or initiating events, the alarm system can prevent users from having to process this information themselves. Models may be used to identify cause-consequence relationships automatically. Alternatively, alarms that are related by cause-consequence relationships may be identified at the time the alarm system is configured. The system should support both of these implementation methods.

  Tagging the related alarms and events when they occur ensures that further processing and display of the alarm and event information can recognize the cause-consequence relationships and provide appropriate aids to the users in assimilating this information.

  In some cases, it may be appropriate to suppress the alarms that are consequences of the event because they do not provide any additional information to the operator in the near term. (The operators can still access the suppressed alarm information through supplemental displays, but it is not presented on the primary alarm display.) The operator may need to focus on the failure that has occurred and work to correct it. An example might be loss of a feeder to an electrical bus. Many alarms may occur because of the loss of voltage on the bus, including low voltage alarms on downstream buses or power panels, and alarms indicating failure of equipment supplied by these buses and panels. The operator's near-term action may be focused on restoring power to the original bus by feeding it from another source, thus restoring power to all of the affected downstream equipment.

  However, simply suppressing the consequential alarms may not be appropriate in all cases. The operator's near-term action may be based on the consequences of the event, rather than the cause. For example, if a pump trips on low suction pressure and this causes low flow in a cooling system, the operator's first response may be to act on the low-flow alarm (the consequence). Flow may need to be restored by starting an additional pump or re-aligning the system to receive flow from another source. Later, once the flow situation is stabilized and the cooling system is adequately performing its function, the operator can concentrate on what caused the low flow in the first place (tracing back to the pump trip and then the low suction pressure condition) and identify appropriate corrective actions. It is important to help the operator identify cause-consequence relationships and

to provide aids that assist in responding to the underlying events. In some cases, this involves supporting rapid identification of the root cause, and in others, it may require initially responding to the consequences and later diagnosing the cause. The alarm system should support the operator in either of these situations.

- 4.2.3.1.2 The alarm system should allow, as part of system configuration, the definition of up to 10 events for event-based alarm processing. During operation, the system should detect the occurrence of any of these pre-defined events. The system should then identify alarms occurring that are expected as a result of the initial event. The system also should identify events that were expected, but did NOT occur, and should present alarms on these missing events. These capabilities may be accomplished through use of models, or by use of pre-defined lists of expected alarms, and the time intervals in which they would be expected to occur relative to the time the event is first detected.

  Major plant events such as a plant trip cause many alarms to occur in existing plants. The alarm generation and processing methods discussed in previous requirements should significantly reduce the number of alarms occurring in such events. Alarm conditioning logic, dynamic setpoints and dynamic priorities in particular should contribute to alarm reduction in these events. However, these techniques may not eliminate cascading alarms completely in all plant events. It is important for the alarm system to have the capability to deal with alarms that may still occur due to major plant upsets. By identifying the expected alarms, the system can aid the operators in focusing on unexpected conditions that may require operator action. This includes identifying conditions that were expected but did not occur.

  The maximum number of events that can be handled by the system can be adjusted based on the expected needs of the plant for event-based alarm processing.

4.2.3.2 Alarm Shelving

- 4.2.3.2.1 The alarm system should provide the capability to “shelve” an alarm that is currently active (in the alarm state), if it is concluded that the alarm will remain active for a long time (e.g., due to the need for repairs that will take some time to complete). A shelved alarm should be processed such that it does not display as an active alarm until it is restored (taken off the “shelf”). Alarm shelving should be accomplished without requiring any change to the configuration of the alarm. The date and time at which an alarm is shelved, and the date and time when shelving is discontinued for that alarm, should be recorded in the alarm history.

  Section 4.2.1.8 addresses the need to “inhibit” or disable the generation of specific alarms prior to beginning planned maintenance or repair activities that would cause the alarms to become a nuisance. This requirement addresses the situation in which an off-normal condition has occurred, resulting in an alarm, and action has begun or has been ordered to correct the condition but will take some time to complete. The alarm can be shelved during this time so that it is not continually displayed, thus reducing the number of standing alarms and helping to ensure that new alarms requiring action are easily recognized.

- 4.2.3.2.2 When an alarm is shelved, all detailed alarm displays showing information about the alarm should clearly indicate that the alarm has been shelved. In addition, users should be able to display and print a list of all shelved alarms to assist in tracking and managing these.

The plant should have appropriate procedures in place to control use of alarm shelving, ensuring that alarms are shelved only with appropriate approvals, and that shelving is removed once the condition has been corrected. The system should support the plant staff in this effort by clearly indicating on any detailed alarm display that the alarm is shelved, and providing the capability to obtain a listing of all currently shelved alarms.

- 4.2.3.2.3 Any spatially dedicated, continuously visible display of an alarm that is shelved should indicate that the alarm has been shelved. For grouped or shared alarms on SDCV displays, the display should indicate when one or more of the inputs to a shared alarm are shelved.

SDCV display of an alarm that has been shelved should indicate this to the users of the information. Then, when the indication for that alarm is inactive (e.g., a tile is unlit or "dark"), users are not confused as to whether condition is truly normal or the alarm has been shelved.

See Section 4.2.6 for additional requirements related to alarm information display.

- 4.2.3.2.4 The alarm system should have the capability to provide a timed reminder or notification that an alarm has been shelved for longer than a preset, configurable time.

This capability can assist the plant staff in ensuring that a shelved alarm is not forgotten.

4.2.3.3 Other Alarm Processing Requirements

- 4.2.3.3.1 The alarm system may receive alarms on the same condition from multiple, redundant systems or redundant communication links. The alarm system should consolidate these to provide a single, validated alarm on that condition. When the alarm system detects a discrepancy, a *system alarm* should be generated to alert personnel to the discrepancy between redundant sources of information.

Redundant alarms on the same condition can cause unnecessary burden on users and generate redundant information in the alarm history database.

- 4.2.3.3.2 The alarm system should provide the capability to configure groups of alarms for "first-out" indication. When more than one alarm occurs within a first-out group, the alarm system should identify the alarm condition that occurred first, distinguishing it from others occurring within that group. The system should allow multiple groups of alarms to be configured for first-out indication.

First-out capability aids the operators in determining the potential cause of an event such as a reactor or turbine trip. The alarm system indicates which trip signal occurred first (based on time of detection by the alarm system), distinguishing it from others that occur as a consequence of the trip and do not indicate the cause. The ability of the alarm system to identify the cause correctly is limited by the relative time delays between actual occurrence of the different trip signals and receipt of the associated alarms or events by the alarm system. The associated inputs should be treated as sequence of events (SOE) points with high-resolution time sampling, as discussed in Section 4.3.1.1.

Alarm displays should have a means of indicating the first alarm to occur in a first-out group. This indication should not interfere with other display functionality. See Section 4.2.6 for requirements on alarm display.

- 4.2.3.3.3 The alarm system should implement dynamic setpoints and dynamic prioritization of alarms as described in Section 4.2.1.4. When the system that generates the alarms cannot provide this functionality, the alarm system should implement it as part of alarm processing.

  As discussed in Section 4.2.1.4, it is best to implement dynamic setpoints and dynamic priorities at the point of alarm generation. However, some systems may not have the information needed to accomplish this function. In those cases, the alarm system should implement the function. This may be done by adjusting setpoints or priorities based on plant mode changes or other events.

- 4.2.3.3.4 All alarm processing should be sufficiently simple and transparent that users can determine how the alarms have been processed.

  It is important that alarm processing methods be understandable by the users. Models used to support alarm processing should meet the requirements discussed in Section 4.2.1.6.

4.2.4 Alarm Routing to Users/Locations

- 4.2.4.1 The alarm system should provide the capability to route alarms and events to any of a number of destinations, including user workstations, alarm displays, other information systems, separate alarm/event analysis applications, and the alarm/event history archive or historian. Any alarm or event should be configurable for routing to any combination of destinations. The system should support routing to a minimum of 20 separate destinations.

  Alarms intended for action by specific users should be routed to the respective users' workstations, including operations, maintenance and engineering workstations. The plant may decide to route sub-sets of the alarms to specific operator workstations according to the division of responsibility among the operators. Alternatively, they may decide to route all alarms intended for operator action to all operator workstations. User-defined alarms can be routed to the users who created them. Typically, all alarms and events should be routed to the historian.

  Alarms also should be routable to other systems and applications as needed. For example, alarms may be provided to other information and display systems, and analysis systems or applications. To provide maximum flexibility, all alarms and events should be configurable for routing to any combination of destinations. Capability to route to up to 20 destinations is based on three to four operator workstations, two supervisor workstations, the shift technical advisor (STA) workstation, three engineering or maintenance workstations, up to two historians, two destinations for emergency response personnel (e.g., technical support center and emergency operations facility), two analysis applications/stations, two separate information or advanced display systems, and margin for additional destinations. However, the number specified should be adjusted based on the expected needs of the particular plant.

- 4.2.4.2 The alarm system should have the capability to transmit notifications of selected alarms and events to pre-designated personnel on site, or to off-site locations or personnel, through e-mail, text messages, pagers or other notification method. These notifications should be user configurable.

Some alarms and events may be important to personnel located off-site, or may require them to come to the site. Alarms and events should be configurable for transmitting notifications to these personnel, along with messages appropriate to their information needs. Personnel who are on site also may benefit from notification of pre-configured events. For example, a system engineer might be notified when a certain event or condition has occurred within a system for which the engineer is responsible. A plant performance engineer may want to configure a notification to be sent by e-mail when a specific event or condition occurs. Special activities that are ongoing, such as a long-duration test evolution or a period of enhanced monitoring of a system or component, may benefit from automatic notifications sent to selected personnel responsible for monitoring these activities.

4.2.5 Alarm Recording

- 4.2.5.1 All alarms and events should be recorded to the alarm/event history, including the date and time of occurrence. The date and time that alarms clear (return to normal) also should be recorded.

- 4.2.5.2 The date and time at which users acknowledge and reset the alarms should be recorded as part of the history. The specific control location that was used should be recorded in each case.

  This information can be very helpful in reviewing past events and being able to reconstruct the behavior of the alarm system including operator acknowledgment and reset of alarms.

- 4.2.5.3 Alarm history records should include the priority of the alarm at the time it was generated. Any re-occurrence at new priority levels also should be recorded, along with the date and time.

  With dynamic prioritization, it is important that alarm history records reflect the priority of each alarm when it occurred, and include records of any re-prioritization of alarms based on the dynamic priority scheme.

- 4.2.5.4 Alarm history records should include, for each alarm, the setpoint that was used when the alarm was generated.

  With dynamic setpoints, it is important that alarm history records reflect the actual setpoint in effect at the time each alarm was generated.

- 4.2.5.5 Tags indicating groups to which an alarm belongs, and those indicating the applicable level in the alarm hierarchy, should be recorded with each alarm record.

  Although this information could be obtained from the alarm configuration database, it is important to recognize that the alarm history records may be used by other systems outside the alarm system. Including this information with the alarm records ensures that other systems or applications that make use of the alarm and event histories will have access to the information.

- 4.2.5.6 Alarm and event histories should be integrated with other plant data records (e.g., the overall plant data historian) so that, from the user's standpoint, all of the data appear to come from a single source. Divisions between alarm/event history and other plant data records should be transparent to the users.

Users should be able to access alarm history records and other plant data in displays that integrate this information, regardless of what database(s) were used to retrieve the data. This may be accomplished by physically integrating the data into a single database, or using separate databases with software that makes the division transparent to the users.

4.2.6 Alarm Information Display

This section provides requirements related to alarm presentation – display of alarm information to the users. The requirements focus on those features and capabilities needed to achieve the advancements summarized in Section 3.2. See EPRI 1010042 [3] for comprehensive human factors engineering guidelines related to information displays (Section 4.1) and alarm displays (Section 4.4). Also, see EPRI 1002830 [15] for additional guidance on design of computer-based information displays. Appendix A of that document gives an example of an approach for integrating alarms with plant information displays.

It is important to note that alarms are used for multiple purposes. Their primary purpose is to alert users to off-normal conditions that require their action. Alarms are also used to help maintain awareness of plant and system states, and to support diagnosis of events to determine root causes and appropriate corrective actions. This is important because different types of displays are needed to serve these different functions. Spatially dedicated, continuously visible (SDCV) displays of the most important alarms, and a prioritized list of all current alarms help users to identify quickly the conditions that require the most urgent response. Situation awareness displays, as well as the SDCV display of important alarm conditions, support maintaining awareness of plant and system states. Other displays such as a chronological alarm and event history and detailed information displays for individual alarms support longer-term diagnosis and troubleshooting of events.

4.2.6.1 SDCV Group-View Alarm Displays

- 4.2.6.1.1 The alarm system should provide the capability to present alarms at the plant level, and at the system or function level, on spatially dedicated, continuously visible (SDCV) displays that are usable by the entire operating crew.

  Important plant-level alarms displayed in a form that is visible to the entire crew can prompt rapid response to major plant events. These displays also support rapid determination of overall plant state. Similarly, SDCV display of alarms at the system or function level assist in quickly determining what systems are affected, and allow the operating crew to continually assess the state of plant systems and functions.

- 4.2.6.1.2 Each plant-level and system/function-level alarm presentation should be configurable to indicate the priority of each alarm. For a grouped or shared alarm, the display should indicate the highest priority of the currently active sub-alarms (constituents of the shared alarm).

  The operators can use priority to help determine which alarms should be attended to first. Use of dynamic priorities helps ensure that the prioritization is applicable in different plant operating states. For example, an alarm indicating an operational problem with System A may be very important and

require urgent attention during normal power operation, but become much less important when the plant is in another operating mode (e.g., cold shutdown) for which that system is much less critical.

- 4.2.6.1.3 For system/function-level alarms, the system should be able to present SDCV alarm presentations that indicate the availability of each system/function, and the operating status of the system/function. These alarm indications also should be capable of indicating the level of degradation of each system/function.

These system-level alarm indications not only alert the operators to problems with system availability or operation, but also provide a ready means for assessing the state of plant systems and functions. At a glance, a crewmember can determine whether a system is operating correctly or not, and how serious the problems are in that system or function. Availability of systems that may be needed also can be determined very quickly.

- 4.2.6.1.4 The alarm system should be capable of presenting, or providing information to another information display system to present, notifications of events important to the operators' ability to maintain situation awareness. This should include capability to present this information on group-view displays usable by the entire operating crew, and on displays at individual users' workstations.

Changes in plant and system status may not require specific operator actions, but it is important to notify the operators of these changes if they are important to maintaining adequate situation awareness. Status changes should be indicated separately from alarms requiring action. This may be done most effectively by providing visual indications on displays specifically designed to support situation awareness.

4.2.6.2 Other Spatially Dedicated Alarm Displays

- 4.2.6.2.1 The alarm system should provide the capability to present alarms related to any system or function on a display that shows each alarm in a fixed position, using an arrangement that replicates conventional alarm tiles or another similar arrangement. Operators and supervisors should be able to display this screen at their workstations on demand. There should be multiple ways to access the display, including selecting it from an overview display, a system graphic display, a menu, and other navigational aids.

See Section 4.1 of EPRI 1010042 [3] for additional guidance on display hierarchies, display navigation, and other human factors guidelines for display design. Section 4.4 of the same document provides human factors guidelines specifically for alarm displays.

- 4.2.6.2.2 For any grouped or shared alarm, users should be able to select a fixed-position display of the individual sub-alarms that make up the shared alarm.

Shared alarms support the capability to provide information at different levels in the hierarchy. By combining lower-level alarm conditions, for example, an alarm can be displayed that indicates whether there are off-normal conditions associated with a system or a major component such as a feedwater pump. However, the operators will need to be able to access the details that feed into the shared alarm to determine what specific conditions are off normal and take appropriate actions. SDCV display of the sub-alarms provides the same advantages as for higher-level alarms shown on SDCV displays – ability to quickly determine which conditions are off normal, to determine

whether a specific condition is NOT in an alarm state (i.e., it is normal), and to take advantage of pattern recognition to identify specify types of failures or events.

- 4.2.6.2.3 If any of the alarms shown on the SDCV display are inhibited or shelved, this should be indicated on the display. The system should provide the capability for users to access a list of all the related shelved or inhibited alarms.

  It is important that users not be confused by the absence of alarm indications when alarms are inhibited or shelved. This is similar to placing an "out of service" tag on the affected alarm indication.

4.2.6.3 Alarms as Part of Graphic Displays

- 4.2.6.3.1 The alarm system should provide the capability to indicate alarm conditions on graphical displays of the plant, systems, functions, components, and sub-components or component support. The alarm hierarchy should map to the hierarchy of the graphical displays so that alarms are defined at each level of the display hierarchy. The displays should be configurable to indicate the priority of each alarm shown.

  Graphical displays such as system mimics or process diagrams show the status of components such as pumps, valves and tanks, and key variables or parameters associated with the system or components. When any conditions become off normal for these variables or components, the graphical display should indicate the presence of the alarm condition. This helps place alarms in context within the system, assisting in understanding the potential causes and consequences of the alarm condition.

- 4.2.6.3.2 When grouped or shared alarms are shown on a graphical display with alarm priorities indicated, each shared alarm should indicate the highest priority of the active sub-alarms. Users should be able to select a fixed-position display of the individual sub-alarms that make up the shared alarm.

  Consider a pump symbol or icon shown on a system graphic. When any alarm occurs related to the pump, the display indicates this and shows the highest priority of the active alarms. An operator can then bring up a display showing all of the individual alarm conditions for that pump, indicating which ones are in an alarm state and their priorities.

- 4.2.6.3.3 If any alarms are inhibited or shelved related to an item (system, function, component, variable, etc.) shown on the display, this should be indicated clearly to the users. The system should provide the capability for users to access a list of all shelved alarms, or inhibited alarms, related to the item.

  It is important that users not be confused by the absence of alarm indications when alarms are inhibited or shelved. This is similar to placing an "out of service" tag on the affected alarm indication.

- 4.2.6.3.4 The alarm system should be capable of indicating cause-consequence relationships among active alarms shown on the graphical display. The user should be able to turn this indication on or off easily.

If a cause-consequence relationship is identified by the system for alarms currently shown on the display, having the capability to indicate this relationship can aid the user in understanding the current alarm situation and determining the cause. However, this must be done in a way that does not interfere with other uses of the display.

4.2.6.4 Alarm Message Lists

- 4.2.6.4.1 The system should be capable of displaying on a dedicated screen a list of the currently active alarms. This display should be configurable in terms of the information provided for each alarm, and the order in which the alarms are listed. The display should be able to list alarms in order of priority, and in chronological order within each priority.

  The system should provide flexibility in the content and organization of the dedicated alarm message list display, so that it can be tailored to meet the plant's specific needs. Typically, the display should indicate at a minimum the time of occurrence, priority, alarm message, setpoint, and current value for each alarm. By displaying the alarms in priority groupings, with the highest priority alarms at the top of the list, the most urgent alarms will be visible on the screen. See Section 4.4 of EPRI 1010042 [3] for guidelines on the content and organization of alarm message list displays.

- 4.2.6.4.2 Users should be able to display alarm message lists that are filtered and sorted according to the users' current information needs. This should include the ability to provide a list of all alarms and events in chronological order, and lists of alarms for selected systems or functions.

  Users should be able to make use of different sorts and sub-sets of alarm information to support their tasks in monitoring systems and processes, investigating problems that have been identified or are suspected, and diagnosing the cause of a transient or upset. Viewing only those alarms associated with a given system or function, and viewing chronological lists of alarms and events can help them perform those tasks.

- 4.2.6.4.3 The system should provide the ability to filter alarm lists based on cause-consequence relationships, where known. This should include capability to eliminate the consequences, showing only the alarms that are the cause in a cause-consequence relationship.

  Alarm message lists may be used to support diagnosis of events. In that case, it may be helpful to eliminate the consequential alarms and indicate only those at the root of the known cause-consequence relationships.

- 4.2.6.4.4 Alarm message lists should be designed to enhance their usability during conditions in which many alarms are occurring. This should include the ability to prevent alarm lists from scrolling rapidly due to a high rate of incoming alarms. When a message list display is frozen, the presence of new alarms that are not displayed should be clearly indicated.

  See the related requirement in Section 4.3.1.4 for an alarm message list "freeze" capability.

- 4.2.6.4.5 The alarm system should provide the capability to compare the sequence of alarms that occur following a pre-defined plant event to a pre-stored list of expected alarms

for that event. Users should be able to filter alarm message lists so that they include only those alarms that are not in the expected sequence of alarms. In addition, users should be able to display an alarm message list that includes all alarms and events, but highlights those that are NOT in the expected sequence of alarms. Finally, the capability should be provided to indicate alarms or events that were expected (based on the pre-stored sequence of alarms) but did NOT occur.

Application of alarm conditioning logic, dynamic setpoints and other alarm generation and processing techniques described in this report should significantly reduce the number of alarms occurring during plant transients or upsets. However, the alarm system should have the capability to aid the operators in evaluating the alarms that may still occur in the wake of a major transient, to determine which alarms are unusual and may require action.

The ability to compare the actual alarm and event history to the expected sequence of alarms and events that typically occur for a given plant upset or transient can be a significant aid to users in determining what conditions occurred that were unusual and require attention. Filtering out the expected alarms allows the user to focus only on those that may indicate a problem beyond the basic event that was unfolding at the time. The ability to include all alarms and events, and highlight the unusual ones in that sequence, allows the user to see the unusual alarms in the context of other alarms and events occurring at that time, helping the user to understand the sequence and what may have caused the unusual alarms. Identifying expected events that did not occur also can help identify unusual situations that may warrant attention.

Pre-stored sequences of alarms can be determined based on simulator runs that identify the expected alarm sequences for different variations of a specific transient such as a reactor trip, safety injection actuation, loss of offsite power, or other anticipated plant event or accident. See EPRI 1003662 [1] for an example and guidance on implementing this feature.

4.2.6.5 Individual Alarm Information Displays

➢ 4.2.6.5.1 The alarm system should provide the capability to configure detailed information displays for individual alarms. These displays should provide current and historical operational data related to the alarm, plus current and historical maintenance and engineering information on the associated equipment.

The intent here is to take advantage of the capability of modern information systems to integrate information from multiple sources to provide task-specific displays, in this case providing information specific to the task of investigating and responding to an alarm. Examples of the types of information that should be considered for this display, or set of displays, include:

- Current values and recent trends for variables and parameters from which the alarm is derived
- Performance statistics related to the alarm, such as how often on average the alarm has occurred, the date and time that it last occurred, the average amount of time the alarm has remained active, etc.; these statistics should be updated automatically each time an alarm occurs, and stored in a database, or at least made available on demand
- Relationships with other alarms and events, such as cause-consequence relationships
- Any incident reports or condition reports related to the alarm
- Maintenance work orders, current or historical, related to the alarm or the affected equipment

- Information on previous or planned engineering changes or design changes related to the alarm
- Relevant drawings and calculations

The ability to store and display notes entered by operators, engineers, or maintenance technicians related to the alarm, actions taken in the past in response to the alarm, and other information that may be useful to operators or maintenance personnel in responding to new occurrences of the alarm, should also be considered.

➢ 4.2.6.5.2 Individual alarm information displays should be accessible from any display that presents the alarm and from the associated alarm response procedure.

Information related to a specific alarm should be readily accessible from any display showing that alarm. For example, links can be provided on alarm message list displays, system or component graphic displays that indicate the alarm, or SDCV displays showing the individual alarm. In addition, this information should be accessible from the corresponding alarm response procedure (ARP). The ARP can provide the information directly, or include a link allowing quick access to the individual alarm information display.

4.2.6.6 Navigating the Alarm Display Hierarchy

➢ 4.2.6.6.1 Means should be provided to assist users in navigating easily between the different levels of the alarm display hierarchy. In particular, when viewing and responding to an alarm, users should be able to examine the impact of the alarm at the plant level and the system/function level, to drill down to the component and sub-component levels, and to access detailed information related to the alarm as well as the associated alarm response procedure (ARP). Moving between these levels of information display should be simple and straightforward, and the means provided should be consistent among different types of displays.

When an alarm occurs, the operators should be able to assess the impact at the plant level by viewing the SDCV display of plant-level alarms. They can then assess the impact at the system level by viewing the SDCV display of system/function alarms, quickly determining what systems were affected and whether an affected system/function has failed or is still operating but degraded. They can then access related system graphics to see the alarm conditions in the context of the overall system and related components. Cause-consequence relationships can be shown to assist in understanding the events. The operator can view the detailed alarm information either by looking at the dedicated alarm list to see the detailed alarm message, or view the alarm on an SDCV display of all alarms for the affected system or function. Finally, the operator can access a detailed information display for the individual alarm (see Section 4.2.6.5) and the associated alarm response procedure (see Section 4.2.8).

This capability to follow a path from the plant to system/function to component and detailed alarm level is especially important when multiple alarms are occurring and the operators need to understand the impact of the event that is unfolding, prioritize their actions, and respond to the individual alarms.

- 4.2.6.6.2 In situations when only one or a few alarms are occurring, users should be able to identify quickly the specific off-normal condition that has occurred.

  During normal operation when a single alarm occurs, the system should make available to the operators the specific alarm message for the off-normal condition without the operators having to go through a selection process to drill down to the level of the detailed alarm message. This can be accomplished through use of the dedicated alarm message list display, by ensuring that the latest alarm is always visible on the display, or by providing the most recent alarm message on other displays (e.g., providing a small window on all alarm displays showing the most recent alarm message).

4.2.6.7 Other Alarm Display Requirements

- 4.2.6.7.1 Alarm displays should continuously indicate to users the current mode of operation of the alarm system.

  When the alarm system can operate in different "modes" that affect alarm generation or alarm processing (e.g., changing alarm setpoints or priorities based on the current plant mode), the system should provide an indication of the mode in which the system is currently operating. This is important to preventing users from making "mode errors" – taking a wrong action or misinterpreting alarm information due to confusion regarding the current operating mode for the system.

- 4.2.6.7.2 The alarm system should provide the ability to overlay alarm and event information on process data trends using a common, configurable time scale and time interval.

  This capability allows the user to relate in time the alarms and events that are occurring as well as the values of related process variables.

- 4.2.6.7.3 Reflash capability should be provided for grouped or shared alarm indications.

  Reflash ensures that a shared alarm indication alerts the users to new sub-alarms occurring after one has already occurred and has been acknowledged, leaving the shared alarm active (in the alarm state).

- 4.2.6.7.4 The system should provide the capability to alert users when an alarm clears (returns to normal), requiring the user to reset the alarm, or to have the alarm "auto-reset" (return to normal without any alert given to the users). This should be configurable on an alarm-by-alarm basis. For alarms configured to alert the users to clearing of the alarm, the alert should be accomplished by separate visual and auditory indications that are easily distinguished from the indication provided for a new, incoming alarm. When an alarm clears, a message should be generated and stored in the alarm and event history, and it should be possible to include this clearing alarm message on appropriate alarm message list displays.

  When an alarm clears, there may be no action required by the operators. However, in some cases it is beneficial to notify the operators that the condition has returned to normal. The importance of this notification can vary from one alarm to another. The system should provide the flexibility to alert the operators to a clearing alarm, but to do this in a way that is different from an incoming alarm that may indicate urgent attention is needed. Alternatively, alarms may be configured to

provide no alert on a return to normal. In either case, SDCV displays of the alarm and the indications on related graphical displays will clearly indicate whether the alarm is still active or has cleared. In addition, a clearing alarm message should be included on alarm message lists.

- 4.2.6.7.5 Temporary user-defined alarms should be presented separately from permanently configured alarms. A separate, distinguishable auditory alert should be used. User-defined alarms should be included (as an option) in alarm message list displays and recorded in the alarm history. User-defined alarms should be distinguished from permanently configured alarms in message lists and alarm history displays.

  User-defined alarms should not interfere with users' ability to view and respond to permanently configured alarms.

- 4.2.6.7.6 First-out alarm indication should be implemented in a way that does not interfere with other functions of the alarm display.

  First-out indication can be helpful in quickly identifying the cause of a trip or similar event. See Section 4.2.3.3. However, it should not interfere with the primary purposes of the alarm display.

4.2.7 Alarm Controls (SART)

- 4.2.7.1 The alarm system should provide the capability to assign any silence, acknowledge, reset and test (SART) control to operate with any one or more alarm displays.

  This provides maximum flexibility in laying out the controls and assigning them to appropriate alarm displays in the control room. This includes both hard controls and soft controls (see the requirements in Section 4.3.2). The arrangement should be chosen such that an operator can acknowledge only those alarms that are visible from the location of the acknowledgment control. However, the system should not require any operator to actuate multiple silence or acknowledgment controls in response to the same alarms. It should always be clear to the operator what specific alarms or alarm displays will be acknowledged when each control is used.

- 4.2.7.2 The capability should be provided for specific silence controls to silence the audible tones for all alarms in the control room ("global silence" capability).

  Global silence capability allows an operator or supervisor to silence all audible devices during events in which multiple alarms are occurring, helping to reduce distraction until the operators have time to review and assimilate unacknowledged alarms.

- 4.2.7.3 The capability should be provided for a global silence control to prevent further audible tones for a preset, configurable time.

  This feature allows a supervisor or other authorized individual to prevent audible distractions in situations when many alarms occur and the operators need time to perform required tasks prior to acknowledging and responding to the alarms.

- 4.2.7.4 User-defined alarms should be acknowledged separately from other alarms.

➢ 4.2.7.5 SART controls for operator alarms should have no effect on alarms intended for maintenance or engineering personnel, and vice versa.

Each set of users should be able to silence, acknowledge, reset and test their own alarms without affecting other users' alarm displays.

4.2.8 Alarm Response Procedures

This section provides requirements related to alarm response procedures (ARPs). For an advanced alarm system, the ARPs should provide much more functionality than conventional paper-based procedures. They should automate the information retrieval and analysis tasks that the operator traditionally has had to perform in order to confirm and respond to an alarm. The ARPs should be well integrated with the plant information system, providing a window or gateway to other information the operator may need when responding to the alarm. Whether a function or display is provided by the ARP, by another part of the alarm system, or by the plant information system is not important. What is important is for the operator to be provided with the specified functionality, regardless of which "system" provides it.

➢ 4.2.8.1 The alarm system should support development, management, maintenance, and display of computer-based alarm response procedures (ARPs).

Computer-based procedures provide many advantages over conventional paper procedures. For alarm response procedures, these include easier access to the information, automatic retrieval and display of live process data and other information needed in responding to an alarm, and tailored instructions based on the current operating situation.

➢ 4.2.8.2 The system should provide features and tools that promote ease of entering, editing, and verifying ARP content and maintaining control over revisions.

These features may include such items as an import capability to bring in fielded text from other electronic documents or databases, an easy-to-use editor, and tools for maintaining version control and tracking changes in a manner consistent with the plant's document control program.

➢ 4.2.8.3 Each computer-based ARP should include instructions and other information needed to confirm and respond to the alarm. This should include the following basic information:

- The system/function with which the alarm is affiliated
- The alarm identifier and alarm message text, as they appear on the alarm display from which the ARP is accessed
- The alarm setpoint
- Priority of the alarm
- Automatic actions that should occur as a result of the alarmed condition
- Instructions for confirming the alarm (e.g., how to distinguish between an instrumentation failure and a true off-normal condition in the plant)
- Instructions for immediate actions that should be taken in response to the alarm

- Instructions for follow-up or longer-term actions that should be taken

➢ 4.2.8.4 The ARP should display or provide ready access to information on how the alarm was generated, including what inputs were used, their sources (e.g., specific instruments, data from another system, etc.), and any conditioning logic that was applied. Information on alarm suppression that may be applied to the alarm, and other alarm processing techniques such as dynamic setpoint or dynamic priority, also should be provided.

When confirming and responding to an alarm, the operators need to understand how the alarm was generated, what specific inputs were used, and any alarm suppression or dynamic processing that may have been applied.

➢ 4.2.8.5 The computer-based ARP should display the current values of the variables or parameters that are used as inputs to the alarm. The ARP should display or provide ready access to trends for these variables.

Automatic retrieval and display of the pertinent parameters can save the operator a significant amount of time, and eliminate potential human errors in obtaining the current readings. Ready access to trends helps the operator understand the recent behavior of the alarmed variable(s), which helps in diagnosing the problem, predicting future behavior, and planning the response.

➢ 4.2.8.6 The computer-based ARP should display automatically any additional real-time information needed by the operator in confirming and responding to the alarm. The information provided should be based on the current operating situation.

Other information may be needed, such as the status or values of related components and parameters. Any information that is needed and is available to the alarm system should be provided to the operator as part of the ARP. The information provided should be tailored to the current operating situation, avoiding having to give instructions with "if" statements that require the operator to determine what specific information to retrieve. For example, if the information needed depends on how the system is currently lined up, the alarm system should check the line-up and provide the information appropriate for that operating configuration.

➢ 4.2.8.7 The ARP should provide links that give access to related system and component information displays.

The operator may need to obtain information on the status and operating condition of the related systems or components, in addition to the specific parameters automatically displayed by the ARP. The other displays that are needed should be easy to access from the ARP itself.

➢ 4.2.8.8 The ARP should give the operator the capability to access additional detailed information that can assist in investigating and responding to the alarm, including the information described for individual alarm information displays in Section 4.2.6.5.

Operations, engineering, and maintenance information related to an alarm should be accessible from the ARP. See Section 4.2.6.5.

➢ 4.2.8.9 The ARP should provide information on the possible causes of the alarm. Cause-consequence relationships, either pre-defined or based on plant models, should be used to diagnose the cause automatically, or to help the operator establish the possible causes of the

alarm. At a minimum, the procedure should list potential causes and assist the operator in determining which of these has occurred (e.g., by providing instructions and displaying information that is relevant to determining the cause). Any automatic diagnosis should be accompanied by information that helps the operator understand the basis for the diagnosis.

Cause-consequence relationships among alarms should be used to provide automatic diagnosis wherever possible. For example, cause-consequence relationships among alarms in the electrical distribution system might be used to indicate automatically the likely cause of a loss of power to a component, identifying the upstream feeder breaker that opened or the highest-level bus that first lost voltage, resulting in a cascade of alarms in downstream power panels and subsequent equipment power losses. System models may be used to generate the cause-consequence relationships, or they can be pre-configured for specific groups of alarms.

When an automatic diagnosis is provided by the system, the operator should be given information to help understand the basis for the diagnosis and confirm or reject it.

- 4.2.8.10 When a control action is needed in response to an alarm, and a soft control is available for taking the action, the ARP should display or provide ready access to the soft control.

This saves time for the operator, and helps avoid errors in selecting the proper control to respond to an alarm.

- 4.2.8.11 Alarm response procedures and associated displays should be designed in accordance with accepted human factors engineering (HFE) principles and HFE guidelines for computer-based procedures and information displays.

See Sections 4.1 and 4.5 of EPRI 1010042 [3] for HFE guidelines on design of information displays and computer-based procedures.

- 4.2.8.12 The system should be capable of printing hard copy versions of the computer-based procedures that are suitable for use by personnel as a backup when the computer-based ARPs are not available.

Backup hard copy versions will not provide all of the information and functionality of the computer-based procedures, but should include the basic instructions, flow charts, and other information needed for confirming and responding to the alarms.

4.2.9 Alarm System Performance Monitoring

- 4.2.9.1 The alarm system should include continuous monitoring of the performance of individual alarms, alarm presentations/displays, and the overall alarm system. Performance monitoring results should be stored and made available to users through standard and custom-designed reports to allow periodic assessment of performance.

System performance monitoring is important for determining whether the system meets performance goals initially and for continued assessment of performance during operation, particularly as changes are made over time that will affect performance.

➢ 4.2.9.2 Performance statistics should be provided for individual alarms based on a pre-defined, configurable data collection and reporting period. The performance data should include as a minimum:

- Number of times the alarm occurred
- Average and maximum amount of time the alarm was active (in the alarm state)
- Number of times automatic chatter suppression was applied, and the average duration of chatter suppression
- Number of times the alarm was shelved or inhibited and average duration of time it was shelved or inhibited

Performance data are needed on individual alarms to assess their performance and to allow identification of problem alarms. The data-reporting period should be configurable to fit the plant's specific needs for reporting, and to allow adjustment over time as experience is gained with the reporting feature and the statistics obtained.

➢ 4.2.9.3 Performance statistics should be provided for specific, pre-defined alarm destinations or displays (e.g., dedicated alarm displays, individual workstations, etc.), and for the alarm system as a whole. These should be based on a pre-defined, configurable data collection and reporting period. The performance statistics provided should include, as a minimum:

- Number of alarms that occurred over the reporting period
- Average and maximum rate of incoming alarms
- Number of times the incoming alarm rate exceeded a pre-determined, configurable rate and the dates and times these events occurred (allowing identification and evaluation of alarm "floods," how many of these occurred, and when)
- Distribution of incoming alarms across priorities (i.e., number and percentage of incoming alarms by priority level)
- Average and maximum number of standing alarms (alarms that remain active for longer than a pre-determined, configurable time)
- Distribution of standing alarms across priorities (i.e., number and percentage of standing alarms by priority level)
- Average and maximum number of standing alarms for each plant mode
- Average and maximum number of standing alarms by system
- Percentage of time that no alarms were active
- Percentage of time that no alarms were active for each plant mode
- Average and maximum number of both shelved and inhibited alarms

Performance data on selected alarm presentations or displays are needed to judge performance with respect to that display, from the user's standpoint. For example, judging the effectiveness of an alarm tile-replica type display, or an alarm message list display, requires examining how many alarms occur and at what rate, and how many standing alarms typically are shown on the display.

Performance of alarms sent to a maintenance workstation should be evaluated separately from those presented at operator workstations. Finally, overall alarm system performance should be judged as part of assessing the plant's alarm management program.

Some statistics, such as standing alarms, should be evaluated across the different plant operating modes. The amount of time an alarm display shows no active alarms also should be examined across plant modes. These statistics help evaluate how well the system is meeting the darkboard criterion (no alarms active if all systems are in their normal configurations for the current mode and no problems are occurring requiring attention), and the effectiveness of mode-based alarm generation and processing (e.g., mode-based alarm conditioning logic mode-based setpoints).

Examining distribution of alarms across priority levels allows evaluation of the effectiveness of the prioritization. For example, EEMUA-191 [8] recommends that, for a three-level prioritization scheme, the target distribution of alarms across priority levels be 5% at Priority 1, 15% at Priority 2, and 80% at Priority 3. Each plant should establish its own goals for prioritization effectiveness, and then measure performance against those goals. The statistics specified here should help support this. Note that evaluation of the effectiveness of prioritization for alarm message list displays should included determining whether and how often the number of standing Priority 1 alarms exceeded the capacity of the display (i.e., required some alarms to scroll off to back pages).

Evaluating statistics across plant systems allows identification of areas of the plant that may be causing problems with nuisance alarms or contributing to alarm floods, helping focus attention on the areas that need the most improvement.

The data-reporting period should be configurable to fit the plant's specific needs for reporting, and to allow adjustment over time as the plant gains experience with the reporting feature and the statistics that are obtained.

➢ 4.2.9.4 The system should provide the capability to view statistics for user-defined alarms separately from permanently configured alarms, or to view overall statistics covering both.

It may be beneficial to examine statistics for user-defined alarms separately as part of evaluating the usage of that system feature. However, for overall assessment of system performance from the user's standpoint, users should be able to examine statistics covering the total set of alarms presented.

➢ 4.2.9.5 The system should monitor and detect patterns of alarm occurrences over time to identify potential relationships among alarms. The system should identify potential relationships, the alarms involved, and the specific historical alarm data that should be reviewed to examine and confirm the relationship.

This can help identify additional cause-consequence relationships or redundancies among the alarms that should be addressed in the alarm configurations and alarm logic.

➢ 4.2.9.6 Additional aids should be provided for system performance analysis, including for example the ability to obtain:

- Graphs or histograms of incoming alarm rate (or number of incoming alarms occurring in a chosen time interval such as 10 minutes) over time for a specified time period (e.g., hours or days)

- Graphs showing the number of standing alarms over time for a specified time period
- List of all alarms that occurred more than a given number of times during a specified reporting period
- Rank-ordered list of alarms based on the number of times they occurred
- List of all alarms that were active (in the alarm state) for more than a given amount of time during a specified reporting period
- Rank-ordered list of alarms based on the amount of time they were active
- List of all alarms that were shelved for more than a given amount of time during a specified reporting period
- Rank-ordered list of alarms based on the amount of time they were shelved or inhibited

These are just examples of some of the capabilities that should be provided. The intent is that the system will provide built-in reporting features, plus a flexible reporting interface that allows the user to obtain different reports covering any of the statistics available for any alarm destinations, plant systems, operating modes, etc.

4.2.10 Alarm System Support for Maintenance

➢ 4.2.10.1 Alarms that require action by maintenance personnel should be presented on maintenance workstations or displays separate from those used by the operating crew, and with alarm messages suitable to their information needs.

Maintenance workstations or other maintenance alarm displays should be located where maintenance personnel can monitor them and respond to alarms needing their action. The alarm messages should provide the information the maintenance staff needs in order to understand and respond to the alarm. This may be different from the message provided to operators.

➢ 4.2.10.2 The alarm system should have the capability to provide visual and auditory alerts to maintenance personnel to ensure they become aware of new alarms needing their attention. An acknowledgment control should be provided to allow acknowledging new alarms.

The plant owner/designer will need to decide whether visual and auditory alerts should be provided to maintenance personnel, or regular monitoring of the alarm display will be relied upon, depending on the plant's concept of maintenance. If visual and/or auditory alerts are provided, then an acknowledgment control will be needed. However, it is unlikely that silence or reset controls would be required for maintenance workstations.

➢ 4.2.10.3 The alarm system should support generation of maintenance work orders as part of the response to alarms.

Maintenance work orders might be generated in any of a number of ways, including:
1) automatically, with appropriate notification of maintenance and operations personnel,
2) in response to operator command as part of the operator's response to alarm conditions, and
3) in response to maintenance personnel command after evaluating alarm conditions at the maintenance workstation.

The approach taken should be consistent with the plant's concept of maintenance – that is, who is responsible for generating maintenance work orders, and what notifications should be provided to maintenance and operations personnel when work orders are generated. Integration with the plant's maintenance management system can save time for both operators and maintenance personnel when responding to alarms that require maintenance action.

- 4.2.10.4 The alarm system should support cooperative work between operations and maintenance personnel in responding to alarm conditions. This should include the ability for operators and maintenance technicians to view the same information displays to facilitate collaboration in deciding on an appropriate course of action. Maintenance personnel and operators should both be able to enter information into the system that is captured for future use when responding to alarms.

The approach should be consistent with the plant's concept of operations and concept of maintenance and goals for improved maintenance support, including division of responsibility between operations and maintenance personnel.

See Section 4.3.10 for additional requirements related to the alarm system's support for surveillance testing of plant equipment and overlap testing that ensures the alarm system inputs are adequately tested.

4.3 System Design and Performance Requirements

This section provides digital system related design and performance requirements for the alarm system. The section addresses attributes such as time response, input-output capabilities, equipment qualification, reliability and availability, maintainability, and testability. While these attributes are in separate sections below, the attributes all affect each other. Therefore, in designing and evaluating the alarm system, changes to any attribute should be evaluated to determine the effect on all of the other attributes.

4.3.1 Time-Related Requirements

This section provides requirements related to time, including time tagging of alarms and events, maintaining the correct time sequence of events, alarm processing rates, display update rates and responses to user requests. Because meeting these time-related requirements can impact the system architecture, they should be considered early in the design effort.

4.3.1.1 Data Sources, Time Stamping, and Time Resolution

- 4.3.1.1.1 Alarms, events, and data values detected by the system should be time-tagged as close as possible to the source of the data, and with as little time delay as possible beyond the inherent digital sampling interval. Data should be time-tagged at the source. The time tag should be communicated along with the data value. Time tagging of data values at the time when they are recorded to the historian introduces the most error in timing accuracy, and should be avoided.

- 4.3.1.1.2 Time tagging of alarm events by the system should preserve, as much as possible, the chronological order or time sequencing among all alarm events detected and recorded by the system.

- 4.3.1.1.3 For data points that are designated as "sequence of events" (SOE) points and for alarms designated as members of "first-out" groups, the system should be able to resolve time sequencing among events to within one millisecond, based on the time at which each event is detected by the system.

- 4.3.1.1.4 Alarm processing algorithms or analyses that rely on chronological order of alarms or events should recognize the inherent limitations in time stamp accuracy and should properly perform their functions in spite of sequencing errors in the chronological order. The design of the algorithms should compensate for inherent timing inaccuracies.

Preserving the time order or chronological sequence of alarms, events, and process data is critical to the ability of operators and engineers to diagnose plant upsets and perform other post-event analyses. This is also important for correct implementation of "first out" capability. However, it should be recognized that there are inherent limitations on the accuracy of time tagging and thus the ability of the system to resolve correctly the order of events based on when they actually occurred in the plant.

First, the inherent delay associated with digital sampling of the inputs must be considered. The system cannot resolve the time at which an event or data value occurs to any closer than the digital sampling interval. Time tagging at the source, before further processing is performed and associated delays are incurred, will help minimize any additional inaccuracy in time stamps beyond the sampling time.

Guidance on sampling rates can be found in NUREG-1709 [9]. For SOE points, the time sampling should be very fast. For other points, the sampling interval should be chosen based on the expected time behavior of the input signal. For example, many temperature measurements change very slowly and thus do not require rapid sampling. Ideally, rapid sampling would be implemented for all inputs so that the greatest accuracy is attained. This likely would increase the initial capital cost of the equipment. However, the long-term costs of maintaining multiple types of input hardware/software also should be considered.

Another inherent factor that needs to be considered when evaluating accuracy of time stamps is the source of the data. For discrete or contact inputs, the time accuracy may be limited by relay contact pickup or drop out times. For signals obtained from analog electronic equipment or systems, delays associated with input filtering and signal processing need to be considered. For data obtained from other digital systems by sampling analog or contact outputs from those systems, the inherent sampling delay and any additional processing and communication delays internal to those systems should be considered. (Data communicated over digital communication links to the alarm system are addressed in Section 4.3.1.2.)

Systems connected in series warrant special scrutiny. For example, consider the case in which data values from an analog control system are captured by sampling them in a digital monitoring or data acquisition system and then transmitting them to the alarm system. The cumulative delay associated with the initial analog system's signal processing, the data acquisition system's sampling interval and processing delays, and the sampling and processing of the alarm system all need to be considered to determine the cumulative time delay associated with time tagging the data values or events.

Finally, it is important that training of operators and engineers reflect known limitations regarding the system's capability to show accurate time sequencing of data and events. The plant simulator should simulate these timing characteristics in order to support operator training under realistic conditions, including timing variability.

4.3.1.2 Time Synchronization Across Systems

- 4.3.1.2.1 When multiple systems are detecting and time-tagging alarms, events and data values, all date and time clocks should be synchronized to a common, correct date and time.

The alarm system and other plant control and information systems should have a built-in means to synchronize themselves with a single, highly accurate clock source.

In order to compare data and events across multiple systems, as well as to evaluate plant behavior, the data sets must use consistent time values, with the time stamps from multiple systems synchronized. Offsets across system boundaries make evaluating data extremely difficult. Trend displays use time as the common coordinate, and it should be possible to overlay alarms and other events on the process data trends to support event analysis and diagnosis. Thus, it is important that all data within the system, including alarms, be tied automatically to a common, correct time reference.

The time reference should be stable, accurate, and automatic. The system design should minimize system time drifts, and should correct time errors gradually. The system should update system time periodically, to minimize errors. The Global Positioning Satellite (GPS) array provides a highly accurate, continuously corrected timing source, available throughout the world. The system should have redundant time servers, fed from redundant GPS receivers. This arrangement provides precise timing information throughout the integrated alarm, control, monitoring, and historian system, even in the presence of single failures. Failure of the time server should not result in loss of timing accuracy within the system.

- 4.3.1.2.2 The common date and time should be based on a standard, unchanging time reference such as Greenwich Mean Time (GMT).

- 4.3.1.2.3 The alarm system software should adjust time values automatically to local time prior to using them, based on conversion factors that are easy to maintain as configurable data and not hard coded into the system software.

Because most of the United States uses Daylight Savings Time (DST) during part of the year, there is a possibility of missing an hour of data and having two overlapping hours time stamped as the same if one or more system clocks do not make the correct time conversion. Therefore, the native time format for the system should not be local time, but some unchanging standard time, such as Greenwich Mean Time (GMT). Then, all uses of time stamped data can adjust the time into local time, with or without DST, as appropriate.

Because the start and stop dates for DST are not fixed, but are subject to legislative change, the dates for transitions should not be hard-coded into the software or firmware, but should be entered as configurable data.

➢ 4.3.1.2.4 Synchronization of date and time between safety related and non-safety related systems should be done in a way that meets all applicable regulatory requirements and is licensable. Synchronization should be implemented such that:

- The date and time are used only for time stamping and information display;
- The date and time are not relied upon for performing any safety function;
- The time and date functions can fail and the system will continue to perform the required safety functions; and
- The safety system is protected from any incorrect operation of non-safety systems, including consideration of data communication issues such as buffer overflow.

Because time tagging should be performed at the point at which data values are sampled and all time tags should be synchronized, safety related and non-safety related systems that provide alarm and event data should be provided with the same date and time. The date and time source is likely to be a non-safety related system. System design, failure analysis, and licensing considerations will dictate that non-safety related date and time information be sent from the non-safety related time server into the safety related system. As long as the safety systems adequately protect themselves from the identified failure mechanisms in the non-safety systems, this should be a licensable design.

➢ 4.3.1.2.5 Means should be provided to sort alarms and events into the correct order even when they are received at different times, so that proper chronology is maintained for all displays and processing algorithms.

Even with a common time reference, propagation times for alarm and event data to reach the alarm system from various other systems will be different. Some means must be provided to sort the alarms into chronological order, without unduly delaying presentation of the alarm information. The maximum propagation delay and its effect on event synchronization should be evaluated.

Even if events are sorted before they are saved in the historian and displayed, it is possible that out-of-order alarms will still exist. If communication path failures can result in systems buffering alarms for transmission when communication is restored, then alarms may come in out of order. Thus, the system may still need to have the capability to sort and reorder the historian's contents after the original alarms have occurred.

4.3.1.3 Alarm Processing and Alarm Rates

➢ 4.3.1.3.1 The system should be designed to accommodate a defined maximum rate at which alarms must be generated, processed, displayed, and recorded. This maximum alarm rate condition should include:

- The rate at which process alarms must be generated by the system;
- The rate at which alarms may be received from other systems at the same time;
- The rate at which internal system alarms may be generated simultaneously; and
- A generous, conservative allowance for future growth and modernization

No data should be lost under any alarm processing condition up to and including this defined maximum alarm rate condition. All alarms and events should be processed, displayed as

required, and recorded in the historian without loss of any data and with correct time stamping of the data.

- 4.3.1.3.2 The alarm system should continue to meet all other functional and time response requirements during the maximum alarm rate condition, including display update rates and response to user requests.

  The maximum alarm rate should be determined based on the worst-case conditions expected in terms of alarm generation. Simulation may be used to determine expected alarm rates. A significant margin should be added to the rates estimated from simulation exercises to ensure that the maximum rate used for design is conservative. Loadings on processors and communication links should not result in significant delays in the system's processing and display of alarms or in response to user requests.

4.3.1.4 Display Update Rates

- 4.3.1.4.1 The timeliness of displayed alarm information should be such that users can consider it to represent current conditions in the plant at the time the information is viewed on the display.

  It is important that displayed alarm information be current from the user's standpoint. Related information used together in assimilating and responding to alarms must appear to be consistent in time. In general, these requirements lead to updating displayed information as rapidly as possible.

- 4.3.1.4.2 Alarm displays, including SDCV displays and alarm message lists, should be updated with new alarm status as soon as the data is available.

  SDCV displays of alarm status are similar to conventional annunciators and should be updated as quickly as possible with new alarm information so that they are current. Alarm lists that present the same or related alarm information (e.g., detailed information on individual alarms represented on the SDCV display) should be kept in synchronism with the SDCV display as much as possible to avoid confusion.

- 4.3.1.4.3 Numerical values displayed as part of alarm information displays should not be updated more often than once per second.

  It is important to maintain current alarm data on displays. However, displays of numerical data are not usable if the data values are changing too rapidly, so there must be a maximum rate of change enforced for this data.

- 4.3.1.4.4 The user should be able to freeze an alarm list display temporarily to facilitate reading and understanding displayed information. The display should provide a clear, attention-getting indication that the display is in freeze mode and not updating.

  Alarm lists can be difficult to use if the information is changing rapidly. The "freeze" capability allows the operator to hold the display in its current state while trying to read and digest the information. Any important alarms that occur while the list is in freeze mode should be presented on other displays such as SDCV alarm displays so that the operator is made aware of new alarms that are occurring.

4.3.1.5 System Response to User Actions/Requests

- 4.3.1.5.1 The alarm system should provide visual acknowledgement of any user actions or requests immediately (0.25 second[1] or less).

- 4.3.1.5.2 System response to a user's request to silence, acknowledge, or reset alarms should be completed essentially immediately (0.25 second[1] or less).

- 4.3.1.5.3 Display updates in response to user requests should be completed within one second. This includes display of additional information to support responding to an alarm, including providing ready access to an ARP or a related process or system display.

- 4.3.1.5.4 Display updates should start immediately on the user's request, and not wait for the next one-second update.

- 4.3.1.5.5 For any actions that require more than one second to complete (e.g., alarm analysis functions, display of historical data for review, etc.), the system should provide indication of the status of processing. The preferred method for accomplishing this is to display the time remaining before completion or the fraction of processing that has been completed. At a minimum, there should be a clear indication that processing is still in progress.

4.3.2 Hardwired Input and Output Requirements

- 4.3.2.1 The system should accept inputs from hardwired silence, acknowledge, reset, and test controls.

  The overall system design may include hard pushbuttons mounted at the operators' workstations for silence, acknowledge, reset, and test (SART) controls. The system should be able to accept these hard control inputs as well as soft controls for these functions.

- 4.3.2.2 The system should accept inputs from soft controls, including silence, acknowledge, reset, and test controls.

- 4.3.2.3 The system should have the capability to drive discrete alarm tiles such as conventional light boxes. The system should be able to implement standard annunciation sequences for the alarm tiles, including different flash rates for incoming and clearing alarms.

- 4.3.2.4 The system should synchronize the flashing of all tiles in the system, so that to the user all tiles flashing at a given rate appear to turn on and off at the same time.

- 4.3.2.5 Reflash capability should be provided for alarm tiles that are driven from multiple individual alarms.

- 4.3.2.6 The system should have the capability to drive discrete outputs that can be assigned to respond directly to the status of individual alarm conditions, or multiple conditions

[1] A system response time of 0.25 second or less has generally been accepted as representing "essentially immediate." See, for example, Table 2.4 of NUREG-0700 [10].

combined to drive a single alarm output. These alarm outputs can be sensed by other systems or used to drive indicators. When multiple alarm conditions are combined, reflash capability should be provided.

For some implementations, it may be beneficial to present selected alarms on discrete back-lit tiles, either in arrays similar to conventional annunciator light boxes, or as individual indicators/tiles (e.g., as part of an overview display or mosaic). When these are to have full annunciator type functionality (multiple flash rates, SART control capability), there are several implementation options, including:

- Driving the tiles directly, which requires implementing the annunciation functionality in the alarm system;
- Driving discrete or contact outputs that are then sensed by an external annunciation system, which like the first option requires potentially significant external wiring; or
- Sending the alarm information over a digital communication link to another system or sub-system, or to special-purpose annunciator equipment that implements the required annunciator sequences.

4.3.3 Data Communication Requirements

➢ 4.3.3.1 The alarm system should be able to accept alarm and event data from other systems using standard communication links or gateways. The types of data connections that are supported should be specified, along with any requirements for custom interface development.

➢ 4.3.3.2 The alarm system should be able to accept alarm data with or without time stamps. For alarms provided with time stamps by external systems, the time stamps should be carried through and used in the same way that internally generated time stamps are used. For alarms that are not accompanied by time stamps, the system should time stamp them, recognizing that there will be inherent inaccuracy in the time stamping as a result.

➢ 4.3.3.3 Because alarm data may be received from systems at different times, the alarm system must be able to function properly when receiving out-of-order alarms and events, and be able to sort all the alarm data into proper time sequence.

➢ 4.3.3.4 The alarm system should have the capability to generate alarms based on data synthesized from multiple systems, adding time stamps to these alarms at the point of generation.

Individual input conditions that are combined to form a synthesized alarm or event may occur at different times. Therefore, the time stamp for the synthesized event should be based on the time at which that combined or synthesized event is generated. Users will need to be aware that synthesized alarms and events are time stamped only after all the input conditions have been detected and combined to generate the synthesized event.

➢ 4.3.3.5 The alarm system should be able to provide alarm and event data to other systems using standard communication links or gateways. The types of data connections that are supported should be specified, along with any requirements for custom interface development. These links should provide access to all of the information associated with

each event or alarm, including time stamp, setpoint, alarm message, priority, and data quality information.

4.3.4 System Configuration and Configuration Management

- 4.3.4.1 The alarm system and associated tools should provide change management and configuration control features that allow secure, controlled access to alarm system configuration data.

- 4.3.4.2 The alarm system and associated tools should provide an easy means of archiving and restoring the current configuration of the entire system.

- 4.3.4.3 The alarm system and associated tools should provide automatic version control of all configuration items, to ensure the capability of removing changes and restoring previous versions of all configuration items. The ability to add comments related to each change should be provided.

- 4.3.4.4 Multiple levels of access should be provided, such that selected personnel have full access and privileges to change any data, while other users have ability to change only an authorized subset of the configuration data. Examples of the latter include the ability for an operator to configure, modify, and remove temporary operator-defined alarms, or to "shelve" alarms that could become nuisances (e.g., during maintenance activities). Another example is providing controlled access to procedure writers or other personnel authorized to make changes to the on-line alarm response procedures.

  The plant should provide appropriate administrative procedures and training to ensure proper use of these alarm system features. The plant should ensure that login information and passwords are properly controlled and protected. Login information and passwords should be specific to an individual, and should be removed or modified promptly when the user's status changes.

- 4.3.4.5 The operator should be able to display a list of all shelved or otherwise disabled alarms.

- 4.3.4.6 The system should record all changes to alarm configuration data, including the date and time, details of the change, and login data identifying the person who made the change.

- 4.3.4.7 The system should provide features that help prevent inadvertent, unintentional, or uncontrolled changes to the alarm system configuration.

- 4.3.4.8 The human-system interface (HSI) provided for configuration management should be designed and evaluated using appropriate human factors engineering methods and principles. The HSI should be easy to use and should minimize the potential for human errors while using the interface.

  EPRI 1010042 [3] provides human factors engineering (HFE) guidelines for design of control room HSIs. It is important for configuration management interfaces to be designed with the same attention to HFE methods and principles as are used in designing other control room HSIs.

Appropriate use of HFE guidelines will help ensure simplicity, consistency, ease of use, and error tolerance for the configuration management interfaces.

➢ 4.3.4.9 The system should provide features that ensure synchronization of common data items between the on-line alarm configuration database and the off-line engineering database. These features should include as a minimum:

- Ability for authorized personnel to view and modify the configuration data items through a single interface, with automatic synchronization of the data items
- Automatic comparison and detection of differences between the common data items in the two databases, with alerts provided for investigation and disposition.

The plant will likely maintain an off-line engineering database, separate from the system's on-line configuration database (see Figure 2-2), which may contain much more than the alarm configuration data. For example, it may include references to drawings, setpoint calculations, and other engineering information needed to maintain the design basis for the alarms. It also may be used to develop the initial configuration, which would then be loaded into the on-line system database. It is important that the common data items in these two databases be maintained in synchronism, without requiring plant personnel to perform burdensome consistency checks. In addition, personnel should be able to make changes using a single interface rather than having to change each database separately. An automated comparison utility should be provided to detect and report on differences in the databases. The utility should provide filtering and sorting tools to simplify comparisons.

4.3.5 Alarm Archiving/Recording Requirements

➢ 4.3.5.1 Alarm history data should be integrated with other plant historical data. The data should be in a single database or, if in separate databases, provided with sufficient integration through the system's software such that the databases appear to the user as a single source for all historical data.

➢ 4.3.5.2 The system should provide sufficient storage capacity to allow on-line storage of alarm history data through at least two fuel cycles, including multiple plant transients (e.g., plant trips).

For plants with continuous refueling, this requirement should be modified to specify the minimum storage capacity in terms of years rather than fuel cycles.

➢ 4.3.5.3 The system should provide means for periodic backup, archiving, and long-term storage of the alarm history data. Recording of real-time alarm data should continue without interruption during any backup or data transfer activity.

➢ 4.3.5.4 Archived alarm history data may be stored within the on-line alarm system, or stored and made available on a separate, off-line system. If a separate system is used, the HSI should provide views similar to those used for the on-line alarm system.

Providing consistent views of the data will make it easier for operators, engineers, and other users to make comparisons between archived data and on-line data. Of course, other displays or presentations of data may be needed as well, to support other uses of the off-line database.

- 4.3.5.5 The archived data should have sufficient precision and accuracy to support off-line engineering and operational analyses. The number of significant digits recorded should not be based solely on the limited requirements for operator display.

4.3.6 Availability Under Accident Conditions

- 4.3.6.1 A portion of the alarm system (referred to here as the "qualified portion") should be capable of generating, processing, and displaying alarms using qualified equipment, so that this portion of the system will continue to function under accident conditions, including seismic events.

  Alarm systems in most operating plants do not use qualified equipment, and they are not classified as nuclear safety related systems. However, alarms play a very important role in safe operation of the plant. Providing at least a minimum level of alarm functionality using qualified equipment can help ensure availability of important alarms to support the operators during emergency operations, including after seismic events, loss of offsite power, and other accidents in which alarms can play a beneficial role and the non-safety portion of the system may not be available. Availability of alarms in these situations may allow improvements in emergency operations and in the corresponding emergency operating procedures.

  In addition, proper separation of the qualified and non-qualified portions of the alarm system can provide some protection against common cause failures of either part. This may help address both licensing and operational concerns regarding potential for large-scale failures of the alarm system.

  Finally, some information must be displayed in the control room on qualified displays (e.g., variables important for post-accident monitoring per Regulatory Guide 1.97). Incorporating alarm functionality, along with comparisons of data across divisions, as part of those displays can provide a better overall solution than separating qualified plant variable displays from the alarms associated with those variables, as well as requiring the operator to cross check variables across divisions.

  Each plant owner/designer will need to decide what capabilities will be provided using qualified equipment, and whether to credit any of these capabilities in licensing. The guidance provided in Sections 6.4 and 6.5 of EPRI 1010042 [3] can be used to help determine what alarm capabilities should be provided on qualified versus non-qualified HSIs. Several "pre-qualified" platforms are available that can be used to implement the qualified portion of the system. If commercial grade equipment is used, EPRI TR-106439 [11] can be used to evaluate the equipment. EPRI 1002835 [12] contains guidance on evaluation of defensive measures taken in the design of qualified or non-qualified equipment that can help protect against common cause failures. EPRI 1011710 [13] provides guidance on performing critical reviews of digital systems to ensure adequate system integrity and reliability.

- 4.3.6.2 The qualified and non-qualified portions of the alarm system should be capable of being powered separately with suitable redundancy of power feeds.

  It will be important for the qualified portion to be fed from qualified power sources to ensure it will continue to operate under accident conditions. Plants will likely also want to ensure that power is maintained to at least this portion of the system during a loss of offsite power.

- 4.3.6.3 The qualified portion of the alarm system should provide capability to generate alarms derived or received from plant safety systems and qualified sensors.

- 4.3.6.4 The qualified portion of the alarm system should have the capability to receive alarms through a qualified, isolated interface from the non-qualified portion of the alarm system.

- 4.3.6.5 These interfaces must be shown to provide adequate protection against hardware or software failures on the non-qualified side of the alarm system, so that no such failures would degrade any functionality of the qualified portion of the alarm system, and so that no failures would degrade any functionality in the safety systems.

- 4.3.6.6 The qualified and non-qualified equipment should be capable of using the same controls (e.g., silence, acknowledge, reset, and test).

  The qualified and non-qualified equipment should be capable of using the same alarm controls, including silence, acknowledge, reset, and test. Appropriate isolation between the qualified and non-qualified equipment should be provided.

- 4.3.6.7 The overall functionality provided by the qualified and non-qualified portions of the system should be well integrated, and there should be similarity in the HSIs provided, so that for the division between the two parts of the system is as transparent to the users as possible.

- 4.3.6.8 The alarm functionality provided using qualified equipment should include the ability to:

  - Generate alarms from discrete inputs, analog variable inputs, and signals provided over digital communication links from other safety and non-safety related systems;
  - Accept alarms from the non-qualified portion of the alarm system and combine these with those generated in the qualified portion;
  - Apply conditioning logic when generating alarms, to help avoid nuisances and prevent alarm overload during transients;
  - Transmit alarms to the non-qualified portion of the system through qualified interfaces;
  - Present alarms on spatially dedicated, continuously visible displays as well as a chronological list of alarm messages; and
  - Record the history of alarms and events covering a period of at least 72 hours.

  It is important that alarms generated by the qualified portion of the system do not create nuisances and do not create or contribute to floods of alarms during transients and accidents. Therefore, the alarm functionality should include ability to apply conditioning logic to minimize unnecessary alarm occurrences during normal or emergency operations. At the same time, in order to ensure that the equipment including hardware and software can be qualified, it is important that the alarm functionality not require complex alarm processing or analysis algorithms, assortments of alarm message lists including different views and sorts of alarms, and other functionality that increases the software complexity. Relatively simple processing and display capabilities are recommended.

4.3.7 System Integrity

- 4.3.7.1 Failure analyses should be performed for all portions of the alarm system, addressing both hardware and software, to identify plausible failure modes, their estimated frequencies, and effects of the failures on functionality of the system. These analyses should demonstrate that no single failure will cause large-scale loss of functionality or availability of alarm information. They also should demonstrate that the likelihood of common cause failures (including failures caused by errors in software or digital system design) resulting in large-scale loss of alarm functionality is very low, and that such failures should not be expected to occur during the plant lifetime.

- 4.3.7.2 Appropriate design and quality assurance practices should be followed during development of the platform and application software for both the qualified and non-qualified portions of the alarm system. Potential failure modes and their effects should be continuously identified and addressed during the design and implementation process, to help ensure that the delivered alarm system has adequate integrity.

EPRI 1002835 [12] contains guidance on evaluation of defensive measures taken in the design of qualified or non-qualified equipment that can help protect against common cause failures. EPRI 1011710 [13] provides guidance on performing critical reviews of digital systems to ensure adequate system integrity and reliability. These techniques can be applied throughout the design and development process to ensure adequate system integrity is designed in and validated.

4.3.8 Reliability and Diagnostics

4.3.8.1 Overall Reliability and Self-Diagnostics

- 4.3.8.1.1 The alarm system should be designed with appropriate redundancy, fault tolerance, and protection against single and common cause failures such that every individual alarm exhibits very high reliability, and the availability of alarm information overall is extremely high.

- 4.3.8.1.2 The system should provide internal self-diagnostics that detect hardware or software failures that occur within the system. The system should take appropriate automatic action to minimize the functional effects of detected failures. In addition, the detected failures should generate a *system alarm* routed for maintenance or engineering attention, and provided to the operators with an appropriate alarm message indicating the operational impact.

- 4.3.8.1.3 Failure analyses should demonstrate that postulated faults and failures within the alarm system will be detected and reported by the self-diagnostics.

- 4.3.8.1.4 The system should provide the capability to place a “heartbeat” indicator on each alarm display. The heartbeat should provide a positive indication that the system is continuing to detect, process, and display updated alarm information.

The self-diagnostics discussed above should detect and alert operators and maintenance personnel to faults or failures occurring within the alarm system. In addition to those features, a heartbeat

indicator can provide additional coverage of potential failure modes and help users remain confident that the alarm system is functioning. The heartbeat shows that the system continues to process and display updated alarm information. At a glance, an operator can verify that the alarm display is operating properly.

- 4.3.8.1.5 Analysis of system failure modes and their effects on alarm functionality should demonstrate that any postulated loss of functionality affecting the system's ability to continue processing and displaying updated information would stop the heartbeat, allowing users to determine that they are not receiving updated alarm information.

4.3.8.2 Data Communication Link Reliability and Diagnostics

- 4.3.8.2.1 In general, communication links associated with the alarm system should be redundant to provide protection against single failures and maximize reliability. However, if a failure of a non-redundant communication link, or a total failure of a redundant communication link occurs and the link is then restored, previously unavailable data stored in the sending system could become available to the system. The system should not automatically present this information to the operators as if these were new alarms. Instead, the system should record the data with corresponding time tags in the alarm history database. In addition, it should prompt the user and then update the alarm displays only when the user gives permission to do the update.

  Alarm information that becomes available after a failed communication link has been restored may be quite old. Presenting the information to the operators immediately upon link restoration, as if they were new alarms, could be confusing to the operators (e.g., it could appear that a new transient is occurring). Diagnostics provided within the alarm system to monitor the communication link should already have notified the operators of the failure to receive updated alarm information through the affected link. Once the link is restored, the operators can be notified of the availability of the data. They can then take deliberate action to update the alarm displays.

- 4.3.8.2.2 If a communication link reports data and status information continuously, and the information may not be changing very rapidly, then the system should provide a means for detecting a failure that causes the data not to be updated (typically called stale data detection).

  There are many methods that can be used for stale data detection, including incorporating message counters in the transmissions and requiring the receiver to detect that the counter is increasing as expected. This allows the system to determine whether conditions are indeed stable, i.e., the data are simply not changing appreciably or at all, or that a failure has occurred and the same stale data values or messages are being transmitted repeatedly.

- 4.3.8.2.3 If data values, alarms and other events are reported over a communication link only when a significant change has occurred (typically called reporting by exception), then the system should provide means to detect when the communication link has failed, causing no data to be reported even when changes are occurring in the plant.

- 4.3.8.2.4 The system should be capable of meeting current nuclear industry standards and practices regarding cyber security.

Cyber security is an issue that is much broader than just the alarm system. However, it is important that the alarm system and its data communication links are capable of meeting the pertinent requirements and fit into the overall approach taken for cyber security for all the digital instrumentation and control and information systems.

4.3.9 Maintainability

- 4.3.9.1 The system design and the documentation and training provided with the system should ensure ease of maintenance of the system over its lifetime.

  It is very important that the system be easy to maintain. EPRI 1008124 [14] and Section 6.1 of EPRI 1010042 [3] provide guidance on maintainability of digital systems. For the alarm system, modifying and loading alarm configuration data must not be difficult or likely to result in errors. The hardware, platform software, application software, and configuration databases must be easy to upgrade. Documentation of the hardware, software, and overall system architecture needs to be accurate, complete, and easy to use to support ease of maintenance and upgrade.

- 4.3.9.2 Specific tasks required to test, maintain, and troubleshoot the alarm system should be defined. The maintenance and configuration interface should include features designed specifically to support these maintenance tasks (e.g., task oriented displays designed to support specific maintenance activities). Human factors engineering (HFE) should be employed in the design and evaluation of these interfaces.

  See EPRI 1008124 [14] and Section 6.1 of EPRI 1010042 [3] for additional guidance on human factors in maintenance of digital systems.

- 4.3.9.3 Failure analyses performed to identify system failure modes and their effects should include consideration of errors that could occur in configuring or maintaining the system, either off-line or on-line.

4.3.10 Testability

- 4.3.10.1 The alarm system should provide a manual test capability that exercises a complete path through the system, starting at the inputs and ending at the various visual and auditory display devices in the control room. One or more “Test” controls should be provided to initiate this test. The test should exercise each of the auditory output devices, visual indicators (e.g., discrete alarm “lights” or indicators driven by the system), and computer-based alarm displays (e.g., flat panel displays or CRTs). The operator should be able to determine that each of these devices is operating correctly. For computer-based displays, this should be accomplished without the system having to alter any valid alarm information currently displayed (e.g., the test function can drive a separate “test icon” or change the appearance of the “heartbeat” indicator to demonstrate to the operator that the system is operating correctly in response to the test). The manual test capability should exercise all critical alarm processing functions and, to the greatest extent possible, exercise the system software in its normal operating mode. It also should test the silence, acknowledge and reset functions of the system.

  Internal system diagnostics, coupled with a “heartbeat” indicator, go a long way toward demonstrating that the alarm system is operating correctly. However, such tests and indicators do

not necessarily test the functionality of system elements such as input circuits, audible output devices, and discrete indicators driven by the system. In addition, operators need to be able to determine for themselves that the system is fully operational, using a positive means to exercise the system from end-to-end. An important aspect of this test is its ability to verify communications between different portions of the system, to verify continued processing of information by the system software, and to ensure that output devices including audible and visual displays are receiving updated alarm information. For computer-based displays, exercising each individual alarm indication is not necessary. Instead, a "test icon" or the "heartbeat" indicator can be used to verify that the display device has responded to the test function and is operating correctly.

It is important that this test function exercise the system software and hardware in their normal operating modes, as opposed to having test software that tests its own functionality. As much as possible, the test inputs should be processed as if they were valid alarms until the point of presentation, when it must be made clear that these are test inputs only. For message lists, this may be accomplished by having a message appear indicating that a test signal has been properly received.

- 4.3.10.2 The alarm system should support surveillance testing of plant equipment including interfaces with the alarm system. In addition to providing the capability to "shelve" alarms whose inputs are under test or maintenance, the alarm system should provide the capability for users to verify that alarm inputs have been received in response to equipment testing while the associated alarms are shelved. This ensures that surveillance tests of plant equipment have adequate overlap with testing of the alarm system.

  Providing testability of the inputs to the alarm system supports maintenance and surveillance testing of plant equipment, and ensures that there is adequate overlap of these surveillance tests with the alarm system tests. Providing the ability to "shelve" the associated alarms yet still provide indication of alarm input activation will allow running surveillance tests without distracting the operators with alarms that are a result of testing and are not valid alarm conditions.

5
PLANT ALARM MANAGEMENT REQUIREMENTS

This section provides high-level requirements for the plant's alarm management activities. As discussed in Section 2, even the best alarm system will not perform well or meet expectations if it is not designed, configured, and maintained within an overall alarm management program. Refer to Figure 2-1, which gives an overview of alarm management.

➢ 5.1 The plant should establish alarm management policies that are consistent with the overall control room design, and with the plant's concept of operations and concept of maintenance. These policies should address:

- Roles, responsibilities, and overall processes that will be used for each element of alarm management, including alarm selection, definition of alarm logic and processing, configuration of alarms and the alarm system, configuration management, performance monitoring, and continued support for the alarm logic
- Roles and responsibilities regarding development and management of alarm response procedures
- Roles and responsibilities for responding to alarms, including division of responsibilities among operating crewmembers and between operations, maintenance, and engineering personnel
- Role of alarms in supporting maintenance and engineering activities, and how operations, maintenance, and engineering personnel will interact with regard to definition, configuration, and administration of alarms
- Other alarm administration policies addressing items such as inhibiting or disabling alarms, alarm shelving, and management and tracking of user-defined alarms
- Alarm system performance goals
- Plans for periodic assessment to monitor and refine the alarm management policies, procedures, and goals as necessary

These alarm management policies set the stage for the remainder of the alarm management program. They should be established early, prior to design and procurement of the alarm system, to ensure that the system is designed and configured using a consistent approach in keeping with the station's alarm management goals.

➢ 5.2 An alarm engineering style guide should be developed and used to control design and implementation of alarms and the alarm system. The style guide should incorporate accepted human factors engineering principles and guidelines, and it should reflect plant-specific conventions and standards regarding items such as use of symbols, abbreviations, system and component names, and color codes. It should include criteria for maintaining consistency between the alarm system and other information systems provided in the control

room. The style guide should include criteria and guidelines for the following aspects of alarm management:

- Alarm definition, including selection of alarm conditions to support an alarm hierarchy, selection of setpoints, and design of alarm conditioning logic to produce alarms that are context-aware
- Identification of cause-consequence relationships among alarms and how these are to be used in alarm processing and presentation
- Alarm prioritization including assigning priorities, and use of the plant's probabilistic risk assessment (PRA) to support prioritization
- Alarm processing, including techniques such as mode-based and event-based alarm suppression
- Alarm routing to users and other destinations
- Recording and archiving of alarm and event history data
- Alarm information display and integration with display of other plant information
- Definition, configuration, and display of events important to situation awareness
- Alarm response procedures
- Other aids to be provided for response to alarms and for diagnosing transients and events

See EPRI 1010042 [3] for guidance on development and use of style guides and for human factors engineering (HFE) guidelines that can be used as a source of HFE criteria and guidelines for the style guide.

➢ 5.3 Alarm system performance measures and performance monitoring procedures should be defined.

It is important that the performance of the alarm system be validated initially, and then monitored regularly. The system should have built-in capabilities for automatic monitoring to generate overall statistics such as average number of alarms occurring per hour, shift, and day, and individual alarm statistics such as how often an alarm occurs and the average amount of time it remains in the alarm state. Performance monitoring also can help identify additional alarm relationships, such as possible cause-consequence relationships identified based on the patterns of alarm occurrences monitored over time.

Alarm management policies should establish goals for alarm system performance. Performance monitoring procedures should identify the specific measures to be used in assessing performance against the goals, who is responsible for making these assessments, and when and how the assessments will be made.

➢ 5.4 Appropriate engineering procedures should be developed (or modified, if existing) to enforce use of the style guide, and to control the initial design and design changes that will be made over time to the alarm configurations and the alarm system. The engineering procedures should address development, design verification, and validation of alarm conditioning logic, cause-consequence relationships, and any models used by the alarm

system in generating or processing alarms. The procedures also should address human factors engineering (HFE) evaluations and HFE verification and validation (V&V) activities that should be performed for the initial design and subsequent modifications. Use of the plant simulator to support design development and HFE evaluations and V&V should be addressed.

> See EPRI 1010042 [3] for guidance on developing and implementing a human factors engineering program, and use of HFE analyses and V&V activities as part of human-system interface (HSI) design and evaluation. That document also provides guidance on use of simulation to support design and evaluation of HSIs.

- 5.5 Appropriate administrative procedures should be developed to support alarm administration. These should address temporary inhibiting or disabling of alarms, alarm shelving, control of user-defined alarms, and configuration management procedures.

6
IMPLEMENTATION GUIDANCE

This section discusses how designers, system integrators, and plant personnel may apply the requirements in this report for different purposes. Guidance is provided for using the requirements to support design, procurement, and implementation of an advanced alarm system.

6.1 Applying the Requirements

The advanced alarm system requirements provided in this document can be used for a number of different purposes. Several potential applications are discussed below.

6.1.1 Designing a New Alarm System

The requirements may be used when designing an advanced alarm system for a new plant, a new control room for an existing plant, or modernization of an existing control room. A vendor or integrator may use the requirements to develop and implement an advanced alarm system design to be offered to plants. Alternatively, plant personnel can use the requirements to develop an initial design concept for a new alarm system, and then provide a conceptual design description and selected requirements from this report to a vendor or integrator for implementation.

6.1.2 Defining an Endpoint Concept for Modernization

When modernizing a control room for an existing plant, it is important to develop a concept for what the control room will be like at the end of the modernization program. This "endpoint" design concept should include a conceptual design for the alarm system. Section 2 of EPRI 1010042 [3] provides guidance on developing a control room endpoint to support modernization.

In this report, Section 2, *Alarm System in the Overall Context of Alarm Management,* and Section 3, *Background and Basis for the Requirements,* should prove useful in developing the endpoint as they describe basic features and capabilities of the advanced alarm system. Section 4.1, *Objectives of the Alarm System,* can be used to define high-level objectives and functional requirements for the alarm system. The more detailed requirements given in the remainder of Section 4 may provide ideas for specific features to be incorporated in the endpoint design.

Section 5, *Plant Alarm Management Requirements,* also should be used when developing the endpoint design concept. It will be important for the design to reflect how the plant expects alarms to be used within the overall concept of operations and maintenance for the modernized control room, and how alarms will be managed once the endpoint is reached.

6.1.3 Alarm System Procurement

The requirements can be used to support procurement of an alarm system or other information system that includes alarm functionality. Use Sections 2 and 3 to help determine what overall capabilities are desired. The high-level requirements in Section 4.1, modified as necessary, can be used in bid or purchase specifications. Detailed requirements can be chosen from the remainder of Section 4 to develop the functional, design, and performance requirements to be included in the specification. It is important to note that this document does not include all requirements needed to specify an alarm system completely. The requirements in this report focus on specific advanced features and capabilities that should be considered. These should be augmented with additional requirements (e.g., detailed input/output requirements, power requirements, cabinet ventilation, etc.) as needed to produce a complete system specification.

6.1.4 Defining a Plant Alarm Management Strategy

Section 5 provides high-level requirements for developing the alarm management strategy, policies, and procedures. In addition, use Sections 2 and 3 to evaluate potential capabilities of the advanced alarm system and see how they fit into alarm management. Use Section 4.1 to help develop overall goals for the alarm system consistent with the alarm management strategy.

6.2 Defining the System Architecture

Many different architectures can be used for the instrumentation and control systems, information systems, and the alarm system. Detailed discussion of the possible architectures is beyond the scope of this report. However, several important points should be made regarding use of the requirements given in this document to support design and implementation of an advanced alarm system within a range of potential architectures.

First, the alarm system need not be a separate, physical system. In fact, the most effective design is likely one that integrates alarm functionality with other control and information system functions. From the standpoint of the users, it does not matter what physical system generates, processes, or displays the alarms. However, the alarm system should not be so integrated with the other systems that alarm-related modules, tasks, and functions cannot be identified.

Important plant-level alarms may be presented on a large display panel for the entire crew. System-level alarms may appear on separate dedicated displays arranged around the control room. Dedicated displays may provide detailed alarm message lists.

In addition, system graphics or mimic diagrams may present alarms indicating problems with specific components or system parameters. An alarm may appear on a soft control display to indicate a problem with actuation of a control function. A computer-based procedure may display an alarm associated with a particular step in the procedure. Alarms may be presented on a safety-related display of post-accident monitoring information, alerting operators to problems with critical safety functions, while others appear on non-safety workstation displays. All of these should be compatible with each other in terms of how the alarms are generated and how the users perceive and interact with the alarms.

Multiple systems from more than one vendor likely will need to be integrated to provide the required advanced alarm system functionality. A single vendor's system (e.g., a distributed control and information system) may provide much of the alarm functionality that resides in the control room, but it will be supplemented by additional alarm functions hosted by other systems from the same or different vendors. Some alarm processing or monitoring functions may be provided by separate software applications from third party vendors. Alarms may be generated and displayed by both safety-related and non-safety related systems from the same or different vendors (see Section 4.3 for related requirements). However, divisions between the physical systems that host the alarm functionality should be transparent to the users.

Finally, the system architecture should be chosen with reliability and availability of alarms in mind. Alarms play an important role in maintaining safe and economical plant operation, and in maintaining the plant in a safe state after an accident, trip, or transient. Section 4.3 provides requirements related to reliability and availability of alarms. The guidance given in Section 6.5 of EPRI 1010042 [3] can be used to assist in defining the overall architecture of the control room human-system interfaces, including alarms. It addresses making decisions on what parts of the HSI should be qualified, what should be spatially dedicated, and other HSI design requirements important in determining the architecture.

6.3 Keeping it Simple

Simplicity is very important to users of the alarm system. If advanced features are incorporated that are difficult for users to understand, or the behavior of the system is not perceived as predictable and understandable, then performance and acceptance by users likely will suffer.

Alarm conditioning logic should be easy for users to understand. This does not mean that the logic cannot incorporate multiple inputs or provide significant functionality. If the logic is based on fundamental relationships among process variables and equipment operating states, this should be understandable to the users as it is consistent with their understanding of how the system works. However, if the logic is based on obscure relationships that are not well understood, then users may not understand the basis for the logic and thus may not trust it.

Cause-consequence relationships also should be simple and understandable. Again, when based on well-understood relationships, this should be acceptable and meaningful to users. If there is uncertainty about the accuracy or reliability of the relationship, or if it is considered tenuous, then it may be best to leave it out of the system. Experience has shown that it only takes a few instances of inaccuracies or improper definitions of alarms to cause users to lose confidence in an alarm system. If in doubt, leave it out.

The same principle applies to models used in processing or displaying alarm information. Models that are based on well-known relationships are most likely to be accepted and trusted by the users. Models should be simple, transparent to users, and fully validated. Many different alarm analysis algorithms and techniques have been proposed or tested, but few have been fielded successfully. The objective of the requirements in this document is to encourage use of simple, well-understood models using known relationships. In addition, the requirements are intended to provide a system that is sufficiently flexible that it can accommodate additional modeling techniques in the future, as modeling capabilities mature over time.

The need for simplicity also applies to the structure provided for navigating the alarm hierarchy and accessing information needed to respond to alarms. Speed of access and consistency in the approach are also important. Methods used to access more detailed information should be consistent among overview displays, system graphic displays, SDCV or tile replica type displays, alarm lists, soft control screens, computer-based procedures and other displays that present alarms. Use of appropriate human factors engineering methods and guidelines can help ensure this.

6.4 Applying Human Factors Engineering (HFE)

This document does not include detailed HFE design criteria. EPRI 1010042 [3] should be used when designing and configuring the alarm system to ensure that appropriate HFE principles, methods, and design guidelines are followed. This should include the alarm system guidelines in EPRI 1010042 (Section 4.4 of that document). This should also include the guidelines provided on the human-system interface (HSI) design process, use of HFE methods and tools (Section 3), and other detailed design guidelines such as those for information display, user interface management, soft controls, computer-based procedures, and computerized operator support systems (Sections 4.1-4.7 of EPRI 1010042). All of these HSI elements may include or interact with alarm functions described in this report.

6.5 User Participation in System Design and Evaluation

User participation in the design, development, implementation, and testing of the alarm system is critical. All potential users of the alarms should be involved, including operations, maintenance, and engineering personnel, and any others who will use alarm information or interact with the alarm system. Simulation to verify and validate the design is very important, particularly when implementing advanced alarm system functions that are new to the plant and may not be fully proven in service.

Alarm system performance goals should be established at the beginning along with suitable performance measures that can be used to assess whether the goals are being met. Users should be involved in setting performance goals and evaluating system performance. HFE verification and validation activities should be planned and carried out at appropriate points in the design and implementation process. See EPRI 1010042 [3] for guidance.

7
DEFINITIONS

This section provides definitions of terms used in this document. When a definition uses or references other terms that are also defined here, those terms are shown in *italics*.

Abnormal condition. See *off-normal condition*.

Acknowledged alarm. An alarm is considered to be acknowledged when the user has made some type of input to the alarm system (such as pressing a button – see *alarm controls*) to indicate receipt of the *alarm message*. The act of acknowledging an alarm typically causes the attention-getting characteristics of its display to cease or decrease (e.g., the sound stops and the flashing display changes to a steady illumination). Alarms may be of an auto-acknowledge type, which are self-acknowledging when the off-normal condition returns to normal or when an event (e.g., a time-out) causes an acknowledgement to occur.

Alarm. Information generated for the purpose of alerting an operator or other user to an off-normal condition that requires action. This includes *process alarms*, which are generated due to off-normal conditions of the plant process, and *system alarms*, which are generated due to off-normal conditions in the systems used to monitor and control the process (e.g., in a digital control or information system, or in the alarm system itself). Note that there can be a hierarchy of alarm information, from low-level conditions such as low oil pressure in a pump bearing, to low flow in a system, to even higher-level alerts such as an alarm indicating that an entire system has become unavailable or a major plant function or process has been lost. *Alarm conditioning logic* and *alarm processing* techniques can be used to create higher-level alarm information.

Alarm administration. Administrative activities associated with maintaining control over the configuration of alarms and the alarm system. For example, alarm administration includes policies regarding the process for identifying and defining new alarms, and procedures for tracking and controlling temporary changes made to alarm configurations (e.g., alarms taken out of service for maintenance reasons, temporary operator-defined alarms or alarm setpoints, etc.). Monitoring of alarm system performance metrics is also an administrative function.

Alarm conditioning logic. Logic, interlocks, or algorithms applied at the point of alarm generation to make the alarm more intelligent and meaningful and to prevent unnecessary occurrences of the alarm in prescribed situations (e.g., logic that prevents a low discharge pressure alarm from occurring unless the pump is turned on). Sometimes referred to as *alarm cutouts*.

Alarm configuration. Determining and installing the specific configuration settings in the alarm system that are required to properly implement an alarm, including settings such as the *alarm setpoint*, the priority of the alarm, and the *alarm message*.

Alarm controls. Controls provided for the user to interact with the alarm presentation or displays provided by the *alarm system*. Typically these include controls for silence, acknowledge, reset and test (SART); that is, controls for silencing audible signals or tones used to alert the user to alarm conditions (see *silenced alarm*), acknowledging alarms (see *acknowledged alarm*), resetting alarms (see *cleared alarm*), and testing alarms or the alarm system. Note that as used here, *alarm controls* is not meant to include control features provided for the user to interact with the alarm displays in a computer-based system, such as selecting different types of displays or sorts of alarm information, or selecting and displaying *alarm response procedures*.

Alarm cutouts. See *alarm conditioning logic.*

Alarm definition. Identification of off-normal conditions that warrant an alarm (see *alarm selection*), the operational context(s) in which an alarm is warranted, the setpoint that should be used in generating the alarm, the actions that should be taken in responding to the alarm, potential consequences resulting from the alarm (e.g., automatic actions that should occur), and definition of *alarm conditioning logic* or algorithms that should be applied in generating the alarm so as to ensure it is meaningful and does not produce a *nuisance alarm*. Alarm definition is part of *alarm engineering*.

Alarm design criteria. Criteria for the definition and configuration of alarms to ensure that a consistent design approach is applied across the entire alarm system, appropriate human factors engineering principles and guidelines are applied in engineering the alarms and alarm response procedures, and plant conventions and standards are adhered to in the design. Use of alarm design criteria is critical to ensuring that performance goals are met for the alarm system, both initially when it is first designed and configured, and over time as alarms are added, deleted or modified during plant operation. Alarm design criteria may be contained in an *alarm style guide*.

Alarm engineering. An engineering design activity that applies a consistent design approach and builds intelligence into the definition and configuration of individual alarms or groups of alarms. It applies standard design criteria, tools, and techniques to define and configure the alarms and associated *alarm response procedures* to minimize *nuisance alarms*, and to ensure that each alarm is meaningful and useful in all operating situations. Thus, alarm engineering includes *alarm definition, alarm configuration,* and development and configuration of alarm displays and *alarm response procedures*.

Alarm flood. See *alarm overload.*

Alarm generation. The activity or function within an *alarm system* that monitors plant conditions and, based on pre-defined *alarm configuration* settings and *alarm conditioning logic*, generates *alarms*. Alarms may be generated by different control and monitoring systems, or at distributed locations within a single system. Alarms may then be combined for more global or higher-level *alarm processing* and routed to displays or workstations for presentation to the intended user(s).

Alarm group. A set of alarms that are tagged as being related to each other. For example, alarm groups might be used to identify alarms associated with different areas of the plant (e.g., primary, secondary, electrical distribution, etc.). This is different from a grouped or shared alarm, which combines multiple sub-alarms together to present a higher-level alarm. See *shared alarm.*

Alarm limit. A configurable setting for an alarm on the value of an analog variable, beyond which an alarm is generated. Multiple alarm limits may be set for a single variable, such as a high limit, high-high limit, low limit, and low-low limit. See also *alarm setpoint*.

Alarm logic. See *alarm conditioning logic*.

Alarm management. The overall set of design, operational and administrative activities associated with managing alarms, the alarm system, and its configuration settings.

Alarm message. The description or text message that is presented to the operator on the occurrence of an alarm. Note that multiple users may need to be alerted to the occurrence of a given alarm condition. In addition, each user may need a different message in order to understand the nature of the alarm and the action the user should take in response. For example, a digital system fault alarm may generate one message for the control room operator, indicating the operational meaning of the alarm, and provide a different message to a maintenance technician or other user who will be responsible for troubleshooting and repairing the condition that led to the alarm.

Alarm overload. A situation in which too many alarms are occurring in too short a period of time for the intended user to be able to assimilate and respond to the alarms. Alarm overload significantly decreases the effectiveness of the alarm system in conveying information, and it can distract operators from performing necessary control and monitoring activities.

Alarm prioritization. The ranking of alarms based on pre-defined criteria such that alarms can be presented in a way that conveys their relative importance in terms of urgency of response. Prioritization can be static or dynamic. Static priorities are pre-assigned and fixed, i.e., they do not change in real time or in response to changing plant conditions. Dynamic priorities, on the other hand, do change in response to changing plant conditions, e.g., the priority of an alarm may be changed when the plant moves from one operating mode to another (i.e., mode-based dynamic priority) or the priority may be escalated if the off-normal condition persists and response becomes more urgent.

Alarm processing. Real-time processing of alarm signals to provide more meaningful and useful information to users, apply global (e.g., system-wide or plant-wide) logic or algorithms to create smarter or higher-level alarms, or adjust alarm configuration settings or the alarm presentation based on changing plant conditions or occurrence of specific events. Examples of advanced alarm processing techniques include dynamic *alarm prioritization* (e.g., changing priorities based on plant mode), identification of “unexpected” alarms for specific operating conditions or events, and notification to the operator of alarms that were “expected” but did not occur.

Alarm response procedure (ARP). A procedure that gives instructions for how the user should respond to an alarm. Typically, an ARP should include more detailed information on the nature and source of the alarm than is provided in the *alarm message* (e.g., the plant conditions and *alarm conditioning logic* used to generate the alarm). It also provides instructions for confirming the alarm, taking necessary actions in response to the alarm condition, and confirming that the actions have been successful. ARPs may be presented by the *alarm system* in a computer-based display format, or in paper form, or both. Computer-based ARPs can include live process data and other aids needed as part of confirming and responding to the alarm.

Alarm selection. Selecting those off-normal conditions that warrant an alarm. See *alarm*.

Alarm setpoint. The value of an *alarm limit* for an analog variable. An alarm is generated when the variable exceeds the *alarm limit* setpoint. In addition, the state defined as the alarm state for a discrete (digital or binary) parameter is referred to here as the setpoint for that alarm. An alarm is generated when the parameter enters the alarm state for that parameter. Alarm setpoints may be changed dynamically based on plant or system operating mode or other event.

Alarm shelving. An alarm that is currently active (in the alarm state) can be shelved if it is concluded that the alarm will remain active for a long time (e.g., due to the need for repairs that will take some time to complete). A shelved alarm is processed such that it does not display as an active alarm until it is restored (taken off the "shelf"). Alarm shelving should be accomplished without requiring any change to the configuration of the alarm.

Alarm style guide. A document that contains *alarm design criteria* and guidelines that have been tailored so they describe the implementation of generic human factors engineering guidance for a specific design, such as for a specific plant's control room.

Alarm suppression. An alarm processing method that does not present alarms determined to be less important, irrelevant, or otherwise unnecessary; however, the suppressed alarms can be accessed by the operator on request, or by the alarm system under certain conditions, such as when plant conditions change the relative priority of the alarms.

Alarm system. The complete set of functionality related to generating, processing, analyzing, and presenting alarms and *alarm response procedures* to the intended users (see Figure 2-2). This functionality may be implemented by more than one physical system. The alarm "system" includes hardware, software, and supporting information (e.g., the alarm response procedures and any procedures for interacting with the alarm system). It includes the controls needed for users to interact with the system (e.g., for acknowledging alarms) and other features for interacting with the alarm displays (e.g., for selecting different types of displays, requesting sorts or analyses of alarm information, or selecting an alarm response procedure).

Alarm tile. A type of spatially dedicated, continuously visible alarm display that changes state (i.e., brightness, color, and/or flash rate) to indicate the presence or absence of an alarm condition, and includes text to identify the nature of the alarm. Tiles are typically illuminated in some way when the alarm is active and dark when the condition is normal.

ARP. See *alarm response procedure*.

Candidate alarm conditions. Off-normal conditions identified based on review of plant processes, systems, and components to identify situations that may require action by operators or maintenance personnel, or which represent significant events to which the operators should be alerted.

Chattering alarm. An alarm that occurs repeatedly within a short period of time, cluttering alarm lists and other alarm information displays and potentially distracting or annoying the operator. A chattering alarm may occur due to contact chatter on a discrete input if appropriate *contact debounce* filtering is not applied. A chattering alarm may also occur when a plant variable hovers near the alarm setpoint, causing repeated activations of the alarm, if time filtering and/or appropriate deadband/hysteresis settings are not applied in generating the alarm.

Cleared alarm. An alarm for which the condition that originally activated the alarm is no longer true (e.g., an analog variable goes back within normal bounds, no longer exceeding the alarm setpoint, or a discrete input goes back to the non-alarmed state). Some alarm systems alert the user by visual and/or auditory means when an alarm clears. The operator may be required to "reset" the alarm to acknowledge receipt of the message that it has cleared. See *alarm controls*.

Common cause failures. Failures of equipment or systems that occur as a consequence of the same cause. The term is usually used with reference to redundant equipment or systems or to uses of identical equipment in multiple systems. Common cause failures can occur due to design, operational, environmental, or human factor initiators. Common cause failures in redundant systems compromise safety if the failures are concurrent failures, that is, failures that occur over a time interval during which it is not plausible that the failures would be corrected.

Concept of maintenance. This refers to how maintenance activities are performed, including how maintenance work is initiated and by whom, relative roles of the operating crew and the maintenance staff in maintenance and testing activities, how the two will work together to support maintenance and testing, and how maintenance activities and information will be managed.

Concept of operations. This refers to how the plant is operated and how the operating crew is organized, including what functional responsibilities reside in the control room, operating crew size and makeup, roles and responsibilities of the crewmembers, and how normal and emergency operations are conducted.

Contact debounce. A means (typically time filtering) for preventing a *chattering alarm* from being caused by bouncing or dirty contacts that drive a discrete input to the system.

Control room alarm system. See *alarm system*.

Darkboard. A criterion or philosophy that no alarms should be active when all systems are in their normal status and lineup for the current operating condition. Thus for a conventional alarm panel, where an individual *alarm tile* is illuminated if the corresponding condition is in the alarm state (alarm activated), and dark (not illuminated) if the condition is in the normal range, this requires that the alarm panel be "dark" when the plant is at power (hence "darkboard"). For an

alarm message list type display, the equivalent criterion would be a requirement that there be no active alarm messages when all equipment is in its expected condition.

Diversity. The use of at least two different means for performing the same function. This can include diversity in how the function is performed (e.g., different algorithms, different variables sensed or physical principles applied, manual versus automatic) or in the equipment (different technologies, different hardware and/or software, different actuation means) used to perform the function.

Dynamic prioritization. See *alarm prioritization.*

Dynamic setpoints. *See alarm setpoint.*

First-out capability. *The ability to define a selected group of alarms as a first-out group, and when any alarms occur within that group, indicate which alarm occurred first. This feature can help users immediately recognize which of several trip alarms came in first, potentially indicating the cause of the trip.*

Grouped alarm. *See shared alarm.*

Human factors engineering (HFE). The application of knowledge about human capabilities and limitations to plant, system, and equipment design. HFE provides reasonable assurance that the design of the plant, systems, equipment, human tasks, and the work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support the plant.

Human-system interface (HSI). A human-system interface (HSI) is that part of the system through which personnel interact to perform their functions and tasks. In this context, "system" refers to the nuclear power plant. Major HSIs include alarms, information displays, controls, and procedures. See EPRI 1010042 [3] for additional information on nuclear power plant HSIs.

Inhibited alarm. An alarm that has been disabled or taken out of service, temporarily preventing generation of that alarm. Typically, an alarm is inhibited when planned testing, maintenance, or repair of the associated equipment would otherwise cause it to become a nuisance or contribute unnecessarily to the number of standing (currently active) alarms.

Intelligent alarm. An alarm is considered intelligent when it is generated with knowledge of the operational status of the plant, associated systems and equipment, so that it is "context-aware" and does not occur unnecessarily or as a *nuisance alarm* requiring no user action. Use of *alarm conditioning logic* and other techniques such as dynamic prioritization and dynamic setpoints can help make alarms more intelligent.

Limit. See *alarm limit*.

Nuisance alarm. An alarm that occurs in circumstances when it does not require any action and provides no provide meaningful information to the user. Such alarms are not useful and can become a nuisance or annoyance. An example is an alarm that is valid and meaningful during

full power operation but is a nuisance if it occurs during other plant operating modes such as cold shutdown. Another example of a nuisance alarm is one that occurs repeatedly without providing any additional useful information (e.g., a *chattering alarm*).

Off-normal condition. A condition that is not normal or expected for the current operating conditions of the plant or the associated system.

Priority. See *alarm prioritization.*

Priority escalation. See *alarm prioritization.*

Process alarm. Information generated for the purpose of alerting an operator or other user to an *off-normal condition* in the plant process.

Reflash. When an individual alarm condition occurs and is part of a *shared alarm*, and that alarm is acknowledged, spatially dedicated continuously visible indications of the shared alarm remain active (e.g., a tile would remain backlit) until the alarm condition clears. Reflash is a feature that causes the shared alarm to alert the operators or other users to occurrence of any subsequent alarm condition that occurs before the first one has cleared. For example, a tile or tile-replica type display would commence flashing again and an audible tone would occur, requiring acknowledgement of the new alarm condition. Reflash does not allow an active alarm condition to prevent users from being alerted to additional alarm conditions occurring as part of the same shared alarm.

SART (silence, acknowledge, reset, test). See *alarm controls*.

SDCV. See *spatially dedicated, continuously visible alarm display*.

Sequence of events (SOE). The ability of a system to sample the values of selected inputs (points) at a rapid rate (e.g., discrete inputs at a one millisecond interval) as compared to other inputs that are sampled less frequently, for the purpose of capturing the sequence of events occurring in the plant. Data points that are designated for sequence of events capability are referred to as SOE points.

Setpoint. See *alarm setpoint*.

Shared alarm. An alarm that combines multiple individual alarm conditions (sub-alarms) using "OR" logic to drive a single, shared alarm indication. Sometimes referred to as a grouped or combined alarm.

Shelved alarm. See *alarm shelving.*

Silenced alarm. An alarm is considered to be silenced when the user has taken action to stop the auditory alert associated with the alarm, but has not acknowledged the alarm. Alarm silencing may be done to reduce the distraction associated with the auditory alerts until the user has time to assimilate the alarm message(s) and acknowledge the alarm(s). See *alarm controls*.

SOE. See *sequence of events.*

Spatially dedicated, continuously visible (SDCV) alarm display. An alarm display that is spatially dedicated (located in a fixed position) and is directly observable without a user action, always indicating whether the corresponding condition is in an alarm or cleared (normal) state. Conventional *alarm tiles* are an example of an SDCV alarm display. Note that spatially dedicated means that the display is always available in the same location in the control room. It does not mean that that location is the only location at which such information can be retrieved. A distributed control system or other computer-based information system may provide access to the same displays at other locations as well, such as other workstations or remote shutdown facilities.

Standing alarm. An alarm that has remained active (in the alarm state) for longer than a pre-set time.

Static prioritization. See *alarm prioritization.*

System alarm. Information generated for the purpose of alerting an operator or other user (e.g., a maintenance technician) to an *off-normal condition* occurring within the systems used to monitor and control the plant process (e.g., a fault or error detected in a digital control or information system or in the alarm system itself).

Time stamp. The date and time at which an alarm is detected, and which are recorded and attached to the alarm when it is generated. The time stamp is carried with the alarm as it is communicated for further processing within the *alarm system* and stored in the alarm history database. The date and time at which the alarm clears (returns to normal) are also time stamped.

8
REFERENCES

1. EPRI 1003662. *Alarm Processing Methods: Improving Alarm Management in Nuclear Power Plant Control Rooms*, EPRI, Palo Alto, CA, 2003. Product ID 1003662.

2. NUREG/CR-6691. J.M. O'Hara, W.S. Brown, B. Hallbert, G. Skraning, J.J. Persensky, J. Wachtel, *The Effects of Alarm Display, Processing, and Availability on Crew Performance*, prepared by Brookhaven National Laboratory for the U.S. Nuclear Regulatory Commission, 2000.

3. EPRI 1010042. *Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance,* EPRI, Palo Alto, CA, and the U.S. Department of Energy, Washington, DC, 2005. Product ID 1010042.

4. NUREG/CR-6684. W.S. Brown, J.M. O'Hara, J.C. Higgins, *Advanced Alarm Systems: Revision of Guidance and Its Technical Basis*, prepared by Brookhaven National Laboratory for the U.S. Nuclear Regulatory Commission, 2000.

5. NUREG/CR-6105. O'Hara, J., Brown, W., Higgins, J., and Stubler, W. *Human Factors Engineering Guidelines for the Review of Advanced Alarm Systems,* prepared by Brookhaven National Laboratory for the U.S. Nuclear Regulatory Commission, 1994.

6. EPRI 1008232. *Application of Modern Visualization Techniques to Improve Human Decision Making*, EPRI, Palo Alto, CA, 2004. Product ID 1008232.

7. Tuszynski 2002. Tuszynski, Jan, et al, *A Pilot Project on Alarm Reduction and Presentation Based on Multilevel Flow Models*, Proceedings of the Enlarged Halden Programme Group Meeting, HPR-358, Storefjell, Gol, Norway: 2002.

8. EEMUA-191. *Alarm Systems, a Guide to Design, Management and Procurement*, Engineering Equipment and Materials Users Association (EEMUA), Publication No. 191, 1999. www.eemua.co.uk

9. NUREG-1709. *Selection of Sample Rate and Computer Wordlength in Digital Instrumentation and Control Systems,* U.S. Nuclear Regulatory Commission, 2000.

10. NUREG-0700 Revision 2. *Human-System Interface Design Review Guidelines*, U.S. Nuclear Regulatory Commission, 2002.

11. EPRI TR-106439. *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications*, EPRI, Palo Alto, CA, 1996.

12. EPRI 1002835. *Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades - Applying Risk-Informed and Deterministic Methods,* EPRI, Palo Alto, CA, 2004. Product ID 1002835.

13. EPRI 1011710. *Evaluating Digital Equipment for High Integrity Applications*, EPRI, Palo Alto, CA, 2005. Product ID 1011710.

14. EPRI 1008124. *Practical Maintenance of Digital Systems: Guidance to Maximize the Benefits of Digital Technology for the Maintenance of Digital Systems and Plant Equipment*, EPRI, Palo Alto, CA, 2004. Product ID 1008124.

15. EPRI 1002830. *Information Display: Considerations for Designing Modern Computer-Based Display Systems*, EPRI, Palo Alto, CA, and U.S. Department of Energy, Washington, DC, 2003. Product ID 1002830.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

© 2005 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc.

Printed on recycled paper in the United States of America

The Electric Power Research Institute (EPRI)

The Electric Power Research Institute (EPRI), with major locations in Palo Alto, California, and Charlotte, North Carolina, was established in 1973 as an independent, nonprofit center for public interest energy and environmental research. EPRI brings together members, participants, the Institute's scientists and engineers, and other leading experts to work collaboratively on solutions to the challenges of electric power. These solutions span nearly every area of electricity generation, delivery, and use, including health, safety, and environment. EPRI's members represent over 90% of the electricity generated in the United States. International participation represents nearly 15% of EPRI's total research, development, and demonstration program.

Together...Shaping the Future of Electricity

Program:
Nuclear Power

1010076

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1395 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com