Alarm Processing Methods

Improving Alarm Management in Nuclear Power Plant Control Rooms

Technical Report

Alarm Processing Methods

Improving Alarm Management in Nuclear Power Plant Control Rooms

1003662

Final Report, November 2003

EPRI Project Manager
J. Naser

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

MPR Associates, Inc.

ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Orders and Conferences, 1355 Willow Way, Suite 278, Concord, CA 94520, (800) 313-3774, press 2 or internally x5379, (925) 609-9169, (925) 609-1310 (fax).

CITATIONS

This report was prepared by

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

Principal Investigators
R. Fink
V. Doumtchenko

This report describes research sponsored by EPRI

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

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

REPORT SUMMARY

When a nuclear plant experiences a transient such as a trip, hundreds of alarms often occur in the first several minutes of the upset, creating an alarm overload that degrades the effectiveness of the system in conveying potentially important information to the control room operators. This report provides information and guidance to help plants manage this problem by taking advantage of the alarm processing capabilities of the newer digital systems now being installed in control rooms. The emphasis is on relatively simple techniques that can be used to substantially reduce alarm overload.

Background
Many alarm-processing schemes have been developed to address the alarm overload problem in nuclear plants, but very few of these approaches have been implemented in operating U.S. plants. Many plants still use conventional annunciator systems, which are very limited in alarm processing and logic capabilities; and utilities are reluctant to invest the considerable time and money that seem to be required to define and implement plant-wide alarm reduction. However, the newer digital monitoring and control systems now operating along side conventional equipment in "hybrid" control rooms provide much more capability to implement alarm processing. At the same time, there is a tendency for alarms to proliferate with such systems because of the ease with which new alarms can be generated in digital systems.

Objectives
To provide practical guidance to assist plants in reducing the alarm overload problem, with a primary focus on applying relatively simple techniques for defining and processing alarms to make alarm information more useful to operators during plant upsets.

Approach
The project team examined the effectiveness of alarm reduction techniques by reviewing previous research, examining the various schemes proposed or implemented for alarm reduction, and identifying fundamental alarm reduction techniques that are common to many of these schemes. Drawing on EPRI and NRC studies of alarm reduction, the team examined data on the effectiveness of the various techniques and collected alarm history data from actual events at operating U.S. plants to understand how alarm overload problems occur and to develop an example of how alarm reduction techniques can be applied to reduce alarms.

Results
Fundamental alarm processing techniques can significantly reduce the number of alarms occurring in nuclear plant transients. Operators consistently prefer alarm-processing schemes that accomplish the greatest amount of alarm reduction in transients, as long as no information is completely taken away from the operators. The greatest improvement is obtained when all of the

existing alarms are reviewed and improved logic is implemented that prevents unnecessary occurrences of the alarms during transients and in various plant-operating modes. If sufficient resources are not available to define and implement improved logic and processing for all alarms plant-wide, there are some relatively simple and less costly techniques that can provide substantial reduction of alarms in transients. For example, alarms occurring after a trip can be processed to provide an operator aid that highlights unusual alarms, without taking away any information from the operators. This type of operator aid can be defined for other transients by making use of the plant simulator and actual alarm histories to identify alarms common to many plant upsets.

The report provides guidance and a checklist for improving the definition of individual alarms. Guidance is also given for developing an overall alarm management strategy for a plant and for specifying and implementing new digital systems to implement this strategy. The report emphasizes simplified methods to develop operator aids to make alarms more useful during transients without a huge investment of resources.

EPRI Perspective

For many years, EPRI and other organizations have sought ways to reduce and prioritize alarms so that operators can get more usable information from alarms during transients to help them understand and diagnose what is going on in the plant and make efficient operation decisions. Digital technology, which is now available for nuclear plants, offers the opportunity to improve alarm systems. This study has gone beyond previous efforts to identify straightforward and practical approaches that are now possible for reduction and prioritization of alarms. The guidance in this report will help plants implement these simple improvements. This work is closely associated with the hybrid control room project. Related EPRI reports are Nuclear Power Plant Control Room Modernization Planning (1003569), Technical Material for a Workshop on Control Room Upgrades (1007795), Critical Human Factors Technology Needs for Digital Instrumentation and Control and Control Room Modernization (1007794), Interim Human Factors Guidance for Hybrid Control Rooms and Digital I&C Systems (1003696), and Information Display: Considerations for Designing Modern Computer-Based Display Systems (1002830).

Keywords

Instrumentation and control systems
Alarm systems
Annunciators
Hybrid control rooms
Human-system interface
Alarm processing
Operator aids

ABSTRACT

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. Alarm systems are effective in this mission when the plant is operating at power and only minor malfunctions occur, generating only a few alarms at a time. However, when the plant experiences a major transient, hundreds of alarms occur in the span of minutes. Operators typically are forced to ignore the alarms during the early stages of transients, thus the alarms act primarily as a distraction and they can increase operator workload if the operators attempt to repeatedly acknowledge them and silence the auditory warnings. Reducing the number of unnecessary alarms occurring in plant upsets promises to reduce operator burden, reduce distractions, and make alarms more useful to the operators in responding to events.

This report identifies fundamental alarm reduction techniques that can be applied in operating nuclear plants, particularly as plants convert their control and monitoring systems to newer digital platforms that provide greater ability to process and present alarms in ways that can improve usability of the alarm information. Effectiveness of the various reduction techniques is examined based on previous studies and evaluation of both simulated and actual transient alarm sequences. Finally, guidance is provided on practical application of these techniques, with the primary focus on relatively simple techniques that are reasonably straightforward to understand and implement. Suggestions on how to make substantial improvement in the current situation without a large investment of resources are provided. Also, guidance is provided on how to avoid making the alarm management problem worse when plants convert to digital systems due to the tendency for alarms to proliferate with these systems.

ACKNOWLEDGMENTS

A number of people provided information to the project team that was very helpful in performing this study. We are particularly grateful to the following individuals and their companies who provided input and insights on the alarm management problem, the features and capabilities of current systems, and approaches for dealing with the alarm problem, plus alarm history data from operating plants to be used in the evaluation: David Poole and Joseph DeBor of Aeroflex, John Blevins of Ameren/UE, Steve Bleier of Ametek, John O'Hara of Brookhaven National Laboratory, Doug Rothenberg of D-Roth, Inc., Bob Scanlan of Dominion, Rob Frank and Cyrus Taft of the EPRI I&C Center, Bill Kurth of Exelon, Juergen Bochtler and Bob Starkey of Framatome-ANP, Tim Hurst of Hurst Technologies, Rob Graham of Matrikon, David Herrell and Doug Hill of MPR Associates, Mark Baird of Qualitrol, Chris Wilson of TiPS Incorporated, Hiroshi Sakamoto of Toshiba, Dave Whitsitt of TXU Electric, and Peter Gordon of Westinghouse.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

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. Without alarms, the operators would be faced with an overwhelming task of actively monitoring all the individual equipment conditions and process variables in the plant to detect any abnormal conditions. Alarm systems are designed to perform this monitoring function continuously and automatically and to provide visual and auditory alerts when a situation occurs that requires operator action.

Alarm systems are effective in this mission when the plant is operating at power and only minor malfunctions occur that generate one or just 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 information needed at the moment 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 important information is not taken away from them. Also, there is evidence that operator performance in using alarm information can be increased when the alarm overload is reduced.

This report identifies fundamental alarm reduction techniques that can be applied in operating nuclear plants, particularly as plants convert their control and monitoring systems to newer digital platforms that provide greater ability to process and present alarms in ways that can improve usability of the alarm information. Effectiveness of the various reduction techniques is examined based on previous studies and evaluation of both simulated and actual transient alarm sequences. Finally, guidance is provided on practical application of these techniques, with the primary focus on relatively simple techniques that are reasonably straightforward to understand and implement. Suggestions on how to make substantial improvement in the current situation without a large investment of resources are provided. Also, guidance is provided on how to avoid making the alarm management problem worse when plants convert to digital systems due to the tendency for alarms to proliferate with these systems.

Background

Although many plants upgraded their alarm and annunciator systems after the Detailed Control Room Design Reviews (DCRDRs) that were mandated following the TMI-2 accident, the problems of information overload and false or nuisance alarms during transients still remain. One reason is that it is very difficult to make substantial improvement with conventional annunciator systems, which still serve as the primary alarm system in many operating plants today. However, even as plants begin to install more modern digital control and monitoring systems, which provide greater capability to implement improved alarm processing, plants typically are not taking advantage of this to reduce alarm overload.

A major reason is the significant investment in resources that must be made, particularly in terms of time from experienced engineering and operations personnel, to perform a plant-wide review of the alarms and then design, verify and implement improved alarm logic. Typical cost estimates for such an effort start in the $200,000 to $300,000 range. Therefore, there is a need for practical guidance on how plants can reduce the effort that is required, or ways to make substantial improvement without such a large investment of resources.

Objective

The objective of this report is to provide information and practical guidance to assist plants in improving human performance when responding to transients by reducing the alarm overload problem. The main focus is on applying relatively simple techniques for defining alarms, alarm logic, and alarm processing to reduce the number of extraneous alarms and make alarm information more useable and useful to the operators during plant upsets.

Approach

Substantial research has been performed over the years by many different organizations on alarm systems and alarm processing methods. The approach taken in this study was to:

- Review the previous research, testing, and implementations of alarm processing methods.
- Compare the various processing systems and methods to identify common elements and relatively simple techniques for alarm reduction.
- Examine the relative effectiveness of the different techniques based on previous studies and additional evaluations using simulated and actual transient alarm histories.
- Examine the capabilities of the systems that plants will be installing as they upgrade their I&C systems and control room human-system interfaces.
- Identify and evaluate other tools that are available to assist with alarm management.
- Develop guidance on implementation of improved alarm definition and alarm processing methods, with a focus on those that are relatively simple and straightforward to implement but still effective in making a substantial improvement in the overload situation facing the crew during plant upsets.

Contents of this Report

Section 2 provides a summary of the findings and conclusions of the project. Given in question-and-answer format, it also provides pointers to the various sections of the report that deal with particular issues or questions a reader may have.

Section 3 describes the alarm overload problem – what it is, what causes it, and how it may change as plants upgrade their I&C systems and control room. It also discusses how the alarm overload is being dealt with now in existing nuclear plants, and makes comparisons to the situations in other industries such as petrochemical, where similar problems exist.

Section 4 discusses conventional annunciators, and more modern digital alarm systems typical of the "hybrid" control rooms resulting from upgrades to the I&C systems and control rooms of operating plants. The overall process of alarm management in a hybrid control room is described.

Section 5 describes methods for defining and processing alarms that show promise for reducing the alarm overload. The focus is on fundamental techniques that are relatively simple and straightforward. Effectiveness of these techniques is examined based on evaluations of simulator alarm data performed previously by EPRI and NRC.

Section 6 illustrates the alarm overload problem and typical contributors to overload based on actual alarm histories from trips in operating plants. An example is shown of a relatively simple method that can be used to highlight important alarms after a plant trip.

Section 7 provides guidance for improving alarm management in existing plants, focusing on implementation of improved alarm logic and processing that are made possible by installation of digital control and monitoring systems. It also gives guidance on how to deal with the fact that moving to digital systems can make the alarm management problem worse if alarms are allowed to proliferate and an alarm definition and presentation strategy is not worked out prior to system implementation.

Finally, Section 8 lists the references that are cited in the text. It also includes a glossary of terms and acronyms that are used in the report.

2
SUMMARY AND CONCLUSIONS

This study concludes that there are a number of fundamental alarm processing schemes that can significantly reduce the number of alarms occurring in nuclear plant transients. However, to date, operating U.S. plants have not implemented these to any significant degree. Part of the reason for this is that conventional alarm systems do not allow very extensive alarm processing to be implemented in any practical way. However, even those plants that have upgraded to digital systems, and in doing so have obtained the capability for better alarm processing, typically have not implemented these features. The primary reason appears to be that significant effort is required to define and implement improved alarm logic and processing across the entire plant, particularly in terms of the amount of time required from experienced operations and engineering personnel.

The best approach for addressing alarm overload is to improve the definition and logic associated with the existing alarms and any that are added, applying fundamental techniques that make the alarms much less susceptible to nuisance alarming and generally improve the usefulness and usability of alarm information. However, there also are some relatively simple techniques that can be used to make substantial improvement with less effort. These are low-risk approaches that do not take any information away from the operators, and which make use of alarm histories from plant upsets and from the plant simulator to help define the alarm reduction scheme.

Frequently Asked Questions

The following questions and the brief answers that are provided serve as an overview of the findings and conclusions from this study. The answers include pointers to specific sections of this report that address issues related to each question.

What is the "alarm overload" problem?

During plant transients, particularly those involving a trip of the reactor and turbine-generator, hundreds of alarms often actuate in the first few minutes of the upset. The actuation of so many alarms in such a short period of time results in an overload of information to the control room operating crew. This significantly decreases the effectiveness of the alarm system in conveying information and it can distract operators from performing necessary control and monitoring activities. Section 3 describes the alarm overload problem in more detail.

What causes it?

The purpose of an alarm is to alert the operator to an off-normal condition. Most alarms have been defined on the basis that normal means steady-state, full-power plant operation. Therefore, any time the plant moves away from this condition, alarms are generated. During a major transient, many plant variables move out of their normal operating ranges and many systems and components change states, away from their normal operating conditions. Some process variables may oscillate around the normal setpoint, resulting in repeated alarms on a single variable. Other variables are sensed by multiple instrument channels, generating multiple alarms when the variable moves out of the normal range. Table 3-2 lists typical contributors to the alarm overload problem.

Is it a problem for conventional or computer-based alarm systems?

It affects both. With a conventional annunciator system, any major transient activates many of the annunciator tiles, presenting the operators with a myriad of flashing lights and audible tones. For example, for one plant examined in this study about 125, or one third, of the installed annunciator alarms actuate in the first ten minutes following an uncomplicated plant trip. Plant computers and other digital control and monitoring systems often present alarms in the form of message lists on a computer screen or video display unit (VDU). In an upset, the alarm messages quickly fill the screen and scroll off to back pages that then must be accessed by the operator to view the entire set of alarms.

How are plants dealing with the situation now?

Operators are highly trained and experienced in dealing with this situation. Operators typically are trained to recognize the normal pattern of alarms that occur after a plant trip. Also, most upsets trigger the use of abnormal or emergency operating procedures that are intended to guide the operators' actions and maintain the plant in a safe condition with or without the alarms. Because of the overload of information, operators often ignore the alarms during the early stages of an upset, concentrating on other indications and displays to maintain awareness of the plant condition and to determine appropriate response to the upset. In some plants operators silence the alarm tones and horns (often repeatedly) in order to minimize distraction and facilitate communication among the crew members. In other plants operators wait until later in the transient to do anything with the alarms. When the flood has subsided and a member of the operating crew has time to deal with the alarms, the annunciators and associated computer alarm displays are reviewed to help diagnose the upset and detect any other secondary malfunctions or failures that may have occurred.

Doesn't prioritization of the alarms solve the problem?

Prioritization can help, but typically does not eliminate the problem. A well-designed prioritization scheme allows the operators to focus on the highest priority alarms (typically those that potentially require short-term action). Computer alarm lists typically show the highest priority alarms first, requiring less paging by the operator to access important alarm information. However, priorities are pre-assigned to the alarms at design time and then typically are changed only when they need to be modified based on experience. The actual urgency of each alarm depends on the current plant situation, the particular upset that is occurring, and the states of other alarms and the associated plant systems and equipment. Also, eventually the operators need to make their way through all the alarms, in order to fully understand what has occurred and ensure that all conditions requiring their action have been identified.

What are the downsides of the present situation? What benefits can be obtained by reducing alarm overload?

It is very difficult to quantify the potential effects on overall operator performance of reducing the alarm overload. Test programs that have addressed this have shown that operators have a tremendous ability to adjust their monitoring strategies depending on the situation they are faced with, and compensate for deficiencies in the human-system interface design, including the alarm overload problem. It may be hypothesized that even though operators are able to handle such situations, their mental resources are challenged leaving little room for additional mental activities to occur in parallel. Previous research studies and experience from applications have shown that operators consistently show a preference for alarm processing schemes that reduce alarm overload, as long as the schemes do not take away any information that they may need. There is a significant body of evidence that indicates alarm reduction can make alarm information more usable in plant transients, reduce operator workload and distraction in critical situations, and reduce the risk that information will be missed that could be important to plant economics and safety. Section 5 discusses this further.

Is there an opportunity to improve the situation when we convert to digital systems?

Yes, but there is also a significant opportunity to make it worse. On the plus side, conversion of I&C and control room systems to newer digital platforms (e.g., a distributed control system or DCS) makes it much easier to apply improved logic and "cutouts" for alarms that can prevent unnecessary alarms and nuisances. Alarms can be integrated with process information in displays designed for monitoring and control. Such systems also can group and sort alarms in various ways and provide different views of the alarm information to support specific operator tasks. On the minus side, experience has shown that alarms tend to proliferate with digital systems, partly because it is much easier to generate alarms from process information, and partly because of built-in diagnostics that can provide many detailed alarms on problems or failures detected within the DCS itself. Also, with digital systems there often is a greater reliance on screen-based alarm presentations, particularly alarm message lists, which are particularly difficult to deal with when there is an overload of alarms.

What kinds of alarm processing can be applied to reduce the number of alarms?

There are many different kinds of alarm definition and alarm processing schemes that can be used. This study reviewed many of these and, by examining common elements among them, identified a number of fundamental alarm reduction techniques that can be used. These are shown in Table 5-1. Section 5 presents data showing the effectiveness of these techniques in reducing the number of alarms in upsets.

Isn't it risky to filter alarms, potentially hiding information from the operator that may be needed in some situations?

Yes, there is some risk if the alarms are totally filtered out such that the operator does not have access to them. However, the operators can be aided considerably by simply providing different views of the alarm information, some of which suppress potentially extraneous information, or highlight the more important information, while still providing access to all the alarms. The fundamental alarm reduction techniques described in Section 5 of this report can be applied in ways that do not eliminate any information completely – all of the information is still available to the operators on request. Section 6 provides an example.

Are there some practical things we can do to implement alarm reduction?

Yes. First, ensure that all new alarms added to the control room apply appropriate logic so they do not contribute to alarm overload. A checklist is provided in Appendix A to assist with this. Also, begin a program of continuous improvement so that all alarms can be upgraded over time. Work with the vendor or supplier of new digital systems to understand their alarm management capabilities and determine how they fit with the plant's alarm management strategy. Get involved in the definition of new alarms generated by the new systems, including internal fault detection alarms. Make use of the plant simulator to identify sets of alarms to tackle that are major contributors to alarm overload – for example, alarms that are common to reactor trips, safety injection actuations, bus losses, etc. Consider providing relatively simple operator aids that make use of this information. For example, a "highlighted" alarm listing that shows all alarm events but highlights the unusual alarms can provide real benefits without a huge investment of resources. Table 6-6 shows an example for the case of post-trip alarms. Section 7 provides guidance on how to address the alarm overload problem.

What should we NOT do?

Don't implement an alarm processing scheme that is so complex or opaque that the operators do not understand it. Don't implement alarm processing without sufficient operator training on how it works, why, and how they should and should not use it. Don't confuse the operators by changing the logic of an alarm in a way that they do not understand or doesn't fit with how they use the alarm. Don't assume that a digital system vendor will know what you want in the way of alarm management. Don't assume that their default way of defining new alarms will fit with the plant's overall alarm strategy. Don't ignore the role of procedures and other information sources in helping the operating crew deal with the underlying problems or malfunctions that initiate the alarm activations.

3
THE ALARM OVERLOAD PROBLEM

The design of the monitoring instrumentation present in conventional control rooms was based primarily on a “single sensor – single indicator” philosophy. This led to the many discrete meters and indicating lights that dominate the display area of conventional control boards. Alarms were designed in a very similar manner – using for the most part a “single condition – single alarm” philosophy. As a result the number of alarms in most nuclear plant control rooms is large, and the number tends to increase over time as equipment and sensors are added to the plant, additional off-normal conditions are identified, and new I&C systems with greater diagnostic and fault detection capabilities are installed.

In order to identify off-normal conditions, there must be a definition of what is “normal.” Alarms typically have been defined on the basis that normal means steady-state, full-power operation, with all systems in their typical lineup for that mode. A criterion often used in alarm system design is that there should be a “dark board” when the plant is at power – no alarms are active as long as all systems are operating normally. Application of the dark board criterion plays an important role in ensuring the alarm system does not exhibit “standing alarms” during power operation, so that true off-normal conditions stand out when they occur.

The situation changes dramatically when the plant suffers a major upset or transient. Large numbers of alarms are activated as the plant moves away from the defined normal condition of steady-state full-power operation, process variables move outside their normal ranges, and many components change state in response to the changing plant conditions. The result of this is “alarm overload” – too much information occurring at too high a rate for the operators to assimilate.

Table 3-1 shows typical data on the number of alarm events that occur in the first few minutes of various plant transients and accidents. Alarm events include new (incoming) alarms and alarms that are returning to normal (clearing). Most alarm systems annunciate both of these types of events using both visual (e.g., flashing message) and auditory (horn or tone) alerts. Note that the number of alarm events varies significantly among the plants and the various transients listed. However, it can be seen that several hundred alarm events often occur within the first several minutes.

Table 3-1
Number of Alarm Events Occurring in Plant Upsets Based on Simulated and Actual Alarm Histories from U.S. Plants

Transient	Total No. of Events[1]				
	Plant Simulator Alarm Data[2]			Actual Plant Alarm Histories[3]	
	Plant A	Plant B	Plant C	Plant D	Plant E
Manual Trip due to Coolant Pump Problem				316	
Automatic Trip from Reduced Power due to Controls Problem				127	
Automatic Trip due to Generator Problem				334	
Automatic Trip due to Control Circuit Failure					520
Automatic Trip due to Transformer Failure Plus Loss of Offsite Power					1,364
Manual Trip Plus Trip of Main Feed Pumps due to Controls Problem					531
Manual Reactor Trip (Uncomplicated)	90	67	63		
Small-Break LOCA	158		76		
Reactor Coolant Pump Seal Leak	26				
Large-Break LOCA	252	166	111		
Feedwater Line Break	115		42		
Main Steam Break Outside Containment			84		
Main Steam Break Inside Containment	195		102		
Steam Generator Tube Rupture	456	327	72		
Loss of Offsite Power	327		195		
Stuck Open Safety Relief Valve			44		

NOTES:

(1) Total number of events includes incoming and clearing (return to normal) alarms

(2) Data from full-scale plant simulator, capturing first few minutes of each transient; only annunciator data are included, not plant computer

(3) Data from microprocessor-based annunciator systems recording actual events in operating plants, covering the first 10-12 minutes; plant computer alarm data are not included

Contributors to Alarm Overload

There are a number of different types of alarms and alarm behaviors that contribute to alarm overload. Table 3-2 lists typical contributors.

Table 3-2
Typical Contributors to Alarm Overload

Contributor	Cause
Repeating or chattering alarms	A plant variable fluctuating around the alarm setpoint may cause repeated alarms. *Example:* Feedwater heater levels after a plant trip
Multi-setpoint alarms	Multiple setpoints on a single variable indicating different levels of severity may result in multiple alarms occurring for a single variable. *Example:* Level Lo Level Lo-Lo Level Lo-Lo-Lo
Process variables exceeding normal setpoints during plant transients or mode changes	A plant upset may cause temporary excursions of a plant variable beyond the normal alarm setpoint, causing a momentary alarm. Plant mode changes may cause a variable to move into a new range that is beyond the normal alarm setpoint, thus generating an alarm. *Examples:* Pressurizer level after a PWR plant trip Reactor coolant system temperature during shutdown
Redundant (multi-sensor) alarms	Multiple redundant alarms can be generated due to a single plant condition or event because of multiple sensors on a single variable, multiple redundant channels of instrumentation in an I&C system, or multiple installed trains of a mechanical or fluid system. *Example:* Level Lo Ch A Level Lo Ch B Level Lo Ch C

Contributor	Cause
System/component state change alarms	When a system or a major component is shut down or changes to a new operating mode, lower-level alarms may occur as a normal result of the new operating state. *Examples:* Low discharge pressure when pump turned off Rod bottom alarms after reactor trip
Other cause-consequence alarms	Logical relationships within a system or across systems (e.g., automatic actuations, interlocks) can cause alarms as a direct consequence of an earlier alarm condition. *Examples:* Turbine trip caused by reactor trip Voltage regulator alarms caused by turbine-generator trip Automatic pump start due to low pressure in a system
Maintenance-related alarms	Alarms that indicate conditions requiring maintenance may not require any specific actions by the operators, and thus simply add to the operator's alarm overload. Note, however, that sometimes the operator needs some notification about the need for maintenance or the operational impact of a failure that maintenance personnel will repair. *Examples:* I&C fault alarms detected by self-testing Low oil reservoir level for a pump

Note that alarms in the last category listed, maintenance-related alarms, typically do not contribute substantially to alarm overload during plant upsets. These are alarms that indicate failures or degradation of equipment over time that would not be expected to occur in large numbers during a transient or other plant event. However, as digital systems with enhanced diagnostics are added to the plant there is a tendency to create more of these alarms and thus the potential for them to become a more significant contributor to the overall problem. Also, distinguishing between alarms that are primarily maintenance-oriented from those that require short-term operator action is important in reducing nuisances and distractions for the operators.

Coping with the Alarm Overload

With alarms occurring at the rates shown in Table 3-1, the alarm system becomes much less useful to the operators. In fact it becomes a major distraction at a time when it is critical that the operators maintain the plant in a safe condition, determine the cause of the transient and the appropriate actions to take to correct it, and monitor for any other malfunctions or off-normal behavior that may occur.

Operators are highly trained to deal with this situation. Typically, in the early stages of the upset their actions are guided by abnormal or emergency operating procedures, which are designed to ensure that critical safety functions are maintained regardless of the event.

However, if the alarm overload can be reduced, then the amount of distraction and added workload associated with the flood of alarms can be lessened. Also, and perhaps most important, by making the alarms more intelligent and aware of plant and equipment states so that nuisance alarms are reduced, and providing the operators with appropriate views of alarms and tools or aids to help them manage the alarm information, it is likely that operator performance can be increased and the risk of missing important alarm information can be reduced.

Impact of Converting to Digital Technology

As plants upgrade or replace their I&C systems and begin to use more modern human-system interfaces in the control room, there is a greater opportunity to make alarms smarter using logic or "cutouts" to help prevent unnecessary alarms. Also, digital systems provide additional flexibility in how alarms are presented and allow better integration of alarms with other information the operators use to monitor the plant – for example, integrating alarms into process mimic displays. Alarms can be sorted and grouped to provide different views of alarm information to support the operator crew's use of alarm information to support various tasks.

On the other hand, digital systems also present the possibility of creating many more alarms that can add to the alarm overload problem. It is much easier to create a new alarm with a digital or distributed control system (DCS). Rather than having to run new wires and find room for a new alarm tile on a conventional annunciator system, a new alarm can be configured in a DCS simply by setting appropriate configuration parameters using an engineering workstation. Also, many systems offer the ability to create many alarms on a single variable, for example, with multiple high and low setpoints or thresholds indicating level of severity.

Also, with digital systems there is a tendency to rely more on alarm message lists presented on a video display unit (VDU). Previous research, testing and experience have shown that message lists are particularly difficult to use when there is a flood of alarms (EPRI NP-5693P, NUREG/CR-6691). Fortunately, modern digital systems can provide alarm presentations that maintain the positive characteristics of fixed-position annunciators along with selected message list presentations. This is discussed further in Section 4.

Situation in Other Industries

Nuclear power is not the only industry experiencing the alarm overload problem. Fossil power plants, chemical and petrochemical processing plants, and other industrial facilities also are attempting to address this problem (NUREG/CR-6684, HSE CRR-166, Campbell-Brown 1999, Mostia 2003, Rothenberg 2003). Some serious accidents have occurred in petrochemical and other facilities in which the flood of alarms has been identified as a contributing or at least a complicating factor. A survey of the European chemical and power industries found that inadequacies in alarm system performance had led to financial loss or to equipment or environmental damage. The Engineering Equipment and Materials Users Association developed a guide on alarm system design, management, and procurement to address these and other problems associated with alarms (EEMUA-191). The guide recommends use of alarm processing methods such as those identified in this report. System vendors are beginning to respond to the problem by providing better alarm management facilities, and third-party software suppliers have developed tools designed to assist plants in assessing their alarm system's performance and developing improved alarm management schemes (e.g., Mostia 2003, Rothenberg 2003, Swanekamp 2003).

4

ALARM MANAGEMENT IN HYBRID CONTROL ROOMS

A variety of methods have been proposed to address the alarm overload problem in nuclear power plants and in other industries. Research studies have examined a number of alarm reduction schemes, and some have been applied in operating facilities, particularly in newer plants built outside the U.S. The ease with which these methods can be applied to operating U.S. nuclear plants varies significantly depending on the capabilities of the installed alarm system. Conventional annunciator systems installed in many plants provide very limited alarm processing capability. However, as plants upgrade their instrumentation and control (I&C) systems and control rooms, the additional capabilities offered by more modern digital systems make it more feasible to apply alarm reduction.

The section begins by describing conventional control room alarm systems. Then, more modern systems that are typical of a "hybrid control room" are described. Hybrid control rooms are those that result from modernizing portions of the I&C systems and associated human-system interfaces with newer digital technologies, while maintaining some conventional systems and equipment such that both old and new technologies are used by the operators. Finally, this section provides an overview of the alarm management process in a hybrid control room and highlights those aspects of alarm management that are most important to reducing alarm overload.

Conventional Control Room Alarm Systems

Most U.S. nuclear power plants have operated for many years with conventional control rooms that have received only relatively minor updates over time. The updates typically have been component-by-component replacements or piecemeal upgrades of subsystems such as the plant computer and other monitoring systems. Alarms have been presented primarily on annunciator systems, with additional alarm information often provided by the plant computer. These systems are described very briefly below in order to set the stage for discussing more modern systems used in hybrid control rooms, and to introduce basic alarm functionality. The discussion is generalized, and it should be recognized that the installed capabilities of alarm systems vary considerably from one plant to the next. For more information on conventional annunciator systems, plant computer systems and their capabilities, contact the system vendors and also consult the pertinent references in Section 7 (e.g., EPRI NP-4361, EPRI NP-3448).

Conventional Annunciators

The primary purpose of an alarm is to alert the operator to off-normal conditions requiring operator action. In most nuclear plants this function has been served by conventional hardwired annunciator systems. As shown in Figure 4-1, an alarm condition is detected when a field contact opens or closes. The annunciator electronics senses this contact change of state and provides both visual and audible indications to alert the operators. Visual indication is typically accomplished using conventional light boxes, arrays of alarm "tiles" or backlighted windows.

When the alarm condition occurs, the corresponding tile begins flashing to provide visual indication of the alarm condition. The tile is engraved with a message, the alarm "legend," which tells the operator the nature of the alarm condition. At the same time, a horn or tone provides audible indication of the new alarm. The operator must acknowledge the alarm to stop the flashing and silence the horn. The tile is then lit steadily until the condition clears. When an alarm condition clears, many annunciator systems flash the tile again (typically at a different rate) and provide an audible tone that may be different from the incoming alarm tone or horn.

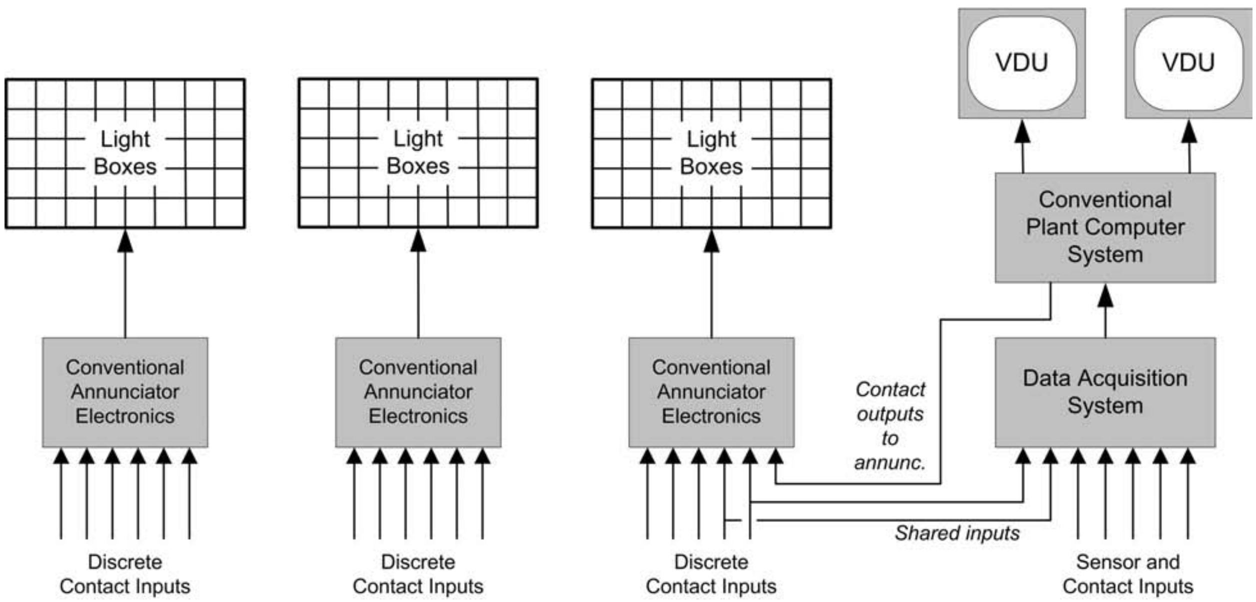

Figure 4-1
Conventional Control Room Alarm Systems

Plant Computers

The plant computer system, or plant monitoring system, typically also provides some type of alarming capability. Alarms can be generated from sensed field contacts (some of which may be shared with the annunciator system), from process conditions sensed by the plant computer and its data acquisition system (see Figure 4-1), or from calculations performed by the plant computer. The plant computer in some plants also provides output contact closures that drive one or more annunciator inputs.

Typically, plant computer alarms have been displayed in the form of message lists. The alarm messages are displayed on one or more video display units (VDUs) and/or on one or more printers. (Newer systems provide additional alarm processing and display capabilities – these will be discussed below in the section on hybrid control room systems.) Plant computer alarms may require separate acknowledgment, and they may or may not have an audible tone associated with them.

Microprocessor-Based Annunciator Systems

As annunciator manufacturers updated their systems from the traditional hardwired, dedicated-function annunciator to digital microprocessor-based technology, the systems began to offer additional features. Many microprocessor-based annunciators can provide a VDU that lists detailed alarm messages to go along with the annunciator windows. Alarms are time-tagged as they are detected, often resolved down to the millisecond. This allows a detailed "sequence of events" to be presented as chronological lists of messages, which also can be printed. Several alarm conditions can be combined on one tile, with a message on the VDU providing detailed information on which of the various input conditions caused the alarm. Time delay or time filtering of alarm inputs (e.g., contact "debounce" filters) can help prevent alarm chattering. Some systems provide automatic detection and suppression of chattering or repeating alarms based on the rate at which an alarm is repeatedly coming in and clearing. Finally, some microprocessor-based systems have provided limited Boolean logic capability for creating smarter alarms, depending on the inputs available to the system. A number of plants have installed microprocessor-based systems and some have taken advantage of features that are relatively straightforward to implement, such as time filtering and chatter detection.

Hybrid Control Room Alarm Systems

As plants upgrade their I&C systems and control room human-system interfaces, a greater variety of methods for generating, processing, and presenting alarms becomes available. In the resulting hybrid control room, alarms can be presented on conventional light boxes, on computer-driven light box replicas shown on VDUs, on process monitoring displays such as mimic diagrams, on a VDU as message lists, and using many other display possibilities. There may no longer be one primary alarm "system" as there was when the annunciators were the primary source of alarm information. As plants define their desired control room endpoint (vision of the control room at the end of the modernization or upgrade program), and various interim configurations that will result from staged implementation of the upgrades, a strategy should be defined for how and where alarms will be generated, processed and displayed to the operators at each interim stage and at the endpoint.

Figure 4-2 illustrates various alarm systems that may be part of a hybrid control room design. Again, this is a generalized description recognizing that the actual configuration of systems, processors and displays used will depend on the endpoint design concept chosen and the specific vendor implementation. See EPRI 1003696 for more information and guidance on choosing a control room endpoint concept and control room migration plan.

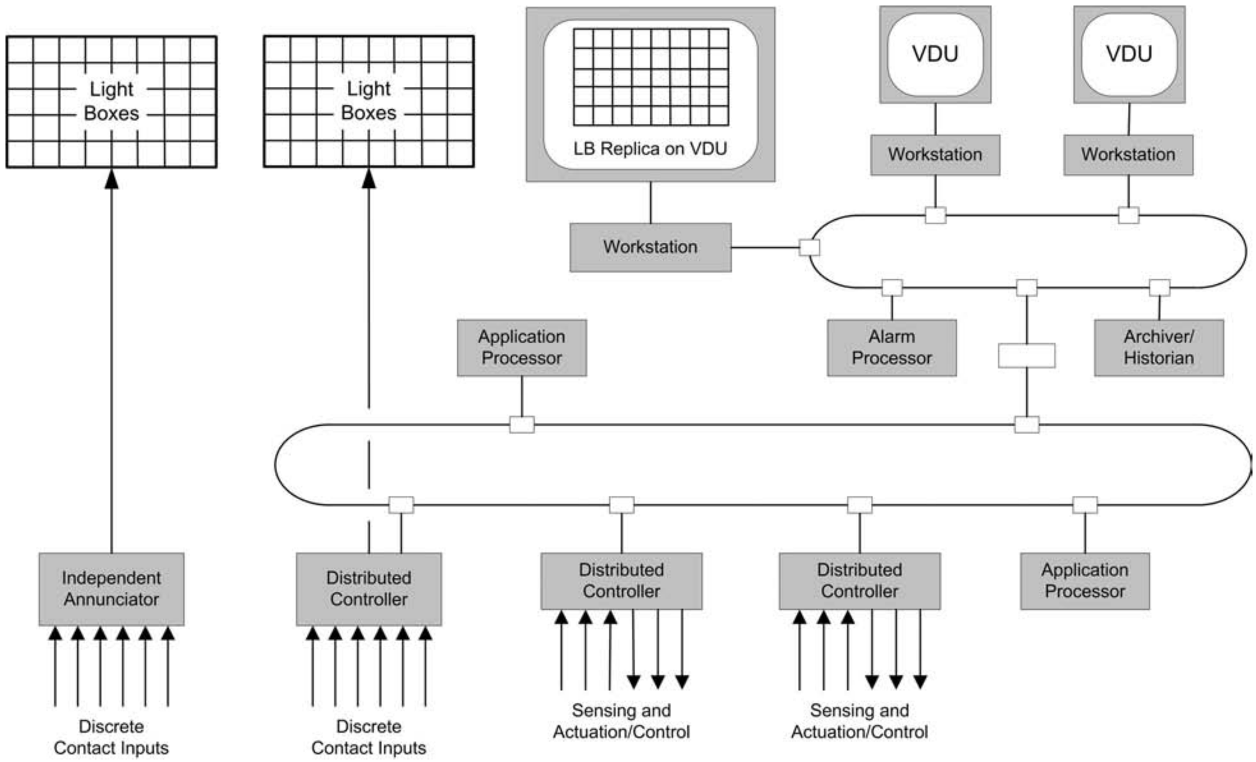

Figure 4-2
Hybrid Control Room Alarm Systems

As shown in the figure, alarms may be detected and displayed by several different systems, including annunciators, computer-driven light boxes, and DCS workstation displays. In addition, large-scale, fixed plant mimics may be added for additional alarm and plant status displays and enhanced situation awareness.

Independent Annunciators

The original annunciator system may be retained in the final endpoint design, or at interim steps in the migration toward a more modern control room. An advantage of this is the diversity offered by a standalone annunciator system, reducing the risk of total loss of annunciation due to problems with the DCS or other digital monitoring system implementation. However, there are several important disadvantages of independent annunciators:

- Limited capability to implement improved alarm processing to make alarms more useful and reduce alarm overload during upsets
- Less flexibility in display of the alarms
- Lack of a single source of time-tagged alarm data
- Difficulty in synchronizing time in the various units, making the post-trip historical data difficult to integrate with data from other systems
- Difficulty in integrating alarm information among the various displays of alarms the operators will be using – similar to the problem in conventional control rooms (Figure 4-1)

where some alarms are only on the annunciators, some only on the plant computer, and some on both but possibly implemented differently between the two

Also, it is important to remember that implementation of DCS-driven workstations for the operator interface for controlling and monitoring the plant requires that the DCS and its data networks be highly reliable. The design should be such that the operators can rely on the workstations to remain functional with very high reliability.

DCS-Driven Light Boxes

It is possible to drive conventional light boxes directly from one or more controllers in the DCS. This allows the familiar light boxes to be retained along with the advantages they provide through the fixed-position arrays of alarms, facilitating pattern recognition and rapid assessment of the alarm situation. Use of a DCS controller allows for improved alarm generation and processing techniques to be applied, and allows better integration of the light box alarms with other alarm displays, including ability to have a complete alarm history available to the operators via DCS displays. Of course, use of conventional light boxes limits the display flexibility by providing only fixed message content.

Light Box Replicas on VDUs

With most systems, fixed-position displays of alarm information can be provided on DCS-driven VDUs. This can include displays that show arrays of alarm boxes that simulate conventional light boxes. However, there is more flexibility with this approach as the alarm messages can be made more context-specific, prioritized or coded more easily, etc. These types of displays can be presented at workstations or on large wall-mounted displays visible to the entire crew. This latter approach retains many of the advantages of conventional annunciators, while providing the processing power and flexibility of the DCS behind the alarms.

Other VDU Alarm Displays

Alarms can be integrated into plant system and process displays (e.g., process mimics) generated by the DCS. Chronological alarm message lists can be provided, along with other sorts of the alarms (e.g., by system or by priority). Operator aids can be created that make use of alarm information. Modern digital systems have the inherent capability to provide many different types of alarm information displays. However, the base system offered by the vendor will have only a fixed set of options for displays that can be produced “out of the box.” It is important to understand the current built-in options and future capabilities that may be added by the vendor to the base system. It is also important to understand the cost and schedule required for the vendor or a third party to produce non-standard or custom displays that may be desired to meet the plant’s specific needs.

Location of Alarm Processing

In modern digital systems, alarm generation and processing may occur at any of a number of locations within the system, often at multiple locations. For example, low-level alarms typically are generated at the controller level and then passed up to the workstations via the data network or highway (see Figure 4-2). A separate processor (or set of redundant processors) may be provided that generates alarms from information passed up by the controllers, including higher-level alarms or alarms that are made smarter through use of logic or cutouts based on other information on the system (e.g., alarms that are conditioned based on the plant mode). Other application processors may also generate alarms or process alarm information. Alarm processing methods are discussed in more detail below. The point here is that alarm generation and alarm processing may be performed at any of a number of different locations within the system depending on the architecture chosen and the vendor's implementation of alarm capabilities. With a modern DCS or other open system, it should not matter where this processing takes place. The important thing is to specify what alarms are to be generated, what processing is to be applied, how time is to be synchronized among the processing elements so the alarms are presented and archived in the correct order, and where and how this information will be presented to the operations and maintenance personnel.

Overview of Alarm Management in a Hybrid Control Room

Figure 4-3 shows a block diagram describing the overall process and key activities related to alarm management in a hybrid control room.

Key Alarm Management Activities Related to Reducing Overload

The aspects of alarm management that relate most closely to the alarm overload problem, and thus are the primary focus of this report, are discussed briefly below.

Alarm Definition

This is the design activity that identifies alarm conditions (off-normal plant conditions that require operator action) and defines the associated setpoints. This activity also should define logic and cutouts that may be needed to ensure that the alarm does not occur unnecessarily or as a nuisance (e.g., alarm low discharge pressure only if the pump is running).

Alarm Generation

The alarm system (or the DCS or other system that can generate alarms) monitors plant conditions, performs comparisons to setpoints, detects alarm conditions, and generates the alarms. As discussed above, in a DCS this may be done in individual distributed controllers or at a centralized alarm processor, or both. As long as the controllers have a means of synchronizing time, the time order displayed to the operator will be correct and not misleading.

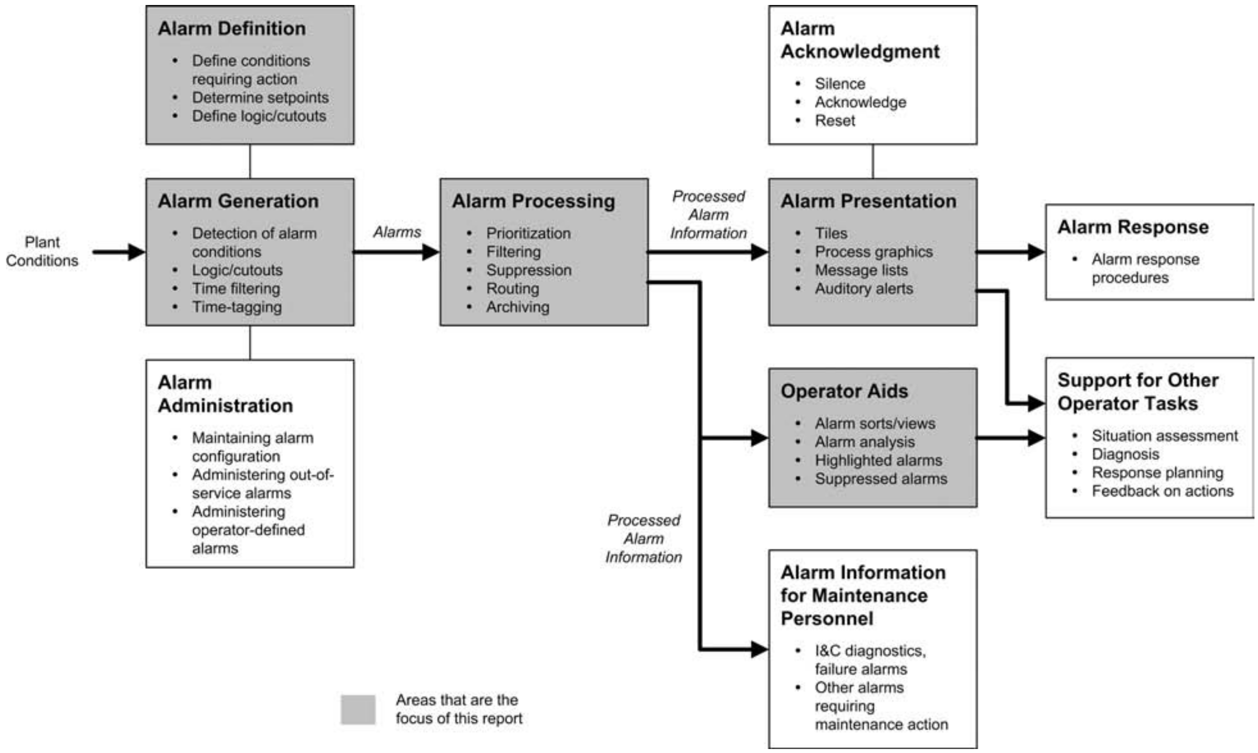

Figure 4-3
Alarm Management in a Hybrid Control Room

Alarm Processing

Once an alarm has been generated, alarm processing methods are used to assign priorities to the alarms and perform any filtering or suppression (eliminating or categorizing alarms based on pre-defined conditions – for example, suppressing selected alarms based on plant mode). Another important function in a modern alarm system is routing – categorizing the alarms according to who should respond and routing them accordingly. For some alarms, the response will be primarily maintenance or troubleshooting related and will be performed by maintenance personnel. Examples are I&C diagnostic alarms and "trouble" alarms on plant equipment. Modern digital systems have the capability to categorize the alarms as such and to route them to a maintenance workstation. This can significantly reduce the number of alarms that the operators must deal with.

It should be noted that even if the primary response will be by maintenance personnel, the operators still may need to be notified that the problem has occurred and maintenance will be needed. However, in that case the message that is presented to the operators should not be a detailed message describing the fault, as this should be given only to the maintenance technician. The message to the operator should be one that describes the significance of the alarm from an operational standpoint, directing the operators toward any action that is appropriate for them to perform. Their response could include increased monitoring of the system, preparing to bring standby equipment into operation as a contingency, or simply being aware that maintenance actions will be required in a particular location.

Finally, alarms should be archived so that a complete alarm history is available for operators, engineers, and maintenance personnel, and to satisfy any record-keeping requirements. This should be integrated with other historian functions (e.g., logging of selected process data and equipment operations, and sequence of events recording).

Alarm Presentation

As discussed above, the processed alarm information can be displayed in a number of different ways in a hybrid control room. Each has its own advantages and disadvantages. Research has shown that the most effective alarm presentation scheme is one that provides multiple ways of viewing alarms, supporting the different ways in which alarm information is used (NUREG/CR-6691, EPRI NP-5693P). Fixed-position alarm tiles are very good at alerting the operator to an off-normal condition and prompting short-term operator response when not too many alarms are occurring. They also support rapid situation assessment and can be used to gain an overview of plant system and equipment status, for example, to check availability of systems to support response planning during an upset.

Integrating alarm information into process displays helps place the alarms in context with the system, equipment, and process functions. This type of display can help support rapid situation assessment at the level of the display – a system or function – and help support tasks performed using this information.

Alarm message lists provide detailed information about the alarms. The displays can include time of occurrence, setpoint and current values along with a more detailed description of the alarm condition than typically can be placed on a tile or in a process display. A chronological list of alarm messages can help the operators examine the progression of a transient, diagnose the cause, and detect unusual behavior if the number of alarms is not too overwhelming. Alarm reduction methods can be of substantial help here, as will be discussed later in this section.

When alarms are presented on multiple types of displays, it is important to coordinate these so that the operators can easily move among them and relate the displays one to another. A DCS implementation that drives light boxes as well as process displays and message lists can help accomplish this integration. If separate annunciators are used, or when other legacy systems such as plant computers or older monitoring systems are retained during the transition to a more modernized design, coordination of the alarm displays is more difficult.

The DOE/EPRI hybrid control room guideline (EPRI 1003696) provides more information and guidance on methods for designing alarm displays and information displays for a hybrid control room.

Operator Aids

In addition to the primary alarm displays (e.g., fixed-position light boxes, alarm indications on process mimics, and chronological message lists), other views of alarm information can be created that aid the operator in using alarm information to support various tasks. These include different sorts of the alarms (e.g., by system or by priority) and results of alarm processing or analysis. For example, an operator aid might provide different views of alarms after a suppression scheme has been applied, allowing the operator to view the reduced set of alarms remaining after suppression, but also providing access to the alarms that were suppressed. Highlighting techniques can be used to draw attention to alarms that may be most important. This is discussed further below, and an example is provided for the case of post-trip alarm reduction.

Other Aspects of Alarm Management

Other aspects of alarm management shown in Figure 4-3 that are not discussed in detail in this report, but are important to the overall performance of the alarm systems, are:

- Alarm administration – this includes items such as maintaining the alarm configuration database, administering out-of-service alarms, and administering operator-defined alarms (temporary alarms defined by the operator to support short-term activities such as enhanced monitoring of equipment)
- Alarm acknowledgment – the controls provided for silencing the auditory alerts (e.g., horns), acknowledging new alarms and resetting alarms that have cleared (gone back to normal)
- Alarm response – provision of alarm response procedures to support taking action required for individual alarms. With digital systems these can be displayed electronically on a VDU. They can include live data from the process that are helpful in confirming and responding to the alarms. Quick access can be provided by cues or hot buttons.
- Support for other operator tasks – operators can use both the primary alarm information displays and operator aids discussed above to support tasks such as situation assessment, diagnosis of plant upsets and events, response planning (e.g., deciding an appropriate success path for restoring a critical function), and obtaining feedback on the results of control actions
- Alarm information for maintenance personnel – with digital systems, maintenance personnel can use workstations with appropriate alarm information and other displays to support diagnosis, troubleshooting, and response to maintenance-related alarms. These alarms would provide different messages for the maintenance staff, with more precise definition of the problem that maintenance needs to resolve.

5
ALARM PROCESSING METHODS AND TOOLS

A number of methods have been proposed for improving the definition of alarms and applying more intelligent alarm processing to reduce the number of alarms the operators must deal with during nuclear plant upsets. This study identified and examined the effectiveness of alarm reduction techniques, with emphasis on fundamental techniques that are relatively simple and straightforward to understand and implement. The following approach was taken:

- Review the literature on alarm system research and applications in nuclear power and in other industries
- Review results of previous EPRI and NRC research on alarms
- Examine common elements among the various schemes proposed or implemented to identify a set of fundamental alarm reduction techniques
- Examine available data on effectiveness of the various techniques, drawing on EPRI and NRC studies of alarm reduction
- Obtain alarm history data from actual trips that have occurred at operating U.S. nuclear plants and evaluate effectiveness of post-trip alarm reduction using relatively simple techniques.

This section describes the results of the first four activities above, identifying alarm processing methods and their effectiveness in reducing the alarm overload. The final item, evaluation of post-trip alarm data and simple post-trip alarm reduction techniques, is discussed in Section 6.

Review of Alarm Processing Methods and Systems

Considerable research has been performed and many alarm processing schemes have been developed in attempts to address the alarm overload problem in nuclear plants. Some comprehensive reviews of alarm processing systems and related research can be found in reports by NRC (NUREG/CR-6684), the U.K. Health and Safety Executive (HSE CRR-166 – Volume 3, Section 6), and EPRI (MPR-1482).

Alarm reduction methods range from relatively simple processing schemes such as suppression of pre-selected alarms based on plant mode, to approaches that apply artificial intelligence or rule-based methods, and systems that use state-based models of the plant and its systems to place alarms in context. Other design approaches rely primarily on prioritization and presentation methods to enable the operators to better deal with large numbers of alarms in upsets.

Implementations of alarm reduction schemes in U.S. nuclear plants have been few and have tended to be relatively limited in scope. This is partly due to the limitations of conventional annunciator systems, but also due to resource constraints. However, some plants have implemented limited alarm reduction. For example, one plant that recently upgraded to a plant computer system using a DCS platform has applied limited alarm suppression based on plant mode. Operators are reportedly pleased with the results and the plant hopes to make more extensive use of this type of suppression in the future.

Fundamental Alarm Reduction Techniques

A review of alarm processing systems shows that there are common elements among them – fundamental alarm reduction techniques that are used in different combinations in the various systems. Table 5-1 summarizes these fundamental techniques, organizing them according to the level at which the processing logic is based: the signal level, the equipment or component level, the system or function level, or the overall plant level.

This section discusses these fundamental alarm reduction techniques and what is known about their effectiveness in reducing alarms, based on studies performed by EPRI and the NRC.

Table 5-1
Fundamental Techniques for Alarm Reduction

Technique	Example
Signal Level	
Time delay filtering, or chatter detection and lockout	Use of low-pass filtering or time delay (on actuation and/or clearing) to prevent repeated alarms when a variable fluctuates around a setpoint and to provide contact "debounce" Chatter detection and lockout feature that looks at the rate of alarm occurrences and blocks an alarm that exceeds a pre-set repeat rate
Severity level	Suppression of a LEVEL LOW alarm when the LEVEL LOW-LOW alarm occurs, because its higher severity makes the earlier one less important
Redundancy	Combining multi-sensor or multi-channel alarms into one, to prevent multiple alarms from individual channels (e.g., a single LEVEL LOW alarm in lieu of LEVEL LOW CH A, LEVEL LOW CH B, etc.) More advanced signal validation techniques that can generate a single alarm from the validated signal (e.g., signal derived from multiple channels by voting, mid-value select or other validation scheme)
Equipment or Component Level	
Event-based	Suppression of consequential alarms caused by a major pump trip Logic that blocks a low discharge pressure alarm for a pre-set time interval after the pump has received a start signal, to allow time for the pump to start and establish pressure

Technique	Example
State-based	Logic or "cutouts" that prevent alarms from occurring when there is a change in the operating mode of a piece of equipment – for example, preventing alarms that otherwise would occur unnecessarily when a pump is shut down intentionally or placed in standby
System or Function Level	
Event-based	Suppression of consequential alarms caused by a system start-up or actuation
State-based	Logic or "cutouts" that prevent alarms from occurring when there is a change in a system's operating mode or state – for example, preventing alarms that otherwise would occur unnecessarily when the system is lined up for testing, or for back-flushing
Plant Level	
Event-based	Suppression of consequential alarms caused by a plant event such as a reactor or turbine trip
State-based	Plant mode-based logic that prevents or suppresses alarms that otherwise would occur unnecessarily when the plant is in cold shutdown or other non-power operation mode
Significance-based	Suppression of lower-priority alarms in situations when many alarms occur, where priority has been assigned on a plant-wide basis

These fundamental techniques for alarm reduction can be applied in a number of ways to reduce alarm overload and assist the operators in assimilating and responding to alarms. For example, the alarm reduction techniques can be used to:

- Prevent or filter out the alarms determined by the reduction logic to be unnecessary. In this case the alarms are not presented and they are not available to the operator.
- Suppress the alarms so that a reduced set of alarms is presented, but retain the suppressed alarms and make them available on demand so they can be accessed by the operating crew if desired.
- Highlight the important alarms (those that are not affected by the logic) or mute those that are determined to be less important, retaining all information but providing the operator a means of distinguishing between the two categories of alarms.
- Change the priority of the affected alarms – often referred to as "dynamic prioritization" or setting dynamic priorities.
- Change setpoints for alarms on process variables – often referred to as "dynamic setpoints."

A Note about Event-Based and State-Based Methods

Event-based and state-based techniques tend to overlap. For example, logic that is triggered on a pump trip might address the same alarms and produce the same results as logic that is based on the current operating mode of the pump – when it trips, it changes from operating to nonoperating state. However, there can be some important differences, and this is why they are described separately here. One potential difference is in time dependency of the suppression. Event-based suppression may be time-limited – for example, suppression of alarms that are caused by temporary excursions of process variables beyond their normal alarm setpoints. Some event-based suppression may need to be reset by the operator after the post-event transient has subsided, in order to re-enable alarms that may be valid again some time after the event. If the triggering signal is a trip signal, the suppression may be removed when that signal is reset – this should be considered when the suppression scheme is designed.

Another potential difference is in how the suppression logic and affected alarms are identified. Event-based alarm suppression can be designed semi-empirically by observing what happens in an event (simulated or actual), identifying alarms that are activated, determining which of these are unnecessary after the event, and setting up logic to suppress them. State-based logic is more structural in nature – it would typically be based on analysis of the system or equipment and its operating modes and determining a priori which conditions represent valid alarms in each of the various states. This is best done when the alarms are initially defined, but it can be implemented later as a design improvement.

Use of state-based logic is a more rigorous approach. If the logic that is devised is based on known physical relationships among the components and processes and it is appropriately verified and tested, it will apply broadly to many situations encountered in plant operation (not just in those events that were anticipated). As a result, it can provide a smarter and more robust alarm set that is much less likely to produce nuisance alarms. Of course, the development of this logic requires more effort. Also, if the logic or cutouts are such that they completely prevent the alarms from occurring in the pre-defined states, then there is some risk that an unanticipated situation will occur in which an alarm is masked by the logic when, in fact, it needs operator attention. The logic design needs to be well thought out and verified with input from engineering and operations.

A Note about Plant Mode-Based Suppression

U.S. nuclear plants have a defined set of operating modes. The Standard Technical Specifications define standard plant modes for each of the different reactor types. For example, PWRs typically have six modes:

1. Power operation (>5% thermal power)

2. Startup (critical, ≤5% thermal power)

3. Hot standby (sub-critical but coolant at or near operating temperature)

4. Hot shutdown (hot but below operating temperature)

5. Cold shutdown (cold but reactor vessel head secure)

6. Refueling (reactor vessel head removed)

These are approximate descriptions – the plant's Technical Specifications define the specific conditions and thresholds that define transitions from one mode to another. These are typically tied to the plant's operating procedures, and the plant management or operating crew makes the decisions as to when each mode is entered.

Alarm reduction schemes based on plant mode can be very effective in reducing the number of extraneous alarms that are active when the plant is not at power, particularly during shutdown. Many of the more advanced alarm systems that have been implemented, as well as a number of systems at operating U.S. plants, have employed some level of mode suppression effectively and operators have been very receptive to this method of alarm reduction.

It should be noted that if the mode suppression scheme is based only on the steady-state operating modes defined by the plant's technical specifications, this type of suppression may not contribute substantially to reducing the number of alarms that occur in plant upsets or transients. However, it can be expanded to address these situations. One way to do this is to define a "post-trip" operating mode. This is illustrated in Figure 5-1. Note that it may be beneficial to define additional modes, including sub-modes of the standard technical specification definitions, to more closely match up with the plant's operating procedures and practices.

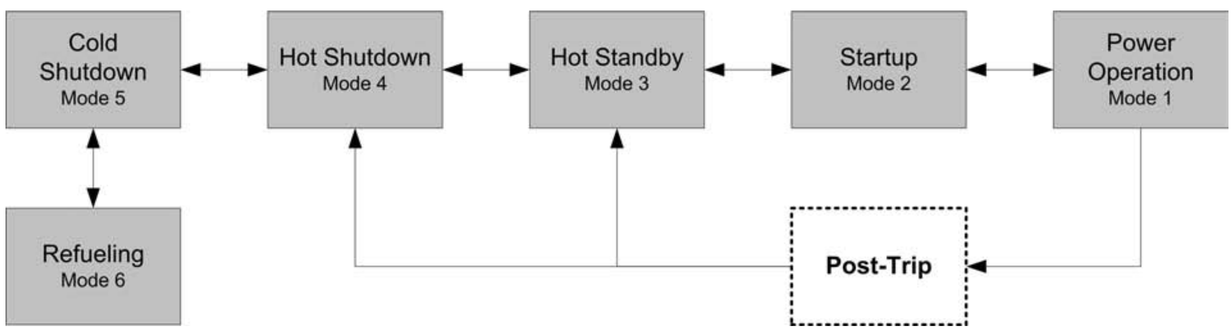

Figure 5-1
Expanded Definition of Plant Modes to Include Post-Trip State

Whereas other mode changes may require the operator to provide inputs manually to the computer system or alarm system that implements mode suppression, entry to the post-trip mode can be triggered automatically by the occurrence of a valid trip signal. This allows post-trip alarm suppression to start immediately following the trip. Post-trip alarm reduction is discussed in more detail in Section 6 using actual post-trip data from a plant as an example.

Effectiveness of Alarm Reduction Techniques – Simulator Data Evaluation

In a previous EPRI study, the effectiveness of several of the fundamental alarm reduction techniques was studied using alarm transient data from simulators at three operating U.S. plants (MPR-1482). All three plants were PWRs with conventional control rooms. At two of these plants the full-scope simulators were able to provide time-tagged alarm sequence data printed using the sequence-of-events capability of the annunciator system. For one plant, the simulator did not have the capability to provide alarm sequence printouts; in that case, "snapshots" of the annunciator alarm tiles were recorded at several intervals during transients using the simulator "freeze" feature.

Simulator Alarm Data

Transient alarm data were obtained for a total of 20 events from the three plant simulators. Table 5-2 indicates the transients for which data were obtained for each plant.

Table 5-2
Alarm Transient Data Obtained from Three Plant Simulators

Transient	Plant A	Plant B	Plant C
Manual reactor trip	X	X	X
Steam generator tube leak	X	X	X
Small-break loss of coolant accident (with reactor trip and high-pressure safety injection)	X		X
Loss of offsite power	X		X
Large-break loss of coolant accident (with reactor trip and low-pressure safety injection)	X	X	X
Feedwater line break	X		X
Steam line break inside containment	X		X
Steam line break outside containment			X
Small reactor coolant system leak (no reactor trip or safety injection)	X		
Manual reactor trip with a stuck-open safety relief valve			X

Alarm Reduction Techniques Evaluated

The alarms that were activated in each of these transients were evaluated to identify candidates for reduction using the following techniques from Table 5-1.

Time Delay Filtering

Alarms that fluctuated around a setpoint value, activating and clearing the alarm many times, were identified as candidates for time delay filtering. It was found that in most cases a delay of five seconds (on actuation or clearing of the alarm) was adequate to prevent the repeated occurrence of these alarms. It should be noted that this type of behavior may not be very accurately represented on the plant simulator for some alarms, depending on the fidelity of the simulation. Also, the effectiveness of this alarm reduction technique tends to be plant-specific as it depends on the specific behavior of plant variables during transients and the alarm setpoint values used. Another caution is that any time delays applied must be such that the operators still receive sufficiently timely notification of alarms that they can take the appropriate actions within the required time. However, based on review of actual plant alarm histories and discussions with operators, it is clear that in many plants there are alarms that could benefit form this type of alarm filtering.

Severity-Based and Redundant Alarm Suppression

Review of the transients identified a number of multi-setpoint alarms on process variables and alarms from multiple redundant sensors or channels of instrumentation that were candidates for suppression using, respectively, severity-based or redundant alarm type suppression.

Event-Based Suppression

The transient alarm sequences for each plant were reviewed to identify alarms that were common to two major plant events: reactor trip and safety injection actuation. Alarm response procedures were used where needed to help determine which of these were expected after the event and did not require any operator response.

Results of Effectiveness Evaluation

A computer simulation was developed specifically for the purpose of evaluating and demonstrating the effectiveness of the alarm reduction techniques. The simulation allowed each transient to be “replayed” with any one or a combination of the four reduction techniques applied. The resulting alarms were displayed on a VDU in a manner similar to the way that alarm message lists are displayed by microprocessor-based annunciator-driven or plant computer-driven VDUs. The reduction in the number of alarms was quantified for each case, allowing evaluation of the effectiveness of each individual reduction technique and the reduction obtained when all of the techniques were used together.

In addition, using the special-purpose simulator, VDU presentations of the alarms both with and without alarm reduction were demonstrated to licensed operators at each plant to allow informal evaluation of the alarm reduction schemes. The reduced set of alarms was presented as the primary alarm display. A “secondary” or suppressed alarm display also was available to the operators and could be called up with a single keystroke. This allowed the operators to examine the effectiveness of the reduced alarm list in aiding their assimilation of the alarm information and understanding of the event in progress, while still providing access to all alarm information if needed.

Finally, as part of the operator demonstrations, “maverick” alarms were added to alarm sequences for several of the events. These are alarms that are unrelated to the primary transient, simulating a situation in which a secondary malfunction occurs that generates one or more alarms within the flood of alarms occurring due to the main event. This allowed the operators to assess effectiveness of alarm reduction in improving the detection of secondary malfunctions.

The results obtained from the quantitative evaluation and the operator demonstrations are summarized below.

Quantification of Alarm Reduction

Table 5-3 shows the results obtained with all of the suppression techniques applied simultaneously to the transients from Plant A. Table 5-4 and Table 5-5 provide the same results for Plants B and C, respectively. The tables indicate the total number of alarm events for each transient, where alarm events include both incoming (new) alarms and alarms returning to normal (clearing). The table also indicates the number of non-clearing alarms – how many alarms remain in the alarm state after several minutes into the transient. Note that this would be the number of standing messages on a screen that displays an alarm message list, after all return-to-normal alarms have been acknowledged (reset). For each transient, data are provided for the base case of no alarm reduction and the case in which all four reduction schemes are applied.

The results show that significant reduction can be achieved for many of the transients analyzed. In most cases the number of non-clearing alarms can be reduced to a number that is much more manageable than the base case with no reduction applied. The number of non-clearing alarms is indicative of the length of an active alarm message display after the first few minutes of the transient.

The greatest percentage reduction occurs for the manual trip, primarily because this relatively uncomplicated event is addressed directly by the event-based suppression scheme. The reduction schemes were considerably less effective on the loss of offsite power events. This is in large part because no effort was made to apply event-based or state-based logic to the electrical distribution system or electrical upsets, as that would have required more detailed investigation of the electrical systems that was beyond the scope of the project. However, a conclusion from the study was that application of event-based or state-based approaches would be particularly effective for the electrical distribution system and such reduction methodologies should be considered for electrical upsets (MPR-1482).

Table 5-3
Results of Applying All Four Alarm Reduction Techniques – Plant A[3]

<table>
<tr><th rowspan="3">Transient</th><th colspan="2" rowspan="2">Without Reduction</th><th colspan="3">With All 4 Reduction Schemes Applied</th></tr>
<tr><th colspan="2">Percent Reduction</th><th rowspan="2">No. of Non-Clearing Alarms[2]</th></tr>
<tr><th>Total No. of Events[1]</th><th>No. of Non-Clearing Alarms[2]</th><th>In Total No. of Events[1]</th><th>In No. of Non-Clearing Alarms[2]</th></tr>
<tr><td>Manual Trip</td><td>90</td><td>48</td><td>91%</td><td>90%</td><td>5</td></tr>
<tr><td>Small-Break LOCA</td><td>158</td><td>108</td><td>69%</td><td>69%</td><td>33</td></tr>
<tr><td>Reactor Coolant Pump Seal Leak</td><td>26</td><td>16</td><td>26%</td><td>12%</td><td>14</td></tr>
<tr><td>Large-Break LOCA</td><td>252</td><td>122</td><td>61%</td><td>48%</td><td>63</td></tr>
<tr><td>Feedwater Break Outside Containment</td><td>115</td><td>55</td><td>71%</td><td>75%</td><td>14</td></tr>
<tr><td>Main Steam Break Inside Containment</td><td>195</td><td>119</td><td>70%</td><td>73%</td><td>32</td></tr>
<tr><td>Steam Generator Tube Rupture</td><td>456</td><td>96</td><td>87%</td><td>74%</td><td>25</td></tr>
<tr><td>Loss of Offsite Power</td><td>327</td><td>113</td><td>29%</td><td>33%</td><td>76</td></tr>
<tr><td colspan="6">NOTES:
(1) Total number of events includes incoming and clearing (return to normal) alarms
(2) Total number of alarms still in the alarm state (not cleared) several minutes following transient initiation
(3) Data based on printed sequence-of-events logs from plant’s annunciator system</td></tr>
</table>

Table 5-4
Results of Applying All Four Alarm Reduction Techniques – Plant B[3]

Transient	Without Reduction		With All 4 Reduction Schemes Applied		
			Percent Reduction		No. of Non-Clearing Alarms[2]
	Total No. of Events[1]	No. of Non-Clearing Alarms[2]	In Total No. of Events[1]	In No. of Non-Clearing Alarms[2]	
Manual Trip	67	37	87%	81%	7
Large-Break LOCA	166	86	61%	57%	37
Steam Generator Tube Rupture	327	45	78%	73%	12

NOTES:

(1) Total number of events includes incoming and clearing (return to normal) alarms

(2) Total number of alarms still in the alarm state (not cleared) several minutes following transient initiation

(3) Data based on printed sequence-of-events logs from plant's annunciator system

Table 5-5
Results of Applying All Four Alarm Reduction Techniques – Plant C[3]

Transient	Without Reduction		With All 4 Reduction Schemes Applied		
			Percent Reduction		No. of Non-Clearing Alarms[2]
	Total No. of Events[1]	No. of Non-Clearing Alarms[2]	In Total No. of Events[1]	In No. of Non-Clearing Alarms[2]	
Manual Trip	63	63	85%	84%	10
Small-Break LOCA	76	76	44%	42%	44
Large-Break LOCA	111	111	44%	41%	65
Feedwater Line Break	42	42	60%	57%	18
Main Steam Break Outside Containment	84	84	52%	51%	41
Main Steam Break Inside Containment	102	102	45%	44%	57
Steam Generator Tube Rupture	72	72	52%	50%	36
Loss of Offsite Power	195	195	22%	19%	157
Stuck Open Safety Relief Valve	44	44	57%	55%	20

NOTES:

(1) Total number of events includes incoming and clearing (return to normal) alarms

(2) Total number of alarms still in the alarm state (not cleared) several minutes following transient initiation

(3) Data based on a series of snapshots of annunciator light boxes during simulator runs; no alarm clearing (return-to-normal) data were collected

Table 5-6 shows, for Plant A, the breakdown of alarm reduction effectiveness for each individual alarm reduction technique. Table 5-7 and Table 5-8 give the breakdown for Plants B and C, respectively. Figure 5-2 summarizes the breakdown of effectiveness in alarm event reduction across all three plants.

The greatest reduction is achieved with event-based suppression – this technique reduced the number of alarm events by an average of 47% across all three plants. Greater reduction could have been achieved if additional events, beyond reactor trip and safety injection actuation, were implemented in the suppression scheme. Suppression of redundant or equivalent alarms provided the next best results, reducing alarm events on average by 13% across the three plants. Severity-based suppression gave an average of 7% reduction.

Time delay filtering is much more plant-specific and alarm-specific in its ability to reduce the number of alarm events. For example, for Plant A the time delay filtering resulted in reduction rates of 0% to 67% depending on the transient. The 67% reduction of alarm events was obtained due to suppression of two particular low flow alarms that accounted for about 300 of the alarm events in that transient – a steam generator tube rupture. Time delay filtering reduced the alarm events for Plant B by an average of 23%. The average reduction for transients across Plants A and B was about 15%. The time delay technique could not be applied to Plant C because of the lack of clearing alarm information.

Table 5-6
Alarm Reduction Effectiveness by Type of Reduction – Plant A(1)

Transient	Alarm Reduction Technique			
	Time Delay Filtering	**Severity-Based Suppression**	**Redundancy Suppression**	**Event-Based Suppression**
Manual Trip	4%	9%	13%	97%
Small-Break LOCA	3%	9%	8%	65%
Reactor Coolant Pump Seal Leak	0%	6%	26%	0%
Large-Break LOCA	14%	7%	10%	40%
Feedwater Break Outside Containment	7%	10%	15%	64%
Main Steam Break Inside Containment	2%	8%	14%	63%
Steam Generator Tube Rupture	67%	3%	7%	20%
Loss of Offsite Power	1%	4%	8%	24%

NOTE:

(1) All values given are in percent reduction of alarm events (incoming and clearing alarms). The sum of the reduction percentages for individual schemes does not equal the overall reduction when using all schemes because there is overlap among them – an alarm may be suppressed by more than one scheme.

Table 5-7
Alarm Reduction Effectiveness by Type of Reduction – Plant B[1]

Transient	Alarm Reduction Technique			
	Time Delay Filtering	Severity-Based Suppression	Redundancy Suppression	Event-Based Suppression
Manual Trip	27%	1%	6%	90%
Large-Break LOCA	17%	6%	29%	30%
Steam Generator Tube Rupture	25%	1%	15%	60%

NOTE:

[1] All values given are in percent reduction of alarm events (incoming and clearing alarms). The sum of the reduction percentages for individual schemes does not equal the overall reduction when using all schemes because there is overlap among them – an alarm may be suppressed by more than one scheme.

Table 5-8
Alarm Reduction Effectiveness by Type of Reduction – Plant C[1]

Transient	Alarm Reduction Technique			
	Time Delay Filtering	Severity-Based Suppression	Redundancy Suppression	Event-Based Suppression
Manual Trip	N/A	6%	12%	89%
Small-Break LOCA	N/A	10%	10%	33%
Large-Break LOCA	N/A	9%	13%	31%
Feedwater Line Break	N/A	9%	17%	52%
Main Steam Break Outside Containment	N/A	11%	9%	43%
Main Steam Break Inside Containment	N/A	12%	11%	35%
Steam Generator Tube Rupture	N/A	11%	11%	40%
Loss of Offsite Power	N/A	4%	7%	15%
Stuck Open Safety Relief Valve	N/A	8%	17%	52%

NOTE:

[1] All values given are in percent reduction of alarm events (incoming and clearing alarms). The sum of the reduction percentages for individual schemes does not equal the overall reduction when using all schemes because there is overlap among them – an alarm may be suppressed by more than one scheme.

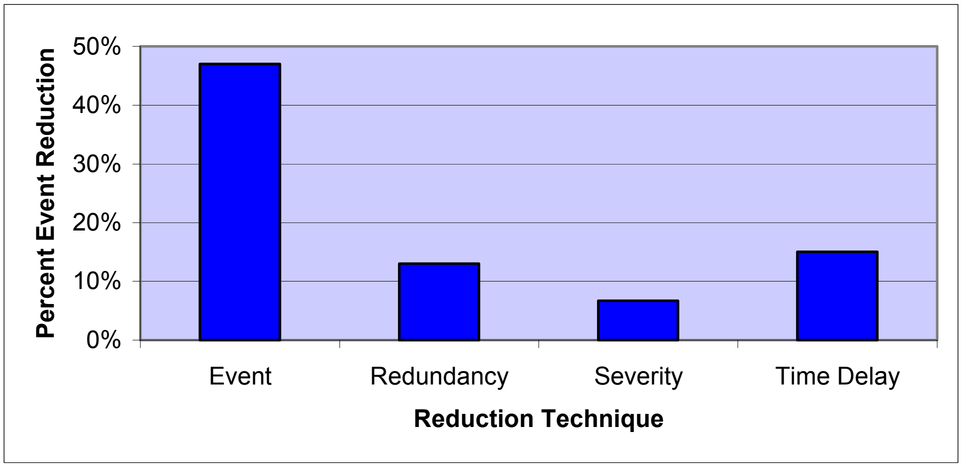

Figure 5-2
Breakdown of Effectiveness by Reduction Technique

Operator Evaluations Including Maverick Alarms

In evaluating the effectiveness of an alarm reduction scheme, it is necessary to assess the capability of the processing scheme to retain information that is considered to be important to the operators. That is, with the use of alarm reduction, the alarm system should still alert operators to conditions that require a timely operator response or are necessary to define the appropriate operator response to the upset.

As a general test of the appropriateness of the alarm suppression and ability to retain key alarm data, demonstrations were performed for licensed operators at each of the three plants. In viewing the demonstrations, the operators were asked to evaluate not only the effectiveness of the approach in reducing the number of alarms, but also whether the information presented on the reduced alarm list was adequate to diagnose the cause of the transient with all reduction schemes applied. In nearly every case, operators from each plant agreed that the information being presented was adequate and that the alarms relegated to the suppressed alarm list were appropriate. In the few cases where the operators were unable to determine the cause of the transient from the reduced alarm list, the operators were still unable to identify the cause when the suppressed alarm information was reviewed. The operators felt that their inability to diagnose the cause of the transient was not due to the reduction of alarm information; rather, they felt that there was simply not enough information in the alarm data to evaluate the cause.

Demonstrations also were performed to illustrate the alarm system performance given the occurrence of “maverick” alarms during a transient. A maverick alarm is an alarm that is unrelated to the primary transient, but indicates a secondary malfunction occurring in the course of the main event. In previous EPRI testing, it was found that providing an alarm message list display that showed only those alarms that do not normally occur after a trip improved the operators’ detection of maverick alarms (EPRI NP-5693P). One objective of the operator demonstrations conducted in this study was to investigate whether this result might be expected to hold true for the alarm reduction schemes evaluated for these three plants.

To demonstrate the performance of the reduction schemes with maverick alarm occurrences, alarms that were unrelated to the primary transient were added to the alarm sequences for several of the events that were demonstrated to the operators. In each case, it was found that the maverick alarms appeared on the reduced alarm list (they were not suppressed). As would be expected, because there were fewer alarms presented using the reduction techniques the operators found that the maverick alarms were more easily identified using the reduced alarm list than when no alarm reduction was applied.

In general, the demonstrations were very useful in eliciting operator opinions on the alarm reduction techniques and their effectiveness. Several conclusions were drawn from the operator evaluations:

- The operators from each plant agreed that the alarm reduction schemes evaluated in this study are relatively straightforward and appropriate for reducing the number of alarms presented during plant transients.
- In general, operators agreed that the alarms that were suppressed (considered less important and placed on a secondary display that could be accessed on demand) were appropriately chosen, and that all important information was correctly assigned to the reduced (unsuppressed) alarm list. Further, in most cases the operators believed that the reduction in alarms would contribute to a quicker and better diagnosis of off-normal transients and upsets.
- There was a consensus among operators regarding the method used in presenting the suppressed alarms. Operators were decidedly against using alarm reduction to completely eliminate alarms; presentation of the suppressed alarms on secondary displays that could be selected by the operators was generally well received.
- Operators liked the capability of the reduction schemes to retain and highlight maverick alarms on the reduced alarm list.

NRC Study of Alarm Reduction

Brookhaven National Laboratory performed a study for NRC to examine the effects of alarm processing and alarm display methods on operating crew performance (NUREG/CR-6691). As part of this study, several alarm reduction techniques were applied to the alarms in a full-scope plant simulator. The amount of alarm reduction achieved was determined for two levels of processing:

- The first level of processing suppressed alarms that indicated only status information (thus were not valid alarms requiring action), and alarms that were expected or irrelevant for the current plant mode or plant systems' state (state-based suppression at the plant and system level). Time delay filtering was applied to eliminate repeating alarms or alarms due to momentary fluctuations. This level of processing achieved a 50% reduction in the number of alarms compared to the baseline (no alarm processing).
- The second level included all of the first-level reduction techniques, and added severity-based suppression (addressing multi-setpoint alarms) and alarms resulting from other cause-consequence relationships. This level achieved a 75% reduction in the number of alarms compared to the baseline (no alarm processing).

A detailed comparison of the alarm sets, suppression schemes and test scenarios has not been performed. However, it can be seen that these results are generally similar to the results of the EPRI evaluation described above. Both studies support the conclusion that substantial alarm reduction can be achieved using the techniques shown in Table 5-1.

Interaction with Prioritization and Presentation

Methods used to prioritize alarms and to display alarm information have a significant effect on the operators' ability to deal with large amounts of alarm information. Also, the effectiveness of alarm reduction techniques in some cases depends on how the alarms are prioritized and presented.

Prioritization

Many plants have assigned a priority to the alarms presented in the main control room. The priority levels typically relate to how quickly the operators need to respond to the alarm and its significance to plant operation and safety. The highest-priority alarms, those that require the most prompt action or are of greatest significance or risk to the plant, are presented in a way that the operators can focus on these first, and then later deal with the lower-priority alarms. On fixed-position displays such as annunciator tiles this can be done using color or (less common) special flash rates. On message lists, alarms often are ordered according to priority so that the highest-priority alarms are in a segregated area or at the top of the list such that they do not scroll off the screen when many lower-priority alarms occur.

Alarm priorities are typically assigned on a global, plant-wide basis. Thus, decisions must be made as to the relative priority compared to all other alarms. This is straightforward for some alarms, but for many it is difficult to assign priorities "a priori" because the importance or urgency depends on what other conditions are occurring, the state of the associated system or the plant mode, and other dependencies.

Priority itself can be used as a basis for alarm suppression. As shown in Table 5-1, it can form the basis for "significance-based" suppression. For example, in an upset a display can be produced that shows only the highest priority alarms and suppresses those of lower priority (making them available only if requested). In fact, many of the alarm reduction schemes can be viewed essentially as another form of alarm prioritization – that is, the suppressed alarms are relegated to a lower priority status and not shown on the primary display. So, for example, alarms that are considered to be normal occurrences following a trip can be suppressed (categorized as lower priority), and the unusual alarms presented as potentially more important to the operators after the trip occurs. It can be seen that prioritization and alarm suppression are closely linked. The design and evaluation of alarm reduction techniques should include consideration of any other alarm prioritization schemes that are currently in use or being considered. The operators should not be confused as to which alarms they are to focus on.

Presentation

In addition, the method of presenting alarms should be considered when designing or implementing alarm reduction schemes. Some reduction techniques are appropriate for some alarm presentations and not for others. For example, consider severity-based alarm suppression. Alarms on an analog variable are suppressed when an alarm indicating a more severe condition occurs (e.g., suppress LEVEL LO when LEVEL LO-LO occurs). This can be effective for alarm message lists because it reduces the number of messages the operator must deal with and (assuming the suppressed alarms are available on a separate display) not deprive the crew of any useful information (it is obvious that if level is LO-LO, it is also LO).

However, if both of these alarms are presented on conventional light boxes as tiles with fixed alarm legends, suppressing the LO level alarm can potentially be misleading. Operators tend to use fixed alarm tiles as indicator lights – a quick glance can determine whether the level is low or it is not. If the tile is dark, but only because a separate LO-LO alarm is activated, the operator may be misled or confused by the lack of the LO level alarm. Also, alarms of different severities are often placed in a hierarchy (e.g., ordered vertically) on the light boxes, so that as the condition worsens the tiles visually indicate this by the number and placement of lighted windows. Thus there are tradeoffs involved in implementing alarm suppression logic for these displays.

There are other display methods that can be used to address this. For example, a computer-generated light box type display can use variable messages on the simulated tiles, as opposed to the fixed alarm legends engraved on conventional annunciator windows. The message can indicate the current level of severity of the alarm. If the operators are fully trained on this system, they will understand that the severity must be determined from the message and not from its position in the array.

Use of Prioritization and Presentation to Address Overload

Some designs use prioritization and presentation as the primary means of dealing with alarm overload. For example, the alarm system design for an advanced boiling water reactor (ABWR) implemented in Japan uses a hierarchy of alarm displays and a somewhat different prioritization scheme to address the problem. Important plant-level alarms are indicated on an array of large, fixed-position tiles visible to the entire crew. System-level alarms are presented on fixed tiles arrayed above a large overview mimic of the plant, positioned near the associated system information displayed in the mimic. Component-level alarms are shown on VDU displays in a fixed-position format; these detailed alarms are accessed via a system-level menu structure. Each system-level alarm is assigned to one of three categories: fatal failure (system has failed), minor failure, and system status change. This within-system prioritization is indicated by color coding applied to the system-level tiles.

An objective of this design is to provide the operators with a hierarchy of information that allows them to progress from the plant level down to lower-level information, using the plant-level alarms, the mimic display and the prioritized system-level alarms to direct their attention to what is most urgent in situations when many alarms occur. A key element of this approach is the categorization of system-level alarms to indicate whether a system has failed or has only minor problems. No sophisticated alarm processing or reduction schemes are used in this design.

More Advanced Alarm Processing Systems

While the focus of this report is on relatively simple and straightforward approaches to alarm reduction, more advanced alarm processing systems that have been developed should also be mentioned. NUREG/CR-6684 and HSE CRR-166 provide good overviews of a number of alarm processing systems. Many of these make use of alarm prioritization (static and dynamic) and various alarm presentation schemes as discussed above. Others use more complex alarm processing methods that go beyond the fundamental techniques listed in Table 5-1. Two examples are described briefly below to illustrate some of the more advanced methods.

Adjustable Alarm Reduction Based on Static and Dynamic Prioritization

The Alarm Processing and Diagnostic System (APDS), developed in conjunction with EPRI research, uses a combination of static and dynamic prioritization in a “filter” that adjusts automatically depending on how many alarms are occurring (EPRI TR-100838). Alarms are presented in a message list, and the filter attempts to keep the length of the list at no more than one screen full. APDS groups all alarms by plant system and then prioritizes each alarm based on its importance to the associated system. A matrix is used to assign the within-system static priority based on several factors, including: whether the alarm condition is at the system, equipment or component level; whether the alarm condition has a direct or indirect effect on operational status of the equipment or system; and how quickly the operator must respond to the condition.

In addition, each plant system is assigned a dynamic priority based on the current plant operating mode. For each mode, the dynamic priority indicates whether the system is critical to that mode of operation, is a support system or in a standby role, or is unrelated to operation in that mode. Another matrix is used to assign a final, composite priority ranking to each alarm based on the alarm’s static priority and the system’s dynamic priority – alarms are given one of four different final priorities (see EPRI TR-100838 for details).

APDS also applies alarm reduction logic in some special cases. For example, equipment-level state-based logic is used in some cases to prevent occurrence of alarms that are irrelevant under certain conditions of equipment operation. This is similar to the state-based logic described in Table 5-1.

APDS uses the final priority ranking to set different levels of filtering. When only a few alarms occur there is no filtering – all alarms are presented. As greater numbers of alarms occur, alarms of lower rankings are successively filtered out with the goal of maintaining the total number of alarms below a preset threshold. The threshold typically would be set equal to the number of alarm messages that fit on one screen or display page.

This approach tries to place each alarm in context by considering its impact on the proper functioning of the system to which it belongs. This is similar to the prioritization scheme described above for the ABWR alarm system. However, APDS goes further by also considering the importance of the system to the current mode of plant operation. It applies filtering automatically based on the result, whereas in the ABWR system the operators choose where to focus their attention based on the plant-level and prioritized system-level alarms.

The effectiveness of APDS was evaluated using alarm data from a plant simulator (MPR-1396) following methods very similar to those described above for the fundamental alarm reduction techniques. It was found that the system was effective in automatically applying successive levels of filtering to the alarms such that the number of alarms was maintained close to the target of one screen full. However, evaluation of the results by plant operators showed that on average about 30% of the alarms there were filtered out by APDS should be retained as they might be important in the short term for determining status of the plant or major systems, or for diagnosing the cause of the transient.

Also, the operators concluded that about half of the alarms that were not filtered (thus were displayed in the list) could have been suppressed. They were considered to be unimportant in the short term. Many of these were normal consequences of the event (e.g., expected post-trip alarms). Finally, when "maverick" alarms were inserted in the scenarios, it was found that while APDS displayed these alarms in some cases, in others it filtered them out due to their lower priority.

The APDS prioritization is based on prioritization within systems, and criticality of systems to plant operating modes. It is not event-based. Thus, it does not necessarily retain alarms that are "unusual" for the current event. A conclusion from the evaluation was that incorporating a form of event-based suppression into APDS could be beneficial. Also, it was concluded that the alarms that APDS filters out should be made available on demand to the operators.

State Model Approach

Several of the fundamental techniques identified in Table 5-1 use knowledge of equipment and system states to place alarms in context. State-based logic at the system level prevents alarms from occurring that would be normal for certain system states. Plant mode-based logic does the same for alarms that would be expected for certain plant operating modes.

This can be formalized in a more structured approach that models the states of equipment, systems, and the overall plant and determines what conditions are expected or unexpected (abnormal or failed) for those states. These can be built into a "state model" that includes interdependencies between systems and the overall plant states. The states can represent both physical configuration (e.g., different valve lineups or operating pump configurations) and operational status of the systems (e.g., on standby and available, unavailable, operating in normal configuration, operating in backup configuration, etc.). In fact, when trying to place alarms in context for the operators, operational states can be more meaningful than physical states. Physical states can be inputs to determining the operational states.

A processing system that is based on state models can include modeling of transitions between states. So, for example, when a condition occurs indicating that a system has tripped (moved out of the operational state), the model can incorporate the expected transition to the next state and thus have knowledge of the conditions that are expected for the system during and after the transition. This helps categorize conditions and events according to whether they are expected occurrences, or they are unexpected and potentially important off-normal conditions.

At least one vendor has incorporated state-based modeling into a software system intended to provide context-based alarm management. This type of system is a logical extension of the fundamental techniques described in Table 5-1, taking them to a more complete and rigorous level of implementation.

State-based modeling also can provide predictive capability by monitoring changes in conditions and predicting when a system will reach a point at which it will transition from one state to the next (e.g., monitor a critical variable and its rate of change and predict when it will reach a trip point). Warnings can be generated to help operators attend to these conditions before they create an upset in the plant. Of course, such warnings must be designed with care. False alarms could contribute to nuisance alarming and add to the alarm overload.

Effect of Alarm Reduction on Operator Performance

Because alarm overload occurs at a very busy and potentially stressful time for the operating crew, it should be expected that substantially reducing the number of alarms and making them more useful to the crew would provide significant benefits. For example, alarm reduction should:

- Reduce distractions for the operators caused by the many alarms occurring, potentially improving performance on other tasks such as following abnormal or emergency operating procedures, diagnosing and responding to the event at hand, and responding to other situations that arise during the upset.
- Reduce the amount of time required to go through the alarms to identify those that are important and require action or that may impact the operator’s response to the event.
- Improve the ability to detect in a timely fashion any alarms that indicate secondary malfunctions or problems that may occur during the transient.
- Increase the operator’s ability to use the alarm information to help understand the event and the status of plant systems and equipment, and in general maintain good situation awareness.

Unfortunately, it is very difficult to quantify these potential effects on operator performance. The alarms are only one factor among many others that influence overall performance, including other parts of the human-system interface (HSI) such as displays and controls, operator experience and training, the particular event or scenario, and the operators’ ability to adjust their monitoring strategies depending on the situation and to compensate if necessary for shortcomings in the HSI design. This was borne out in a recent NRC study that tested operator performance with different levels of alarm reduction (NUREG/CR-6691). Tests were run with experienced operators in a full-scope simulator using a number of representative scenarios. The types of alarm processing that were tested included time delay filtering, suppression based on plant mode and system states, severity level (multi-setpoint alarms), and other cause-consequence relationships. The alarm processing reduced the number of alarms by 50-75%. Different alarm presentations also were studied, including fixed tiles, message lists, and alarms integrated into process mimic displays. Operator performance was measured by assessing performance on specific tasks, overall plant performance during the scenarios, and operator cognitive processes (situation awareness and cognitive workload).

The test results did not show significant differences in operator performance with different levels of alarm reduction. However, operator ratings of the alarm processing schemes and the comments they provided indicated that the operators responded positively to alarm reduction. After testing multiple levels of alarm processing, they preferred the processing scheme that achieved the maximum level of alarm reduction (75%). The alarm processing made it easier to identify and understand the important alarms, and it did not take away any meaningful information. See NUREG/CR-6691 for more details.

Previous testing performed by EPRI included a limited evaluation of the effect of post-trip alarm reduction on operator performance in assimilating alarm information, and in using the alarms by themselves to attempt to identify and diagnose malfunctions during plant upsets (EPRI NP-5693P). The tests showed that alarm reduction significantly improved the operators' ability to identify alarms that indicated possible secondary malfunctions and were considered important in the flood of alarms accompanying plant upsets. There was a statistically significant difference in the number of these "maverick" alarms that were detected by the operators when the normal or expected post-trip alarms were removed from message lists presented on VDUs.

As demonstrated in both the NRC and EPRI studies, operators are able to achieve high performance levels even when faced with floods of alarms. However, there is plenty of evidence from research studies and experience indicating that reducing the alarm floods and making the alarm information more usable in plant transients can reduce operator workload and distraction in critical situations, and reduce the risk that information will be missed that could be important to plant economics and safety.

Alarm Management Tools

As discussed in Section 3, a number of third-party software products have been developed to assist with alarm management (e.g., Mostia 2003, Rothenberg 2003, Swanekamp 2003). These have been applied primarily in the process industries, and to an extent in fossil power plants. Some of the features these products offer are more applicable to the operating situation in process plants, where changes in the process often occur on a daily or hourly basis as the plant's products and processing routines change, different batch operations are conducted, etc. However, there are features of these software tools that may helpful to nuclear plants in monitoring the alarm system's performance and identifying improvements in alarm management. Cost effectiveness of the tools will need to be evaluated on a case by case basis.

The following features may be of interest – note that these are only examples, and the vendors continue to improve and add functionality to the tools:

- Interface to gain access to real-time alarm data – some relatively inexpensive tools are available that provide interfaces to essentially all the major DCS systems so that alarm data can be accessed for separate processing, analysis, and display. For example, alarm data can be made available in a standard format that allows viewing and analysis using standard tools such as a spreadsheet.

- Alarm system performance metrics – some tools monitor the real-time alarm data stream and measure the performance of the system based on predefined metrics. The metrics include characteristics such as incoming alarm rates, standing time for alarms (how long they remain in the alarm state), alarm counts by point/ID, etc. These can be used for benchmarking and examining performance differences after improvements are made.
- Identification of chattering alarms
- Identification of relationships among alarms – for example, identifying patterns such as certain alarms always occurring after another alarm occurs, possibly indicating a cause-and-effect relationship with the first alarm.

6
POST-TRIP ALARM REDUCTION

Plant trips, which include trips of both the reactor and the turbine-generator, are a major contributor to the alarm overload problem. An uncomplicated trip, when it occurs by itself (e.g., a manual reactor trip), generates many alarms. Also, most other major plant upsets and accidents typically involve a trip, so post-trip alarms contribute to alarm overload in many of the transients the plant may encounter.

In order to provide an illustration of the alarm overload problem and the typical contributors to overload using real alarm data, and to evaluate possible simplified methods for reducing the overload, alarm histories from actual plant trips were obtained from several operating plants and evaluated as part of this study. The use of microprocessor-based annunciator systems with sequence-of-events recording capability at these plants allowed the alarm histories to be obtained relatively easily from archived, time-stamped alarm data. Two plants, one a PWR and the other a BWR, were each able to provide alarm histories from three different trips at the same site. This allowed an evaluation of the data across multiple trips, identifying alarms that typically occur and would be expected as consequences of a plant trip.

PWR Trip Alarm Histories

Table 6-1 provides some summary data regarding the alarm histories from the PWR plant. Two of the trips were from full power, and one was from a reduced power level. The data shown in the table are based on analysis of incoming and clearing alarms received during a time period from just before each trip to about 10-12 minutes after the trip. Alarm data files covering this time period were imported into an Excel spreadsheet and macros were written to analyze the data across all three trips, identifying common alarms (those occurring in more than one of the trips), and generating the descriptive data shown in the table. Note that plant computer alarms are not included; the data include only the alarms that are presented on the annunciator system, which is the primary source of alarm information for the operators in the conventional control room at this plant.

The plant has 445 annunciator alarms. About 125 of these were activated in the full-power trips. Fewer alarms (on the order of 70) were activated in the trip from a reduced power level. As shown in the table, over 50 alarms were common to all three trips. A similar number were common to two of the three trips, but did not appear in all three. Many of these occurred in both of the full-power trips but did not actuate in the trip from a reduced power level. Trips from lower power levels do not cause as much of an upset to the plant process as does a full-power trip. The total number of alarms activated across all the trips was over 150, more than a third of the installed annunciator alarms.

Table 6-1
Analysis of Three Reactor Trip Alarm Histories at a PWR Site[(1)]

Trip No.	Nature of Trip	No. of Alarm Events[(2)]	No. of Unique Alarms[(3)]
1	Manual reactor trip from 100% power due to coolant pump problem	316	124
2	Automatic reactor trip from 27% power due to control problem during power ascension	127	69
3	Automatic reactor trip from 100% power due to generator trip caused by an equipment failure	334	127
Overall statistics:			
Total number of alarms (tiles) in system			445[(4)]
No. of unique alarms that occurred in all 3 trips			54
No. of unique alarms that occurred in only 2 of the 3 trips			56
No. of unique alarms that occurred in only one of the 3 trips			46
Total number of unique alarms activated (across all 3 trips)			156

NOTES:

(1) These data are from a two-unit plant. Two of the trips occurred in one unit and the third occurred in the other unit. Because the alarms are nearly identical between units, for the purpose of this study the analysis was performed across all three data sets without regard to which unit was affected.

(2) Alarm events include both incoming and clearing (return to normal) alarms. An alarm that comes in and then clears within the time frame creates two events. An alarm that chatters or repeats 5 times (comes in and out 5 times) generates 10 events.

(3) This is the number of unique alarms that occurred any time during the time interval (regardless of whether they returned to normal or how many times they occurred). It represents the number of alarms that participated in the event.

(4) This is for a single unit and does not include alarms on equipment shared between the two units.

Examination of Common Post-Trip Alarms

Table 6-2 lists the alarms that occurred in at least two of the three trips described in Table 6-1. There are 110 of these alarms. The table indicates the number of times each alarm occurred in each of the three trips. The time at which each alarm first occurred is shown as a range, from minimum to maximum. This provides an indication of how repeatable the pattern of alarms is, and which alarms occur earlier or later in the 10-12 minute time period that was analyzed. This information also could be used to determine when alarms that are expected following a trip do not occur. Detection of missing alarms is discussed further below.

Table 6-2
Alarms Occurring in at Least Two of the Three Trips (Core Alarm Set)

Sheet 1 of 3

Alarm ID	Alarm Message	Frequency of Occurrence			First Occurrence Time Range*
		Trip 1	Trip 2	Trip 3	
8--11	E-B8 MAN RX TRIP	1	1	1	0 --> 8
8--8	E-A8 RX TRIPPED BY TURB TRIP	1	1	1	0 --> 1
8--9	E-A9 RX TRIP BKRS OPEN	1	1	1	0 --> 1
9--16	F-A4 RX TRIP CH 1 AUTO STOP OIL DUMP	1	1	1	0 --> 1
9--17	F-A5 RX TRIP CH 2 AUTO STOP OIL DUMP	2	2	1	0 --> 1
9--18	F-A6 RX TRIP CH 3 AUTO STOP OIL DUMP	1	1	1	0 --> 1
8--39	E-C6 RX TRIP CH 1 OT DELTA T LOOP 1A	1	0	1	1
8--40	E-C7 RX TRIP CH 1 OP DELTA T LOOP 1A	1	0	1	1
8--42	E-D6 RX TRIP CH 2 OT DELTA T LOOP 1B	1	0	1	1
8--43	E-D7 RX TRIP CH 2 OP DELTA T LOOP 1B	1	0	1	1
8--45	E-E6 RX TRIP CH 3 OT DELTA T LOOP 1C	1	0	1	1
8--46	E-E7 RX TRIP CH 3 OP DELTA T LOOP 1C	1	0	1	1
10--18	G-F3 OT DELTA T TURB RNBK & ROD STOP CH 1	1	0	1	1
10--19	G-F4 OP DELTA T TURB RNBK & ROD STOP CH 1	1	0	1	1
10--26	G-G3 OT DELTA T TURB RNBK & ROD STOP CH 2	1	0	1	1
10--27	G-G4 OP DELTA T TURB RNBK & ROD STOP CH 2	1	0	1	1
10--34	G-H3 OT DELTA T TURB RNBK & ROD STOP CH 3	1	0	1	1
10--35	G-H4 OP DELTA T TURB RNBK & ROD STOP CH 3	1	0	1	1
8--14	E-C8 OP DELTA T	1	0	1	1
8--17	E-D8 OT DELTA T	1	0	1	1
10--3	G-D4 LOWER ION CHAMBER DEVIATION OR AUTO DEFEAT < 50%	1	0	1	1 --> 2
9--59	G-C4 UPPER ION CHAMBER DEVIATION OR AUTO DEFEAT < 50%	1	0	1	1
10--5	G-D6 ROD CONT SYS NON-URGENT FAILURE	1	0	1	34
9--45	G-A6 ROD CONT SYS URGENT FAILURE	1	1	1	0 --> 1
9--61	G-C6 ROD CONT MG TRIPPED	1	0	1	34
10--33	G-H2 RPI ROD BOTTOM < 20 STEPS	1	1	1	2 --> 3
10--32	G-H1 NIS DROPPED ROD FLUX DECREASE > 5% PER 2 SEC	1	1	1	0 --> 1
6--23	C-B8 PRZR LO PRESS	1	1	1	2 --> 4
6--39	C-D8 PRZR LO LVL	1	1	1	4 --> 72
7--44	D-E5 CHG PP TO REGEN HX HI-LO FLOW	0	2	27	6 --> 131
10--43	H-A4 T AVG >< T REF DEVIATION	2	1	2	1 --> 23
10--42	H-A3 HI-LO T AVG LOOP 1A	1	1	1	32 --> 44
10--50	H-B3 HI-LO T AVG LOOP 1B	1	1	1	32 --> 45
10--58	H-C3 HI-LO T AVG LOOP 1C	1	1	1	34 --> 47
10--59	H-C4 LO T AVG TO FW CONT	1	1	1	18
11--19	H-F4 LO T AVG INTLK LOOP 1C	2	1	1	48 --> 372
11--11	H-E4 LO T AVG INTLK LOOP 1B	0	1	1	56 --> 327
11--3	H-D4 LO T AVG INTLK LOOP 1A	0	1	1	56 --> 398
8--56	F-A1 TURB TRIPPED BY RX TRIP	1	1	1	0 --> 1
8--57	F-A2 SOV TURB TRIP	1	1	1	1

* Times are in seconds after trip (minimum --> maximum)

Sheet 2 of 3

Alarm ID	Alarm Message	Frequency of Occurrence			First Occurrence Time Range*
		Trip 1	Trip 2	Trip 3	
8--59	F-B1 MAN TURB TRIP	1	1	1	9 --> 53
12--36	J-H5 TURB STOP V V CLOSED	1	1	1	0 --> 1
12--48	K-B1 GEN BKR AUX REL FAIL TURB TRIP CKT	1	1	1	0 --> 28
12--6	J-D7 GEN MOTORING TURB LO DP	2	1	0	1
1--51	T. 51 GEN PCB TURB TRIP	1	0	1	0 --> 26
12--38	J-H7 VOLTAGE REGULATOR TRIP	1	1	1	0 --> 28
11--54	J-B7 VREG LOCAL ALARM	1	1	0	56 --> 58
2--15	T. 79 UNIT ON LINE BKR 44 TRIPPED	3	2	1	0 --> 28
2--8	T. 72 UNIT ON LINE BKR 4C TRIPPED	1	1	1	0 --> 28
13--21	K-F6 4KV BUS NORM SUP BKR TRIP	1	0	1	0 --> 26
9--31	F-F4 STM GEN 1A CH 3 HI STM LINE FLOW	1	0	1	1
9--32	F-F5 STM GEN 1B CH 3 HI STM LINE FLOW	1	0	1	1
9--33	F-F6 STM GEN 1C CH 3 HI STM LINE FLOW	1	0	1	1
9--34	F-G4 STM GEN 1A CH 4 HI STM LINE FLOW	1	0	1	1
9--35	F-G5 STM GEN 1B CH 4 HI STM LINE FLOW	1	0	1	1
9--36	F-G6 STM GEN 1C CH 4 HI STM LINE FLOW	1	0	1	1
11--12	H-E5 STM GEN 1A FW >< STM FLOW	2	1	3	0 --> 1
11--13	H-E6 STM GEN 1B FW >< STM FLOW	1	3	4	0 --> 1
11--14	H-E7 STM GEN 1C FW >< STM FLOW	1	1	3	1
11--28	H-G5 STM GEN 1A LVL ERROR	1	1	1	1 --> 4
11--29	H-G6 STM GEN 1B LVL ERROR	1	0	1	3 --> 4
11--30	H-G7 STM GEN 1C LVL ERROR	1	0	1	3 --> 4
10--52	H-B5 STM GEN 1A LO LVL	1	1	4	4 --> 5
10--53	H-B6 STM GEN 1B LO LVL	1	0	1	4 --> 5
10--54	H-B7 STM GEN 1C LO LVL	1	1	1	-155 --> 4
8--28	E-G10 STM GEN LO-LO LVL	1	1	1	0 --> 6
10--60	H-C5 STM GEN 1A LO-LO LVL	1	1	2	5 --> 7
10--61	H-C6 STM GEN 1B LO-LO LVL	1	0	1	5 --> 678
10--62	H-C7 STM GEN 1C LO-LO LVL	1	1	1	-112 --> 5
14--8	F-A7 STM GEN 1A LO LVL CH 1	1	1	1	6 --> 9
14--9	F-A8 STM GEN 1B LO LVL CH 1	1	0	1	5 --> 657
14--10	F-A9 STM GEN 1C LO LVL CH 1	1	1	1	2 --> 6
14--12	F-B7 STM GEN 1A LO LVL CH 2	1	1	1	5 --> 11
14--13	F-B8 STM GEN 1B LO LVL CH 2	1	0	1	6 --> 644
14--14	F-B9 STM GEN 1C LO LVL CH 2	1	2	1	-6 --> 6
14--24	F-E7 STM GEN 1A LO-LO LVL CH 1	1	1	1	6 --> 18
14--25	F-E8 STM GEN 1B LO-LO LVL CH 1	1	1	1	-18 --> 7
14--26	F-E9 STM GEN 1C LO-LO LVL CH 1	1	1	1	4 --> 6
14--28	F-F7 STM GEN 1A LO-LO LVL CH 2	1	1	1	6 --> 22
14--29	F-F8 STM GEN 1B LO-LO LVL CH 2	1	1	1	0 --> 7

* Times are in seconds after trip (minimum --> maximum)

Sheet 3 of 3

Alarm ID	Alarm Message	Frequency of Occurrence			First Occurrence Time Range*
		Trip 1	Trip 2	Trip 3	
14--30	F-F9 STM GEN 1C LO-LO LVL CH 2	1	1	1	3 --> 6
14--32	F-G7 STM GEN 1A LO-LO LVL CH 3	1	1	1	6 --> 14
14--33	F-G8 STM GEN 1B LO-LO LVL CH 3	1	1	1	0 --> 7
14--34	F-G9 STM GEN 1C LO-LO LVL CH 3	1	1	1	3 --> 6
7--49	D-F2 STM GEN BD HI-LO FLOW	1	0	1	109 --> 210
11--38	H-H7 STM DUMP V V TRIP OPEN	1	0	1	1
11--6	H-D7 STM DUMP PERM	1	0	1	1 --> 56
10--64	H-D1 AMSAC ARMED	1	0	1	7
8--61	F-B3 AMSAC INITIATED	1	0	1	34
11--41	J-A2 FW HTR 1A LO LVL	1	1	4	2 --> 210
11--49	J-B2 FW HTR 1B LO LVL	1	1	2	12 --> 119
11--48	J-B1 FW HTR 1B HI LVL	2	0	3	2 --> 3
11--42	J-A3 FW HTR 2A HI LVL	15	2	4	18 --> 517
11--50	J-B3 FW HTR 2B HI LVL	10	0	4	18 --> 50
11--57	J-C2 FW HTR 3A LO LVL	6	0	1	60 --> 84
11--56	J-C1 FW HTR 3A HI LVL	4	2	2	3 --> 466
11--64	J-D1 FW HTR 3B HI LVL	2	0	3	4
12--1	J-D2 FW HTR 3B LO LVL	2	0	4	35 --> 114
12--9	J-E2 FW HTR 4A LO LVL	10	0	1	12 --> 140
12--8	J-E1 FW HTR 4A HI LVL	11	0	2	5
12--17	J-F2 FW HTR 4B LO LVL	2	0	3	70 --> 78
12--16	J-F1 FW HTR 4B HI LVL	3	0	3	4 --> 5
12--25	J-G2 FW HTR 5A LO LVL	1	0	4	2 --> 27
12--24	J-G1 FW HTR 5A HI LVL	1	0	3	4 --> 5
12--33	J-H2 FW HTR 5B LO LVL	1	0	2	26 --> 39
12--32	J-H1 FW HTR 5B HI LVL	1	0	3	4 --> 5
11--51	J-B4 HP HTR DR RCVR TK HI-LO LVL	1	1	1	82 --> 679
11--35	H-H4 REHEATER DR RCVR TK 1B OR 1D LO LVL	1	0	1	81 --> 88
11--2	H-D3 CN POLISHING BYPASS AOV OPEN	1	1	1	2 --> 5
12--19	J-F4 CST 110,000 GAL LO LEVEL	1	1	1	36 --> 424

* Times are in seconds after trip (minimum --> maximum)

It is important to point out that this list of alarms was determined without any operator input. The list was created using Excel macros that simply compared the three trip histories, found the common alarms, identified the number of occurrences and the time range, and listed them.
A review by experienced operators likely would find some alarms that would not be expected (they happened to occur in two of the trips analyzed but this is not normally the case), and some that are not listed but should be (for some reason they did not occur in more than one of these trips but they typically do occur and are expected). However, the list shown serves to illustrate the point. Also, the intent here is to examine methods that do not require significant time from operations or engineering personnel, so simple techniques such as this are appropriate.

Examination of the listing shows that there are several significant contributors to the set of post-trip alarms for this plant:

- Trip signals from the reactor trip system, including many that are multi-channel
- Alarms related to rod control that are brought in by the scram
- Pressurizer level and reactor coolant system temperature (T AVG) alarms caused by the excursion in RCS temperature that results from the trip
- Alarms from the turbine-generator protection system caused by the unit trip
- Steam generator level alarms brought in because of the shrinkage of steam generator water level that normally occurs after a trip; many of these are multi-channel and multi-setpoint (LO and LO-LO) alarms
- AMSAC (ATWS mitigation system actuation) alarms caused by the drop in steam generator level – this is an expected occurrence on a trip from a high power level (although AMSAC initiation did not lead to large numbers of alarms, it is listed here because of its importance to plant operation)
- Feedwater heater levels and other alarms related to the turbine extraction, feed and condensate systems that occur repeatedly in the transient following turbine trip, particularly when the trip is from a high power level.

Application of the alarm definition and alarm processing techniques described in the previous section could address many of these situations and significantly reduce the number of post-trip alarms. For example, many of the alarms from the reactor trip system, rod controls, and turbine trip system could be conditioned on the trip state of the reactor and turbine-generator (e.g., to prevent the "reactor trip breakers open" alarm from occurring if a valid reactor trip signal has been received – the important condition in this case would be the reverse: if the trip breakers did <u>not</u> open following the trip). Techniques that address repeating or chattering alarms could eliminate the large number of feedwater heater level alarms and other repeating alarms shown in Table 6-2. Note that 17 feedwater heater alarms alone accounted for almost 150 of the 316 alarm events (incoming and clearing alarms) in Trip 1. Another repeating alarm by itself accounted for over 50 of the alarm events in Trip 3. These results are not unique to this plant, but typical of many operating plants. For most conventional control room alarm systems, it is not practical to implement extensive alarm logic or alarm processing. Upgrading to more modern digital systems provides greater capability to do so, but definition and verification of the logic still requires a significant investment of resources in terms of time from experienced operations and engineering personnel.

Simple Methods for Highlighting Unusual Alarms

Another way to deal with the post-trip overload situation that requires less effort is to provide additional views of the alarm information that can help the operator quickly identify the unusual and potentially important alarms that may require action. This can be done by removing the expected alarms, leaving only those that are unusual – not in the "core set" of alarms that typically occur post-trip. Alternatively, a list can be provided that retains all the alarms but highlights those that are not expected.

Table 6-3 shows the reduction in the number of alarms that can be achieved by removing those that normally occur after a trip, based on analysis of the three PWR trip histories discussed above. Two cases are shown. In the first, the only alarms that are removed are those that occurred in all three trips. In the second case, any alarm that occurred in at least two of the three trips is removed. The table shows the effect in each case on the number of alarm events (incoming and clearing alarms) and the number of unique alarms activated in the transient.

As can be seen in the table, significant reduction occurs in the first case. However, in the second case, which is more aggressive in terms of alarm reduction, the number of alarms is brought down to a much more manageable level. Because either of these can be implemented in a way that still makes all of the alarm information available to the operator, there is lower risk to these approaches than with an approach that completely filters out the expected alarms – the operators are not deprived of any information. Thus the more aggressive reduction shown in the second case may make sense as an aid to the operator (examples of this will be discussed further below).

Table 6-3
Reduction of Post-Trip Alarms by Removing Expected Alarms – PWR

Trip No.	Prior to any Reduction		After Removal of Alarms Occurring in all 3 Trips		After Removal of Alarms Occurring in at Least 2 of the 3 Trips	
	Alarm Events	Unique Alarms	Alarm Events	Unique Alarms	Alarm Events	Unique Alarms
1	316	124	199	70	36	**17**
2	127	69	28	15	15	**10**
3	334	127	227	73	45	**19**

Table 6-4 shows the alarm listing from the annunciator system for the first trip analyzed in Table 6-1. This illustrates the amount and type of information an operator might see if alarms are presented as a simple chronological list of alarm messages and the operator chooses to view the list after the initial burst of activity has subsided. (Note: The list in Table 6-4 is ordered with the latest at the bottom – a display for the operator might order them with the latest at the top, pushing older alarms down and off the screen when they exceed one screen's capacity.) The status designator in the first column indicates whether the alarm is coming in (Stat = 1) or clearing (Stat = 0). The next two columns identify the particular alarm point (input to the annunciator).

Faced with this amount of information, the operators use their experience and training as they go through the list to distinguish important or unusual alarms from those that normally occur after a trip (the "core set" of alarms referred to above). For conventional systems that may provide only a chronological list of alarm events without any processing, this is the operators' only choice if the alarm sequence is to be used at all. However, with more modern systems having greater alarm processing and display capabilities, the system can do some of the work for the operators and make the alarm information more useable. For example, if the core set of trip alarms has been previously identified, the system can distinguish these from the other unusual and potentially important alarms. There are a number of ways in which the results of this processing can be displayed to the operators.

Table 6-4
Alarm Messages for Trip 1 of Table 6-1 (Unfiltered)

Sheet 1 of 8

Stat	Alarm ID		Alarm Message	Time
1	11	18	H-F3 CN POLISHING SYS TRBL	00:26:57:159
0	11	18	H-F3 CN POLISHING SYS TRBL	00:27:26:992
1	16	15	VSP-E8 CVCS HT TRACE TRBL	00:45:49:628
0	16	15	VSP-E8 CVCS HT TRACE TRBL	00:59:27:322
1	6	60	C-G5 RCP SHAFT ALERT	01:26:33:346
1	7	4	C-H5 RCP SHAFT DANGER	01:26:52:809
0	7	4	C-H5 RCP SHAFT DANGER	01:33:57:393
1	8	11	E-B8 MAN RX TRIP	01:37:05:979
1	8	9	E-A9 RX TRIP BKRS OPEN	01:37:06:03
1	8	56	F-A1 TURB TRIPPED BY RX TRIP	01:37:06:035
1	9	36	F-G6 STM GEN 1C CH 4 HI STM LINE FLOW	01:37:06:229
1	9	35	F-G5 STM GEN 1B CH 4 HI STM LINE FLOW	01:37:06:236
1	9	34	F-G4 STM GEN 1A CH 4 HI STM LINE FLOW	01:37:06:237
1	9	32	F-F5 STM GEN 1B CH 3 HI STM LINE FLOW	01:37:06:238
1	9	31	F-F4 STM GEN 1A CH 3 HI STM LINE FLOW	01:37:06:239
1	9	33	F-F6 STM GEN 1C CH 3 HI STM LINE FLOW	01:37:06:24
1	9	45	G-A6 ROD CONT SYS URGENT FAILURE	01:37:06:281
1	9	18	F-A6 RX TRIP CH 3 AUTO STOP OIL DUMP	01:37:06:301
1	10	32	G-H1 NIS DROPPED ROD FLUX DECREASE > 5% PER 2 SEC	01:37:06:31
1	10	43	H-A4 T AVG >< T REF DEVIATION	01:37:06:312
1	9	17	F-A5 RX TRIP CH 2 AUTO STOP OIL DUMP	01:37:06:324
1	8	8	E-A8 RX TRIPPED BY TURB TRIP	01:37:06:33
1	9	16	F-A4 RX TRIP CH 1 AUTO STOP OIL DUMP	01:37:06:332
1	11	6	H-D7 STM DUMP PERM	01:37:06:34
1	9	59	G-C4 UPPER ION CHAMBER DEVIATION OR AUTO DEFEAT < 50%	01:37:06:378
1	11	38	H-H7 STM DUMP V V TRIP OPEN	01:37:06:414
0	9	17	F-A5 RX TRIP CH 2 AUTO STOP OIL DUMP	01:37:06:48
1	12	36	J-H5 TURB STOP V V CLOSED	01:37:06:481
1	10	27	G-G4 OP DELTA T TURB RNBK & ROD STOP CH 2	01:37:06:544
1	8	43	E-D7 RX TRIP CH 2 OP DELTA T LOOP 1B	01:37:06:553
1	10	26	G-G3 OT DELTA T TURB RNBK & ROD STOP CH 2	01:37:06:561
1	8	42	E-D6 RX TRIP CH 2 OT DELTA T LOOP 1B	01:37:06:578
1	10	19	G-F4 OP DELTA T TURB RNBK & ROD STOP CH 1	01:37:06:581
1	11	13	H-E6 STM GEN 1B FW >< STM FLOW	01:37:06:586
1	8	40	E-C7 RX TRIP CH 1 OP DELTA T LOOP 1A	01:37:06:588
1	8	14	E-C8 OP DELTA T	01:37:06:588
1	10	18	G-F3 OT DELTA T TURB RNBK & ROD STOP CH 1	01:37:06:597
1	11	14	H-E7 STM GEN 1C FW >< STM FLOW	01:37:06:598
1	8	17	E-D8 OT DELTA T	01:37:06:604

Sheet 2 of 8

Stat	Alarm ID		Alarm Message	Time
1	8	39	E-C6 RX TRIP CH 1 OT DELTA T LOOP 1A	01:37:06:605
1	8	57	F-A2 SOV TURB TRIP	01:37:06:609
1	10	35	G-H4 OP DELTA T TURB RNBK & ROD STOP CH 3	01:37:06:612
1	11	12	H-E5 STM GEN 1A FW >< STM FLOW	01:37:06:612
1	8	46	E-E7 RX TRIP CH 3 OP DELTA T LOOP 1C	01:37:06:631
1	10	34	G-H3 OT DELTA T TURB RNBK & ROD STOP CH 3	01:37:06:647
1	8	45	E-E6 RX TRIP CH 3 OT DELTA T LOOP 1C	01:37:06:656
1	9	17	F-A5 RX TRIP CH 2 AUTO STOP OIL DUMP	01:37:06:656
1	12	6	J-D7 GEN MOTORING TURB LO DP	01:37:06:682
0	9	35	F-G5 STM GEN 1B CH 4 HI STM LINE FLOW	01:37:06:688
0	12	6	J-D7 GEN MOTORING TURB LO DP	01:37:06:711
0	9	32	F-F5 STM GEN 1B CH 3 HI STM LINE FLOW	01:37:06:757
1	12	6	J-D7 GEN MOTORING TURB LO DP	01:37:06:779
0	9	31	F-F4 STM GEN 1A CH 3 HI STM LINE FLOW	01:37:06:78
0	9	36	F-G6 STM GEN 1C CH 4 HI STM LINE FLOW	01:37:06:804
0	9	34	F-G4 STM GEN 1A CH 4 HI STM LINE FLOW	01:37:06:813
0	9	33	F-F6 STM GEN 1C CH 3 HI STM LINE FLOW	01:37:06:823
1	10	3	G-D4 LOWER ION CHAMBER DEVIATION OR AUTO DEFEAT < 50%	01:37:06:892
0	8	39	E-C6 RX TRIP CH 1 OT DELTA T LOOP 1A	01:37:07:09
0	10	18	G-F3 OT DELTA T TURB RNBK & ROD STOP CH 1	01:37:07:099
0	8	42	E-D6 RX TRIP CH 2 OT DELTA T LOOP 1B	01:37:07:128
0	8	17	E-D8 OT DELTA T	01:37:07:128
0	10	26	G-G3 OT DELTA T TURB RNBK & ROD STOP CH 2	01:37:07:139
0	8	40	E-C7 RX TRIP CH 1 OP DELTA T LOOP 1A	01:37:07:14
0	10	19	G-F4 OP DELTA T TURB RNBK & ROD STOP CH 1	01:37:07:154
0	8	45	E-E6 RX TRIP CH 3 OT DELTA T LOOP 1C	01:37:07:179
0	10	34	G-H3 OT DELTA T TURB RNBK & ROD STOP CH 3	01:37:07:183
0	8	43	E-D7 RX TRIP CH 2 OP DELTA T LOOP 1B	01:37:07:194
0	8	14	E-C8 OP DELTA T	01:37:07:195
0	8	46	E-E7 RX TRIP CH 3 OP DELTA T LOOP 1C	01:37:07:207
0	8	11	E-B8 MAN RX TRIP	01:37:07:207
0	10	27	G-G4 OP DELTA T TURB RNBK & ROD STOP CH 2	01:37:07:221
0	10	35	G-H4 OP DELTA T TURB RNBK & ROD STOP CH 3	01:37:07:228
1	6	23	C-B8 PRZR LO PRESS	01:37:07:799
1	10	33	G-H2 RPI ROD BOTTOM < 20 STEPS	01:37:07:977
1	11	48	J-B1 FW HTR 1B HI LVL	01:37:08:689
1	11	30	H-G7 STM GEN 1C LVL ERROR	01:37:09:205
1	6	39	C-D8 PRZR LO LVL	01:37:09:364
1	11	56	J-C1 FW HTR 3A HI LVL	01:37:09:434
1	11	28	H-G5 STM GEN 1A LVL ERROR	01:37:09:54

Sheet 3 of 8

Stat	Alarm ID		Alarm Message	Time
1	12	24	J-G1 FW HTR 5A HI LVL	01:37:09:696
1	11	64	J-D1 FW HTR 3B HI LVL	01:37:09:697
1	12	32	J-H1 FW HTR 5B HI LVL	01:37:09:698
1	10	54	H-B7 STM GEN 1C LO LVL	01:37:09:738
1	11	29	H-G6 STM GEN 1B LVL ERROR	01:37:09:859
1	12	16	J-F1 FW HTR 4B HI LVL	01:37:09:938
1	11	2	H-D3 CN POLISHING BYPASS AOV OPEN	01:37:09:995
1	12	8	J-E1 FW HTR 4A HI LVL	01:37:10:189
1	10	52	H-B5 STM GEN 1A LO LVL	01:37:10:214
1	10	53	H-B6 STM GEN 1B LO LVL	01:37:10:301
1	10	62	H-C7 STM GEN 1C LO-LO LVL	01:37:10:732
1	10	60	H-C5 STM GEN 1A LO-LO LVL	01:37:10:851
1	10	61	H-C6 STM GEN 1B LO-LO LVL	01:37:11:1
1	14	14	F-B9 STM GEN 1C LO LVL CH 2	01:37:11:247
1	14	10	F-A9 STM GEN 1C LO LVL CH 1	01:37:11:358
1	14	8	F-A7 STM GEN 1A LO LVL CH 1	01:37:11:434
1	14	12	F-B7 STM GEN 1A LO LVL CH 2	01:37:11:53
1	14	9	F-A8 STM GEN 1B LO LVL CH 1	01:37:11:543
1	10	57	H-C2 DELTA T DEVIATION LOOP 1A >< LOOP 1C	01:37:11:576
1	14	13	F-B8 STM GEN 1B LO LVL CH 2	01:37:11:672
1	14	32	F-G7 STM GEN 1A LO-LO LVL CH 3	01:37:11:818
1	14	30	F-F9 STM GEN 1C LO-LO LVL CH 2	01:37:11:841
1	8	28	E-G10 STM GEN LO-LO LVL	01:37:11:878
1	14	24	F-E7 STM GEN 1A LO-LO LVL CH 1	01:37:11:878
1	14	26	F-E9 STM GEN 1C LO-LO LVL CH 1	01:37:11:918
1	14	34	F-G9 STM GEN 1C LO-LO LVL CH 3	01:37:11:935
0	11	48	J-B1 FW HTR 1B HI LVL	01:37:11:953
1	10	49	H-B2 DELTA T DEVIATION LOOP 1B >< LOOP 1C	01:37:11:969
1	14	28	F-F7 STM GEN 1A LO-LO LVL CH 2	01:37:12:048
1	14	25	F-E8 STM GEN 1B LO-LO LVL CH 1	01:37:12:151
1	14	29	F-F8 STM GEN 1B LO-LO LVL CH 2	01:37:12:157
0	11	38	H-H7 STM DUMP V V TRIP OPEN	01:37:12:239
1	14	33	F-G8 STM GEN 1B LO-LO LVL CH 3	01:37:12:251
1	10	64	H-D1 AMSAC ARMED	01:37:12:986
0	6	39	C-D8 PRZR LO LVL	01:37:13:297
1	16	6	VSP-F3 FIRE DETECTOR SYS TRBL	01:37:14:69
1	8	59	F-B1 MAN TURB TRIP	01:37:14:83
0	8	59	F-B1 MAN TURB TRIP	01:37:16:088
0	12	32	J-H1 FW HTR 5B HI LVL	01:37:17:452
0	12	24	J-G1 FW HTR 5A HI LVL	01:37:17:46

Sheet 4 of 8

Stat	Alarm ID		Alarm Message	Time
0	10	57	H-C2 DELTA T DEVIATION LOOP 1A >< LOOP 1C	01:37:17:678
1	12	9	J-E2 FW HTR 4A LO LVL	01:37:17:95
0	12	8	J-E1 FW HTR 4A HI LVL	01:37:17:956
0	10	49	H-B2 DELTA T DEVIATION LOOP 1B >< LOOP 1C	01:37:17:994
0	12	9	J-E2 FW HTR 4A LO LVL	01:37:18:181
1	12	8	J-E1 FW HTR 4A HI LVL	01:37:18:182
0	10	43	H-A4 T AVG >< T REF DEVIATION	01:37:18:469
1	12	9	J-E2 FW HTR 4A LO LVL	01:37:19:71
0	12	8	J-E1 FW HTR 4A HI LVL	01:37:19:716
0	12	9	J-E2 FW HTR 4A LO LVL	01:37:19:934
1	12	8	J-E1 FW HTR 4A HI LVL	01:37:19:936
1	10	59	H-C4 LO T AVG TO FW CONT	01:37:23:212
0	16	6	VSP-F3 FIRE DETECTOR SYS TRBL	01:37:23:577
0	11	14	H-E7 STM GEN 1C FW >< STM FLOW	01:37:23:938
0	11	12	H-E5 STM GEN 1A FW >< STM FLOW	01:37:24:029
1	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:339
0	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:358
0	11	13	H-E6 STM GEN 1B FW >< STM FLOW	01:37:24:367
1	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:381
0	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:41
1	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:442
1	11	12	H-E5 STM GEN 1A FW >< STM FLOW	01:37:24:443
0	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:473
1	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:505
0	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:536
1	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:566
0	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:596
1	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:618
0	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:656
1	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:687
0	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:724
1	11	42	J-A3 FW HTR 2A HI LVL	01:37:24:761
0	11	12	H-E5 STM GEN 1A FW >< STM FLOW	01:37:25:276
1	11	48	J-B1 FW HTR 1B HI LVL	01:37:25:433
0	12	8	J-E1 FW HTR 4A HI LVL	01:37:25:718
1	12	9	J-E2 FW HTR 4A LO LVL	01:37:25:724
0	12	9	J-E2 FW HTR 4A LO LVL	01:37:25:935
1	12	8	J-E1 FW HTR 4A HI LVL	01:37:25:936
1	12	9	J-E2 FW HTR 4A LO LVL	01:37:26:954
0	12	8	J-E1 FW HTR 4A HI LVL	01:37:26:96

Sheet 5 of 8

Stat	Alarm ID		Alarm Message	Time
0	12	9	J-E2 FW HTR 4A LO LVL	01:37:27:182
1	12	8	J-E1 FW HTR 4A HI LVL	01:37:27:184
1	10	43	H-A4 T AVG >< T REF DEVIATION	01:37:28:085
1	11	43	J-A4 CNDSR HOTWELL HI-LO LVL	01:37:28:79
1	12	33	J-H2 FW HTR 5B LO LVL	01:37:31:695
1	1	54	T. 54 GEN BKRS CLOSED TURB TRIP TRAIN A	01:37:31:752
1	9	4	F-E1 GEN BACK UP LOCKOUT REL TRIP	01:37:31:777
1	2	50	T. 114 GENERATOR BACKUP DIFF REL TRIPPED	01:37:31:778
1	12	38	J-H7 VOLTAGE REGULATOR TRIP	01:37:31:791
1	12	48	K-B1 GEN BKR AUX REL FAIL TURB TRIP CKT	01:37:31:847
1	2	15	T. 79 UNIT ON LINE BKR 44 TRIPPED	01:37:31:853
1	13	21	K-F6 4KV BUS NORM SUP BKR TRIP	01:37:31:855
0	12	6	J-D7 GEN MOTORING TURB LO DP	01:37:31:863
0	2	15	T. 79 UNIT ON LINE BKR 44 TRIPPED	01:37:31:864
1	1	51	T. 51 GEN PCB TURB TRIP	01:37:31:866
1	2	15	T. 79 UNIT ON LINE BKR 44 TRIPPED	01:37:31:869
1	2	8	T. 72 UNIT ON LINE BKR 4C TRIPPED	01:37:31:878
0	2	15	T. 79 UNIT ON LINE BKR 44 TRIPPED	01:37:31:882
1	2	15	T. 79 UNIT ON LINE BKR 44 TRIPPED	01:37:31:884
0	1	54	T. 54 GEN BKRS CLOSED TURB TRIP TRAIN A	01:37:32:031
0	11	48	J-B1 FW HTR 1B HI LVL	01:37:32:433
1	12	25	J-G2 FW HTR 5A LO LVL	01:37:32:916
0	12	8	J-E1 FW HTR 4A HI LVL	01:37:33:188
1	12	9	J-E2 FW HTR 4A LO LVL	01:37:33:194
0	12	9	J-E2 FW HTR 4A LO LVL	01:37:33:414
1	12	8	J-E1 FW HTR 4A HI LVL	01:37:33:416
1	10	42	H-A3 HI-LO T AVG LOOP 1A	01:37:37:142
1	10	50	H-B3 HI-LO T AVG LOOP 1B	01:37:37:389
1	10	58	H-C3 HI-LO T AVG LOOP 1C	01:37:39:093
1	3	41	AMSAC INIT TRB	01:37:39:701
1	8	61	F-B3 AMSAC INITIATED	01:37:39:701
1	3	40	AMSAC INIT TRA	01:37:39:702
1	9	61	G-C6 ROD CONT MG TRIPPED	01:37:39:808
1	10	5	G-D6 ROD CONT SYS NON-URGENT FAILURE	01:37:39:904
1	1	19	T. 19 REACTOR COOL PP 1C BKR TRIPPED	01:37:40:446
1	13	43	E-A4 RC LOOP 1C LO FLOW CH 1	01:37:41:504
1	13	51	E-C4 RC LOOP 1C LO FLOW CH 3	01:37:41:58
1	13	47	E-B4 RC LOOP 1C LO FLOW CH 2	01:37:41:609
0	12	8	J-E1 FW HTR 4A HI LVL	01:37:49:191
1	11	19	H-F4 LO T AVG INTLK LOOP 1C	01:37:53:346

Sheet 6 of 8

Stat	Alarm ID		Alarm Message	Time
1	11	50	J-B3 FW HTR 2B HI LVL	01:37:55:29
0	11	56	J-C1 FW HTR 3A HI LVL	01:37:59:686
0	12	16	J-F1 FW HTR 4B HI LVL	01:37:59:697
1	11	54	J-B7 VREG LOCAL ALARM	01:38:01:827
1	12	9	J-E2 FW HTR 4A LO LVL	01:38:02:667
1	11	57	J-C2 FW HTR 3A LO LVL	01:38:05:387
0	12	9	J-E2 FW HTR 4A LO LVL	01:38:06:141
1	12	8	J-E1 FW HTR 4A HI LVL	01:38:07:651
1	10	49	H-B2 DELTA T DEVIATION LOOP 1B >< LOOP 1C	01:38:07:894
1	10	57	H-C2 DELTA T DEVIATION LOOP 1A >< LOOP 1C	01:38:07:976
0	11	43	J-A4 CNDSR HOTWELL HI-LO LVL	01:38:09:599
1	12	9	J-E2 FW HTR 4A LO LVL	01:38:10:909
0	12	8	J-E1 FW HTR 4A HI LVL	01:38:10:914
0	12	9	J-E2 FW HTR 4A LO LVL	01:38:11:14
1	12	8	J-E1 FW HTR 4A HI LVL	01:38:11:141
1	12	17	J-F2 FW HTR 4B LO LVL	01:38:15:413
0	11	64	J-D1 FW HTR 3B HI LVL	01:38:17:666
0	11	19	H-F4 LO T AVG INTLK LOOP 1C	01:38:17:787
0	10	57	H-C2 DELTA T DEVIATION LOOP 1A >< LOOP 1C	01:38:22:04
0	10	49	H-B2 DELTA T DEVIATION LOOP 1B >< LOOP 1C	01:38:22:087
1	11	43	J-A4 CNDSR HOTWELL HI-LO LVL	01:38:24:497
1	11	35	H-H4 REHEATER DR RCVR TK 1B OR 1D LO LVL	01:38:26:091
1	10	49	H-B2 DELTA T DEVIATION LOOP 1B >< LOOP 1C	01:38:28:428
1	10	57	H-C2 DELTA T DEVIATION LOOP 1A >< LOOP 1C	01:38:28:813
1	11	19	H-F4 LO T AVG INTLK LOOP 1C	01:38:32:113
0	11	57	J-C2 FW HTR 3A LO LVL	01:38:35:127
0	12	8	J-E1 FW HTR 4A HI LVL	01:38:36:135
1	12	9	J-E2 FW HTR 4A LO LVL	01:38:36:142
0	12	9	J-E2 FW HTR 4A LO LVL	01:38:36:362
1	12	8	J-E1 FW HTR 4A HI LVL	01:38:36:363
0	11	43	J-A4 CNDSR HOTWELL HI-LO LVL	01:38:49:831
1	11	43	J-A4 CNDSR HOTWELL HI-LO LVL	01:38:51:553
0	11	43	J-A4 CNDSR HOTWELL HI-LO LVL	01:38:53:26
1	7	49	D-F2 STM GEN BD HI-LO FLOW	01:38:54:407
1	12	1	J-D2 FW HTR 3B LO LVL	01:38:59:861
0	10	50	H-B3 HI-LO T AVG LOOP 1B	01:39:00:709
0	12	8	J-E1 FW HTR 4A HI LVL	01:39:01:644
1	11	57	J-C2 FW HTR 3A LO LVL	01:39:01:862
0	10	42	H-A3 HI-LO T AVG LOOP 1A	01:39:03:803
1	11	49	J-B2 FW HTR 1B LO LVL	01:39:04:591

Sheet 7 of 8

Stat	Alarm ID		Alarm Message	Time
0	11	2	H-D3 CN POLISHING BYPASS AOV OPEN	01:39:05:744
0	12	17	J-F2 FW HTR 4B LO LVL	01:39:05:844
1	12	8	J-E1 FW HTR 4A HI LVL	01:39:08:338
1	12	16	J-F1 FW HTR 4B HI LVL	01:39:11:34
0	11	50	J-B3 FW HTR 2B HI LVL	01:39:11:388
1	12	9	J-E2 FW HTR 4A LO LVL	01:39:20:104
0	12	8	J-E1 FW HTR 4A HI LVL	01:39:20:109
0	12	9	J-E2 FW HTR 4A LO LVL	01:39:20:336
1	12	8	J-E1 FW HTR 4A HI LVL	01:39:20:338
0	11	19	H-F4 LO T AVG INTLK LOOP 1C	01:39:36:962
1	11	50	J-B3 FW HTR 2B HI LVL	01:39:48:688
0	11	50	J-B3 FW HTR 2B HI LVL	01:40:02:593
0	12	1	J-D2 FW HTR 3B LO LVL	01:40:10:062
0	1	51	T. 51 GEN PCB TURB TRIP	01:40:12:558
0	10	43	H-A4 T AVG >< T REF DEVIATION	01:40:20:904
0	12	16	J-F1 FW HTR 4B HI LVL	01:40:27:819
0	12	8	J-E1 FW HTR 4A HI LVL	01:40:31:818
1	11	41	J-A2 FW HTR 1A LO LVL	01:40:35:022
1	12	16	J-F1 FW HTR 4B HI LVL	01:40:47:538
1	11	50	J-B3 FW HTR 2B HI LVL	01:40:51:432
1	11	64	J-D1 FW HTR 3B HI LVL	01:40:57:782
1	12	9	J-E2 FW HTR 4A LO LVL	01:41:06:28
0	11	50	J-B3 FW HTR 2B HI LVL	01:41:08:021
0	8	8	E-A8 RX TRIPPED BY TURB TRIP	01:41:22:719
0	12	16	J-F1 FW HTR 4B HI LVL	01:41:57:271
0	11	49	J-B2 FW HTR 1B LO LVL	01:41:57:764
1	11	50	J-B3 FW HTR 2B HI LVL	01:42:18:145
1	12	17	J-F2 FW HTR 4B LO LVL	01:42:19:263
0	11	57	J-C2 FW HTR 3A LO LVL	01:42:22:511
1	11	57	J-C2 FW HTR 3A LO LVL	01:42:26:737
0	11	57	J-C2 FW HTR 3A LO LVL	01:42:40:989
0	11	50	J-B3 FW HTR 2B HI LVL	01:42:42:459
1	11	57	J-C2 FW HTR 3A LO LVL	01:42:43:723
0	11	64	J-D1 FW HTR 3B HI LVL	01:42:44:5
0	11	57	J-C2 FW HTR 3A LO LVL	01:42:46:238
1	11	56	J-C1 FW HTR 3A HI LVL	01:42:54:228
0	11	56	J-C1 FW HTR 3A HI LVL	01:43:02:972
1	11	56	J-C1 FW HTR 3A HI LVL	01:43:16:476
1	12	1	J-D2 FW HTR 3B LO LVL	01:43:26:712
0	11	56	J-C1 FW HTR 3A HI LVL	01:43:31:972

Sheet 8 of 8

Stat	Alarm ID		Alarm Message	Time
1	11	56	J-C1 FW HTR 3A HI LVL	01:43:36:462
0	11	56	J-C1 FW HTR 3A HI LVL	01:43:37:468
1	11	50	J-B3 FW HTR 2B HI LVL	01:43:44:545
1	11	57	J-C2 FW HTR 3A LO LVL	01:43:57:457
0	11	57	J-C2 FW HTR 3A LO LVL	01:44:03:203
1	11	57	J-C2 FW HTR 3A LO LVL	01:44:06:185
1	12	19	J-F4 CST 110,000 GAL LO LEVEL	01:44:09:427
0	11	50	J-B3 FW HTR 2B HI LVL	01:44:16:663
0	11	42	J-A3 FW HTR 2A HI LVL	01:45:05:118
1	11	42	J-A3 FW HTR 2A HI LVL	01:45:05:127
0	11	42	J-A3 FW HTR 2A HI LVL	01:45:05:169
1	11	42	J-A3 FW HTR 2A HI LVL	01:45:05:199
1	11	50	J-B3 FW HTR 2B HI LVL	01:45:05:324
0	11	50	J-B3 FW HTR 2B HI LVL	01:45:20:31
1	11	50	J-B3 FW HTR 2B HI LVL	01:45:23:334
0	11	50	J-B3 FW HTR 2B HI LVL	01:45:30:48
0	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:195
1	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:218
0	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:253
1	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:273
0	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:303
1	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:324
0	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:363
1	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:388
0	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:429
1	11	42	J-A3 FW HTR 2A HI LVL	01:45:31:459
1	11	50	J-B3 FW HTR 2B HI LVL	01:46:08:08
0	11	50	J-B3 FW HTR 2B HI LVL	01:46:35:242
0	6	60	C-G5 RCP SHAFT ALERT	01:46:54:29
1	11	50	J-B3 FW HTR 2B HI LVL	01:47:04:901
0	11	50	J-B3 FW HTR 2B HI LVL	01:47:25:621
1	11	50	J-B3 FW HTR 2B HI LVL	01:48:03:533
0	11	50	J-B3 FW HTR 2B HI LVL	01:48:24:18
1	11	51	J-B4 HP HTR DR RCVR TK HI-LO LVL	01:48:24:888
0	6	23	C-B8 PRZR LO PRESS	01:48:26:557
0	11	51	J-B4 HP HTR DR RCVR TK HI-LO LVL	01:48:27:888
0	11	41	J-A2 FW HTR 1A LO LVL	01:48:45:143

Table 6-5 shows an alarm listing for Trip 1 that has removed the core set of alarms (those that occur in at least 2 out of 3 trips). Of course, in practice this core set could be determined based on examination of more than just three trips. For the purpose of this illustration, we use the core set identified in Table 6-2. In addition to removing the expected alarms, the listing of Table 6-5 also eliminates clearing alarm events (alarms returning to normal) and it shows only the first occurrence of each alarm. This keeps repeating alarms from cluttering the message list and in general helps reduce the number of messages the operator must sort through. Also, instead of the actual clock time this listing provides time of occurrence as the number of seconds after the trip. This conversion is easily done by the computer if the valid trip signals are predefined so that it can identify the time of initial trip.

Note that the number of messages in this reduced list is very manageable – something an operator can scan very quickly to try to pick up anything unusual, anything that adds to an understanding of the current trip and its cause, and any secondary failures or conditions that may require operator action. The length of the list has been reduced from 316 messages to 17 messages (almost 95% reduction in length). Table 6-3 indicates what level of reduction would be achieved with the other trip transients that were analyzed.

Note that, as discussed above, the set of expected alarms was determined simply by comparing three trip alarm sequences, without any operations input. It can be seen from Table 6-5 that some alarms that were not removed appear similar to others that are on the expected alarm list and probably should also be on that list. Use of additional trip histories, perhaps from the simulator as well as the actual plant, and a brief review by experienced operators likely would address these and improve the core set of expected alarms.

If a reduced alarm list like that in Table 6-5 is provided to the operator, it is very important to also make available the full list of alarm events so that the operator is not deprived of information that could turn out to be important, and also to allow the operator to go through the entire sequence of alarms as part of diagnosing or analyzing the event. In a diagnosis or analysis task, even the expected alarms can provide useful information about the progression of the event, relative timing of plant or equipment status changes, etc.

Table 6-5
Reduced Alarm Listing (Core Alarms Removed) – Trip 1

Sheet 1 of 1

Stat	Alarm ID	Alarm Message	Seconds After Trip
1	11--18	H-F3 CN POLISHING SYS TRBL	-4208
1	16--15	VSP-E8 CVCS HT TRACE TRBL	-3076
1	6—60	C-G5 RCP SHAFT ALERT	-632
1	7—4	C-H5 RCP SHAFT DANGER	-613
1	10--57	H-C2 DELTA T DEVIATION LOOP 1A >< LOOP 1C	6
1	10--49	H-B2 DELTA T DEVIATION LOOP 1B >< LOOP 1C	6
1	16—6	VSP-F3 FIRE DETECTOR SYS TRBL	9
1	11--43	J-A4 CNDSR HOTWELL HI-LO LVL	23
1	1--54	T. 54 GEN BKRS CLOSED TURB TRIP TRAIN A	26
1	9—4	F-E1 GEN BACK UP LOCKOUT REL TRIP	26
1	2--50	T. 114 GENERATOR BACKUP DIFF REL TRIPPED	26
1	3--41	AMSAC INIT TRB	34
1	3--40	AMSAC INIT TRA	34
1	1--19	T. 19 REACTOR COOL PP 1C BKR TRIPPED	35
1	13--43	E-A4 RC LOOP 1C LO FLOW CH 1	36
1	13--51	E-C4 RC LOOP 1C LO FLOW CH 3	36
1	13--47	E-B4 RC LOOP 1C LO FLOW CH 2	36

Table 6-6 shows another option for presenting alarm information that retains all the alarms that occurred, but highlights those that are not in the core, expected set of alarms. In this case the highlighting is done by coloring the unusual alarm messages red. This type of aid allows the operator to go through the entire set of alarms that occurred so that the full chronology of incoming alarms is there, but at the same time the operator can easily pick out those alarms that were not expected. Note that the list in Table 6-6 has removed clearing alarm events (alarms going back to normal) and it shows only the first occurrence of any alarms that repeat. This again helps shorten the list and reduces the difficulty associated with chattering alarms. Options could be provided to include return-to-normal alarm messages and, if desired, repeated alarm occurrences.

Table 6-6
Highlighted Alarm Listing (Unusual Alarms Highlighted) – Trip 1

Sheet 1 of 3

Stat	Alarm ID	Alarm Message	Seconds After Trip
1	**11—18**	**▶ H-F3 CN POLISHING SYS TRBL**	**-4208**
1	**16—15**	**▶ VSP-E8 CVCS HT TRACE TRBL**	**-3076**
1	**6—60**	**▶ C-G5 RCP SHAFT ALERT**	**-632**
1	**7—4**	**▶ C-H5 RCP SHAFT DANGER**	**-613**
1	8—11	E-B8 MAN RX TRIP	0
1	8—9	E-A9 RX TRIP BKRS OPEN	1
1	8—56	F-A1 TURB TRIPPED BY RX TRIP	1
1	9—36	F-G6 STM GEN 1C CH 4 HI STM LINE FLOW	1
1	9—35	F-G5 STM GEN 1B CH 4 HI STM LINE FLOW	1
1	9—34	F-G4 STM GEN 1A CH 4 HI STM LINE FLOW	1
1	9—32	F-F5 STM GEN 1B CH 3 HI STM LINE FLOW	1
1	9—31	F-F4 STM GEN 1A CH 3 HI STM LINE FLOW	1
1	9—33	F-F6 STM GEN 1C CH 3 HI STM LINE FLOW	1
1	9—45	G-A6 ROD CONT SYS URGENT FAILURE	1
1	9—18	F-A6 RX TRIP CH 3 AUTO STOP OIL DUMP	1
1	10—32	G-H1 NIS DROPPED ROD FLUX DECREASE > 5% PER 2 SEC	1
1	10—43	H-A4 T AVG >< T REF DEVIATION	1
1	9—17	F-A5 RX TRIP CH 2 AUTO STOP OIL DUMP	1
1	8—8	E-A8 RX TRIPPED BY TURB TRIP	1
1	9—16	F-A4 RX TRIP CH 1 AUTO STOP OIL DUMP	1
1	11—6	H-D7 STM DUMP PERM	1
1	9—59	G-C4 UPPER ION CHAMBER DEVIATION OR AUTO DEFEAT < 50%	1
1	11—38	H-H7 STM DUMP V V TRIP OPEN	1
1	12—36	J-H5 TURB STOP V V CLOSED	1
1	10—27	G-G4 OP DELTA T TURB RNBK & ROD STOP CH 2	1
1	8—43	E-D7 RX TRIP CH 2 OP DELTA T LOOP 1B	1
1	10—26	G-G3 OT DELTA T TURB RNBK & ROD STOP CH 2	1
1	8—42	E-D6 RX TRIP CH 2 OT DELTA T LOOP 1B	1
1	10—19	G-F4 OP DELTA T TURB RNBK & ROD STOP CH 1	1
1	11—13	H-E6 STM GEN 1B FW >< STM FLOW	1
1	8—40	E-C7 RX TRIP CH 1 OP DELTA T LOOP 1A	1
1	8—14	E-C8 OP DELTA T	1
1	10—18	G-F3 OT DELTA T TURB RNBK & ROD STOP CH 1	1
1	11—14	H-E7 STM GEN 1C FW >< STM FLOW	1
1	8—17	E-D8 OT DELTA T	1
1	8—39	E-C6 RX TRIP CH 1 OT DELTA T LOOP 1A	1
1	8—57	F-A2 SOV TURB TRIP	1
1	10—35	G-H4 OP DELTA T TURB RNBK & ROD STOP CH 3	1
1	11—12	H-E5 STM GEN 1A FW >< STM FLOW	1
1	10—34	G-H3 OT DELTA T TURB RNBK & ROD STOP CH 3	1
1	8—46	E-E7 RX TRIP CH 3 OP DELTA T LOOP 1C	1

Sheet 2 of 3

Stat	Alarm ID	Alarm Message	Seconds After Trip
1	8—45	E-E6 RX TRIP CH 3 OT DELTA T LOOP 1C	1
1	12—6	J-D7 GEN MOTORING TURB LO DP	1
1	10—3	G-D4 LOWER ION CHAMBER DEVIATION OR AUTO DEFEAT < 50%	1
1	6—23	C-B8 PRZR LO PRESS	2
1	10—33	G-H2 RPI ROD BOTTOM < 20 STEPS	2
1	11—48	J-B1 FW HTR 1B HI LVL	3
1	11—30	H-G7 STM GEN 1C LVL ERROR	4
1	6—39	C-D8 PRZR LO LVL	4
1	11—56	J-C1 FW HTR 3A HI LVL	4
1	11—28	H-G5 STM GEN 1A LVL ERROR	4
1	12—24	J-G1 FW HTR 5A HI LVL	4
1	11—64	J-D1 FW HTR 3B HI LVL	4
1	12—32	J-H1 FW HTR 5B HI LVL	4
1	10—54	H-B7 STM GEN 1C LO LVL	4
1	11—29	H-G6 STM GEN 1B LVL ERROR	4
1	12—16	J-F1 FW HTR 4B HI LVL	4
1	11—2	H-D3 CN POLISHING BYPASS AOV OPEN	4
1	12—8	J-E1 FW HTR 4A HI LVL	5
1	10—52	H-B5 STM GEN 1A LO LVL	5
1	10—53	H-B6 STM GEN 1B LO LVL	5
1	10—62	H-C7 STM GEN 1C LO-LO LVL	5
1	10—60	H-C5 STM GEN 1A LO-LO LVL	5
1	10—61	H-C6 STM GEN 1B LO-LO LVL	6
1	14—14	F-B9 STM GEN 1C LO LVL CH 2	6
1	14—10	F-A9 STM GEN 1C LO LVL CH 1	6
1	14—8	F-A7 STM GEN 1A LO LVL CH 1	6
1	14—12	F-B7 STM GEN 1A LO LVL CH 2	6
1	14—9	F-A8 STM GEN 1B LO LVL CH 1	6
1	**10—57**	**► H-C2 DELTA T DEVIATION LOOP 1A >< LOOP 1C**	**6**
1	14—13	F-B8 STM GEN 1B LO LVL CH 2	6
1	14—32	F-G7 STM GEN 1A LO-LO LVL CH 3	6
1	14—30	F-F9 STM GEN 1C LO-LO LVL CH 2	6
1	8—28	E-G10 STM GEN LO-LO LVL	6
1	14—24	F-E7 STM GEN 1A LO-LO LVL CH 1	6
1	14—26	F-E9 STM GEN 1C LO-LO LVL CH 1	6
1	14—34	F-G9 STM GEN 1C LO-LO LVL CH 3	6
1	**10—49**	**► H-B2 DELTA T DEVIATION LOOP 1B >< LOOP 1C**	**6**
1	14—28	F-F7 STM GEN 1A LO-LO LVL CH 2	7
1	14—25	F-E8 STM GEN 1B LO-LO LVL CH 1	7
1	14—29	F-F8 STM GEN 1B LO-LO LVL CH 2	7
1	14—33	F-G8 STM GEN 1B LO-LO LVL CH 3	7

Sheet 3 of 3

Stat	Alarm ID	Alarm Message	Seconds After Trip
1	10--64	H-D1 AMSAC ARMED	7
1	**16--6**	**► VSP-F3 FIRE DETECTOR SYS TRBL**	**9**
1	8--59	F-B1 MAN TURB TRIP	9
1	12--9	J-E2 FW HTR 4A LO LVL	12
1	10--59	H-C4 LO T AVG TO FW CONT	18
1	11--42	J-A3 FW HTR 2A HI LVL	19
1	**11--43**	**► J-A4 CNDSR HOTWELL HI-LO LVL**	**23**
1	12--33	J-H2 FW HTR 5B LO LVL	26
1	**1--54**	**► T. 54 GEN BKRS CLOSED TURB TRIP TRAIN A**	**26**
1	**9—4**	**► F-E1 GEN BACK UP LOCKOUT REL TRIP**	**26**
1	**2--50**	**► T. 114 GENERATOR BACKUP DIFF REL TRIPPED**	**26**
1	12--38	J-H7 VOLTAGE REGULATOR TRIP	26
1	12--48	K-B1 GEN BKR AUX REL FAIL TURB TRIP CKT	26
1	2--15	T. 79 UNIT ON LINE BKR 44 TRIPPED	26
1	13--21	K-F6 4KV BUS NORM SUP BKR TRIP	26
1	1--51	T. 51 GEN PCB TURB TRIP	26
1	2--8	T. 72 UNIT ON LINE BKR 4C TRIPPED	26
1	12--25	J-G2 FW HTR 5A LO LVL	27
1	10--42	H-A3 HI-LO T AVG LOOP 1A	32
1	10--50	H-B3 HI-LO T AVG LOOP 1B	32
1	10--58	H-C3 HI-LO T AVG LOOP 1C	34
1	**3--41**	**►AMSAC INIT TRB**	**34**
1	8--61	F-B3 AMSAC INITIATED	34
1	**3--40**	**► AMSAC INIT TRA**	**34**
1	9--61	G-C6 ROD CONT MG TRIPPED	34
1	10--5	G-D6 ROD CONT SYS NON-URGENT FAILURE	34
1	**1--19**	**►T. 19 REACTOR COOL PP 1C BKR TRIPPED**	**35**
1	**13--43**	**► E-A4 RC LOOP 1C LO FLOW CH 1**	**36**
1	**13--51**	**► E-C4 RC LOOP 1C LO FLOW CH 3**	**36**
1	**13--47**	**►E-B4 RC LOOP 1C LO FLOW CH 2**	**36**
1	11--19	H-F4 LO T AVG INTLK LOOP 1C	48
1	11--50	J-B3 FW HTR 2B HI LVL	50
1	11--54	J-B7 VREG LOCAL ALARM	56
1	11--57	J-C2 FW HTR 3A LO LVL	60
1	12--17	J-F2 FW HTR 4B LO LVL	70
1	11--35	H-H4 REHEATER DR RCVR TK 1B OR 1D LO LVL	81
1	7--49	D-F2 STM GEN BD HI-LO FLOW	109
1	12--1	J-D2 FW HTR 3B LO LVL	114
1	11--49	J-B2 FW HTR 1B LO LVL	119
1	11--41	J-A2 FW HTR 1A LO LVL	210
1	12--19	J-F4 CST 110,000 GAL LO LEVEL	424
1	11--51	J-B4 HP HTR DR RCVR TK HI-LO LVL	679

BWR Trip Alarm Analysis

A similar analysis was performed for a BWR plant, for which three trip histories were obtained. Summary data for these trips are presented in Table 6-7 below. As for the PWR, the data covered two units on one site. Note that this plant has a larger number of annunciator alarms installed – on the order of 1200-1500 (depending on the unit) compared to just under 450 for the PWR of Table 6-1. The number of alarm events occurring after a trip is also larger – over 500 for a relatively uncomplicated trip. The second trip shown in the table included a loss of offsite power, which occurred because of a secondary failure following the scram. The loss of offsite power brought in many additional alarms. However, the data for all three trips still could be analyzed for common alarms as all of them involved reactor and turbine-generator trips.

Table 6-7
Analysis of Three Reactor Trip Alarm Histories at a BWR Site[1]

Trip No.	Nature of Trip	No. of Alarm Events[2]	No. of Unique Alarms[3]
1	Automatic reactor scram on low reactor water level due to control circuit failure	520	189
2	Automatic scram due to transformer failure plus loss of offsite power caused by secondary failure	1364	520
3	Manual reactor scram on high reactor water level due to control system problem, plus trip of reactor feed pumps	531	189
Overall statistics:			
Total number of alarms (tiles) in system			1222-1512[4]
No. of unique alarms that occurred in all 3 trips			130
No. of unique alarms that occurred in only 2 of the 3 trips			57
No. of unique alarms that occurred in only one of the 3 trips			394
Total number of unique alarms activated (across all 3 trips)			581

NOTES:

(1) These data are from a two-unit plant. Two of the trips occurred in one unit and the third occurred in the other unit. Because the alarms are similar between units, for the purpose of this study the analysis was performed across all three data sets without regard to which unit was affected.

(2) Alarm events include both incoming and clearing (return to normal) alarms. An alarm that comes in and then clears within the time frame creates two events. An alarm that chatters or repeats 5 times (comes in and out 5 times) generates 10 events.

(3) This is the number of unique alarms that occurred any time during the time interval (regardless of whether they returned to normal or how many times they occurred). It represents the number of alarms that participated in the event.

(4) The number of annunciators varies between the two units; the values given do not include alarms on equipment shared between the two units.

Common alarms occurring in all of the three trips, and in two out of three trips, were identified as was done before for the PWR analysis. Again, the effect of removing these alarms from the post-trip alarm history was analyzed. The results are shown in Table 6-8 below. As expected, the number of alarms for the scram that included loss of offsite power remains high even after the expected post-trip alarms are removed. However, for the other two trips the number of alarms is reduced dramatically and to a level that would be much more easily assimilated by the operators.

Table 6-8
Reduction of Post-Trip Alarms by Removing Expected Alarms – BWR

Trip No.	Prior to any Reduction		After Removal of Alarms Occurring in all 3 Trips		After Removal of Alarms Occurring in at Least 2 of the 3 Trips	
	Alarm Events	Unique Alarms	Alarm Events	Unique Alarms	Alarm Events	Unique Alarms
1	520	189	296	59	253	**31**
2	1364	520	1130	390	1062	**350**
3	531	189	312	59	222	**13**

Application to Other Events

The approach described here for a plant trip also can be applied to other transients and events. Examples might be safety injection actuation (see the results given earlier from the study using simulator alarm data), trips of major components, and major electrical bus trips. Electrical upsets in particular bring in many alarms, as seen in the loss of offsite power event for the BWR above and the simulator alarm analysis described earlier. Thus, electrical upsets would be good candidates for post-event suppression. The plant simulator could be used to generate a number of these transients and capture alarm histories, with different variations representing the typical spectrum of events that might actually occur, allowing the core post-event alarm sets to be determined without a major investment of resources.

As discussed earlier, if these are used simply to provide operator aids that highlight potentially unusual alarms without depriving the operator of any information, then there is less risk and thus less need for detailed verification of the alarm sets. If the simulator is used, fidelity of the alarms on the simulator needs to be considered. But again, it does not have to be perfect to allow a useful operator aid to be created. A modest amount of review time from one or more operators might be sufficient to ensure that the post-event alarm sets are sufficiently accurate and appropriate.

Operators must of course be trained on any operator aids like this that are provided in the control room. The operators should understand the basis for the alarm highlighting or suppression that is applied, and how the core alarm sets were generated. This should not be difficult for a scheme such as this, because its derivation is relatively simple – just highlighting the alarms that don't typically occur in a given transient.

Identifying Missing Alarms

A logical extension of the highlighting technique described above is to also identify expected alarms that do NOT occur. Often this can indicate unusual behavior of the plant or systems or a secondary malfunction that has caused the alarms to deviate from the normal pattern after the event. As shown in Table 6-2, the time interval within which each expected alarm normally occurs after the event initiation can be determined through analysis of multiple alarm histories for similar events. A macro in Excel was used to determine the times shown in the table. If an alarm does not occur within the expected timeframe, the operator aid software could flag this. For example, the DCS could insert the "missing" alarm in the chronological alarm listings of Table 6-5 or Table 6-6 and distinguish it from the other alarm messages, through color-coding or other means. Or, a list of expected but missing alarms could be provided separately.

Of course, more advanced approaches using pattern recognition algorithms could be employed that would provide greater functionality. However, a relatively simple scheme that identifies alarms not occurring in the expected timeframe could be implemented more easily and increase the usefulness of an operator aid that highlights unusual alarms.

7 GUIDANCE FOR IMPROVING ALARM MANAGEMENT

The purpose of this section is to give practical guidance that plants can use to help implement improved alarm definition, alarm processing, and display methods that will reduce the alarm overload problem. The guidance is intended primarily for use by operating plants who will be upgrading their I&C systems and control rooms over time, resulting in a "hybrid" control room that uses both conventional and more modern digital human-system interfaces. These plants will be making decisions on how to take advantage of alarm handling capabilities of the digital systems that will be installed, and what to do with the existing or "legacy" alarms (keep them as is, move them to the new system, etc.). This provides an opportunity to make substantial improvements in the alarm overload situation. However, portions of the guidance given here can also be used by plants who are not planning major upgrades or changes to the control room but want to make whatever improvements they can within the limitations of their current systems.

The intent of the activities recommended here is to make alarm information more useful, easier to use, and less distracting to the operating crew during plant upsets. Another important objective is to avoid the tendency for the alarm overload problem to get worse when newer digital systems are installed without sufficient attention to alarm management. Guidance is provided on planning, budgeting, and specifying digital control and monitoring systems so that plants can take advantage of their capabilities to improve the alarm situation, and avoid the potential to make it worse, as digital I&C and control room systems are introduced over time.

The bases for the guidance provided in this section may be found in earlier sections of this document. Section 3 described the alarm overload problem and what causes it. Section 4 described how alarm management in general can be improved when digital systems are used to process and present alarms. Section 5 identified alarm processing methods that can be very effective in reducing the number of alarms presented in plant transients. Section 6 provided an example of a relatively simple operator aid that can be used to improve assimilation and use of post-trip alarms.

Guidance is given in the following areas:

- Defining the plant's alarm management strategy
- Improving alarm definition and alarm logic for existing and new alarms
- Using simplified methods for defining improved alarm processing techniques and operator aids that can substantially reduce the alarm overload
- Specifying, designing and configuring new digital systems for improved alarm management
- Taking advantage of alarm prioritization, presentation, and acknowledgment methods to make alarm overload easier to deal with

- Making use of third-party software tools to help improve alarm management.

It is important to remember that any changes to the control room alarm system should involve significant input from the users: the operations staff and the maintenance staff if they also are to use the alarm information. A good human factors engineering design process should be followed and the modifications should undergo appropriate human factors verification and validation. EPRI 1003696 provides guidance on the engineering design process, verification and validation techniques, design guidelines and methods that can be used to help ensure the modification meets its design objectives in terms of improvement in human performance.

Defining an Alarm Management Strategy

► Define the plant's alarm management strategy and any changes desired

Even if there is no intent to change the strategy, it is important to understand and communicate the current alarm management strategy so that design engineers and vendors can incorporate it into the design, and enforce it during the configuration, of new control and monitoring systems. As the I&C systems and main control room are modernized over time to address obsolescence, resulting in a hybrid control room with some digital human-system interfaces, there likely will be new alarms and new ways of presenting alarms that should be considered within an overall strategy. The Operations group may have particular ideas as to how the alarm strategy should change, and what characteristics of the current alarm systems should be retained as the changes are made. The alarm management strategy should be developed in concert with the overall design concepts and "endpoint vision" for the main control room, as described in EPRI 1003696.

The alarm management strategy should include items such as the following. Note that these are just examples – the plant staff should identify the issues that are of particular concern to them related to alarm management:

- What constitutes a valid alarm to be presented in the main control room? The guidance in EPRI 1003696 and EPRI NP-3448 can be used to help define this.
- How will maintenance-related alarms be handled – for example, will there be a separate maintenance workstation where alarms primarily for maintenance personnel will be routed? The alarm definition checklist in Appendix A discusses maintenance related alarms and the information that may be needed by operators related to these.
- How and when will the operating crew be expected to use alarm information? For example:
  - During normal power operation, what will be the primary means of alerting operators to alarms requiring short-term action (e.g., existing annunciators or new computer-driven replicas of annunciator light boxes)? Where will the operators go for more detailed information on the alarm and to confirm it (e.g., alarm message list with details or a system display)? How will alarm response procedures be accessed and how will they be displayed?

   - How will the operators use the alarms to help maintain awareness of plant and system states (e.g., scanning annunciators or use of an overview display with integrated alarm information)?
   - During upsets, how will alarms be used initially to identify the transient and the appropriate procedures to be entered? Will the alarms be used in the early stages of the upset (if substantial alarm reduction is achieved, this might be a goal)? After the initial actions have been taken, will alarms be used to determine plant and system states, diagnose the cause of the event and identify any secondary malfunctions?
   - Are there any particular strategies, or changes or improvements desired in how operators use alarms during other plant operating modes such as startup and shutdown? During shift turnover? To support maintenance or surveillance testing?
- How will the use of alarm information in these situations differ for different members of the operating crew (e.g., supervisor, senior operator, board operator, shift technical advisor)?
- Which alarms should be displayed on fixed-position light boxes (or light box replicas on VDUs)? Which alarms should be on displays that are continuously visible to the entire crew (e.g., on overhead annunciator tiles or on overview displays)? See EPRI 1003696 for guidance on various types of alarm displays.
- How will alarm information be coordinated with, or integrated into, other displays and systems used by the operators for monitoring and control? For example, will alarms be integrated into process mimic type displays? Will alarms be integrated into the control displays or windows (e.g., a control window for operating a pump or valve)?
- How will acknowledgment of alarms be handled, and how will this be coordinated among the various systems that present alarms? How will audible tones be silenced and by whom?
- Will temporary operator-defined alarms be allowed, and if so, how will they be administered?
- How will out-of-service alarms be administered?
- How will operations be affected and what procedures will be used if there is a credible failure causing loss of some of the alarms (e.g., partial or full loss of annunciators, loss of workstation displays that provide alarm information, loss of any overview alarm displays, or loss of an alarm processor)?

Improving Alarm Definition and Alarm Logic

► Improve the logic for existing alarms

For alarms that are to be retained on conventional annunciators, the ability to implement improved or smarter alarm logic is very limited. However, as alarms are moved onto newer digital platforms, such as a DCS, there is much more capability for improved alarm logic to be applied. The greatest reduction in alarm overload will be achieved if all of the existing alarms, as well as any new ones that are created, are reviewed to ensure they are valid alarm conditions and to identify changes in their definition and logic that will reduce unnecessary alarms in transients and non-power operating modes.

Appendix A provides a checklist that can assist in this review. It helps identify conditions under which the alarm might be expected to occur and not require any operator action (for example, following a plant trip, on shutdown of the associated equipment, or changes in a system operating mode). It also addresses whether the alarm might "chatter" or cause repeated occurrences, and whether it is redundant with other alarms and might be combined with them. It suggests measures that might be taken to deal with each of these situations.

► Ensure all new alarms are defined with appropriate logic

As new alarms are identified, appropriate alarm logic should be defined at the outset to ensure that the alarms are meaningful and do not contribute to alarm overload. Use the checklist in Appendix A when defining any new alarms.

► Implement a continuous alarm improvement process

If sufficient resources are not available initially to review all the existing alarms, then at least ensure that all new alarms created are defined properly and appropriate logic is applied per the guideline above, and begin a program of continuous improvement for the existing alarms. Any nuisances or other problem alarms that are identified during operation should be specifically addressed. In addition, plan to go through the alarms in a methodical way over time so that all alarms eventually are reviewed and smarter logic is defined. Use the alarm definition checklist in Appendix A to support this continuous improvement process.

Simplified Methods for Reducing Alarm Overload

A complete review of all the existing alarms to identify improved alarm definition and alarm logic can require a significant investment of resources, including time from experienced operations and engineering personnel. However, there are some things that can be done with fewer resources that can make substantial improvement in the alarm overload situation. Two of these were discussed in the last two guidelines presented above – making sure that all new alarms are defined with alarm reduction in mind, and starting a continuous improvement process for the existing alarms. The plant can then, over time, move toward a smarter alarm set that will reduce or eliminate the alarm overload problem.

In addition, there are ways to target groups of alarms that are major contributors to the problem, and to define relatively simple operator aids to help deal with the alarm overload that are less resource-intensive to develop. These are described in the guidelines below.

► Identify and target alarms that are significant contributors to alarm overload

One way to reduce the level of effort required to reduce alarm overload is to target the alarms that are the biggest contributors to the problem. Review the alarm histories, if available, for actual transients that have occurred in the plant, such as reactor trips. See Section 6 for an example of such a review. Table 6-2 identified alarms that occurred in two of the three trips examined for the plant used in that example. By reviewing the "core set" of expected post-trip alarms, blocks of alarms can be identified for which alarm reduction techniques might be applied to reduce the post-trip alarm flood.

For example, alarms that repeat or chatter can be identified from this review. Also, groups of alarms that result directly from the trip because of system state changes can be identified relatively easily (e.g., alarms from the rod control system, turbine-generator controls, etc.). These can be targeted for alarm suppression logic or cutouts based on the trip signal or other system-level conditions that indicate the alarms are irrelevant and can be suppressed. Redundant (multi-sensor) alarms and sets of alarms that tend to repeat or chatter also can be identified.

The plant simulator can be used to generate alarm histories for trips and for other transients for which actual alarm data are not available. Examples are safety injection actuation, containment isolation, and electrical upsets such as loss of a major bus. By running these scenarios in the simulator multiple times with different variations (e.g., different power levels and different causes), the alarm data can be reviewed to identify the patterns of alarms – core sets of alarms that are expected to occur following each type of event. Again, blocks of alarms and individual problem alarms (e.g., repeating alarms) can be targeted for alarm reduction using the techniques described in Section 5. Once the alarms are identified, the checklist in Appendix A can be used to help define the appropriate logic.

► Provide an operator aid that highlights unusual alarms in transients

Section 6 illustrated an example of a relatively simple operator aid that can display only the unusual or unexpected alarms, while still providing access to all the alarm information. Simulator alarm histories can be used, along with any actual plant transient alarm sequences, to identify the "core set" of expected alarms for each of several major transients, as described in the guideline above. However, in this case, rather than build in logic to address these alarms and eliminate unnecessary occurrences, the core set of alarms can be used to identify expected and unexpected alarms when a transient occurs in the plant. The unexpected alarms can be presented as a listing on a separate display, as shown in the example of Table 6-5. Or all of the alarms can be listed with the unusual (unexpected) alarms highlighted, as illustrated in Table 6-6.

As described for that example, there are options regarding whether only incoming alarms are shown, or incoming and clearing alarms are listed. Repeating alarms can be eliminated from the list as another way to reduce its length. Again, all alarm event information can still be made available to the operators on demand so that nothing is lost. With this type of approach, the core or expected alarm list need not be perfect. It can be created initially in a semi-automatic fashion (spreadsheet macros were used to create the example in Section 6).
A modest amount of review by experienced operators should be sufficient to identify any obvious omissions or alarms that should be removed from the list. As discussed in Section 6, the operators should be trained to use this type of operator aid and should fully understand its basis.

Work with the DCS vendor or integrator to implement a software application that can provide the operator aid. If it is not practical to implement it as an application within the DCS, then consider using third-party software that can access the DCS alarm data and allow development of a separate operator aid. Third-party tools are available that can interface with all the major DCS systems.

Specifying and Implementing DCS Alarm Management

It is important to remember that the DCS vendors will not know what the plant wants in the way of alarm management unless this is communicated clearly to them. Most vendors have seen many different customer preferences as to what makes a good alarm system, as there is no real standard within the industry that defines this. There may be a number of options available within the set of standard offerings, and vendors are responding to customer requests to develop additional capabilities. Communication of what is desired and what is mandatory is very important to ensure the plant gets what it wants and the costs are well understood by both parties. Use the guidance given below to help define, specify and implement alarm management capabilities that fit the plant's overall alarm management strategy.

Note: Throughout this report we use "DCS" to refer to any digital control or monitoring system the plant will be installing that will generate or present alarms in the main control room. The guidance can be applied to a variety of systems including new plant computer systems, control/monitoring systems based on programmable logic controllers, or distributed control systems.

► Understand the DCS alarm management capabilities

The plant should develop a good understanding of the alarm management capabilities that are part of the base system (standard offering), additional capabilities that may be available as options beyond the base offering, any future capabilities that are under development and the likelihood that these will be available for the current project or as future enhancements. As part of developing this understanding, ask the vendor or supplier for the following kinds of information. Refer to the information given in Sections 4 and 5 and in particular Table 5-1 for more details on these items:

- Ability to apply logic or "cutouts" to individual alarms based on the values of other points within the system (sensed or calculated)
- Capability for mode-based alarm setpoints (ability to set different setpoints for the same variable depending on the plant operating mode)
- Capability to define a post-trip mode that is automatically determined by the system (see Figure 5-1)
- Capability for time delay filtering and chatter detection to address repeating alarms
- Ability to apply severity-based suppression to alarm message lists
- Capability for suppression based on redundancy (multi-sensor alarms)

- Capability to build state-based models of the plant and its systems to support a more structured alarm definition based on state information (see the discussion under *More Advanced Alarm Processing Systems* in Section 5)
- Ability to segregate maintenance-related alarms from those that require operator action; ability to route these to a maintenance workstation or separate display for maintenance personnel.

The best approach is to obtain much of this information during the evaluation of the available systems, prior to selecting a specific system for procurement. However, at a minimum, this understanding of system capabilities should be obtained prior to development of the purchase specification for the chosen system so that appropriate decisions can be made regarding the features that will be implemented.

► Specify alarm management capabilities and their implementation

Decide what alarm management features are needed and work with the system vendor or supplier to specify these in detail. This should include clearly defining what capabilities are needed "out of the box" for use in the first application of the system, and what capabilities should be built into the purchased system but will be implemented in the future.

Determine how the detailed configuration of alarms will be done, when it will be done, and by whom. Ensure that this is properly reflected in the specifications and contractual arrangements with the vendor. If the responsibility for configuration is left to the vendor without any specific instructions, the vendor may use default settings for alarms that will later have to be reconfigured at the plant. This can be much more costly and cause delays in implementation. It is best to define clearly, up-front, who will do the alarm configuration, how it will be done, and how the plant's alarm management strategy and practices will be enforced. Lack of attention to this can lead to proliferation of alarms, generation of alarm messages that are not understandable to the plant's operators, and lack of appropriate alarm logic, which can lead to a worsening of the alarm overload situation during transients.

The vendor should be required to provide information on all diagnostic and failure detection alarms that are provided as part of the system for <u>internal</u> faults and failures. The vendor should specify what action is required for each of these conditions and its effect on system functionality and operation. This information will be needed to support development of alarm response procedures and ensuring that the alarms are routed properly to operations and/or maintenance personnel for action.

The plant should specify what is wanted in terms of detection and alarming of <u>external</u> fault and failure conditions where these features are optional or configurable. This would include, for example, signal validation features such as out-of-range detection, open/short circuit detection, etc.

► Plan for iteration

Experience has shown that it is very difficult to accurately budget and plan for a DCS installation, particularly on the first application. In order to work within a given budget and project schedule constraints without major rework or disappointment at the time of installation, significant communication and cooperation is needed between the supplier and the plant. This is very important so that clarifications in requirements and as-delivered system capabilities, any difficulties in system configuration and implementation, and other issues can be worked out as the project progresses. Plan for some iteration and allow for this in the project schedule and in the commitment of plant resources to be available and involved during the system development.

Alarm Prioritization, Presentation and Acknowledgment

► Do as much as possible with prioritization, presentation, and acknowledgment

Although they are not the focus of this report, alarm prioritization, methods of presenting alarms, and controls provided for acknowledging alarms and silencing horns can have a significant impact on the operating crew's ability to deal with alarm overload during upsets. As discussed in Section 5, methods for prioritizing and presenting alarms interact with alarm processing methods in determining the overall effectiveness in alleviating alarm overload. It is important to include these when considering improved alarm definition and processing, and to take advantage of prioritization and presentation methods that can help operators deal with large numbers of alarms and support their tasks during transients.

Also, alarm acknowledgment and silencing controls and features that can reduce the amount of distraction from alarms during upsets should be considered. For example, some plants make use of a "global silence" feature that allows an operator or supervisor to silence all control room audible tones with a single switch until another alarm occurs. Another approach is to provide a keylock switch that disables audible devices so that no further audible alerts are received while the switch is enabled. This can be combined with a timer that restores the audible alerts after a time, to help ensure that alarm tones are not disabled indefinitely. The burden and distraction associated with acknowledgment of alarms and dealing with audible nuisances should be considered along with alarm processing methods when addressing the alarm overload problem.

Using Third-Party Tools

► Consider third-party software tools as possible aids for alarm management

As discussed in Section 5, there are software tools available that can assist with alarm management. Such tools can interface with the DCS and provide metrics that examine alarm system performance, identify potential nuisance alarms, and possibly identify groups of alarms that are related and thus may be candidates for improved alarm logic. At present these tools have been applied primarily in the process industries and are best suited to the particular situation in those facilities. However, it is expected that over time the tools will become more advanced and others will be developed that may be of help in defining changes that improve alarm management with less investment of time from plant personnel.

8
REFERENCES AND GLOSSARY

References

Campbell-Brown 1999. Campbell-Brown, Donald, *Alarm Management: A Problem Worth Taking Seriously – Part 1*, Control Magazine, July 1999.

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

EPRI 1003696. *Interim Human Factors Guidance for Hybrid Control Rooms and Digital I&C Systems*, EPRI, Palo Alto, CA, and Department of Energy, Washington, DC, September 2003. Product ID 1003696. (Note: this report will be revised and the latest revision should be used)

EPRI NP-3448. MPR Associates, *Procedure for Reviewing and Improving Power Plant Alarm Systems (Revision 1)*, NP-3448 Revision 1, Electric Power Research Institute, Palo Alto, CA, April 1990.

EPRI NP-4361. MPR Associates, *Power Plant Alarm Systems: A Survey and Recommended Approach for Evaluating Improvements*, NP-4361, Electric Power Research Institute, Palo Alto, CA, 1985.

EPRI NP-5693P. MPR Associates, *An Evaluation of Alternative Power Plant Alarm Presentations*, Electric Power Research Institute, Palo Alto, CA, March 1988.

EPRI TR-100838. Bechtel Corporation, *Alarm Processing and Diagnostic System*, TR-100838, Electric Power Research Institute, Palo Alto, CA, June 1992.

HSE CRR-166. M. L. Bransby and J. Jenkinson, *The Management of Alarm Systems*, U.K. Health and Safety Executive, HSE Books, Sudbury, Suffolk, Co., 1998. www.open.gov.uk/hse/hsehome.htm

Mostia 2003. Mostia, William L., *How to Perform Alarm Rationalization*, Control Magazine, August 2003.

MPR-1396. F.S. Corey, B.T. Ettinger, R.T. Fink, A. Zarechnak, *Application of the Alarm Processing and Diagnostic System Alarm Suppression Schemes to the Kewaunee Nuclear Power Plant*, MPR Associates, Alexandria, VA, June 1993.

MPR-1482. F.S. Corey, B.T. Ettinger, R.T. Fink, A. Zarechnak, *Evaluation of Two Alarm-Based Operator Aid Methodologies: Alarm Reduction and Diagnostics*, MPR Associates, Alexandria, VA, June 1993.

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, November 2000.

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, November 2000.

Rothenberg 2003. D. Rothenberg and C. Wilson, *Best Practices in DCS Alarm Management*, ISA POWID Conference, Williamsburg, VA, June 2003.

Swanekamp 2003. R. Swanekamp, *Older Coal-Fired Plants Implement Newest IT Tools*, Power Magazine, January/February 2003.

Glossary and Acronym List

alarm	An abnormal process condition requiring action by the operator
alarm cutouts	Logic or interlocks applied at the point of alarm generation to prevent unnecessary occurrences of an alarm in prescribed situations (e.g., logic that prevents a low discharge pressure alarm from occurring unless the pump is turned on – the alarm is defined as DISCHARGE PRESSURE LOW AND PUMP ON)
alarm definition	The design activity that identifies alarm conditions and defines associated setpoints. This activity also should define logic or cutouts needed to insure against unnecessary occurrences of the alarm.
alarm filtering	An alarm processing method that eliminates alarms determined to be less important, irrelevant, or otherwise unnecessary, such that these alarms are not available to the operator (see also *alarm suppression*)
alarm generation	The detection of off-normal conditions that have been defined as alarm conditions, and generation of an associated alarm signal or event for processing and presentation
alarm legend	The label or message describing an alarm, located on fixed-position tiles or alarm windows (for conventional annunciators the legend is typically engraved on the tile)
alarm management	The overall process of managing alarm information, including alarm definition, generation, processing, presentation, acknowledgment, and administration
alarm message	Description of the alarm condition that is given on an alarm display, e.g., in a chronological list of alarms on a VDU
alarm prioritization	The ranking of alarms based on pre-defined importance criteria such that alarms can be presented in a way that conveys their relative importance. Prioritization can be static or dynamic. Static priorities are pre-assigned and fixed – they do not change in real time or in response to changing plant conditions. Dynamic priorities do change in response to changing plant conditions – for example, priority of an alarm may be changed when the plant moves from one operating mode to another (mode-based dynamic priorities).

alarm processing	Real-time processing of alarm data – the link between alarm generation and alarm display. Processing may include assignment of priorities, alarm filtering, alarm suppression, creation of higher-level alarms, routing of alarms (e.g., routing maintenance related alarms to a maintenance workstation for action), and archiving of alarms.
alarm reduction	Use of alarm definition and/or alarm processing techniques to reduce the number of alarms occurring in plant transients or modes other than normal power operation (e.g., through use of *alarm filtering* or *alarm suppression*)
alarm suppression	An alarm processing method that does not present to the operator alarms determined to be less important, irrelevant, or otherwise unnecessary; however, the suppressed alarms can be accessed by the operators on request, or by the alarm system under certain conditions (see also *alarm filtering*)
alarm tile	In an annunciator system, a component of the visual display typically made from a translucent material that is illuminated from the rear and labeled or engraved with an *alarm legend* to identify the alarm condition being annunciated.
annunciator	A device or group of devices that call attention to changes in off-normal process conditions (*alarms*) using visual displays (typically *alarm tiles* arrayed on *light boxes*) and audible alerts (tones or horns)
annunciator window	See *alarm tile*
BWR	Boiling water reactor
DCS	Distributed control system, or digital control system
dynamic prioritization	See *alarm prioritization*
HSI	Human-system interface including elements such as displays, alarms, controls and procedures
I&C	Instrumentation and control
light box	An array of fixed-position windows or tiles that light or flash to signify an alarm. These can be driven by a conventional annunciator or shown on a computer-driven VDU
LOCA	Loss of coolant accident
message list	A list of *alarm messages*, often displayed on a VDU (e.g., a chronological list of alarm messages)

PWR	Pressurized water reactor
RCS	Reactor coolant system
SOE	Sequence of events – a time-ordered list of alarm and return-to-normal events used for determining time sequences and durations between events, most useful in post-trip analysis or root cause investigations of equipment failure
state model	A model of equipment, systems and/or the plant that represents the states of these entities and determines when the equipment, system or plant transitions from one state to another. A state model can be used to determine what conditions are normal for a given state and what conditions would be abnormal and unexpected for that state. States of lower-level entities can be used as inputs to determining states of higher-level entities (e.g., plant state depends on the states of the plant systems).
static prioritization	See *alarm prioritization*
tile	See *alarm tile*
VDU	Video display unit – a computer-driven display or screen-based device using any of the available computer-driven display technologies such as cathode ray tube, liquid crystal display, plasma display, etc.

A
ALARM DEFINITION CHECKLIST

This appendix provides a checklist for defining individual alarms and designing logic or "cutouts" that prevent unnecessary occurrences of the alarms. This checklist or one like it should be applied when any new alarms are defined. It also can be applied in a review of existing or "legacy" alarms to determine what improvements might be made to reduce nuisance alarm occurrences, or to make the alarms smarter and more meaningful to the operators.

The checklist is intended primarily for use with modern, digital control and monitoring systems such as a DCS. However, it also can be applied to alarms on plant computer systems and other standalone systems that generate or process alarms, depending on their capabilities. Also, it can be used to a degree with annunciator systems, particularly microprocessor-based systems, which provide some capability for alarm logic, chatter detection, etc., and also may allow alarms to be communicated to another system for further processing.

Checklist for
Alarm Definition and Logic Design

Alarm ID___________ Description ____

Operator Action

☐ Is operator action required in response to this alarm condition?

Be sure it is not just a "status alarm," signaling a change in the status of equipment or a system where the status change does not require any operator action. For example, a system designed to automatically transition to different modes may do so normally during a startup. It may be informative to the operator to know this has happened as expected, but it may not require any operator action. In fact, the reverse situation, when it does not occur as expected, may be a valid alarm. The normal or expected change of state might best be indicated on a display that the operator monitors during startup, with no annunciation. (Note that some status changes do require operator action – for example, an automatic control loop reverting suddenly to manual control due to a sensed failure – the operator needs to take manual control of the loop, so this is a valid and important alarm condition. In this case, the alarm should remain active until the operator can place the loop back into automatic control successfully, when the alarm would clear.)

A change in operating or monitoring strategy (e.g., monitoring an automatic action to verify it occurs and to back it up if it does not) may be a valid action.

Make sure the action to be taken is well defined so that it can be expressed clearly in an alarm response procedure. NOTE: Drafting the alarm response procedure at the time the alarm is defined is a very good practice. If you find it hard to write the response procedure, for example, if the operator action to be taken depends on the status of other conditions in the plant, this may indicate that additional logic is needed to properly define this alarm such that it will not occur unnecessarily – see questions below.

NOTES: ____

____

Maintenance Action

☐ Does the alarm primarily require action by maintenance personnel?

If so, it may be best to route this alarm to a maintenance workstation. The alarm message should be readily understandable by the maintenance technician who responds to it.

Even if the action is primarily by maintenance personnel, the operators may need to be alerted to the condition as well. But the information they need may be different, leading at least to a different alarm message and possibly to the need to create a higher-level alarm condition. For example, a low-level I&C fault alarm generated by self-diagnostics in a redundant system may require action only by maintenance personnel to investigate and repair the condition if both redundant channels are still functioning satisfactorily. A detailed message indicating the nature of the fault can be given to the maintenance technician. However, if the fault has placed the I&C system in a mode where redundancy has been lost (one channel is non-functional or in a tripped state), the operators may need to be made aware of this. The message to the operators should indicate the functional or operational impact, while the message to the maintenance tech should describe the details of the problem. For some faults, additional processing (e.g., combining several conditions or generating alarms at higher levels) may be needed in order to convey the true operational impact of the faults in a message that is appropriate for the operators.

NOTES: ____

____

Redundant Sensors

☐ Are there multiple redundant sensors or instrument channels for this same condition, which would also be alarmed? If so, should these be combined to form one alarm?

Simple OR logic can be used to combine multi-sensor alarm conditions such that any individual channel in the alarm state will trigger the alarm. Multiple channels often feed some type of voting logic (e.g., two out of four actuation logic), and there is a separate alarm indicating that the logic has tripped (an actuation alarm). The single-channel alarm may indicate a “half-tripped” condition, warning that actuation will occur on the next failure or next single-channel signal. In that case, the single-channel alarm (which can use OR logic combining all channels into one alarm) could be cut out if the actuation alarm has occurred, because it would be irrelevant after the trip or actuation. However, note that alarms on each individual channel may need to be captured and archived for sequence-of-events and diagnostic purposes (but not presented to the operators for short-term action – the actuation alarm does that).

Signal validation techniques can help when there are multiple sensors. For example, rather than having separate LOW LEVEL alarms on each instrument channel (LEVEL LO CH A, LEVEL LO CH B, etc.), the setpoint comparison can be applied to the validated signal to generate one alarm (LEVEL LO). In that case, the validation algorithm may generate additional alarms if there are discrepancies among any of the input channels, so that this can be investigated. Those might be maintenance alarms, where action is primarily by maintenance personnel to investigate the discrepancy (see separate question on alarms primarily requiring maintenance action).

NOTES: ____

____

Chatter Potential

☐ For alarms on analog variables, are there situations that could cause the variable to fluctuate or oscillate around the setpoint, making the alarm chatter?

Should the alarm have time delay filtering applied (e.g., low-pass filter or time delay) to prevent unnecessary alarms during momentary excursions or to prevent fluttering or chattering? Or should the alarm generation logic have hysteresis applied? Should time filtering be applied during equipment startup to prevent momentary alarms (e.g., alarm low discharge pressure only after a certain time has passed since the pump was commanded to start)?

NOTES: ____

____

Post-Trip Alarm

☐ Will this alarm occur normally following a plant trip?

If so, would altering the setpoint post-trip make the alarm meaningful and prevent unnecessary occurrences? Or could the alarm be conditioned on a signal (trip signal or other condition) that would prevent post-trip occurrences? If the alarm is expected, would its absence indicate an off-normal condition needing operator attention? Should an alarm be created to annunciate this situation?

NOTES: ____

____

Expected in Other Transients

☐ Would the alarm be expected to occur (and require no action) as a result of other plant transients or upsets?

Would it be expected after a Safety Injection actuation? After containment isolation? Electrical distribution system upsets? Could logic be applied in the alarm definition to prevent occurrence in these situations? If the alarm is expected, would its absence indicate an off-normal condition needing operator attention? Should an alarm be created to annunciate this situation?

For analog variables, could transients cause acceptable momentary excursions of the variable beyond the setpoint that should not be alarmed? Could the alarm be inhibited for a pre-determined period of time after the onset of such disturbances, such that it is re-enabled once the variable is expected to be back in bounds?

NOTES: ____

____

Plant Mode-Dependent

☐ Would this condition be expected to be in the alarm state in other plant modes?

Should different setpoints be applied for different modes, because the variable will normally operate in different ranges depending on the mode (e.g., the expected range for reactor coolant temperature is different for hot shutdown and cold shutdown than for normal power operation)? Or should the alarm be conditioned or cut out in certain modes because it is irrelevant in those cases? If the alarm is expected, would its absence indicate an off-normal condition needing operator attention? Should an alarm be created to annunciate this situation?

NOTES: ____

____

System State-Dependent

☐ Will the alarm occur unnecessarily when the associated system is in a state other than the normal full-power operation state?

Would the alarm be expected to occur when the system is out of service, in standby, in a test mode, or in an alternate operating lineup? Should the alarm be cut out in those situations? If the alarm is expected, would its absence indicate an off-normal condition needing operator attention? Should an alarm be created to annunciate this situation?

NOTES: ____

____

Equipment State-Dependent

☐ Will this alarm occur normally when the associated equipment is in a different state?

Would the alarm be expected when the equipment trips or is shut down? Momentarily when the equipment is started up? Should it be cut out in those situations? If the alarm is expected, would its absence indicate an off-normal condition needing operator attention? Should an alarm be created to annunciate this situation?

NOTES: ____

____

Other Unnecessary Occurrences

☐ In what other circumstances might this alarm occur and NOT require any operator action?

Would this alarm be brought in as a consequence of other conditions that generate their own alarms? Should it be cut out based on the other condition that brings this one in, or should the two be combined? If the alarm is expected, would its absence indicate an off-normal condition needing operator attention? Should an alarm be created to annunciate this situation?

NOTES: ____

____

WARNING: This Document contains information classified under U.S. Export Control regulations as restricted from export outside the United States. You are under an obligation to ensure that you have a legal right to obtain access to this information and to ensure that you obtain an export license prior to any re-export of this information. Special restrictions apply to access by anyone that is not a United States citizen or a Permanent United States resident. For further information regarding your obligations, please see the information contained below in the section titled "Export Control Restrictions."

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.

About EPRI

EPRI creates science and technology solutions for the global energy and energy services industry. U.S. electric utilities established the Electric Power Research Institute in 1973 as a nonprofit research consortium for the benefit of utility members, their customers, and society. Now known simply as EPRI, the company provides a wide range of innovative products and services to more than 1000 energy-related organizations in 40 countries. EPRI's multidisciplinary team of scientists and engineers draws on a worldwide network of technical and business expertise to help solve today's toughest energy and environmental problems.

EPRI. Electrify the World

Program:

Nuclear Power

1003662

Printed on recycled paper in the United States of America

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com