Pipeline SCADA Alarm Management

API RECOMMENDED PRACTICE 1167
SECOND EDITION, JUNE 2016

REAFFIRMED, OCTOBER 2021

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed. The use of API publications is voluntary. In some cases, third parties or authorities having jurisdiction may choose to incorporate API standards by reference and may mandate compliance.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to ensure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Foreword

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Shall: As used in a standard, “shall” denotes a minimum requirement in order to conform to the specification. Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the specification.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 200 Massachusetts Avenue, NW, Washington, DC 20001. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 200 Massachusetts Avenue, NW, Washington, DC 20001.

Suggested revisions are invited and should be submitted to the Standards Department, API, 200 Massachusetts Avenue, NW, Washington, DC 20001, standards@api.org.

Contents

Contents

Introduction

This publication was created by an API subcommittee. The members of this subcommittee were predominantly pipeline operators of liquid pipelines, but included participation from pipeline operators of gas pipelines, as well as members from the alarm management and control systems communities and U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration representatives.

With the technological advances of SCADA systems within the pipeline industry over the past two decades, it has become relatively simple to supply pipeline controllers with a wealth of information regarding the pipeline systems that they are operating. As the amount of information available to a controller increases, the importance of having a program in place to manage this information also increases. Alarm information should be presented to the controller in a manner that allows for easy identification and clear expectations as to the response required.

Pipeline SCADA Alarm Management

1 Scope

This document is intended to provide pipeline operators with recommended industry practices in the development, implementation, and maintenance of an alarm management program. It provides guidance on elements that include, but are not limited to, alarm definition, philosophy, documentation, management of change, and auditing.

This document is not intended to be a step-by-step set of instructions on how to build an alarm management system. Each pipeline operator has a unique operating philosophy and will therefore have a unique alarm philosophy as well. This document is intended to outline key elements for review when building an alarm management system.

SCADA systems used within the pipeline industry vary in their alarm-related capabilities. There are also many different software systems available to aid in alarm management. It is the responsibility of the pipeline operator to determine the best method to achieve their alarm management goals.

This document uses industry best practices to help to illustrate aspects of alarm management. The scope is intended to be broad. There are several publications and standards listed in Section 2 and the Bibliography that provide greater detail on the various elements of alarm management. Pipeline operators are encouraged to consult these publications.

2 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

API Recommended Practice 1165, *Recommended Practice for Pipeline SCADA Displays*

ANSI/ISA[1] 18.2-2009, *Management of Alarm Systems for the Process Industries*

49 CFR Part 192[2], *Transportation of Natural Gas and Other Gas by Pipeline: Minimum Federal Safety Standards*

49 CFR Part 195, *Transportation of Hazardous Liquids by Pipeline*

---

[1]The Instrumentation, Systems, and Automation Society, 67 Alexander Drive, Research Triangle Park, North Carolina, 22709, www.isa.org

[2]U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration, East Building, 2nd Floor, 1200 New Jersey Ave., SE, Washington, DC 20590, www.phmsa.dot.gov

3 Terms, Definitions, and Abbreviations

3.1 Definitions

For the purposes of this document, the following definitions apply.

3.1.1
alarm
Visible and/or audible means of indicating to the controller an equipment malfunction, an analog or accumulation process deviation, or other condition requiring a controller's response.

3.1.2
alarm configuration
(alarm attributes, alarm settings)
Setup of individual alarms (such as their setpoints, priorities, deadbands, delay times, etc.) produced by SCADA systems.

3.1.3
alarm flood
Condition determined by the operator, during which the alarm rate is greater than the controller can effectively manage.

3.1.4
alarm management
Processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems.

3.1.5
alarm objective analysis
AOA
See definition of "rationalization."

3.1.6
alarm occurrence
Audible and/or visible indication of the alarm, along with a time-stamped electronic record containing information about the particular alarm generated when the conditions of the alarm configuration are met (such as an analog value exceeding a high alarm setpoint).

NOTE Different alarm analyses can be made of both alarm configuration and alarm occurrences.

3.1.7
alarm philosophy
Document that establishes the basic definitions, principles, and processes to determine, design, document, implement, operate, monitor, and maintain an alarm system.

3.1.8
alarm priority
Relative importance assigned to each alarm indicating the urgency of response, typically using an allowable response time and consequence severity.

3.1.9
alarm setpoint
(alarm limit, alarm trip point)
Threshold value of an analog or discrete state or logic condition that triggers the alarm indication.

3.1.10
alarm system
Collection of hardware and software that detects a change in an operating condition, communicates the indication of that state to the controller either through an alarm or an alert, and records changes of the operating condition.

3.1.11
alert
Visible and/or audible means of notifying the controller when a controller-predefined operating condition has attained a certain value.

NOTE These notifications are used to drive controller awareness.

3.1.12
control system
See definition of “SCADA.”

NOTE This recommended practice uses the term “SCADA” as generic and inclusive of a variety of control system types.

3.1.13
diagnostic alarm
Alarm indicating sensor or hardware malfunction.

NOTE Controller’s reactions to diagnostic alarms may be limited to notification of the maintenance function.

3.1.14
human-machine interface
HMI
Collection of screens, displays, keyboards, switches, and other technologies used by the controller to monitor and interact with the SCADA system.

3.1.15
management of change
MOC
Process used by pipeline operators to manage changes to their facilities and processes, organizations, and documents to ensure that changes are adequately identified, evaluated, planned, controlled, and communicated.

NOTE “Change management” and “management of change” are interchangeable throughout this document.

3.1.16
master alarm database
Approved list of all rationalized alarms for a SCADA control system and their correct attributes and settings.

NOTE This information can be gathered, stored, and maintained using a variety of formats or methods.

3.1.17
nonannunciated event
An event occurrence that is not annunciated to the controller, does not impose a load on the controller, and is therefore not considered when determining controller alarm rates.

NOTE Some SCADA systems have the ability to route some event occurrences directly to electronic storage, without any indication to the controller, or to other functions (such as maintenance). Such nonannunciated events do not meet the general definition of an alarm used in this recommended practice.

3.1.18
nuisance alarm
Alarm that annunciates excessively or unnecessarily or does not return to normal after the correct response is taken (e.g. chattering, fleeting, false, or stale alarms).

3.1.19
operating position
Span of control and alarm responsibility of a single pipeline controller, generally involving computer consoles, graphical displays, and communication equipment enabling a controller to interact with the SCADA system.

NOTE A pipeline control room can have multiple operating positions.

3.1.20
pipeline control room
Operations center staffed by personnel charged with responsibility for remotely monitoring and/or controlling entire or multiple sections of pipeline systems.

NOTE For the purposes of this document, “pipeline control room” and “control room” are synonymous.

3.1.21
pipeline controller
Qualified individual whose function is to remotely monitor and/or control the operations of the entire or multiple sections of pipeline systems via a SCADA system from a pipeline control room and who has operational authority and accountability for the daily remote operational functions of pipeline systems as defined by the pipeline operator.

NOTE For the purposes of this document, “pipeline controller” and “controller” are synonymous.

3.1.22
pipeline controller response
Action that extends beyond the mental notation, visual recognition, or electronic acknowledgment of an alarm occurrence.

NOTE An action may include, but is not limited to, a change to operating parameters, modification to alarm limits, internal or external notifications, increased or more frequent monitoring of an operation, recording of process or operating data, or other specific action as defined by an alarm’s design.

3.1.23
pipeline operator
Entity that owns or operates pipeline facilities.

NOTE For the purposes of this document, “pipeline operator” and “operator” are synonymous.

3.1.24
rationalization
(alarm objective analysis [AOA])
Process to determine and ensure that alarms are selected, designed, prioritized, and documented in accordance with the principles of the pipeline operator’s alarm philosophy.

3.1.25
safety-related alarms
Alarms that specifically indicate that equipment, systems, or processes are outside operator-defined safety-related parameters.

3.1.26
shelve
Mechanism, typically initiated by the controller, to temporarily suppress an alarm, following proper administrative and functional requirements.

3.1.27
Supervisory Control and Data Acquisition
SCADA
Computer-based system that collects information about a pipeline facility, generates alarms, and provides a structured view of the pipeline system with the capability to control the pipeline operation.

NOTE 1 This is a generic definition of SCADA.

NOTE 2 The use of the term “SCADA” in this document is intended to be inclusive of industry-specific use of the term SCADA as well as including distributed control systems (DCSs) or systems that utilize programmable logic controllers (PLCs), remote terminal units (RTUs), or similar technologies. Commonly used terms such as “basic process control system” (BPCS) and “process control system” (PCS) are also synonyms for the purposes of this recommended practice.

3.1.28
suppress
Any mechanism to prevent the indication of a configured alarm to the controller when the alarm condition is present.

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

ACK	acknowledgment [event]
AMP	alarm management plan
AOA	alarm objective analysis
API	American Petroleum Institute
BPCS	basic process control system
CFR	*Code of Federal Regulations*
CTA	common trouble alarm
D&R	documentation and rationalization
DI	digital input
DO	digital output
ESD	emergency shutdown
HAZOP	hazard and operability
HH	HI-HI or high-high
HMI	human-machine interface
KPI	key performance indicator
LASD	local area shutdown
LL	LO-LO or low-low
MOC	management of change

PFD	process flow diagram
PHA	process hazard analysis
P&ID	piping and instrumentation diagram
PID	proportional-integral-derivative
PLC	programmable logic controller
RTU	remote terminal unit
SCADA	Supervisory Control and Data Acquisition
UPS	uninterruptible power supply

4 Alarm Management Plan

The purpose of the alarm management plan (AMP) is to establish alarm management effectiveness criteria and to evaluate the effectiveness of such criteria. Additionally, the AMP addresses how the alarm philosophy is utilized.

The AMP, intended to meet the requirements of 49 CFR 192 and 195, should include the following:

— alarm maintenance,

— identification of factors and criteria to measure alarm management effectiveness,

— governance items involving alarm setpoints and limits.

The AMP encompasses:

— alarm standardization and aligns with SCADA system design,

— best practices where applicable,

— well-defined and rationalized alarms.

It is recommended that the AMP contain:

— description of procedures and how they are implemented,

— planned alarm management effort for the year,

— project target to improve the alarm rates.

Control center personnel receive and are trained on this AMP as part of the overall control room management plan (refer to API RP 1168). Others with identified responsibilities within this plan also are provided access to this document and appropriate training.

5 Alarm Philosophy

5.1 Alarm Philosophy Purpose

An alarm philosophy is a comprehensive document that covers the proper ways to define, design, implement, maintain, monitor, and test an alarm system. It establishes the pipeline operator’s criteria, definitions, and principles for effective alarm management, including the required procedures or work processes, and metrics used to identify, classify, rationalize, prioritize, document, and manage alarms. All pipeline operators should develop, document, and follow their own comprehensive alarm philosophy.

A documented alarm philosophy helps to ensure:

— consistency of alarm design and presentation,

— consistency of alarms with the pipeline operator's risk management goals/objectives,

— agreement with good engineering practices,

— effective controller response to alarms.

The alarm philosophy should be designed to meet the federal regulation requirements of 49 CFR 192 and 195 and for having a written AMP to provide for effective controller response to alarms.

5.2 Alarm Philosophy Use and Contents

The philosophy document covers both new SCADA systems and existing systems. It is for both in-house use and contractor use during projects. Due to the wide variety of equipment used within the pipeline industry, the detailed contents of the alarm philosophy may vary from one location to another. However, alarms should be implemented consistently within a single SCADA system and across operating positions.

The philosophy document should provide a consistent and optimum basis for the following topics:

— alarm definition and principles;

— alarm selection and configuration;

— alarm system performance monitoring;

— procedures or work processes for resolution of alarm problems;

— methods for alarm rationalization and priority determination;

— alarm detection, presentation, annunciation, navigation, and controller interface;

— alarm documentation, including controller response to alarms;

— considerations for alarms routed to multiple controllers/locations;

— alarm handling methods;

— defined alarm design topics that are "up-front" decisions regarding the consistent implementation practices to be followed for the configuration of certain types of alarms;

— alarm system maintenance and testing;

— alarm system management of change (MOC);

— alarm system training;

— alarm system improvement process;

— alarm system roles and responsibilities;

— alarm system audit;

— definitions (not included in “alarm definition and principles” above) and references;

— alarm system training for noncontrol center personnel (e.g. staff, control system technicians, etc.).

The alarm philosophy should be based on several key principles as follows:

— The alarm system is to be designed to notify the controller of events requiring a response. Alarms are not a substitute for the controller’s routine monitoring of a pipeline or facility operation.

— Controllers are trained on the alarm management strategy.

— Proper alarm management enhances the controller’s ability to make a decision using experience, skill, and available information.

— Alarm priorities define the order of the controller’s response.

— The alarm system is routinely maintained.

— Controllers respond to all alarms, regardless of priority.

— The system design, therefore, should not produce more alarms than those to which the controller can respond.

— Alarms are not created solely upon the assumption that the controller will fail to respond to a different alarm.

NOTE Some of these may also be addressed in other company documents, such as operating procedures or engineering standards.

An alarm philosophy document need not be specific to a particular type of SCADA system as the principles and concepts are system independent. It is common to have SCADA system-specific appendices to the philosophy (or separate documents) that translate the principles to the particular features, capabilities, and limitations of a particular SCADA system.

Consideration should be given to each of the mentioned topics when preparing an alarm philosophy document.

6 Alarm Application and Determination

6.1 General Considerations

SCADA systems are structured to manage more than just alarms. A typical SCADA system structure may consist of alarms, alerts, and nonannunciated events. The primary focus of this document is on alarms because alarms have a significant importance in safely and effectively operating the pipeline. Alerts are used to drive awareness. The pipeline operator may choose to present alerts on a separate display or on the same display as alarms but with a lower priority. Nonannunciated events are configured similarly to an alarm, yet are not annunciated to the controller.

Properly implemented alarm systems play a key role in safe and effective pipeline operations. Improperly implemented, maintained, or overloaded alarm systems can significantly detract from the controller’s ability to accomplish effective operations and handle nonnormal conditions.

Alarms are used to indicate the need for controller action to return the pipeline to normal and safe operation or to avoid automated shutdowns. Alarms may also indicate the need for controller action in response to operational changes in hydraulics, volume measurement, or product quality operating situations.

The alarm system should be designed, configured, implemented, maintained, and managed in order to be an effective tool that assists in the controller's response.

Note that all references to alarms in this document exclude alerts and nonannunciated events. There are separate sections that define the use of these functions. All other information that is not an alarm, alert, or nonannunciated event should be excluded from the alarm system because it dilutes the importance of actual alarms. Such information can be more properly conveyed to the controller via a variety of other methods in the human-machine interface (HMI).

6.2 Alarm Determination

For alarms to have significance, alarms must be clearly distinguishable from alerts and from other information annunciated to the controller that does not adhere to the definition of an alarm.

The following characteristics are desirable for achieving effective alarm management:

— each alarm should require controller action;

— each alarm should be clear, meaningful, and relevant to the tasks of the controller;

— alarms should be properly chosen, designed, and implemented;

— each alarm should be documented and have a defined response;

— a single event should not produce multiple alarms signifying essentially the same thing;

— alarms should not activate during routine pipeline variable changes or from normal, expected modes of operation that do not require additional controller action;

— alarms should be designed to give the controller appropriate time to respond to the alarmed situation;

— alarms should be configured consistently;

— alarm rates should be within the handling capability of the controller;

— alarms should be prioritized in a manner that indicates their importance;

— the alarm system should perform as a useful tool for the controller in all operating modes and upset conditions;

— alarm systems should be properly controlled, monitored, and maintained.

6.3 Purpose and Use of Alarm Priority

Alarm priority indicates the relative importance of an alarm compared with other alarms. An effective alarm system uses multiple alarm priorities, which are clearly indicated to the controller. Consideration should be given to the several principles addressed below when determining the number and characteristics of the different alarm priorities. The determination of an alarm's priority should be accomplished in a consistent fashion. Consider the following characteristics when defining priorities:

— Each alarm priority should display in its own unique color.

— Each alarm priority should have its own sound.

— Alarms should present on an alarm summary type display and when appropriate on the controller's graphic displays.

— Unacknowledged alarms should have a different appearance than acknowledged alarms.

No more than four alarm priorities are recommended. Table B.1 is an example of distribution of percentages of alarms (configured and occurring) a pipeline operator might use, with four alarm priorities. In general, for higher priorities to have significance, they must be used sparingly.

6.4 Diagnostic Alarm Priority

Diagnostic alarms indicate a malfunction of a sensor or similar hardware. These are conditions about which the controller needs to know. Sensor malfunction may be a serious condition requiring a variety of controller actions. In many cases, however, only very limited controller action is desirable—action such as initiating a routine maintenance work request or a routine callout. The use of a separate priority for indication of such less serious conditions is often useful, since such alarms can be dealt with less urgently than other alarms in high alarm rate, upset situations. Some SCADA control systems allow for the temporary "filtering out" of such a priority.

6.5 Safety-related Alarms

Safety-related alarms are those that specifically indicate that pipeline equipment or operating conditions are outside pipeline operator-defined safety-related parameters. Federal regulations 49 CFR 192 and 195 specify certain requirements around safety-related alarms. It is therefore desirable for each pipeline operator to identify and document any safety-related alarms along with the criteria for that identification.

Some examples of methods for the identification of safety-related alarms are as follows:

— alarms designed to protect the public, property, or the environment;

— alarms indicating the failure of a safety system;

— alarms indicating the occurrence of safety-related conditions as identified pursuant to 49 CFR 192 and 195;

— alarms indicating the malfunction of sensors or equipment on a safety-related preventative maintenance schedule;

— alarms indicating conditions threatening product containment of hazardous materials;

— alarms designated as safety related resulting from a pipeline operator–conducted review or analysis.

Each pipeline operator should document his or her own criteria for this determination. Some pipeline operators have identified the following as examples of safety-related alarms:

— pressure exceeding the maximum established limit,

— pressure beneath minimum safe operating pressure,

— gas system odorization outside of allowable parameters,

— indications of an overfill or leak of hazardous material,

— fire,

— hazardous atmosphere.

6.6 Other Uses of the Alarm System

Often, certain uses of alarm records and alarm system functionality may be pertinent for analysis and activities other than those performed by a controller (e.g. diagnostic and reliability alarms). In such cases, care should be taken to ensure that the function does not subject the controller to nonrelevant alarms.

7 Alarm Documentation and Rationalization

7.1 General

Alarm documentation and rationalization (D&R) is a sound, consistent, and logical methodology by which alarms are determined, prioritized, and documented. Alarms resulting from the methodology are said to be rationalized.

Rationalization is the method by which existing or proposed alarms are reviewed and altered in order to be consistent with a pipeline operator's alarm philosophy or with recommended practices.

It is useful to identify identical equipment groups and create rationalization templates that minimize effort and increase consistency. A project approach or the accomplishment of rationalization in stages can also be effective.

7.2 Documentation & Rationalization Process

The D&R process involves a thorough examination of existing and potential alarms on a SCADA system. Any new alarms requested to be placed into service should be documented and rationalized prior to implementation to ensure compliance with the pipeline operator's alarm philosophy.

D&R should be implemented for the following purposes:

— to configure or reconfigure the alarms on new or existing SCADA systems in accordance with the pipeline operator's alarm philosophy;

— to identify and reduce duplicate alarms;

— to ensure proper and meaningful alarm setpoints and priorities;

— to configure alarms on points added or modified by projects or as needed based on changes in operations;

— to provide detailed alarm information for use by the controllers;

— to assist in the creation of the master alarm database, used as a reference for several aspects of alarm management (see 7.8).

7.3 Documentation & Rationalization Methodology

The D&R methodology involves a team of knowledgeable people doing the following:

— Discussing each configured and possible alarm on a point.

— Verifying that any configured alarm should exist at all, in accordance with the principles of alarm determination or the principles defined in the alarm philosophy.

— Verifying that an alarm does not duplicate another similar alarm that occurs under the same conditions.

— Determining the proper priority of each alarm in a consistent manner.

— Documenting alarm information in the following areas, as determined to be appropriate or applicable:

  — tag name or point name;

  — alarm identifier (the specific alarm on the tag being documented);

  — alarm message;

  — possible alarm causes;

  — method of alarm verification;

  — nature and severity of the consequences that will follow if proper controller response is not made to the alarm;

  — proper controller response to the alarm;

  — time available for the appropriate controller response to be made;

  — other tags or points likely to be involved with the alarm;

  — relevant operating procedures, piping and instrumentation diagrams (P&IDs), or safety studies;

  — normal operating range and proper alarm setpoint;

  — proper selection of other alarm attributes such as deadband and delay time;

  — appropriate maintenance response, if applicable;

  — applicability to this alarm of techniques such as state-based alarming, alarm flood suppression, or logic-based suppression;

  — other special considerations.

— Noting any modifications to the alarm needed, such as introduction of logic, reconfiguration of alarm type, alarm message rewording, graphic changes, etc.

— Recording the appropriate settings for each configuration for pipelines or facilities with different operating configurations; several different alarm values may be desirable.

The information captured in the D&R process becomes part of the pipeline operator's documentation. The documentation (i.e. master alarm database, spreadsheets, etc.) may be used for several purposes, such as meeting management of change requirements, training of controllers, auditing of alarm determination and attributes, and evaluation and analysis of alarm monitoring and effectiveness.

7.4 Documentation & Rationalization Preparation

In order to provide a more complete alarm review, for D&R, it is desirable that participants with expertise in these functional areas be involved, as applicable:

— experienced controllers from different shifts or teams;

— SCADA system engineers, programmers, and technicians;

— safety and environmental experts;

— pipeline engineer and/or hydraulic expert;

— maintenance or field personnel;

— personnel knowledgeable about applicable regulations (safety, environmental, etc.).

Desirable information as preparation for a D&R includes the following, as appropriate:

— process flow diagrams (PFDs) and P&IDs;

— operating procedures and similar documents;

— list of all alarmable SCADA system points by system and location and their configuration;

— results from audits or similar reviews such as process hazard analysis (PHA) or hazard and operability (HAZOP) study;

— emergency shutdown (ESD) system logic or cause/effect diagrams;

— SCADA system operating graphic screens/printouts;

— online access to historical data (analogs, event logs, alarm logs, etc.).

It is useful to identify identical equipment groups and create rationalization templates to minimize effort and increase consistency. Providing guidance for alarm design for specific situations as defined in the alarm philosophy can also improve productivity in the effort.

7.5 Determination and Assignment of Alarm Priority

It is important that alarm priority be determined in an effective and consistent manner. Proven methods for priority determination include examination of the following factors:

— the nature and severity of the consequence that will occur without proper controller response to the alarm,

— the time available to the controller to make the response before the consequence becomes unavoidable.

A specific example of a grid-based method for the determination of priority is provided in Annex A.

7.6 Determination of Alarm Setpoint

The proper alarm setpoint is determined or verified during rationalization. Relevant information for the determination includes the following:

— examination of alarm history;

— examination of relevant operational procedures;

— examination of equipment specifications from the manufacturer (which may dictate limits on rates of change or time to respond);

— examination of related design limits and/or safety system design and specifications;

— examination of equipment or system response time to the alarm event;

— understanding of the nature of the controller activities in diagnosing and responding to the situation.

The value for each alarm setpoint should be such that, in response, the controller will likely have enough time to reasonably manage the situation before undue consequences occur.

7.7 Staged Approaches to Alarm Rationalization

Because rationalization may involve a significant use of pipeline operator resources, a project approach or the accomplishment of rationalization in stages can also be effective and efficient. Several approaches are possible, and the selection is generally guided by the alarm performance data from the system to be rationalized.

Such staged approaches may include, but not limited to, the following:

— rationalization beginning with the most frequent, nuisance, or otherwise problematic alarms;

— rationalization beginning with systems seen to have the highest criticality;

— rationalization beginning with the most significant or important alarms as identified in various owner documents;

— rationalization of the first of many similar systems and the subsequent application of the results to the other systems;

— rationalization of classes or types of similar equipment;

— rationalization beginning with alarms seen by the controllers or other staff as being nonpertinent based on surveys or similar identification methods.

7.8 Recommended Storage of Documentation & Rationalization Information

The master alarm database information captured in the D&R process is valuable. It should be available and accessible by controllers and staff, and under MOC control.

There are many different tools that can be used to store the information developed in the D&R process. These tools range from third-party software specifically designed for a D&R process to in-house tools, such as spreadsheets, content management systems, or databases. Additional information can be stored along with the D&R information that may be beneficial to the users.

8 SCADA System Alarm Functionality and Alarm Design

8.1 General

Several different alarm types are associated with the control systems commonly used in pipeline facilities. SCADA system alarm functionality differs from vendor to vendor. The commonly available capabilities are covered in this section. Recommendations for the appropriate design and use of these alarms are also provided.

Field sensors transmit data to the central SCADA system. Points (or tags) are basic structures built in the SCADA system to represent various inputs, outputs, and control structures. Several different alarm types are associated with the SCADA systems commonly used in pipeline operations. The most typical point and alarm types are described in 8.2.1 through 8.2.8.

8.2 Point Types and Alarm Types

8.2.1 Analog Point

These points indicate a variable pipeline value from a field sensor, such as a temperature, pressure, tank level, or flow transmitter. Available analog point alarms are typically as follows:

— HIGH or LOW—Analog is above or below a certain alarm setpoint. The alarm setpoint should be determined based on consequence avoidance (such as equipment safety or operating limits) and not as a substitute for appropriate pipeline or facility monitoring.

— HI-HI (HH) or LO-LO (LL)—Analog is above or below a certain alarm setpoint higher or lower than the HIGH or LOW setting. This second level of alarm should not be configured by default but should be used only to indicate a significantly different situation than the HIGH or LOW alarm. The controller action for the HH or LL alarm should be significantly different in kind or degree from the action taken at the high or low value. HH and LL alarms should not be used as “reminders.”

— Rate-of-change (positive and negative)—Rate-of-change alarms should be used with care as they can generate spurious alarms during normal transitions.

— Failure (indicating a sensor malfunction)—The potential use of a diagnostic priority for such alarms is covered in Section 6.

8.2.2 Proportional-integral-derivative Controller Point

The proportional-integral-derivative (PID) controller point encompasses an analog input, a PID controller function, and an analog output. Alarm capabilities for controller points generally include all of the available types for analog points, with several additions. Use of these alarms should be determined by the process of rationalization and consequence avoidance; they should not be set by default. Available PID alarms are typically as follows:

— DEVIATION FROM PID CONTROLLER SETPOINT—HIGH and LOW. Deviation alarms should be used with care as they can generate spurious alarms during normal transitions.

— PID CONTROLLER OUTPUT (HIGH and LOW).

— PID CONTROLLER MALFUNCTION or ERROR. See the discussion of diagnostic alarm priority in Section 6.

8.2.3 Digital Input and Output Points

Digital input (DI) and digital output (DO) points indicate a binary value from or to a sensor or field element. Examples include a switch with two positions, or an on-off motor or valve. Available DI and DO alarms are typically as follows:

— OFF-NORMAL—An alarm is assigned to one or the other states of the input or output signal. Common misuse of this alarm type often results in inappropriate alarms.

— CHANGE-OF-STATE—An alarm is produced whenever the DI or DO changes state.

— Failure—The potential use of a diagnostic priority for such alarms is covered in Section 6.

These types of alarms are often misused to indicate normal and appropriate status change that does not require controller action.

8.2.4 Digital Composite Point

These points combine DI, DO, and a command function. They are often used for such things as manual starting of a device. The additional alarms made possible by this structure are as follows:

— COMMAND-DISAGREE—The device's status does not match the command given to it. Usually a time delay for the alarm is provided to avoid inappropriate activation.

— UNCOMMANDED CHANGE—The device's status changed without a command given to it.

8.2.5 Logic Point

Logic points are general-purpose structures that can compare multiple inputs and outputs from many different point types and can compare those readings in logical ways, typically Boolean. Logic points may have several designated alarms that can be activated based on the results of the logic evaluation.

8.2.6 Program Point

Some SCADA systems have a programming language that can be used to create very sophisticated functionality. Various custom alarms can be created via program action. All program-related alarms should be clear and understandable by the controller, including diagnostic alarms indicating the malfunction or failure of the program itself.

8.2.7 Other Special-purpose Points

Other point types are available in SCADA systems (e.g. selector points, ratio points, calculation points, etc.) and may contain other special-purpose alarm types.

8.2.8 Common Trouble Alarms

Logic constructs can be used to create summary-type alarms based on inputs from several different sensors, such as a "lubrication problem" alarm that is activated based on a variety of oil pressure, flow, level, and temperature conditions. Common trouble alarms (CTAs) can be effective in reducing the number of alarms resulting from a common cause. There should be associated graphics that indicate the particular inputs that have activated the CTA.

8.3 Alarm Priority

An important selectable attribute of an alarm is its priority, which is used as a differentiator of the importance of an alarm compared with other alarms. SCADA systems may offer from a few priorities to hundreds of them. Guidance for proper usage of alarm priority is provided in the Alarm Documentation and Rationalization and other sections of this document (e.g. Section 6, Section 13, Annex A, and Annex B). Priority is often misconfigured if proper guidance is not provided in the alarm philosophy and followed.

Different colors and sounds in the HMI are typically used to differentiate alarm priorities. A sorting mechanism for priority is often available. Other annunciation, display, and acknowledgment behavior is typically related to the alarm priority selection. Some SCADA systems include special-purpose "priorities" or capabilities. These may provide for functions such as the creation of a nonannunciated event to the controller that only generates a time-stamped occurrence into the historical journal (a "JOURNAL-ONLY" priority).

8.4 Alarm Settings and Alarm Occurrences

Alarm settings are the underlying configuration of the alarm system, such as the various alarm types, setpoints, and priorities. The collection of all correct alarm settings that should be in effect in the SCADA system constitutes the master alarm database. MOC of these settings is an important issue to be addressed (see Section 14).

Configured alarms produce alarm occurrences when the SCADA point or value matches or exceeds the alarm settings. Alarm occurrences are time-stamped electronic records. They typically contain the following types of data:

— time stamp—date and time (with one-second resolution or better);

— point identification and description;

— alarm message or descriptor;

— type of alarm;

— location;

— priority;

— alarm setpoint and current value at the time of the alarm;

— unit of measure;

— console or system indicator (where the alarm was annunciated).

8.5 Other Alarm-related Electronic Records

Alarm-related records typically include the following items:

— Return-to-normal (alarm clear) event—This record is produced when the SCADA point or value changes to a condition that would no longer generate the alarm.

— Acknowledgment (ACK) event—The act of a controller acknowledging that an alarm produces this record.

SCADA systems may allow for single-alarm acknowledgment, full-page-at-a-time acknowledgment, simultaneous acknowledgment of alarms in groups such as individual or multiple pieces of equipment, or total area acknowledgment. Inferences about controller awareness and behaviors are difficult to make based solely on alarm acknowledgment records.

These records typically contain similar information content to alarm occurrences but are usually not annunciated. Pipeline operators should understand the particular SCADA system's methods of alarm acknowledgment.

8.6 Alarm Logs/Alarm Summaries

Alarm occurrences are typically logged electronically by the SCADA system. For more extensive alarm system analysis, the alarm records may also be captured in an external database. There are a variety of ways to accomplish this based on the SCADA system connectivity capabilities. Many facilities have several years of online alarm data available for analysis.

8.7 Event Logs/Event Summaries

SCADA systems also capture all controller-initiated changes (alarms, PID controller setpoints and modes, analog outputs, digital states, numeric entries, etc.) in similar event records and electronic logs. The analysis of these records can yield important insights as to the SCADA system's functioning and behavior.

8.8 Alarm Summary Display

The SCADA system typically comes with a predefined alarm summary display, which generally shows the alarm occurrences in a scrollable list. The display will typically have a variety of sorting, filtering, and paging features. New unacknowledged alarms typically display a different visual behavior on the screen (such as “flashing” that changes when the alarm is acknowledged. When alarms return to normal, they usually disappear from the screen. The alarm summary display is often “left up all the time” on one of the physical display screens.

It is generally possible to select an alarm occurrence from the summary display and navigate to a predetermined screen, for that alarm, that gives the controller the information needed for proper response. Such functionality should be configured and used when available.

SCADA systems may have many optional settings for the form and nature of information displayed on the alarm summary. Those options should be examined and understood in detail rather than using the manufacturer’s default settings. Desired settings and functionality should be documented in the alarm philosophy.

SCADA systems may provide functionality that allows a controller to acknowledge multiple active alarms simultaneously. The primary purpose of this feature is to allow acknowledgment of multiple alarms generated when communications from the field are lost or restored. Since acknowledging multiple alarms simultaneously can cause a controller to miss an alarm that requires an action, each pipeline operator should have a written process in place, for using the “acknowledge all” feature, to prevent such occurrences.

8.9 Alarm Deadband

Alarm deadband is the change in the analog from the alarm setpoint necessary to clear the alarm. Because all analog signals have noise, without a proper deadband an analog value moving through the alarm setpoint will likely produce multiple unnecessary alarm occurrences. Proper engineering judgment should be used when setting deadbands in order to minimize nuisance alarms. Excessive deadband values can act as an alarm latch, creating stale alarms. Deadband settings should be documented and reviewed based on operating experience. Some examples of commonly accepted starting values for deadband are as follows:

Signal type	Deadband (percent of operating range)
Flow rate	5 %
Level	5 %
Pressure	2 %
Temperature	1 %

8.10 Alarm On-Delay and Off-Delay

Some SCADA systems make it possible to delay the activation or clearing of individual alarms. This is useful, when done with care, in addressing chattering and fleeting alarms.

For an on-delay, the SCADA point or value must remain in the alarm state for a specified number of seconds before the alarm is initially annunciated. An off-delay requires that the SCADA point or value that would result in the alarm clearing must remain in that state for a specified number of seconds before the alarm is cleared.

Often, very small delay values (e.g. 15 seconds) can solve specific alarm problems. Calculation methods are documented in reference literature. Good engineering judgment should be applied to the selection of values of on-delay and off-delay times. On-delay times can reduce the available response time for the Controller, and off-delay times affect the display of a cleared alarm status. The alarm philosophy should document proper principles for the use of delay times and deadbands.

8.11 Alarm Suppression and Alarm Shelving

SCADA systems usually provide the capability to manually suppress an already-configured alarm. Alarm suppression is therefore an override of a previous decision to have an alarm. It is different than an intentional choice to either deconfigure or explicitly not have a particular alarm. SCADA systems handle and allow suppression in a variety of ways, both manual and automatic (i.e. designed).

Manual alarm suppression is typically controlled via SCADA system security settings, keys, and passwords of varying effectiveness. Care should be taken to ensure that any alarm that is manually suppressed is properly documented, tracked, communicated, and addressed through an appropriate MOC process.

Alarm shelving describes alarm suppression for a predetermined period of time, as determined by the pipeline operator. The pipeline controller usually places an alarm in a temporarily suppressed “shelved” state if it is malfunctioning or chattering or to allow for alarm testing. When the time has elapsed for the chosen suppression period, the suppression is cleared and the alarm is back in service. Alarm shelving is manually initiated and automatically cleared.

The design, implementation, and use of any alarm suppression capabilities should be rigorously controlled because hazardous situations and accidents have been traced to improper, uncontrolled, and unmonitored alarm suppression or shelving.

8.12 Alarm System Reliability

Generation of alarms in a modern SCADA control system is a deterministic and generally reliable process. If alarms are configured to occur under given conditions, they will. The primary reasons that the alarm process fails are as follows:

— The alarm has been improperly suppressed or its settings have been improperly altered.

— Improper sensor placement where an alarm may not activate if the sensor is placed in a location that can be isolated or bypassed under normal system operation.

— The sensor has malfunctioned, which affects not only the alarm but also anything else using the reading.

— Normally a sensor failure causes a diagnostic alarm on that sensor that would indicate to the controller that the signal and any alarms based on it are no longer available.

— Communication from the sensor has malfunctioned.

— Improper sensor calibration or drift.

— There is some sort of logic error in any special-handling structure designed to affect the alarm.

Sensor types can affect alarm function and reliability. For example, analog sensors providing information into a SCADA system tend to provide good reliability, whereas simple “switches” can be less dependable. Therefore, it is important to manage the devices providing information to the alarm system including measuring the reliability of the devices and quantifying the impact on effectiveness of the alarm system.

Instrument reliability and maintenance issues can be a source of nuisance or false alarms. Excessive quantities of nuisance alarms or false alarms can have a detrimental effect on alarm system and controller effectiveness.

8.13 Defined Alarm Design Cases

Up-front decisions around alarm configuration will aid in design consistency. Such decisions can usually be made in advance about several topics. The alarm philosophy should document and define the proper approach to the creation, configuration, prioritization, and controller response for alarms dealing with the following situations.

Each of the following is an alarm topic for which up-front decisions can ensure proper design consistency:

- examples of alarms that may be used to avoid harm to personnel:
  - flammable and toxic gas detectors,
  - leak or hydrocarbon detection alarms,
  - safety shower/eyebath actuation alarms,
  - uninterruptible power supply (UPS) malfunction,
  - field or remote manual emergency stop functions,
  - any similar alarm where controller action is the method by which harm to a person is avoided;
- building-related alarms;
- handling of diagnostic alarms from instrument malfunctions;
- alarms for redundant sensors and voting systems;
- complex external device health and status alarms;
- ESD systems or local area shutdown (LASD) systems;
- ESD bypasses;
- pre-alarms/combination alarms;
- leak detection alarms;
- duplicate alarms;
- consequential alarms;
- deviation alarms;
- communication alarms;
- off-normal alarms;
- reannunciation of alarms (rarely appropriate);
- alarm handling for programs;
- point, interlock, and program references to alarms;
- SCADA or control system status alarms.

9 Roles and Responsibilities

9.1 Overview and Introduction

The roles and responsibilities of pipeline operator personnel should be defined and documented as part of the overall alarm management program. Following is an example of a role and responsibility breakdown for various alarm management tasks. Each pipeline operator should provide the breakdown that meets his or her own organizational structure.

9.2 Management

The management team is the sponsor of the alarm management program that may consist of the following:

— Philosophy—Responsible for development of the overall philosophy and strategy; ensures compliance with stated requirements of the philosophy.

— D&R—Provides resources, scheduling, and oversight of alarm rationalization efforts.

— Auditing—Ensures that audits are performed and actions taken on the findings.

— MOC—Responsible for the design of the MOC process.

— Staffing and resources—Responsible for providing the tools and means to carry out the alarm management program.

9.3 Technical

The technical support team includes pipeline engineering, SCADA systems support, and instrumentation engineering and consists of the following:

— Philosophy—Provides input to the philosophy development.

— Design—Ensures that alarm system design, procurement, configuration, and implementation meets the needs as stated in the alarm philosophy.

— MOC—Performs alarm system changes in accordance with pipeline operator MOC policies.

9.4 Operations

The operations team (controllers) is the owner of the alarm system. The operations team may address the following areas:

— Design—Responsible for ensuring that the design of the alarm system meets the required operational performance.

— MOC—Responsible for implementation of the MOC process for the alarm system.

— Alarm documentation—Ensures that alarms are properly documented.

— Alarm handling—Responsible for ensuring proper controller response to alarms.

— Alarm system performance monitoring—Responsible that performance is assessed in accordance with the philosophy and actions taken as needed in response to problem areas.

10 Alarm Handling

10.1 General

There are several methods that are commonly used to ensure proper handling of alarms and acceptable system performance. The key principles used to govern these methods should be documented to ensure consistent application.

10.2 Nuisance Alarms

Nuisance alarms should be identified and properly addressed to ensure optimal system performance, while meeting any applicable management of change and communication requirements with controllers. Excessive quantities of nuisance alarms can have a detrimental effect on alarm system and controller effectiveness. Chattering, fleeting, frequent, false, stale, and other nuisance alarms should be analyzed and a proper solution or repair applied. They should not be ignored or indefinitely suppressed.

10.3 Alarm Shelving

Individual alarms or groups of associated alarms may need to be suppressed for temporary periods. “Alarm shelving” is the term used for manually initiated alarm suppression accomplished with proper administrative controls. Shelving is a useful short-term way to handle a nuisance alarm between its identification and return to service.

Alarm shelving methodologies should ensure proper alarm reactivation, as the potential for undetected hazardous situations associated with suppressed alarms is high.

Shelving functionality should include the following:

— an easy and logical structure to find, shelve, and unshelve individual alarms;

— easily accessed and accurate lists of shelved alarms (generally accessed at shift change and monitored by appropriate staff);

— time limits and other exclusions and restrictions (i.e. authorization) for individual alarm shelving;

— the ability to suppress an individual alarm on a point, rather than unintended suppression of all alarms on the point;

— proper security access and approvals;

— capture of shelving initiation time, person responsible, and reason.

Alarm suppression outside of a controlled shelving methodology should be avoided, and regular checks should be made to identify any alarms that are improperly suppressed.

Any shelving solution should work in proper coordination with other alarm handling methodologies, state-based alarming, alarm flood suppression, and alarm settings audit and enforce mechanisms.

Manual and/or automated alarm shelving methods should be used in a consistent manner and should suppress only the specifically desired alarm functions.

10.4 Designed Alarm Suppression

Some SCADA systems have the capability to configure specific, automatic alarm suppression based on logic conditions. Upon predetermined combinations of conditions, certain alarms are automatically suppressed or unsuppressed. The intent is to reduce nuisance alarms and ensure that alarms are relevant for the conditions in effect.

Such implementations should be tested upon implementation to ensure proper functioning. In some cases, electronic records of the suppression function can be generated, and these can be used to verify the ongoing proper operation of the designed suppression functionality.

The design, implementation, and use of any alarm suppression capabilities should be controlled because hazardous situations and accidents have been traced to improper, uncontrolled, and unmonitored alarm suppression.

10.5 State-based or State-dependent Alarms

The basis for alarms generally pertains to the normal operating states of equipment or systems with the understanding that the equipment or systems often have several normal, but differing, operating states. SCADA system alarm capabilities are normally intended for single-state, single-value alarm setpoints and priorities. State examples include startup, shutdown, product transition, full or partial rates, open, closed, etc.

Besides individual pieces of equipment, sections of a pipeline system may have different operating states where fixed alarms produce inconsistent results. For example, the system may run in states where certain subsections are intentionally shut down, producing a variety of alarms, or redundant equipment may produce alarms when unused, even though that is a normal and proper operating condition. In these circumstances, the alarms produced do not meet the real criteria for an alarm (there is no controller action to take) and will become stale and contribute to alarm floods and confusion.

Recommended practice should be that all such normal operating states do not cause alarms. Alarms should be produced only upon nonnormal conditions or unexpected events. State-based methodologies involve dynamic alarm configurations based on the specific systems and equipment conditions. Multiple alarm setpoints and priority settings are configured for appropriate alarms and enabled based on system or device state.

State detection is accomplished by the automatic monitoring of operating conditions. Algorithms are created (which can include controller input if required) to correctly identify the current operating state of the equipment. Then, other automatic mechanisms (which can also include controller authorization) actually make the predetermined alarm modifications to match the current state. Any software methodology for dynamic change of alarms should be robust and have fail-safe mechanisms.

Multiple operating configurations and alarm settings are documented during alarm rationalization.

10.6 Alarm Flood Suppression

Many operating conditions, such as equipment shutdowns, can produce scores of alarms. Alarm floods can make a difficult operating condition much worse. In a severe flood, the alarm system becomes a nuisance, a hindrance, or a distraction rather than a useful tool. A controller’s effectiveness is diminished during an alarm flood, and important alarms are likely to be missed.

Alarm flood suppression is the dynamic management of predefined groups of alarms based on detection of equipment state and triggering events.

A proper flood suppression methodology detects that a compressor trip has occurred and immediately and temporarily suppresses those expected alarms that are closely associated with the compressor trip. They are then unsuppressed as part of the compressor trip diagnosis and restart.

A recommended strategy for alarm suppression is to identify those events that can cause severe flooding to occur and methodically analyze the events to determine which alarms can be modified or suppressed.

In SCADA systems, the alarm summary screen may have a variety of possible filtering mechanisms. Such capabilities can be useful in alarm floods, if they are carefully and thoughtfully configured and implemented.

10.7 Alarm Audit and Enforcement

SCADA systems are susceptible to alarm settings changes from a variety of sources. Periodic checks should be made to ensure that the current alarm configuration matches the proper settings as recorded in the master alarm database. Any deviations should be reported and appropriately dealt with.

Manual audit/comparison methods can be used, although these may be time-consuming and tedious in some cases. Automated systems can be used to accomplish such comparison. If an automated system is used, it should include the following characteristics:

— automated comparison (audit functionality) and production of exception reports;

— variable frequency scheduling (every shift, every day, etc.) for different selection groups of alarms;

— selectable automatic enforcement of alarm settings that do not match those in the master alarm database, back to the master values.

Automated audit and enforcement techniques should work correctly with any state-based, flood suppression, shelving, or other alarm handling strategies being used.

10.8 Special-purpose Priorities and Alarm Routing

Some SCADA systems have sophisticated diagnostic-type alarm capabilities that may not be relevant to the controller's task and have no possible controller response. If possible, such alarms should be routed directly to the maintenance or other function concerned with them rather than annunciating them to the controller.

10.9 Controller-adjustable Alarms

The alarm system is reserved for situations requiring controller action in order to prevent a consequence. The proper setpoints for alarms are independent of the individual controller's preference and are determined by rationalization. In general, controller change of alarm setpoints is a practice to be avoided, as it can result in such phenomena as shift-based variation. Since security settings for control of alarm setpoint change are not always effective, in some cases automated audit and enforce mechanisms are used to ensure proper alarm setpoints.

In some predetermined cases, it may be desirable that certain specific alarms have controller-adjustable alarm setpoints. Such cases should be documented and the adjustability criteria, conditions, and allowable ranges defined. Proper access control and monitoring of the alarm setpoints should ensure their correct use.

Examples of situations that might utilize controller-adjustable alarm setpoints include:

— Adjustable high- and low-level alarms used for tank switching or product changes. In such cases high-high or low-low alarms that provide protective functionality should not be controller adjustable.

— Pressure alarm settings for optimizing hydraulic efficiencies (excluding alarms indicating proximity to pressure relief conditions).

Alarms that have been rationalized to Priority 2 or 1 are generally not suitable to be controller adjustable.

11 Controller Alert Systems

There are situations where this restriction of controller change to alarms may present problems. There is often a need for “on-the-fly” configuration of various system reminders and functions based on the operating conditions attaining certain values. These situations will vary from day to day. The equivalent of a controller-determined “temporary notification or reminder” is sometimes desirable. These are referred to as “alerts.” Alerts are used to drive controller awareness. Such situations should be addressed in such a way that the proper Controller action (if there is an associated controller action) reliably occurs and that the integrity and functionality of the alarm system is not compromised. It is usually impractical to be constantly configuring and deconfiguring temporary alarms to meet these needs.

Alerts have the following characteristics:

— Alerts are often transient in nature and would not be suitable if implemented as a long-term alarm.

— Alerts are items that do not generally meet the rationalization criteria for alarms. For example, they may be administrative in nature regarding periodic reporting, sampling, testing, etc.

— Alerts are not alarms and must be clearly distinguishable from alarms.

— Alerts should have their own unique visual and audible characteristics.

— Alerts can appear on the alarm summary display as long as there is a distinguishable means of identifying alerts from alarm. (If the SCADA system is capable, alarms and alerts should be separated.)

Independent controller alert systems are available either from a SCADA system vendor or third-party vendor or can be proprietary.

The following characteristics are desirable for a controller alert system:

— Alerts may be user configurable (by individual controllers and by shift groups) and user controllable.

— Alerts may be configurable by the controller based on analog, digital, or logical points, singly or in combination.

— Alerts are often time based. Simple timers are also a useful controller alert tool.

— The audible notification of alerts may be capable of being temporarily suspended.

The intent is to ensure that any notification from the alert system is of lesser importance than a rationalized alarm. Therefore, the proper controller action is always to address alarms before dealing with alerts.

12 Nonannunciated Events

There can be events that are not relevant to the controller that are either not important while certain conditions exist or are for diagnostic purposes only.

Nonannunciated events may also have importance to other individuals within the organization, such as maintenance and management, for reporting, troubleshooting, etc. These events need to be stored as journal entries with time-stamped occurrences.

Pipeline operators should be mindful of the additional volume of journal entries because a significant increase in journal entries can affect the overall performance of the SCADA system. Only useful information should be designated as nonannunciated events.

13 Alarm Audits and Performance Monitoring

13.1 Overview and Introduction

Alarm system performance should be monitored and periodically audited. Auditing verifies that design, implementation, rationalization, operation, and maintenance of the alarm system are satisfactory. Pipeline operators are encouraged to have alarm system audits and performance analyses in an on-going improvement process to identify problems and drive corrective action. This section provides guidance on the use of alarm system analysis for both ongoing monitoring and periodic performance assessment. Several performance measures are described. Alerts do not need to be included in alarm metrics.

13.2 Audits of Managerial and Work Practices

Periodic audits should include a review of the managerial and work practices associated with the alarm system and determine whether those practices are adequate.

Personnel interviews should be conducted as part of the audit to identify performance and usability issues. Interview topics may include whether:

— alarms occur only on events that require controller action,

— alarm priority is consistently applied and meaningful,

— alarms occur in time for effective action to be taken,

— roles and responsibilities for the alarm system users and support personnel are clear,

— training regarding the proper use and functioning of the alarm system is effective.

The work processes and procedures that ensure compliance with the alarm philosophy should be evaluated for effectiveness on a periodic basis. The audit should review work practice documentation, including the following:

— alarms are used only to represent situations that require controller action in order to avoid defined consequences;

— alarms are well documented;

— alarm response information is current and sufficient to provide proper controller guidance;

— modification of alarm attributes is properly controlled via MOC and has not been subjected to improper change;

— alarm performance is monitored;

— malfunctioning alarms are fixed in a timely fashion;

— roles and responsibilities for the alarm system users and support personnel are clear, documented, and known by appropriate personnel.

Written audit reports are required. Action plans, including timelines and accountabilities, should be developed for problems identified during the audit.

13.3 Alarm System Performance Metrics

Various types of alarm system analyses are possible. Analyses are of two types: alarm occurrences (i.e. dynamic or real-time data) and alarm configuration data, such as:

— Alarm occurrences produce time-stamped records that contain specific alarm-related information.

— Alarm configuration is the underlying structure that is necessary in order that alarm records are produced, including the decisions about alarm types, alarm setpoints, priorities, deadbands, and similar items. This includes the configuration of advanced methodologies such as state-based alarming.

In general, at least 30 days of alarm occurrence data are desirable for calculating the key performance indicator (KPI) metrics in this section.

13.4 Alarm System Key Performance Indicators

13.4.1 General

Alarm system KPI targets depend on many factors, such as controller skill, HMI design, degree of automation, operating environment, types and significance of the alarms produced, and additional controller duties.

Sustained operation above the maximum manageable guidelines indicates an alarm system that is annunciating more alarms than a controller may be able to handle, and the likelihood of missing alarms increases.

When alarms have been properly rationalized and designed and nuisance alarms (e.g. chattering alarms) eliminated, the resulting alarm rate reflects the SCADA and/or local control system's ability to keep the pipeline or facility operating within bounds without requiring manual controller intervention. The solutions to high alarm rates may involve improvements to the SCADA and/or control system or to the operating procedures rather than adjustments to the alarm system.

The use of averages in evaluating alarm system performance can be misleading. Any period of time that produces more alarms than can be handled presents the likelihood of missed alarms, even if the average for that interval seems acceptable.

Some of the more common alarm system performance indicators, with their descriptions, are listed in 13.4.2 through 13.4.10.

13.4.2 Average Annunciated Alarm Rate per Controller Position

Annunciated alarms are those presented to the controller. Analysis of annunciated alarm rates is a good indicator of the overall health of the alarm system. The average annunciated alarm rate per controller position (i.e. the span of control and alarm responsibility of a single controller) based on one month of data should be less than the metrics shown in Annex C (see Table C.1). These rates are based on the ability of a controller and the time necessary to:

— detect an alarm,

— navigate within the SCADA system to the relevant information,

— analyze the situation,

— determine the proper corrective actions,

— perform the corrective actions,

— monitor the situation to ensure that the alarmed condition is successfully handled.

After alarms are rationalized, the resulting rate of alarms will provide part of the analysis for continued controller loading analysis.

13.4.3 Peak Annunciated Alarm Rates per Controller Position

Peak or average alarm rates that exceed the controller's capability for effective alarm handling increase the likelihood of missing an alarm. It is beneficial to take both the peak and average alarm rates into account simultaneously because either measurement on its own can be misleading.

13.4.4 Alarm Floods

Alarm floods are variable-duration periods of alarm activity with annunciation rates having the potential to exceed the controller's response capabilities.

Flood events should be analyzed for:

— overall number of floods per day and week,

— total duration of each flood event,

— total number of alarms generated during each flood,

— alarms making up each flood,

— total percentage of time that the alarm system spends in a flood condition.

Floods should be of short duration (minutes rather than hours) and low total alarm count during each flood.

13.4.5 Frequently Occurring Alarms

A relatively few individual alarms often produce a large percentage of the total alarm system load. The most frequent alarms should be reviewed at regular intervals (e.g. daily, weekly, or monthly). Substantial performance improvement can be made by addressing the most frequent alarms.

The most frequent alarms are likely not working properly or as designed. High-frequency alarms often have major skewing effects on other performance measurements. For example, the top ten most frequent alarms should comprise a small percentage of the overall system load. Action steps based on this analysis include review for proper functioning and design.

13.4.6 Chattering and Fleeting Alarms

A chattering alarm repeatedly transitions between the alarm state and the normal state in a short period of time. Fleeting alarms are similar short-duration alarms that do not immediately repeat. In both cases, the transition is not due to the result of controller action.

It is possible for a chattering alarm to generate hundreds or thousands of records in a few hours. This results in a significant distraction for the controllers. Chattering alarms are often high in the listing of the most frequent alarms.

Chattering and fleeting alarm behaviors should be eliminated. In many cases, they may be corrected by examining or increasing the deadband in the field device or alarmed input point. Alarm on-delay and off-delay adjustment can also address chattering and fleeting alarms.

13.4.7 Stale Alarms

Alarms that remain in effect continuously for more than 24 hours may be considered as stale. Some alarms may remain in the alarm state continuously for days, weeks, or months. Such alarms provide little valuable information to the controllers. They clutter the alarm displays and often represent conditions that should not be alarmed. Stale alarms should be examined to ensure that they were properly rationalized. Logic, programmatic, state-based, or similar methods can be used to eliminate stale alarms.

No alarm should be intentionally designed to become stale, and there is no long-term acceptable number of stale alarms.

13.4.8 Annunciated Alarm Priority Distribution

Effective use of alarm priority can enhance the ability of the controller to manage alarms and provide proper response. The effectiveness of alarm priority is related to the distribution of the alarm priorities: higher priorities should be used less frequently. Alarm priority should be implemented consistently throughout the SCADA system.

Additional special-purpose priorities may be useful, such as an additional highest priority for a very few selected alarms (“critical”), or a lowest priority for instrument malfunction or diagnostic alarms with very limited and prescribed controller action (“diagnostic”). There is no recommended frequency for critical situations or for instrument failure. Low numbers are better.

Various nonannunciated or special-purpose priorities are sometimes used for special circumstances. There is no recommended distribution for such priorities.

13.4.9 Unauthorized Alarm Suppression

All alarm suppression should be accomplished using a controlled methodology. However, it is possible for alarms to be suppressed outside of such a methodology. It is necessary to detect and report any such alarms; the potential for mistakes and the resulting risk are high. Analysis methods should be used at regular intervals to detect and report any alarms suppressed outside of proper methods. There should be no alarms that are improperly suppressed.

13.4.10 Alarm Attribute Monitoring

Unauthorized alarm configuration changes and/or discrepancies should be detected and resolved. Periodic monitoring should be made of the actual alarm attributes in effect on the SCADA system compared with the rationalized attributes in a master alarm database or with allowable alarm configuration changes specified in the alarm philosophy. Discrepancies should be identified and resolved quickly through appropriate processes.

13.5 Reporting of Alarm System Analyses

Alarm system performance should be regularly and properly reported. Reporting should be distributed to the appropriate personnel concerned with the alarm system, at a frequency appropriate to the nature of the data contained and the needs of the recipients. Typical methods include automatically generated reports posted to internal websites or distributed via email to appropriate recipients.

At various phases of an improvement effort, different analyses should likely be performed at different frequencies. As performance improves, less frequent reporting can be used.

13.6 Regulatory Requirements for Alarm System Monitoring

Regulations 49 CFR 192.631 and 195.446 require the following monitoring activities:

— Monthly monitoring of points affecting safety that have been taken off scan, have alarms inhibited, generated false alarms, or have forced or manual values for durations exceeding those needed for appropriate maintenance or operating activities.

— Once each calendar year (with intervals not to exceed 15 months), verification of proper setpoints and descriptions of safety-related alarms.

— Once each calendar year (with intervals not to exceed 15 months), review of the AMP.

— Once each calendar year (with intervals not to exceed 15 months), review of alarm system performance.

The regulation itself should be consulted for precise wording.

14 Management of Change

14.1 Purpose and Use

The alarm system is an important part of the SCADA system. Any inappropriate alarm system change could provide misleading information or result in a failure to alert the controller to potential problems. Alarm system change should be managed appropriately and prevent incorrect changes. Each pipeline operator's MOC process should appropriately cover the alarm system.

A pipeline operator's MOC process should outline:

— the scope of changes that require the relevant MOC process (e.g. alarm additions, changes, or deletions);

— roles that have the appropriate rights to make alarm system changes;

— what requirements should be met for evaluating change (e.g. risk assessment, if appropriate);

— authorization of changes;

— testing and testing methods, if appropriate;

— documentation of the change;

— notifications to personnel regarding the change;

— training of controllers prior to their operating the changed system.

14.2 Testing

Changes to the alarm system may require testing. Proper testing ensures that changes have had the expected effect on the alarm system and the alarm system is operating as desired. The determination of the testing methodology should include an evaluation of the inputs and outputs that the change will affect. Some changes may require a rigorous or end-to-end testing methodology. Testing should be appropriately documented.

14.3 Documentation

The MOC procedure should define what documentation needs to be updated with an alarm addition, change, or deletion. Changes should include updating the master alarm database and ensuring synchronization with the

changed alarm settings in effect on the SCADA system. Change documentation and revision history should be specified by the pipeline operator.

Change impact on related controller graphics, reports, and related documentation should be evaluated and updated in an appropriate timeframe.

14.4 Notification and Training

For each change, appropriate personnel to be trained should be determined. Personnel may include, but are not limited to, controllers, technicians, support personnel, and SCADA system support staff. The scope of training and/or notification should be based on the nature (e.g. scope or criticality) of the change.

14.5 Emergency Management of Change

The MOC procedure should address emergency changes, documenting what constitutes an emergency change and how they should be handled. Typically emergency changes are used to address safety or operational issues that require immediate response. The formal notification or training for the emergency change may come after the actual change is implemented. Explanation of the change should be communicated with appropriate personnel before they operate the changed system.

14.6 Temporary Management of Change

Consideration also needs to be given to temporary changes. Temporary changes to alarms typically occur when there is a malfunction in the system and an alarm needs to be altered to prevent it from becoming a nuisance to the controller. Controllers should review the altered alarms at each shift change to ensure that they are aware of all of the alarms that have been altered. The altered alarms should also be reviewed periodically to ensure that they still need to be altered.

The change process should address temporary changes (e.g. temporary alarm suppression related to malfunctions). Controllers should be aware of all temporary changes as part of beginning a shift. Temporary changes should be periodically reviewed to ensure their continued relevance. The temporary change process should incorporate time limitations for such changes.

14.7 Regulatory Requirements for Management of Change

Regulations 49 CFR 192.631 and 195.446 require the following alarm-related MOC activities. The regulation itself should be consulted for precise wording.

Pipeline operators must verify the correct safety-related alarm setpoint values and alarm descriptions once each calendar year (with intervals not to exceed 15 months) or when associated field instruments are changed.

Annex A
(informative)

Determination of Alarm Priority

A.1 General

This annex covers an example method for the determination of alarm priority.

This grid-based method is well referenced and proven in use to provide consistent results that align to the desired alarm priority percentage distributions. The method combines both severity of consequences and available time to respond in determining alarm priority. Three grids are used and should follow along the principles of the examples in this section.

The priority grid determination examples are generic. Each pipeline operator should customize these grids to reflect his or her particular operating culture, work practices, and regulatory situation.

A.2 Methods of Priority Determination

Priority assignment can be successful using only the determination of the severity of consequence to directly drive alarm priority selection.

Priority assignment can also be successful using only the determination of the time availability for response to directly drive priority selection.

A widely used and proven method that combines both of these factors is provided here as an example. The alarm management literature also mentions the use of probabilistic risk assessment methods as a part of priority determination; however, this is generally seen as greatly overcomplicated for the task and is rarely done.

A.3 Areas of Impact and Severity of Consequence

The first grid is for areas of impact and severity of consequences (see Table A.1). The grid addresses the question, How severe are the consequences, if the alarm occurs and the controller does not take the correct action in response? Each impact category is discussed separately. The highest response of “minor,” “major,” or “severe” for any row is the overall severity of the event.

A severity grid should contain sufficient detail so that different groups of people discussing the same situation should come up with the same result. The grids should be customized for each individual operating company to match its particular conditions, local or state regulations, management structure, etc.

A.4 Example Grid for Maximum Time Available for Response and Correction

“Maximum time to respond” is the time within which the controller can take action(s) to prevent or mitigate the undesired consequence(s) resulting from the alarmed situation (see Table A.2). This response time includes any needed action of outside personnel following direction from the console controller.

To clarify, this is *not* how long it actually takes the controller to take the action. This might only be a few seconds in the best possible scenario. Instead, it is how much time is *available* to take the effective action from when the alarm sounds to when the consequence becomes *unavoidable*.

Priority is a tool for the controller that responds to the alarm; these times and responses have to do with that person. In some cases a controller response is to dispatch personnel to a remote site. Such dispatched personnel may spend several hours in route. This time factor needs to be accounted for when determining priority and should not be considered as response by others or transportation delay.

Table A.1—EXAMPLE Areas of Impact and Severity of Consequences Grid

Impact Category	Severity: NONE	Severity: MINOR	Severity: MAJOR	Severity: SEVERE
Personnel safety	No injury or health effect	Any alarm for which controller action is the primary method by which harm to a person is avoided shall be configured at the highest priority used on the SCADA control system. See "Special Guidelines: Alarms that Prevent Personnel Injury."		
Public or environmental	No effect	Operating permit levels or other mandates not exceeded. Local environmental effect not crossing fence line or right-of-way, no community complaints. Contained release with little, if any, cleanup and negligible financial consequences. Internal or routine reporting requirements only.	Operating permit levels exceeded to a degree involving local or state reporting. Single exceedance of statutory or prescribed limit. Contamination causes some nonpermanent damage. Single or very few community complaints expected. Reporting required at the local or state agency level.	Operating permit levels exceeded to a degree involving federal reporting. Limited or extensive release, crosses fence line or right-of-way. Impact involving the community; multiple complaints expected. Repeated exceedances of limits. Uncontained release of hazardous materials with environmental and third-party impact. Extensive cleanup measures or financial consequences.
Cost/financial loss/downtime	No loss	Event costing <$10,000. Only internal reporting required. No pipeline outage or delivery impact.	Event costing $10,000 to $100,000. Reporting required at the regional level. Short-duration outage; daily throughput not significantly affected.	Event costing >$100,000. Reporting required at senior management level. Pipeline outage; customer deliveries and/or schedule affected.

Additional Information:

a) It is normal and expected that any single consequence scenario may have different severities in the different impact categories. Assign the overall severity for the event to be whichever one is highest.

b) This grid should be kept simple in the number of impacts and severities.

c) Use sufficient words and examples so that each alarm discussion produces a severity choice that is clear, repeatable, and unambiguous.

d) The probability of the alarmed situation is not a factor. The assumption is that the alarm has occurred. The consequence to be considered is the reasonable, likely event that will take place if no controller action is taken in response to the alarm.

e) Multiple, cascading failures that are not likely should not be discussed in an alarm consequence scenario. If a multiple cascading failure is likely and has been known to occur, it should not be ignored. For example, a delivery valve failure or supply interruption can lead to multiple unit trips and affect large portions of a pipeline system.

f) During prioritization, it should be assumed that all protective systems (e.g. shutdown systems, pressure relief devices, interlocks, other independent alarms) are active and functional. If those devices are needed, assume in prioritization that their design and reliability are proper. Prioritization is not an equipment design exercise or safety review. Following this common sense principle is needed, otherwise alarm priorities will be vastly skewed toward the higher end and priority will be ineffective.

Only three choices for maximum time to respond are recommended. They are as follows:

— “Less than 5 minutes” or “immediately.” Drop all tasks but the response to this alarm. Another value than 5 (often 3) can be used.

— “5 to 15 minutes” or “rapidly.” Quickly finish some in-progress task, but nothing new is started until this alarm is dealt with. Another value than 15 (often 10) can be used.

— “15 to 30 minutes” or “promptly.” Accomplishment of some short-duration task is possible before addressing this alarm. Another value than 30 (sometimes 60) can be used.

Table A.2—EXAMPLE Maximum Time Available for Response and Correction Grid

Classes for Maximum Time to Respond	
Response Time Description	**Response Time in Minutes**
Immediately:	<5 minutes
Rapidly:	5 to 15 minutes
Promptly:	15 to 30 minutes
Upper limit:	>30 minutes

Controllers are the primary sources of this choice. Detailed calculation of available times is generally not necessary. If a scenario requires a reliable controller response in much less than 5 minutes, an automated response, if possible, should be considered.

Note the 30-minute upper limit. Alarms should have an aspect of urgency. If a condition does not require a response within 30 minutes, then the condition is likely not an urgent one. Ideally, alarms are to signal conditions that require relatively quick action and have a characteristic of urgency. Something that can be avoided for long periods with no effect is not a condition requiring quick action. Such alarms should be reconfigured, if possible, to retain the attribute of urgency. This is not an absolute principle; there will be some exceptions.

A.5 Priority Determination Grid

This final grid puts together the results of the first two and determines the most appropriate priority for the alarm (see Table A.3).

Table A.3—EXAMPLE Severity of Consequences and Time to Respond Grid for Alarm Priority Determination

Maximum Time to Respond	**Alarm Consequence Severity**		
	MINOR	**MAJOR**	**SEVERE**
>30 minutes	Reconfigure alarm for Urgency	Reconfigure alarm for Urgency	Reconfigure alarm for Urgency
15 to 30 minutes	Priority 3	Priority 3	Priority 2
5 to 15 minutes	Priority 3	Priority 2	Priority 2
<5 minutes	Priority 2	Priority 1	Priority 1

Some important points:

— Note that every Priority 1 alarm requires immediate action on the part of the controller.

— Experience has shown that following this methodology will result in an alarm priority distribution close to the best practice recommendations of ~80 % Priority 3, ~15 % Priority 2, and ~5 % Priority 1.

— If the optional “critical” priority is to be used, specific additional criteria should be developed to determine which alarms should have that priority.

A.6 Special Guidelines: Alarms that Prevent Personnel Injury

In actual practice, most alarms are prioritized from the environmental or cost consequences. For modern pipeline operations with properly designed safety systems, there are few cases where a controller’s manual response to an alarm is the means by which harm to a person is avoided. The most common such cases where this is true should be explicitly defined in the alarm philosophy to nonexclusively use alarm Priority 1. Typical sensors that could be considered for such treatment are as follows:

— alarms indicating the release of significant quantities of toxic or flammable materials,

— ambient toxic gas or flammable gas detection sensors,

— leak detection systems,

— smoke or fire detector systems,

— activation of field-mounted “help” switches,

— any other condition where controller response to an alarm is the means by which harm to a person is avoided,

— inappropriate closure of remote gate valves.

All such applicable items are preidentified in the alarm philosophy and therefore need not be individually prioritized.

Annex B

(informative)

Priority Distribution for Alarm Configuration and Occurrence

Commonly used designations for alarm priority are shown in Table B.1.

Table B.1—Recommended Priority Distribution for Alarm Configuration and Occurrence

Critical priority (optional)	Rarely used, this priority should be constrained to <1 % of the configured alarms, and occurrences should be quite rare
Priority 1 (P1)	~5 % of the configured alarms
Priority 2 (P2)	~15 % of the configured alarms
Priority 3 (P3)	~80 % of the configured alarms
Priority 4 (P4) diagnostic (optional)	Excluded from percentage calculations

The priority order is Critical (highest); P1 (highest if Critical is not used); P2 (lower than P1); P3 (lower than P2); and P4 (lower than P3). The percentage numbers above are approximate and can vary based on a variety of factors.

Diagnostic alarms are excluded from the 80-15-5 percentage calculations of either alarm configuration or occurrence. There is no recommended percentage breakdown for configuration of such alarms because at least one diagnostic-type alarm is usually implemented for each sensor, and their inclusion skews the other percentages. Similarly, there is no recommended percentage of diagnostic alarm occurrences because sensor failure rates should be low. Other special-purpose priorities may be used for particular situations and have no recommended percentage distribution.

Annex C

(informative)

Guidelines for Determining Possible Alarm System Key Performance Indicators

Table C.1 is a summary of the most important alarm performance indicators. It is taken from the Informative Annex of ANSI/ISA 18.2-2009, *Management of Alarm Systems for the Process Industries*. Analysis descriptions follow the table.

The numbers in Table C.1 are approximate and depend on many factors, such as controller skill, HMI design, degree of automation, operating environment, types and significance of the alarms produced, and additional controller duties.

Sustained operation above the maximum manageable guidelines indicates an alarm system that is annunciating more alarms than a controller may be able to handle, and the likelihood of missing alarms increases.

When alarms have been properly rationalized and designed and nuisance alarms (e.g. chattering alarms) eliminated, the resulting alarm rate reflects the SCADA and/or local control system's ability to keep the pipeline or facility operating within bounds without requiring manual controller intervention. The solutions to high alarm rates may involve improvements to the SCADA and/or control system or to the operating procedures rather than adjustments to the alarm system.

The use of averages in evaluating alarm system performance can be misleading. Any period of time that produces more alarms than can be handled presents the likelihood of missed alarms, even if the average for that interval seems acceptable.

Table C.1—Alarm KPI Summary

Alarm Performance Metrics per Controller Position Based on at Least 30 Days of Data		
Metric	**Target Value**	
Annunciated Alarms per Time	**Target Value: Very Likely to Be Acceptable**	**Target Value: Maximum Manageable**
Annunciated alarms per day per controller position	~150 alarms per day	~300 alarms per day
Annunciated alarms per hour per controller position	~6 (average)	~12 (average)
Annunciated alarms per 10 minutes per controller position	~1 (average)	~2 (average)
Metric	**Target Value**	
Percentage of hours containing more than 30 alarms	~ <1 %	
Percentage of 10-minute periods containing more than 5 alarms	~ <1 %	
Maximum number of alarms in a 10-minute period	10 or less	
Percentage of time the alarm system is in a flood condition	~ <1 %	
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	~<1 % to 5 % maximum, with action plans to address deficiencies	
Quantity of chattering and fleeting alarms	Zero, action plans to correct any that occur	
Stale alarms	Less than 5 present on any day, with action plans to address	
Annunciated or configured priority distribution	3 priorities: ~80 % Priority 3, ~15 % Priority 2, ~5 % Priority 1 or 4 priorities: ~80 % Priority 3, ~15 % Priority 2, ~5 % Priority 1, ~<1 % “Priority Critical”	
Unauthorized alarm suppression	Zero alarms suppressed outside of controlled or approved methodologies	
Improper alarm attribute change	Zero alarm attribute changes outside of approved methodologies or MOC	

Bibliography

[1] API Recommended Practice 1130, *Computational Pipeline Monitoring for Liquids*, 2007

[2] API Standard 1164, *Pipeline SCADA Security*

[3] API Recommended Practice 1168, *Pipeline Control Room Management*

[4] Bransby, M. and J. Jenkinson. “HSE Contract Research Report 166: The Management of Alarm Systems.” London: Health & Safety Executive, 1998

[5] Doran, K. *Managing Alarms for Pipeline Operations*. ISA 55th International Instrumentation Symposium, 2009

[6] Engineering Equipment and Materials Users Association. *Alarm Systems: A Guide to Design, Managementand Procurement*, Second Edition, 2007

[7] Errington, J., Reising, D., Burns. *ASM Consortium Guidelines: Effective Alarm Management Practices,* Phoenix, AZ, ASM Consortium, 2009

[8] Grosdidier, P., Connor, P., Hollifield, B., Kulkarni, S. “A Path Forward for DCS Alarm Management.” *Hydrocarbon Processing* (November 2003)

[9] Health & Safety Executive. “The Explosion and Fires at the Texaco Refinery, Milford Haven, 24 July 94.” London: Health & Safety Executive, 1997

[10] “Better Alarm Handling” [Brochure]. London: Health & Safety Executive, 2000

[11] Hollifield, B. and E. Habibi. *The Alarm Management Handbook*. PAS, 2006

[12] Hollifield, B., Oliver, D., Nimmo, I., Habibi, E. *The High Performance HMI Handbook*. PAS, 2006

[13] National Transportation Safety Board (NTSB) and PHMSA websites, for accident reports sometimes containing references to SCADA systems and alarms. http://www.ntsb.gov/Publictn/P_Acc.htm; http://www.phmsa.dot.gov

[14] Occupational Safety and Health Administration. “Occupational Safety and Health Standards.” Chapter 17, Section 1910.119 in *Process Safety Management of Highly Hazardous Chemicals*

[15] Reising, D.V. and T. Montgomery. *Achieving Effective Alarm System Performance: Results of ASM® Consortium Benchmarking against the EEMUA Guide for Alarm Systems*. Presentation, 20th Annual CCPS International Conference, Atlanta, GA, April 2005

[16] Rothenberg, DH. *Alarm Management for Process Control: A Best-Practice Guide for Design, Implementation, and Use of Industrial Alarm Systems*. Momentum Press, First Edition, March 2009

200 Massachusetts Avenue, NW
Suite 1100
Washington, DC 20001-5571
USA

202-682-8000

Additional copies are available online at www.api.org/pubs

Phone Orders:	1-800-854-7179	(Toll-free in the U.S. and Canada)
	303-397-7956	(Local and International)
Fax Orders:	303-397-2740	

Information about API publications, programs and services is available on the web at www.api.org.

Product No. D116702