ANSI/ISA–18.2–2009

Management of Alarm Systems for the Process Industries

Approved 23 June 2009

ANSI/ISA–18.2–2009
Management of Alarm Systems for the Process Industries

ISBN: 8-1-936007-19-6

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709
E-mail: standards@isa.org

Preface

This preface as well as all footnotes, annexes, and draft technical reports associated with this standard are included for information purposes only and are not part of ANSI/ISA–18.2–2009.

This standard has been prepared as part of the service of ISA, the International Society of Automation, toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA, 67 Alexander Drive; P.O. Box 12277; Research Triangle Park, NC 277099; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

This ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards, recommended practices, and technical reports. The Department is further aware of the benefits of USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, the Department will endeavor to introduce SI and acceptable metric units in all new and revised standards to the greatest extent possible. The Metric Practice Guide, which has been published by the Institute of Electrical and Electronics Engineers (IEEE) as ANSI/IEEE Std. 268-1992, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

This standard is structured to follow the IEC guidelines. Therefore, the first three sections discuss the *Scope* of the standard, *Normative References* and *Definitions*, in that order.

CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE STANDARD, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE STANDARD OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS STANDARD, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE STANDARD MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE STANDARD. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE STANDARD OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE STANDARD FOR THE USER'S INTENDED APPLICATION.

HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS STANDARD WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE STANDARD NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER. ADDITIONALLY, THE USE OF THIS STANDARD MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE STANDARD CANNOT ANTICIPATE ALL POSSIBLE

APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS STANDARD MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS STANDARD.

THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.

The following people served as voting members of ISA18 and approved this standard on 17 April 2009:

NAME	**COMPANY**
Erwin E. Icayan, Managing Director	ACES Inc.
Donald G. Dunn, Co-chair	Aramco Services Co.
Nicholas P. Sands, Co-chair	DuPont
Joseph S. Alford	
Stephen M. Apple	TiPS Inc
Joe L. Bingham	AES Automation
Alex D. Boquiren	Bechtel Corp
Alan W. Bryant	Oxy Inc
John R. Campbell	ConocoPhillips
Bridget Fitzpatrick	Mustang Engineering
Max L. Hanson	Meyer Control Corp
David Hatch	Exida
Bill R. Hollifield	PAS
Alan Hugo	Capstone Technology
Lokesh Kalra	Chevron
Edward M. Marszal	Kenexis Consulting Corp
Michael T. Marvan	Matrikon Inc
Douglas P. Metzger	Consultant
Ian Nimmo	User Centered Design Services LLC
Patrick O'Donnell	BP
Douglas H. Rothenberg	D Roth Inc
Todd R. Stauffer	Siemens Energy & Automation
David Strobhar	Beville Engineering Inc.
Angela E. Summers	SIS-TECH Solutions LP
Beth E. Vail	Washington Safety Management Solutions/ URS

This published standard was approved for publication by the ISA Standards and Practices board on 12 June 2009.

NAME	**COMPANY**
J. Tatera, Vice President	Tatera & Associates, Inc.
P. Brett	Honeywell, Inc.
M. Coppler	Ametek, Inc.
E. Cosman	The Dow Chemical Co.
B. Dumortier	Schneider Electric
D. Dunn	Aramco Services Co.
R. Dunn	DuPont Engineering
J. Gilsinn	NIST/MEL
E. Icayan	ACES, Inc.
J. Jamison	EnCana Corporation Ltd
D. Kaufman	Honeywell International, Inc.
K. Lindner	Endress+Hauser Process Solutions AG
V. Maggioli	Feltronics Corp.
T. McAvinew	Jacobs Engineering Group
G. McFarland	Emerson Process Management
R. Reimer	Rockwell Automation
N. Sands	E I Du Pont
H. Sasajima	Yamatake Corp.
T. Schnaare	Rosemount, Inc.
I. Verhappen	MTL Instrument Group
R. Webb	ICS Secure, LLC

W. Weidman	Parsons Energy & Chemicals Group
J. Weiss	Applied Control Solutions, LLC
M. Widmeyer	Consultant
M. Zielinski	Emerson Process Management

Table of Contents

Figures

Introduction

Purpose

This standard addresses the development, design, installation, and management of alarm systems in the process industries. Alarm system management includes multiple work processes throughout the alarm system lifecycle. This standard defines the terminology and models to develop an alarm system, and it defines the work processes recommended to effectively maintain the alarm system throughout the lifecycle.

This standard was written as an extension of existing ISA standards with due consideration of other guidance documents that have been developed throughout industry. Ineffective alarm systems have often been cited as contributing factors in the investigation reports following major process incidents. This standard is intended to provide a methodology that will result in the improved safety of the process industries.

This standard is not the first effort to define terminology and practices for effective alarm systems. In 1955 ISA formed a survey committee titled Instrument Alarms and Interlocks. The committee evolved to Standard & Practices committee 18. In 1965 the committee completed ISA–RP18.1, *Specifications and Guides for the Use of General Purpose Annunciators*. In 1979 ISA released, as a product of the ISA18 and ISA67 committees, ISA–18.1–1979 (R2004), *Annunciator Sequences and Specifications*. In 1994 Amoco, Applied Training Resources, BP, Exxon, Gensym, Honeywell, Mobil, Novacor, Texaco, Shell, and others formed the Abnormal Situation Management Consortium (ASM) to develop a vision for better response to process incidents, with additional support in 1994 from the U.S. National Institute of Standards and Technology (NIST). In 1999 the Engineering Equipment and Materials Users' Association (EEMUA) issued Publication 191, *Alarm Systems: A Guide to Design, Management and Procurement*, which was updated in 2007. In 2003 the User Association of Process Control Technology in Chemical and Pharmaceutical Industries (NAMUR) issued recommendation NA 102, *Alarm Management*.

During the development of this standard every effort was made to keep terminology and practices consistent with the previous work of these respected organizations and committees.

This document provides requirements for alarm management and alarm systems. It is intended for those individuals and organizations that:

a) manufacture or implement embedded alarm systems,

b) manufacture or implement third-party alarm system software,

c) design or install alarm systems,

d) operate and/or maintain alarm systems,

e) audit or assess alarm system performance.

Organization

This standard is organized in two parts. The first part is introductory in nature, (Clauses 1-5). The main body of the standard (Clauses 6-18) presents mandatory (normative) requirements or non-mandatory (informative) recommendations as noted. If a clause contains no mandatory requirements then it is noted as informative.

1 Scope

1.1 General Applicability

This standard addresses alarm systems for facilities in the process industries to improve safety, quality, and productivity. The general principles and processes in this standard are intended for use in the lifecycle management of an alarm system based on programmable electronic controller and computer-based Human-Machine Interface (HMI) technology. Implementation of this standard should consider alarms from all systems presented to the operator, which may include basic process control systems, annunciator panels, safety instrumented systems, fire and gas systems, and emergency response systems.

The practices in this standard are applicable to continuous, batch, and discrete processes. There may be differences in implementation to meet the specific needs based on process type.

1.2 The Alarm System

The alarm system serves to notify operators of abnormal process conditions or equipment malfunctions. It may include both the basic process control system (BPCS) and the safety instrumented system (SIS), each of which uses measurements of process conditions and logic to generate alarms (see Figure 1). The alarm system also includes an alarm log and a mechanism for communicating the alarm information to the operator via a HMI, usually a computer screen or an annunciator panel. There are other functions outside the alarm system that are important to the effectiveness of the alarm system, which many include an alarm historian.

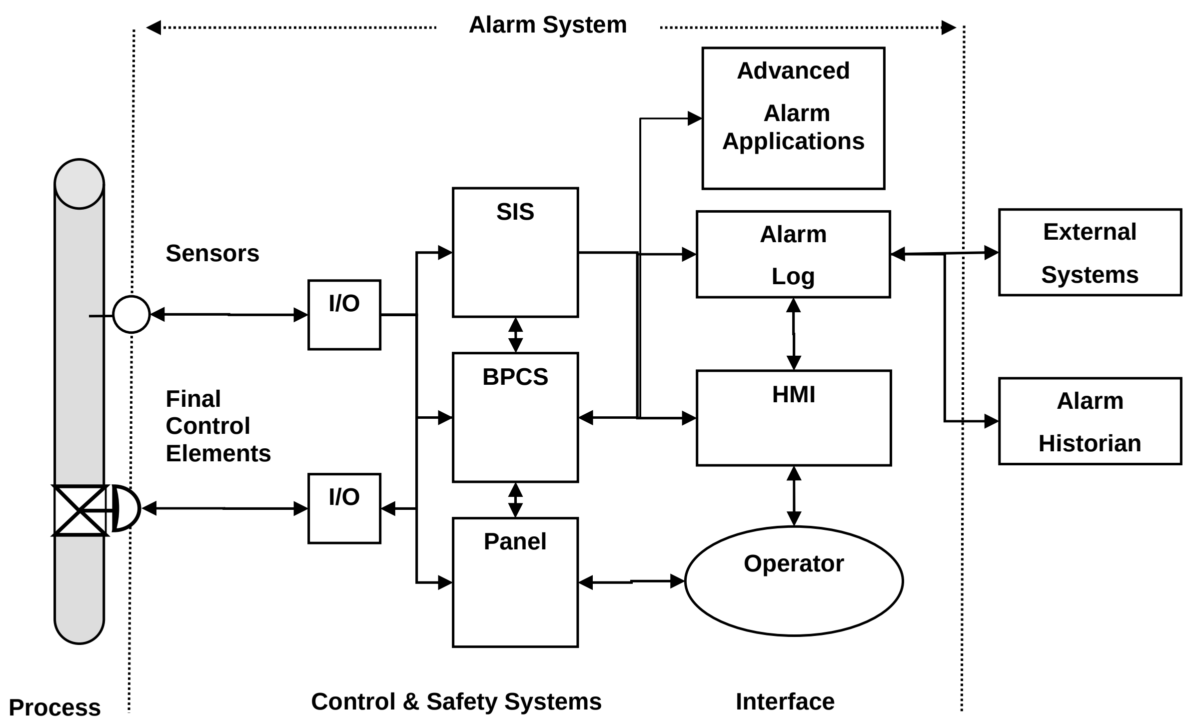


Figure 1 – Alarm System Dataflow

1.3 Exclusions

1.3.1 Process Sensors and Final Control Elements

Process sensors and final control elements are shown in Figure 1 to indicate alarms may be implemented in these devices. The design and management of process sensors and final control elements are excluded from the scope of this standard. The alarms and diagnostic indications from sensors and final control elements are included in the scope of this standard.

1.3.2 Safety Instrumented Systems

The safety instrumented system (SIS) is shown in Figure 1 to indicate alarms may be implemented in these devices. The design and management of safety instrumented systems are excluded from this standard (refer to ANSI/ISA–84.00.01–2004 Part 1 (IEC 61511 Mod) *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements*). The alarms and diagnostic indications from safety instrumented systems are included in the scope of this standard.

1.3.3 Annunciator Panels

The specification and design of annunciator panels is excluded from the scope of this standard. ISA–18.1–1979 (R2004), *Annunciator Sequences and Specifications,* provides information on alarm annunciator functions. The integration of independent alarm annunciator panels into an alarm system is included in the scope of this standard.

1.3.4 Fire Detection and Suppression Systems and Security Systems

Fire detection and suppression systems and security systems are governed by other standards and are excluded from the scope of this standard. The alarms and diagnostics from fire detection and suppression systems or security systems that are presented to the process operator through the control system are included in the scope of this standard.

1.3.5 Event Data

The indication and processing of analog, discrete, and event data other than alarm indications are outside the scope of this standard. The analysis techniques using both alarm and event data are outside the scope of this standard.

1.3.6 Alarm Identification Methods

Required methods of alarm identification are not specified in this standard. Examples of alarm identification methods are listed.

1.3.7 Management of Change

A specific management of change procedure is not included in this standard. Some requirements and recommendations to be included in a management of change procedure are included.

1.3.8 Jurisdictions

In jurisdictions where the governing authorities (e.g., national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, these take precedence over the requirements defined in this standard.

1.3.9 Purchase Specification

This standard is not intended to be used as an alarm system purchase specification. It will not eliminate the need for sound engineering judgment. No particular technology is mandated.

2 Normative References

2.1 References

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

ANSI/ISA–84.00.01–2004 *(IEC 61511 Mod) Part 1 Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*

ANSI/ISA–91.00.01–2001 *Identification of Emergency Shutdown Systems and Controls That Are Important to Maintaining Safety in Process Industries*

3 Definition of Terms and Acronyms

Defined terms are used in this standard. Synonymous terms, which are not used in this standard, are listed in parentheses.

3.1 Definitions

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

3.1.1 Absolute alarm

An alarm generated when the setpoint is exceeded.

3.1.2 Acknowledge

The operator action that confirms recognition of an alarm.

3.1.3 Activate

The process of enabling an alarm function within the alarm system.

3.1.4 Adjustable alarm (Operator-set alarm)

An alarm for which the setpoint can be changed manually by the operator.

3.1.5 Advanced alarming

A collection of techniques (e.g., state-based alarming, and dynamic prioritization) that can help manage alarm rates in specific situations.

3.1.6 Alarm

An audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response.

3.1.7 Alarm attributes (Alarm parameters)

The settings for an alarm within the process control system (e.g., alarm setpoint, alarm priority).

3.1.8 Alarm class

A group of alarms with common alarm management requirements (e.g., testing, training, monitoring, and audit requirements).

3.1.9 Alarm deadband (Alarm hysteresis)

The change in signal from the alarm setpoint necessary to clear the alarm.

3.1.10 Alarm flood (Alarm shower)

A condition during which the alarm rate is greater than the operator can effectively manage (e.g., more than 10 alarms per 10 minutes).

3.1.11 Alarm group

A set of alarms with common association (e.g., process unit, process area, equipment set, or service).

3.1.12 Alarm historian

The long term repository for alarm records.

3.1.13 Alarm log

The short term repository for alarm records.

3.1.14 Alarm management (Alarm system management)

The processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems.

3.1.15 Alarm message

A text string displayed with the alarm indication that provides additional information to the operator (e.g., operator action).

3.1.16 Alarm off-delay (Debounce)

The time a process measurement remains in the normal state before the alarm is cleared.

3.1.17 Alarm on-delay

The time a process measurement remains in the alarm state before the alarm is annunciated.

3.1.18 Alarm overview indicator

The composite indicator of alarm status for a process unit or area.

3.1.19 Alarm philosophy

A document that establishes the basic definitions, principles, and processes to design, implement, and maintain an alarm system.

3.1.20 Alarm priority

The relative importance assigned to an alarm within the alarm system to indicate the urgency of response (e.g., seriousness of consequences and allowable response time).

3.1.21 Alarm setpoint (Alarm limit, Alarm trip point)

The threshold value of a process variable or discrete state that triggers the alarm indication.

3.1.22 Alarm summary

A display that lists alarms with selected information (e.g., date, time, priority, and alarm type).

3.1.23 Alarm system

The collection of hardware and software that detects an alarm state, communicates the indication of that state to the operator, and records changes in the alarm state.

3.1.24 Alarm system requirements specification

The document which specifies the details of the alarm system design which are used in selecting components of an alarm system.

3.1.25 Alarm type (Alarm condition)

A specific alarm on a process measurement (e.g., low process variable alarm, high process variable alarm, or discrepancy alarm).

3.1.26 Alert

An audible and/or visible means of indicating to the operator an equipment or process condition that requires awareness, that is indicated separately from alarm indications, and which does not meet the criteria for an alarm.

3.1.27 Allowable response time

The maximum time between the annunciation of the alarm and the time the operator must take corrective action to avoid the consequence.

3.1.28 Annunciator

A device or group of devices that call attention to changes in process conditions.

3.1.29 Bad measurement alarm

An alarm generated when the signal for a process measurement is outside the expected range (e.g., 3.8mA for a 4-20mA signal).

3.1.30 Bit-pattern alarm

An alarm that is generated when a pattern of digital signals matches a predetermined pattern.

3.1.31 Calculated alarm

An alarm generated from a calculated value instead of a direct process measurement.

3.1.32 Call-out alarm

An alarm that notifies and informs an operator by means other than, or in addition to, a console display (e.g., pager or telephone).

3.1.33 Chattering alarm

An alarm that repeatedly transitions between the alarm state and the normal state in a short period of time.

3.1.34 Classification

The process of separating alarms into classes based on common requirements (e.g., testing, training, monitoring, and auditing requirements).

3.1.35 Clear

An alternate description of the state of an alarm that has transitioned to the normal state.

3.1.36 Console

The interface for an operator to monitor and/or control the process, which may include multiple displays or annunciators, and defines the boundaries of the operator's span of control.

3.1.37 Control system

A system that responds to input signals from the equipment under control and/or from an operator and generates output signals that cause the equipment under control to operate in the desired manner.

Note: The control system may include both Basic Process Control Systems (BPCS) and Safety Instrumented Systems (SIS).

3.1.38 Decommission

The change process to remove an alarm from the alarm system.

3.1.39 Deviation alarm

An alarm generated when the difference between two analog values exceeds a limit (e.g., deviation between primary and redundant instruments or a deviation between process variable and setpoint).

3.1.40 Discrepancy alarm (Mismatch alarm)

An alarm generated by error between the comparison of an expected plant or device state to its actual state (e.g., when a motor fails to start after it is commanded to the on state).

3.1.41 Dynamic alarming

The automatic modification of alarms based on process state or conditions.

3.1.42 Enforcement

An enhanced alarming technique that can verify and restore alarm attributes in the control system to the values in the master alarm database.

3.1.43 First-out alarm (First-up alarm)

An alarm determined (i.e., by first-out logic) to be the first, in a multiple-alarm scenario.

3.1.44 Highly managed alarm

An alarm belonging to a class with more requirements than general alarms (e.g., a safety alarm).

3.1.45 Implementation

The transition stage between design and operation during which the alarm is put into service.

3.1.46 Instrument diagnostic alarm

An alarm generated by a field device to indicate a fault (e.g., sensor failure).

3.1.47 Interim alarm

An alarm used on a temporary basis (e.g., in place of an out-of-service alarm) without completing the management of change process.

3.1.48 Latching alarm

An alarm that remains in alarm state after the process has returned to normal and requires an operator reset before it will clear.

3.1.49 Manual safety function alarm (Safety related alarm)

An alarm that indicates an operator action is required to complete a safety function (e.g., operator initiated instrumented function).

3.1.50 Master alarm database

The authorized list of rationalized alarms and associated attributes.

3.1.51 Nuisance alarm

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

3.1.52 Operator (Controller)

The person who monitors and makes changes to the process.

3.1.53 Out-of-service

The state of an alarm during which the alarm indication is suppressed, typically manually, for reasons such as maintenance.

3.1.54 Plant state (Plant mode)

A defined set of operational conditions for a process plant (e.g., shutdown, operating).

3.1.55 Prioritization

The process of assigning a level of operational importance to an alarm.

3.1.56 Rate-of-change alarm

An alarm generated when the change in process variable per unit time, (dPV/dt), exceeds a defined limit.

3.1.57 Rationalization

The process to review potential alarms using the principles of the alarm philosophy, to select alarms for design, and to document the rationale for each alarm.

3.1.58 Recipe-driven alarm

An alarm with limits that depend on the recipe that is currently being executed.

3.1.59 Remote alarm

An alarm from a remotely operated facility or a remote interface.

3.1.60 Reset

The operator action that unlatches a latched alarm.

3.1.61 Return to normal

The indication an alarm condition has transitioned to the normal state.

3.1.62 Re-alarming alarm (Re-triggering alarm)

An alarm that is automatically re-annunciated to the operator under certain conditions.

3.1.63 Safety alarm

An alarm that is classified as critical to process safety or the protection of human life.

3.1.64 Safety function alarm

An alarm that indicates a demand on a safety function.

3.1.65 Shelve

A mechanism, typically initiated by the operator, to temporarily suppress an alarm.

3.1.66 Silence

The operator action that terminates the audible alarm indication.

3.1.67 Stale alarm

An alarm that remains in the alarm state for an extended period of time (e.g., 24 hours).

3.1.68 Standing alarm

An alarm in an active alarm state (e.g., unack alarm, ack alarm)

3.1.69 State-based alarm (Mode-based alarms)

An alarm that is automatically modified or suppressed based on process state or conditions.

3.1.70 Station

A single human-machine interface within the operator console.

3.1.71 Statistical alarm

An alarm generated based on statistical processing of a process variable or variables.

3.1.72 Suppress

Any mechanism to prevent the indication of the alarm to the operator when the base alarm condition is present (i.e., shelving, suppressed by design, out-of-service).

3.1.73 Suppressed by Design

A mechanism implemented within the alarm system that prevents the transmission of the alarm indication to the operator based on plant state or other conditions.

3.1.74 System diagnostic alarm

An alarm generated by the control system to indicate a fault within the system hardware, software or components (e.g., communication error).

3.1.75 Tag (Point)

The unique identifier assigned to a process measurement, calculation, or device within the control system.

3.1.76 Unacknowledged

A state in which the operator has not yet confirmed recognition of an alarm indication.

3.2 Acronyms

3.2.1 Ack: Acknowledge or Acknowledged

3.2.2 ASRS: Alarm System Requirements Specification

3.2.3 BPCS: Basic Process Control System

3.2.4 cGMP: current Good Manufacturing Practice

3.2.5 EEMUA: Engineering Equipment and Materials Users' Association

3.2.6 EPA: Environmental Protection Agency (US government)

3.2.7 ERP: Enterprise Resource Planning

3.2.8 ESD: Emergency Shutdown System

3.2.9 FDA: Food and Drug Administration (US government)

3.2.10 FMEA: Failure Mode and Effects Analysis

3.2.11 HMA: Highly Managed Alarms

3.2.12 HMI: Human-Machine Interface

3.2.13 HAZOP: Hazard and Operability Study

3.2.14 MES: Manufacturing Execution System

3.2.15 MOC: Management of Change

3.2.16 OSHA: Occupational Safety and Health Administration (US government)

3.2.17 P&ID: Piping (or Process) and Instrumentation Diagram

3.2.18 PHA: Process Hazards Analysis

3.2.19 RTN: Return to Normal

3.2.20 SIF: Safety Instrumented Function

3.2.21 SIL: Safety Integrity Level

3.2.22 SIS: Safety Instrumented System

3.2.23 SRS: Safety Requirements Specification

3.2.24 SOP: Standard Operating Procedure

3.2.25 UNACK: Unacknowledged

4 Conformance to this Standard

4.1 Conformance Guidance

To conform to this standard, it must be shown that each of the requirements in the normative clauses has been satisfied.

4.2 Existing Systems

For existing alarm systems designed and constructed in accordance with codes, standards, and/or practices prior to the issue of this standard, the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operated in a safe manner. The practices and procedures of this standard shall be applied to existing systems in a reasonable time as determined by the owner/operator.

5 Alarm System Models

5.1 Alarm Systems

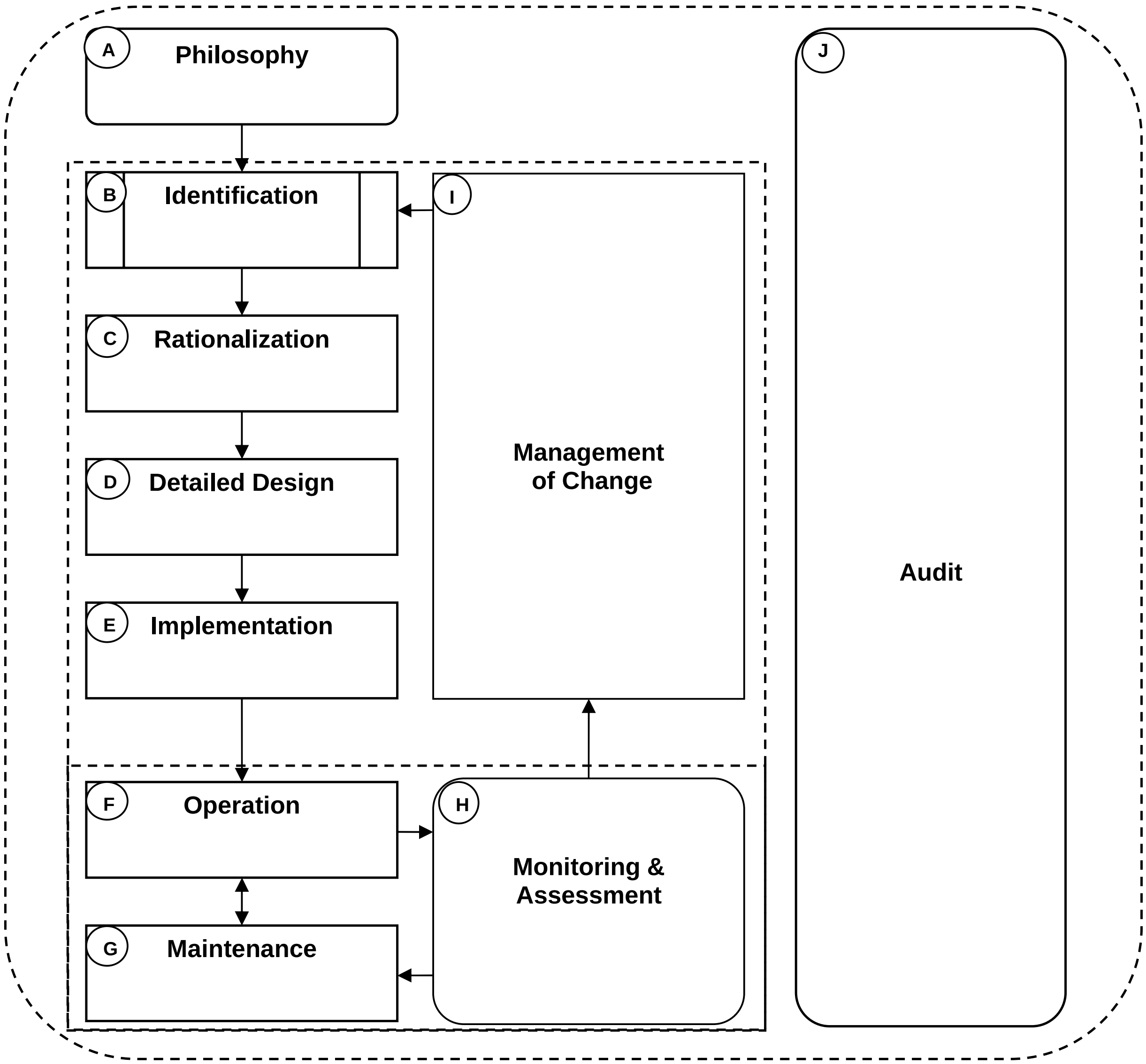
Alarm systems are used to communicate indications of abnormal process conditions or equipment malfunctions to the operators, the personnel monitoring and operating the process. Effective alarm systems are well designed, implemented, operated, and maintained. Alarm management is the set of practices and processes that ensures an effective system.

A foundational part of alarm management is the definition of an alarm; an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response. The essential element of this definition is the response to the alarm. This definition is reinforced in the alarm management processes described in this standard.

5.2 Alarm Management Lifecycle

Figure 2 illustrates the relationship between the stages of the alarm management lifecycle described in this standard. The alarm management life cycle covers alarm system specification, design, implementation, operation, monitoring, maintenance, and change activities from initial conception through decommissioning.

The lifecycle model is useful in identifying the requirements and responsibilities for implementing an alarm management system. The lifecycle is applicable for the installation of new alarm systems or managing an existing system.



Note 1: The box used for stage B represents a process defined outside of this standard per 5.2.1.2.

Note 2: The independent stage J represents a process that connects to all other stages per 5.2.1.10

Note 3: The rounded shapes of stages A, H, and J represent entry points to the lifecycle per 5.2.2.

Note 4: The dotted lines represent the loops in the lifecycle per 5.2.4.

Figure 2 – Alarm Management Lifecycle

5.2.1 Alarm Management Lifecycle Stages

The alarm management lifecycle stages shown in Figure 2 are briefly described in the following sections. The letter label is an identifier used in the text. The requirements and recommendations for each stage are described in Clauses 6 -18 of this standard.

5.2.1.1 Alarm Philosophy (A)

Basic planning is necessary prior to designing a new alarm system or modifying an existing system. Generally the first step is the development of an alarm philosophy that documents the objectives of the alarm system and the processes to meet those objectives. For new systems the alarm philosophy serves as the basis for the alarm system requirements specification (ASRS) document.

The philosophy starts with the basic definitions and extends them to operational definitions. The definition of alarm priorities, classes, performance metrics, performance limits, and reporting requirements are determined based on the objectives, definitions, and principles. The schemes for presentation of alarm indications in the HMI, including use of priorities, are also set in the alarm philosophy, which should be consistent with the overall HMI design.

The philosophy specifies the processes used for each of the lifecycle stages, such as the threshold for the management of change process and the specific requirements for change. The philosophy is maintained to ensure consistent alarm management throughout the lifecycle of the alarm system.

The development of the alarm system requirements specification is included in the philosophy stage of the lifecycle. Most of the specification is system independent and can be the basis for determining which systems most closely meet the requirements. The specification typically goes into more detail than the alarm philosophy and may provide specific guidance for system design.

5.2.1.2 Identification (B)

The identification stage is a collection point for potential alarms proposed by any one of several methods for determining that an alarm may be necessary. These methods are defined outside of this standard so the identification stage is represented as a predefined process in the lifecycle. The methods can be formal such as process hazards analysis, safety requirements specifications, recommendations from an incident investigation, good manufacturing practice, environmental permits, P&ID development or operating procedure reviews. Process modifications and operating tests may also generate the need for alarms or modifications. Some alarm changes will be identified from the routine monitoring of alarm system performance. At this stage the need for an alarm has been identified and it is ready to be rationalized.

5.2.1.3 Rationalization (C)

The rationalization stage reconciles the identified need for an alarm or alarm system change with the principles in the alarm philosophy. The steps can be completed in one process or sequentially. The product of rationalization is clear documentation of the alarm, including any advanced alarm techniques, which can be used to complete the design.

Rationalization is the process of applying the requirements for an alarm and generating the supporting documentation such as the basis for the alarm setpoint, the consequence, and corrective action that can be taken by the operator.

Rationalization includes the prioritization of an alarm based on the method defined in the alarm philosophy. Often priority is based on the consequences of the alarm and the allowable response time.

Rationalization also includes the activity of classification during which an alarm is assigned to one or more classes to designate requirements (e.g., design, testing, training, or reporting requirements). The type of consequences of a rationalized alarm, or other criteria, can be used to separate the alarms into classes as defined in the alarm philosophy.

The rationalization results are documented, typically in the master alarm database (i.e., an approved document or file), which is maintained for the life of the alarm system.

5.2.1.4 Detailed Design (D)

In the design stage, the alarm attributes are specified and designed based on the requirements determined by rationalization. There are three areas of design: basic alarm design, HMI design, and design of advanced alarming techniques.

The basic design for each alarm follows guidance based on the type of alarm and the specific control system.

The HMI design includes display and annunciation for the alarms, including the indications of alarm priority.

Advanced alarming techniques are additional functions that improve the effectiveness of the alarm system beyond the basic alarm and HMI design. These methods include state based alarming and dynamic prioritization.

5.2.1.5 Implementation (E)

In the implementation stage, the activities necessary to install an alarm or alarm system and bring it to operational status are completed. Implementation of a new alarm or a new alarm system includes the physical and logical installation and functional verification of the system.

Since operators are an essential part of the alarm system, operator training is an important activity during implementation. Testing of new alarms is often an implementation requirement. The documentation for training, testing, and commissioning may vary with classification as defined in the alarm philosophy.

5.2.1.6 Operation (F)

In the operation stage, the alarm or alarm system is active and it performs its intended function. Refresher training on both the alarm philosophy and the purpose of each alarm is included in this stage.

5.2.1.7 Maintenance (G)

In the maintenance stage, the alarm or alarm system is not operational but is being tested or repaired. Periodic maintenance, (e.g., testing of instruments), is necessary to ensure the alarm system functions as designed.

5.2.1.8 Monitoring and Assessment (H)

In the monitoring and assessment stage, the overall performance of the alarm system and individual alarms are continuously monitored against the performance goals stated in the alarm philosophy. Monitoring and assessment of the data from the operation stage may trigger maintenance work or identify the need for changes to the alarm system or operating procedures. Monitoring and assessment of the data from the maintenance stage provides an indication of the maintenance efficiency. The overall performance of the alarm system is also monitored and assessed against the goals in the alarm philosophy. Without monitoring an alarm system is likely to degrade.

5.2.1.9 Management of Change (I)

In the management of change stage, modifications to the alarm system are proposed and approved. The change process should follow each of the lifecycle stages from identification to implementation.

5.2.1.10 Audit (J)

In the audit stage, periodic reviews are conducted to maintain the integrity of the alarm system and alarm management processes. Audits of system performance may reveal gaps not apparent from routine monitoring. Execution against the alarm philosophy is audited to identify system improvements, such as modifications to the alarm philosophy. Audits may also identify the need to increase the discipline of the organization to follow the alarm philosophy.

5.2.2 Alarm Lifecycle Entry Points

Depending on the selected approach, there are three points of entry to the alarm management lifecycle:

a) alarm philosophy,

b) monitoring and assessment,

c) audit.

These entry points are represented by rounded boxes in the diagram. As entry points these lifecycle stages are only the initial step in managing an alarm system. All stages of the lifecycle are necessary for a complete alarm management system.

5.2.2.1 Start with Alarm Philosophy (A)

The first possible starting point is the development of an alarm philosophy which establishes the objectives of the alarm system and may be used as the basis for the alarm system requirements specification. This is the lifecycle entry point for new installations.

5.2.2.2 Start with Monitoring and Assessment (H)

The second possible starting point is to begin monitoring an existing alarm system and assess the performance. Problem alarms can be identified and addressed through maintenance or management of change. The monitoring data can be used in a benchmark assessment.

5.2.2.3 Start with Audit (J)

The third possible starting point is an initial audit, or benchmark, of all aspects of alarm management against a set of documented practices, such as those listed in this standard. The results of the initial audit can be used in the development of a philosophy.

5.2.3 Simultaneous and Encompassing Stages

The lifecycle diagram is drawn to represent sequential stages. There are several simultaneous stages which are represented at the same vertical point in the lifecycle. Some stages encompass the activities of other stages.

The monitoring and assessment stage (H) is simultaneous to the operation and maintenance stages.

The management of change stage (I) represents the initiation of the change process through which all appropriate stages of the lifecycle are authorized and completed.

The audit stage (J) is an overarching activity that can occur at any point in the lifecycle and includes a review of the activities of the other stages.

5.2.4 Alarm Management Lifecycle Loops

In addition to the lifecycle stages, there are three loops in the lifecycle. Each loop performs a function during the cycle.

5.2.4.1 Monitoring and Maintenance Loop

The operation-monitoring and assessment-maintenance loop is the routine monitoring that identifies problem alarms for maintenance. Repaired alarms are returned to operation.

5.2.4.2 Monitoring and Management of Change Loop

The operation-monitoring and assessment-management of change loop is triggered when routine monitoring indicates an alarm is working per design but is not compatible with the alarm philosophy. The design may need to be modified or an advanced alarm technique may need to be applied. The alarm may remain in operation while the management of change process is initiated and the stages of the lifecycle are repeated.

5.2.4.3 Audit and Philosophy Loop

The audit-philosophy loop is the lifecycle itself and the process of continuous improvement of the alarm system. The audit process identifies processes in the lifecycle to strengthen.

5.2.5 Alarm Management Lifecycle Stage Inputs and Outputs

The alarm lifecycle stages are connected as the outputs of one stage are often the inputs to another stage. The connections are not fully represented in the lifecycle diagram (Figure 2). Figure 3 provides more information on the relationships between the inputs and outputs of the lifecycle stages.

Alarm Management Lifecycle Stage		Activities	Clause Number	Inputs	Outputs
Stage	**Title**				
A	Philosophy	Define processes for alarm management and ASRS.	6,7	Objectives and standards.	Alarm philosophy and ASRS.
B	Identification	Determine potential alarms.	8	PHA report, SRS, P&IDs, operating procedures, etc...	List of potential alarms.
C	Rationalization	Rationalization, classification, prioritization, and documentation.	9	Alarm philosophy, and list of potential alarms.	Master alarm database, alarm design requirements.
D	Detailed Design	Basic alarm design, HMI design, and advanced alarming design	10,11,12	Master alarm database, alarm design requirements.	Completed alarm design.
E	Implementation	Install alarms, initial testing, and initial training.	13	Completed alarm design and master alarm database.	Operational alarms, Alarm response procedures.
F	Operation	Operator responds to alarms, refresher training.	14	Operational alarms, alarm response procedures.	Alarm data.
G	Maintenance	Maintenance repair and replacement, periodic testing.	15	Alarm monitoring reports and alarm philosophy.	Alarm data.
H	Monitoring & Assessment	Monitoring alarm data and report performance.	16	Alarm data and alarm philosophy.	Alarm monitoring reports, proposed changes.
I	Management of Change	Process to authorize additions, modifications, and deletions of alarms.	17	Alarm philosophy, proposed changes.	Authorized alarm changes.
J	Audit	Periodic audit of alarm management processes.	18	Standards, alarm philosophy and audit protocol.	Recommendations for improvement.

Figure 3 – Alarm Management Lifecycle Stage Inputs and Outputs

5.3 Process Condition Model

The process condition model, Figure 4, shows the boundaries of process conditions, from normal and target conditions to the abnormal conditions of upset and shutdown or disposal. This simple model is a useful reference in the development of alarm principles and the alarm philosophy. The warnings and indications are not to suggest alarms are required, only that under some circumstances alarms may be warranted. Every alarm is rationalized to ensure it is necessary.

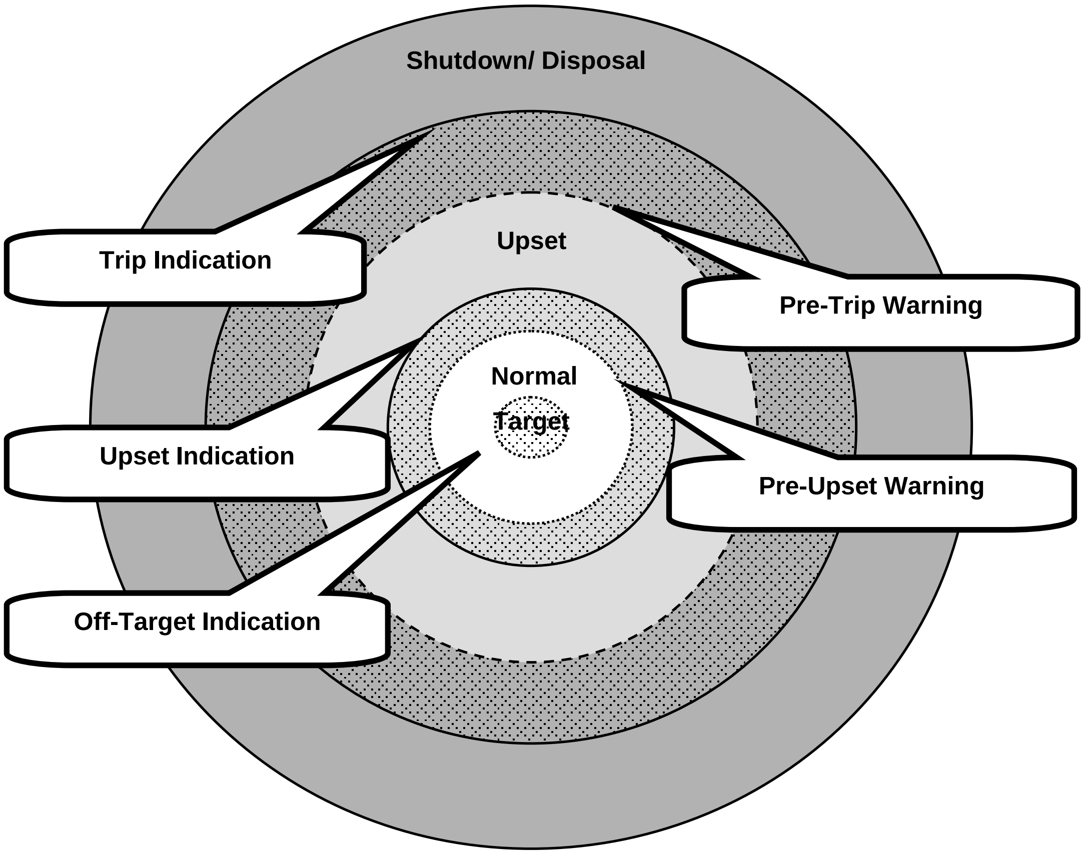


Figure 4 – Process Condition Model

5.3.1 Process Conditions

The process conditions illustrated in Figure 4 are described in the following sections.

5.3.1.1 Target

The target range is the set of optimal operating conditions within the normal range. These conditions may reflect highest yield, lowest cost, or target capacity operation of the process. Optimal conditions usually apply to only a subset of process variables. The target range may change with time or operating condition.

5.3.1.2 Normal

The normal range of operation is the expected operating envelope around the optimal target value. The normal range is sometimes called standard operating conditions.

5.3.1.3 Upset

The upset condition is an abnormal condition that may result in off-quality material, non-standard product, increased emissions, or may lead to more severe consequences.

5.3.1.4 Shutdown/ Disposal

The shutdown or disposal condition is the result of manual or automatic functions to avoid unacceptable operating conditions or unacceptable product.

5.3.2 Process Condition Warnings and Indications

The transitions between process conditions are the usual points for alarm indications. This model should not be interpreted to suggest alarms are necessary for all of the transitions, but that for different process variables different transitions may be selected for alarms.

5.3.2.1 Off-Target Indication

The off-target indication is triggered at the boundary of the target operating envelope. These indications provide the notification that a process variable is still in the normal range and is no longer in the optimal target range.

5.3.2.2 Pre-Upset Warning

The pre-upset warning provides advance notice of abnormal conditions. Where upset or non-standard conditions have significant consequences (e.g., equipment damage or off-quality product), there may be a warning that provides enough time to avert the upset conditions.

5.3.2.3 Upset Indication

The upset condition indication provides notification of the upset condition. When a pre-upset warning is not justified, this may be the first notification of an abnormal condition. Where pre-upset warnings are provided, the upset condition indication may be a confirmation of upset operation such as off-quality material or a permit violation.

5.3.2.4 Pre-Trip Warning

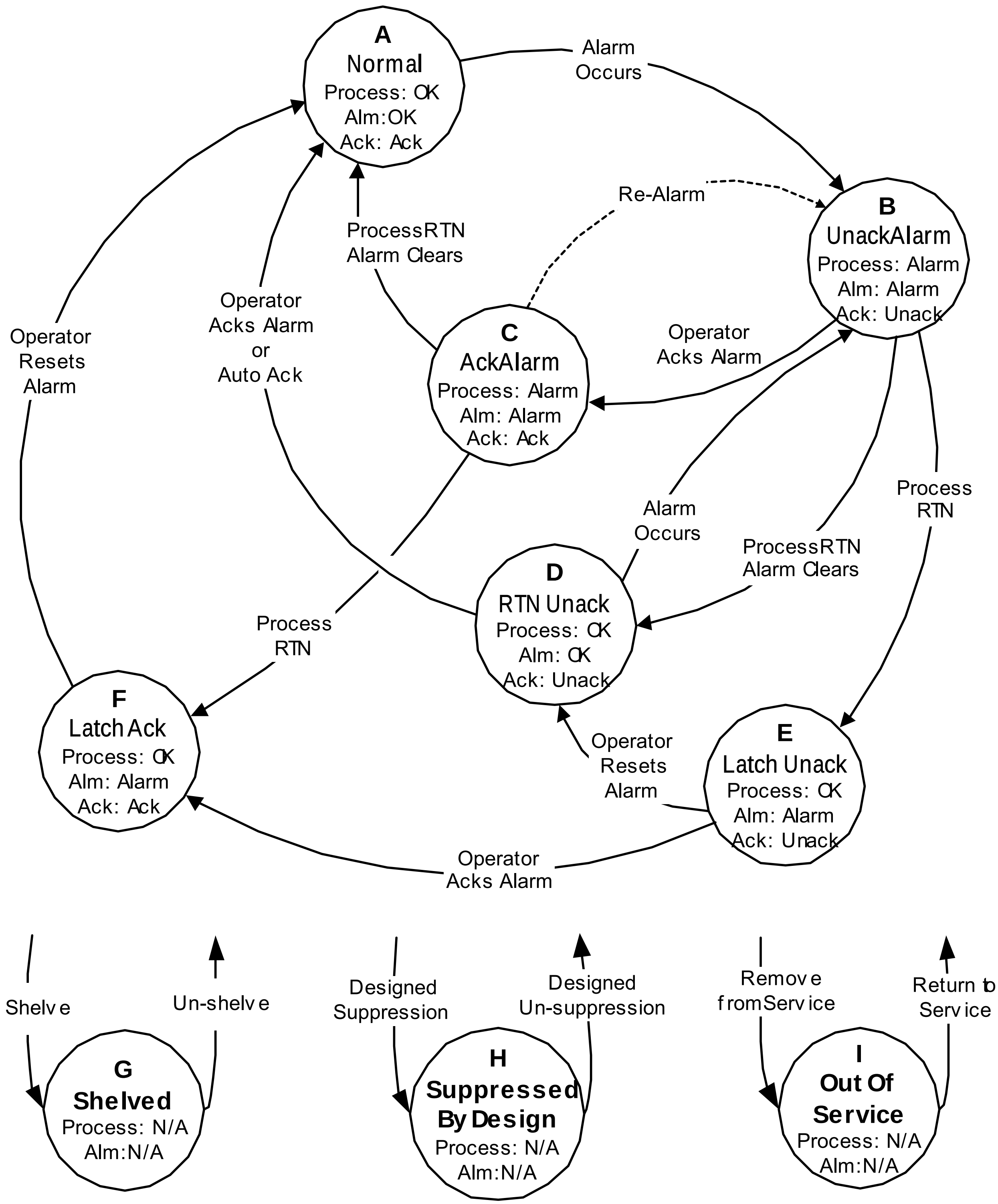
The pre-trip warning provides an opportunity to avoid the shutdown trip or condition that requires disposition of the product. Not all process indications provide warning of trip conditions. The term trip may refer to an emergency shutdown of a plant or a local process interlock on a single piece of equipment.

5.3.2.5 Trip Indication

The trip indication provides an indication that a shutdown has occurred or a disposition limit has been violated. The disposition limit is the point of no return after which a product is unusable. Post-trip alarms may indicate the need for further action (e.g., failure of the trip function).

5.4 Alarm States

The alarm state transition diagram shown in Figure 5 represents the states and transitions for typical alarms. While there are exceptions, this diagram describes the majority of alarms and serves as a useful reference for the development of alarm system principles and HMI functions. Note some terms used in this diagram were used in the process condition model, Figure 4.



Note 1: States G, H, and I can connect to any alarm state in the diagram.

Note 2: The dotted line indicates an infrequently implemented option.

Figure 5 – Alarm State Transition Diagram

5.4.1 Alarm States

The circles in the Figure 5 represent the states of an alarm. The letter label is an identifier used in the text. The second line is a state name, often abbreviated. The third line describes process conditions, the fourth and fifth lines list the alarm status and its acknowledgement status, respectively. The possible states of alarm suppression are shown on the lower part of the diagram.

5.4.1.1 Normal (A)

The normal alarm state is defined as the state in which the process is operating within normal specifications, the alarm is clear and past alarms have been acknowledged.

5.4.1.2 Unack Alarm (B)

The unacknowledged alarm state is the initial state upon trigger of an alarm due to off-target, upset, or shutdown process conditions. In this state the alarm is unacknowledged. Previously acknowledged alarms may be designed to re-alarm, triggering a return to this state. The alarm may be silenced in the unacknowledged alarm state.

5.4.1.3 Ack Alarm (C)

The acknowledged alarm state is reached when an alarm has not cleared, but an operator has received the alarm and acknowledged the alarm condition.

5.4.1.4 RTN Unack (D)

The returned to normal unacknowledged alarm state is reached when the process returns within normal limits and the alarm clears automatically (sometimes called auto-reset) before an operator has acknowledged the alarm condition.

5.4.1.5 Latch Unack (E)

Similar to the RTN Unack state, the latched unacknowledged alarm state occurs when the process returns to normal before the operator has acknowledged the alarm. The alarm itself remains latched and requires further action by the operator to reset the alarm. The latch function is an option.

5.4.1.6 Latch Ack (F)

The latched acknowledged alarm state is the state in which the operator has acknowledged the alarm and the process has returned within normal limits but the alarm remains latched, pending operator reset. The latch function is an option.

5.4.1.7 Shelved (G)

The shelved state is used when an alarm is temporarily suppressed using a controlled methodology. An alarm in the shelved state is under the control of the operator. The shelving system may automatically unshelve alarms.

5.4.1.8 Suppressed by Design (H)

The suppressed by design state is used to suppress alarms based on operating conditions or plant states. An alarm in the suppressed by design state is under the control of logic that determines the relevance of the alarm.

5.4.1.9 Out-of-Service (I)

The out-of-service alarm state is used to manually suppress alarms, (e.g., use control system functionality to remove alarm from service), when they are removed from service, typically for maintenance. An alarm in the out-of-service state is under the control of maintenance.

5.4.2 Alarm Cycle Transition Paths

The arrows in the diagram represent transitions between states. For simplicity, the diagram does not illustrate effects of deadband and time delays. When the process is considered to be in alarm, the process variable has exceeded the alarm setpoint for the alarm on-delay period.

5.4.2.1 Alarm Occurs (A->B)

The process has gone out of the normal range beyond the alarm setpoint and has remained in this state long enough to trigger the alarm.

5.4.2.2 Operator Ack (B->C)

An operator acknowledges an active alarm before taking action to return the process to normal.

5.4.2.3 Re-Alarm (C->B)

The re-alarm path shows the infrequently used option that periodically generates repetitive alarm indications for a single alarm while the alarm remains in the alarm state.

5.4.2.4 Process RTN Alarm Clears (C->A)

This is part of a normal sequence for a non-latching alarm that does not require a separate action to reset it. The alarm moves from the acknowledged state to normal.

5.4.2.5 Process RTN (C->F)

The latched alarm remains in the alarm state when the process condition returns to normal.

5.4.2.6 Process RTN and Alarm Clears (B->D)

The process returns to normal before an operator has acknowledged the alarm and the alarm does not latch.

5.4.2.7 Operator Ack (D->A)

An alarm that has already cleared the normal state may require operator acknowledgment.

5.4.2.8 Process RTN (B->E)

The process returns to normal before an operator acknowledges the alarm but the alarm is latched.

5.4.2.9 Operator Resets (E->D)

An operator resets an alarm before acknowledging it.

5.4.2.10 Operator Ack (E->F)

An operator acknowledges a latched alarm for which the process has returned to normal.

5.4.2.11 Operator Resets (F->A)

The latching alarm has been acknowledged and the process has returned to normal. When the alarm is reset, the alarm returns to the normal state.

5.4.2.12 Shelve (Any State -> G) and Un-shelve (G -> Any State)

An operator may shelve an alarm to avoid clutter in the active alarm displays. Shelving and un-shelving are typically manual operations.

5.4.2.13 Designed Suppression (Any State -> H) and Designed Un-suppression (H -> Any State)

Process conditions or states may be used to suppress alarms by design. Process conditions or states may also un-suppress alarms when appropriate. Designed suppression and designed un-suppression are typically automatic operations.

5.4.2.14 Remove-from-Service (Any State -> I) and Return-to-Service (I -> Any State)

An operator may remove an alarm from service for maintenance or other reasons and return an alarm to service when it is available. Remove from service and return to service are typically manual operations.

5.5 Alarm Response Timeline

Figure 6 represents a process measurement that increases from a normal condition to an abnormal condition and the two possible scenarios based on whether the operator takes the corrective action or not. Using Figure 5, it is possible to map some states to this timeline to clarify the definition of terms related to time.

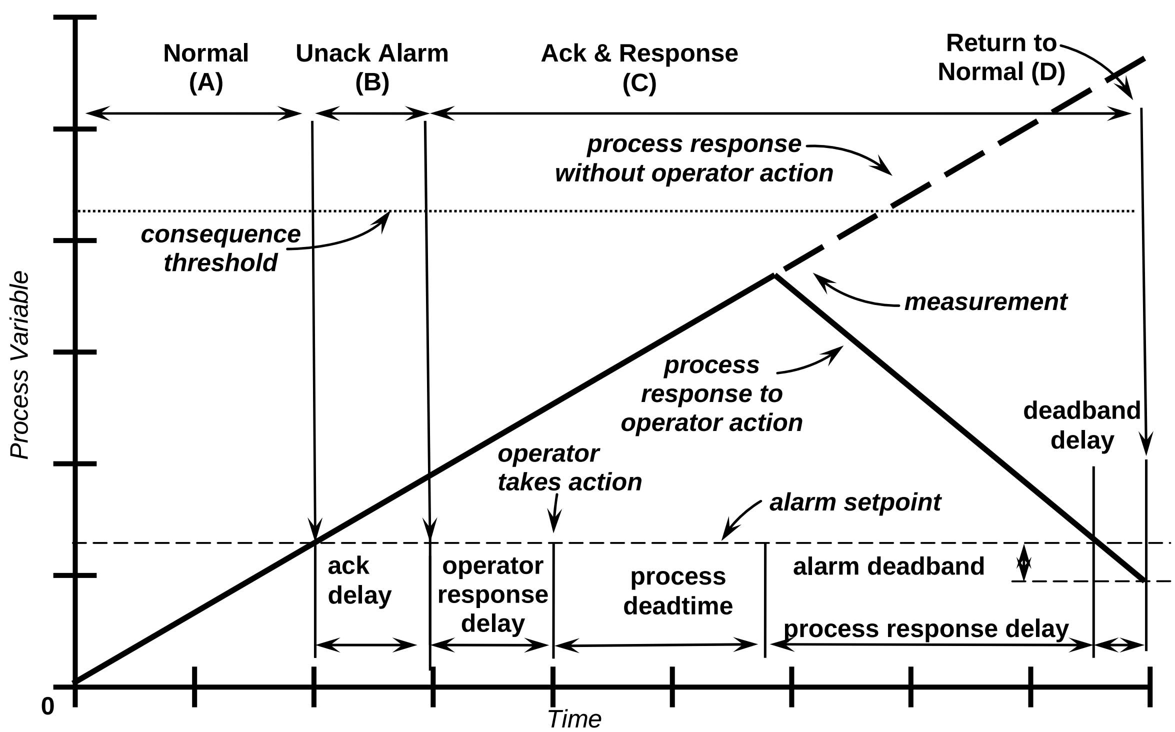


Figure 6 – Alarm Timeline

5.5.1 Normal (A)

The normal alarm state is defined as the state in which the process is operating within normal specifications, the alarm is clear and all past alarms have been acknowledged.

5.5.2 Unack Alarm (B)

The unacknowledged alarm state results when the measurement crosses the alarm setpoint. There are several factors that affect the uncertainty of the alarm trigger time such as:

a) measurement accuracy,

b) alarm delay time.

5.5.3 Ack and Response (C)

The acknowledged alarm state is reached when an operator acknowledges the alarm condition, after the acknowledge delay. In this state the alarm has not cleared. There are several factors that affect the uncertainty of the operator response time such as:

a) system processing speed,

b) HMI design and clarity,

c) operator awareness and training,

d) operator workload,

e) complexity of determining the corrective action,

f) complexity of the corrective action.

From the time the alarm is triggered until the operator takes the correct action is the actual response time for the alarm, or operator response delay. It includes the detection of the alarm, the diagnosis of the situation and determination of the corrective action in response, and the execution of that response. The upper limit of the response time is the allowable response time, the point beyond which the consequence will occur even if action is taken.

5.5.4 Return to Normal (D)

The return to normal alarm state should result from the correct operator action within the allowable response time. There are several factors that affect the uncertainty of the return to normal time. These include:

a) the operator response delay,

b) the degree of action taken,

c) the process deadtime in response to the corrective action,

d) the process response time to the corrective action,

e) the accuracy of the process measurement,

f) the deadband of the alarm setpoint,

g) the operational speed of the alarm system.

5.5.5 Consequence Threshold

The consequence results when no operator action is taken, the incorrect or insufficient action is taken, or the action is not completed within the allowable response time. The consequence begins to occur at the consequence threshold. The total time from the alarm to the consequence threshold includes the acknowledge delay, the operator response delay, the process deadtime, and the process response delay.

5.6 Feedback Model of Operator – Process Interaction

A model of operator-process interaction is shown in Figure 7. In response to a disturbance or malfunction, the process or system undergoes some change. If that change deviates significantly from the reference or objective for the process, the operator takes action to bring the process back to the reference and continues to monitor the measurement as it returns. In order for the action to occur, three stages of activity occur:

a) the deviation from desired normal operation is detected,

b) the situation is diagnosed and the corrective action determined,

c) the action is implemented to compensate for the disturbance.

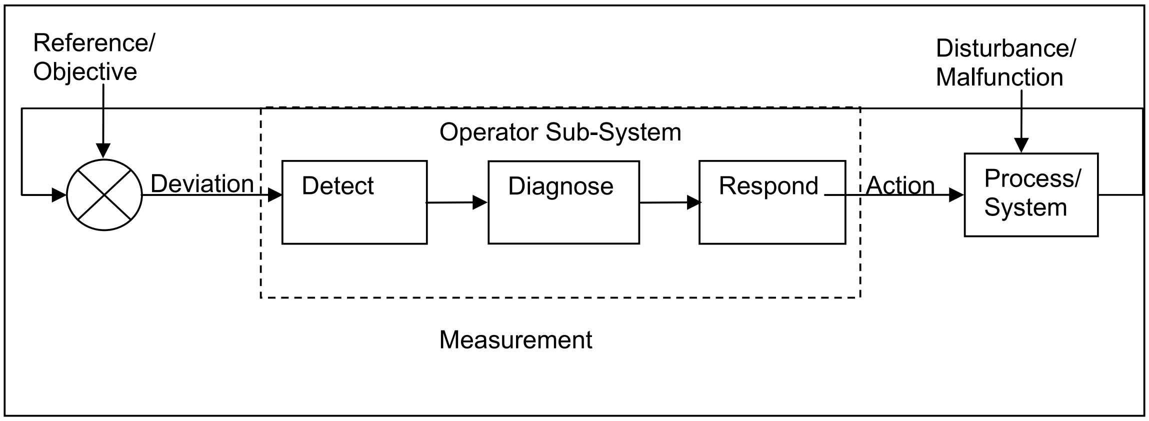


Figure 7 – Feedback Model of Operator Process Interaction

5.6.1 Detect

The operator becomes aware of the deviation from the desired condition. The design of the alarm system and the operator interface impact detection of deviation.

5.6.2 Diagnose

The operator uses knowledge and skills to interpret the information and diagnose the situation and determine the corrective action to take in response.

5.6.3 Respond

The operator takes corrective action in response to the deviation.

5.6.4 Performance Shaping Factors

The ability of the operator to carry out the sub-system functions is affected by a variety of variables, including workload, short term or working memory limitations, fatigue, training, and motivation.

6 Alarm Philosophy

6.1 Purpose

Alarm philosophy is a separate stage of the alarm lifecycle. The alarm philosophy serves as the framework to establish the criteria, definitions and principles for the alarm lifecycle stages by specifying items including the methods for alarm identification, rationalization, classification, prioritization, monitoring, management of change, and audit to be followed. An alarm philosophy document ensures that facilities can achieve:

a) consistency across process equipment,

b) consistency with risk management goals/objectives,

c) agreement with good engineering practices,

d) design and management of the alarm system that supports an effective operator response.

6.2 Alarm Philosophy Contents

This section provides the minimum and recommended content to be addressed in the alarm philosophy. Due to the wide variety of equipment used within the process industry, the detailed content of the alarm philosophy may vary between industries and from one location to another. The required and recommended contents of the alarm philosophy are listed in Figure 8.

ALARM PHILOSOPHY CONTENTS	REQUIRED	RECOMMENDED
Purpose of alarm system	Y	
Definitions Y		
References		Y
Roles and responsibilities for alarm management	Y	
Alarm design principles	Y	
Rationalization Y		
Alarm class definition	Y	
Highly managed alarms (or site equivalent)		Y
HMI design guidance	Y	
Alarm setpoint determination		Y
Prioritization method	Y	
Alarm system performance monitoring	Y	
Alarm system maintenance	Y	
Testing of alarms	Y	
Approved advanced alarm management techniques		Y
Alarm documentation		Y
Implementation guidance	Y	
Management of change	Y	
Training	Y	
Alarm history preservation	Y	
Related site procedures		Y
Special Alarm Design Considerations		Y

Figure 8 – Required and Recommended Alarm Philosophy Content

For systems designed for new plants, the alarm philosophy should be drafted as part of the project planning and development, and be fully defined and approved before the system has been commissioned.

For existing systems which are being remediated, and no philosophy exists, the alarm philosophy should be one of the first stages of the remediation effort.

6.2.1 Purpose of Alarm System

Defining the purpose and objectives of a process plant alarm system serves to orient participants in design and improvement activities. Having this definition ensures that participants can implement and maintain an effective alarm system based on informed decisions during the execution of these activities.

6.2.2 Definitions

Terms that will be encountered in the course of design and improvement of an alarm system shall be defined to ensure that all participants share a common understanding.

6.2.3 References

A list of appropriate references for alarm management should be included. References can be internal company documents (e.g., management of change) or external published material (e.g., OSHA, ISA).

6.2.4 Roles and Responsibilities for Alarm Management

Responsibility for the activities of the alarm life cycle shall be established in the alarm philosophy. Specific aspects to cover include the following:

a) the owner of the alarm system, the philosophy and related documents,

b) the role responsible for management and regular maintenance of the alarm system,

c) the role responsible for technical support to resolve problems with the alarm system,

d) the role responsible to ensure that the requirements outlined in the alarm philosophy are followed.

6.2.5 Alarm Design Principles

The definition of an alarm, with examples that meet and do not meet the definition, shall be documented in the alarm philosophy. The criteria for selection and principles for design of alarms should be consistent with the definition of an alarm.

The criteria and principles should address:

a) the role of the alarm system in identifying approaches to unsafe or sub-optimal operation, warning of malfunctions, and prompting the operator of actionable changes in the process,

b) the methods to be used for alarm identification,

c) the alarm states (e.g. normal, acknowledged, latched, shelved, etc.) that the facility will use.

6.2.6 Rationalization

In order to maximize the functionality of the alarm system it is important that the operator receive only those alarms that are meaningful and actionable. Ensuring that an alarm is actionable is done through alarm rationalization. This section of the alarm philosophy should list the criteria for alarms and the information to be captured during rationalization.

6.2.7 Alarm Class Definition

Alarm classes are used to set common characteristics and requirements for managing alarms. An alarm may belong to more than one class. This section should include the definition of the alarm class. It should also include the following requirements:

a) alarm documentation,

b) operator training and training documentation,

c) operating procedures associated with these alarms,

d) alarm maintenance,

e) alarm testing,

f) alarm monitoring and assessment,

g) alarm management of change,

h) alarm history retention,

i) alarm audit,

j) alarm prioritization,

k) HMI design,

l) alarm operation.

6.2.7.1 Highly Managed Alarms

Highly Managed Alarms (HMA) are classes of alarms that require more administration and documentation than others. Since the criteria may vary by process, industry or location, the alarm philosophy shall define the criteria for assigning alarms to HMA classes. The designation of alarm classes as highly managed should be based upon one or more of the following:

a) alarms critical to process safety or the protection of human life (e.g., safety alarms),

b) alarms for personnel safety or protection,

c) alarms for environmental protection,

d) alarms for current good manufacturing practice,

e) alarms for product quality,

f) alarms for process licensor requirements,

g) alarms for company policy.

Not all sites will have HMAs. If a site does use HMAs, this section of the alarm philosophy shall be used to explicitly document the requirements for this alarm class.

6.2.8 HMI Design Guidance

Documenting the method, format, and coding (e.g., color, symbol, alpha-numeric) for alarm presentation to the operator establishes guidelines for display and annunciation so that they are consistent throughout the plant

Specific elements that should be covered in this section include:

a) the mechanism used (e.g., panel, BPCS console screens, etc.) to communicate the alarms to the operator,

b) recommendations for the indications on the HMI of the alarm states (e.g., normal, acknowledged, latched, shelved, etc.) that will be used at the facility,

c) the types of displays that will be used (e.g., alarm summary, overview, first-out, etc.),

d) the functions that will be available in the HMI, including shelving and suppression.

6.2.9 Prioritization Method

Consistent priorities aid the operator in deciding the order of response during high alarm events. Specific elements that shall be covered in this section include:

a) the basis for alarm prioritization (e.g., time to respond, severity of consequence, etc.),

b) the metrics for alarm configuration (e.g., alarm count, priority distribution),

c) any impact of classification on prioritization.

6.2.10 Alarm Setpoint Determination

This section should provide guidance on the methods used for determination of alarm setpoints.

6.2.11 Alarm System Performance Monitoring

Metrics are used to monitor alarm system performance against the target performance levels. This section provides a basis for assessing performance to decide if improvements are required.

Specific elements that should be covered in this section include:

a) the objective for monitoring and assessment,

b) the monitoring metrics and target values,

c) guidance on the approach to improve performance on the metrics.

6.2.12 Alarm System Maintenance

This section identifies the activities necessary to maintain the alarm system.

Specific elements that should be covered in this section include:

a) alarm maintenance record keeping,

b) the requirements around out-of-service alarms,

c) the policy on the use of interim alarms.

6.2.13 Testing of the Alarm System

This section identifies procedures to ensure consistent and adequate testing of the alarm system throughout the alarm lifecycle. Decisions around applicability, criteria, methods, and frequency should be thoroughly documented by alarm classes.

6.2.14 Approved Advanced Alarm Management Techniques

Approved advanced alarm management techniques and the conditions or criteria for their use, should be identified. Identification of approved advanced alarm techniques supports the training of personnel on these techniques.

Not all sites will use the advanced/enhanced alarm management techniques (see Clause 12). If a site does use advanced enhanced alarm management techniques, this section of the alarm philosophy shall be used to identify the techniques to be used and related responsibilities and work processes.

6.2.15 Alarm Documentation

Appropriate documentation should be defined and retained, including:

a) rationalization information (e.g., a master alarm database),

b) periodic alarm performance reports.

Other documentation needs may be identified by the requirements of the different alarm classes.

Appropriate documentation ensures that advanced techniques are implemented consistently, providing expected behaviors to the operator across all modes of operation

6.2.16 Implementation Guidance

Defining the basic approach for commissioning and checkout of the alarm system ensures that this is done in an effective and consistent manner throughout the plant or company. This assures the effective deployment of the alarm system.

6.2.17 Management of Change

This section identifies the types of changes and the applicable procedures. Types of changes may include:

a) temporary changes to alarms (e.g., out-of-service),

b) temporary changes to alarm attributes in conjunction with an advanced alarm system for alarm attribute enforcement,

c) permanent changes to the master alarm database, alarm attributes, or designed suppression.

Permanent changes follow a management of change procedure to ensure that changes made during design, implementation, operation, or maintenance are appropriately evaluated and approved by the authorized parties and documented. This typically includes documented assessment of each change, records of system modifications, and authorization.

6.2.18 Training

This section specifies how plant personnel are to be trained on the use, management, and design of the alarm system. This is included to ensure that the instructors responsible for training are aware of the need for and their responsibility to provide appropriate training on the alarm system and any changes made to the alarm system. This section should also specify the training documentation requirements.

Specific aspects of training that should be covered in the alarm philosophy or other equivalent documentation for each of the alarm classes include:

a) the job roles or personnel requiring training relating to the alarm system,

b) an outline of the training contents,

c) when training is required.

6.2.19 Alarm History Preservation

This section defines what aspects of the alarm history (e.g., annunciations, acknowledgements, return to normal, operator actions) should be preserved and for how long in response to specific events (e.g., incidents, violation of safe operating limits). In some industries and regions, regulatory bodies or local statute may require preservation of this information.

6.2.20 Related Site Procedures

To avoid inconsistencies between the alarm philosophy and other site procedures, the alarm philosophy should cite relevant procedures. The following documents may be related to the alarm philosophy:

a) standard operating procedures,

b) operator training policies and guides,

c) safety, health and environmental procedures,

d) maintenance procedures,

e) alarm handling policies and codes,

f) application programming guidelines,

g) commissioning or qualification processes and procedures,

h) other site procedures related to the alarm philosophy depending on the specific site.

6.2.21 Special Alarm Design Considerations

The philosophy document should specify rules and methods for the design of alarms covering specific circumstances where consistency is important (e.g., bypass alarms, alarms from redundant sensors). Alarm classes may be the source of such specific design considerations.

6.3 Alarm Philosophy Development and Maintenance

Personnel who apply the alarm philosophy should be involved in developing the alarm philosophy. Personnel involved should be equipped with detailed knowledge and understanding of design, operation and maintenance of the process related to the site. Specific areas of expertise include:

a) process operations,

a) process instrumentation,

b) control systems,

c) process technology,

d) mechanical/reliability engineering,

e) safety, health and environmental,

f) alarm management,

g) management of change process.

7 Alarm System Requirements Specification

NOTE: THIS CLAUSE IS INFORMATIVE AND DOES NOT CONTAIN MANDATORY REQUIREMENTS.

7.1 Purpose

The alarm system requirements specification (ASRS), which may also be called an alarm functional requirements specification, is part of the philosophy lifecycle stage. This clause provides guidance on the development and uses of an alarm system requirements specification. The ASRS documents the alarm functionality expected of the control system. The ASRS is often a subset of the overall system requirements specification of a control system.

The alarm system requirements specification is typically specific to a site, an individual control system, or group of similar control systems. While the ASRS is consistent with the alarm philosophy, it contains more detailed functional requirements of the alarm system than the alarm philosophy, including detailed user requirements and considering relevant site infrastructure requirements. These requirements are used to help evaluate systems, guide the detailed system design, help determine if any system customization or use of third party products is necessary, and serve as the primary basis of alarm system function testing during implementation. It is important to distinguish an ASRS from individual alarm activities that occur later on in the lifecycle of a system. The ASRS specifies what alarm functionality to be available when rationalizing, designing, implementing, visualizing and recording individual alarms, and in analyzing alarm records.

The ASRS is typically generated early in the planning for a new control system. It is updated through the implementation stage to ensure consistency with the targeted capabilities of the chosen system and, therefore, relevant in driving system design, system testing, and training activities. The ASRS is not normally updated following system implementation. Changes to alarm system functionality can occur during the life of a system. These changes can be managed and documented via management of change.

7.2 Recommendations

Planning for new control systems and major revisions to the alarm functionality of existing control systems should include an ASRS, with the ASRS containing specifications for some or all of the following:

a) alarm attributes,

b) alarm HMI,

c) alarm communication infrastructure,

d) alarm record logging,

e) alarm record analysis,

f) other capabilities that facilitate alarm lifecycle activities.

There may be new control system projects in which it is determined an ASRS is not necessary, (e. g., replicating existing systems). The decision to omit the ASRS and the rationale supporting it should be documented.

7.3 Development

The alarm system is only one of the functional systems within a control system and the performance of the overall system may require compromise on the alarm system requirements. The alarm philosophy may contain guidance that can be used to generate some of the alarm system requirements specification, including:

a) alarm priorities available,

b) visual alarm indication capabilities, such as colors and symbols,

c) audible alarm indication capabilities,

d) alarm summary display functionality,

e) alarm shelving functionality,

f) alarm suppression capabilities,

g) alarm configuration capabilities, such as deadband and time delay,

h) alarm log capabilities, such as operator response entry and batch identification,

i) alarm monitoring and assessment capabilities,

j) alarm system audit functionality,

k) advanced alarming functionality.

Note: Some alarm requirements may exist in other documents, such as in a safety requirements specification for SIS applications, as defined in ANSI/ISA 84.00.01-2004 Part 1 (IEC 61511 Mod).

7.4 Systems Evaluation

Alarm system functionality should be evaluated against requirements during control system selection. The alarm system functionality of process control systems varies from the very limited to the very advanced. The alarm system requirements specification provides a list of specific criteria which can contribute to the comparative evaluation of different systems.

7.5 Customization and Third-Party Products

If important system requirements in the specification are not met by standard commercial products, it may be necessary to develop custom solutions, which may include third-party products, or to reconsider the specification. Custom developed solutions may have higher lifecycle costs than use of single supplier commercially available solutions. The alarm system requirements specification facilitates early recognition of the need for customized solutions, including use of third party products, and can initiate associated cost /benefit analysis.

7.6 Alarm System Requirements Testing

Each alarm system requirement should be tested prior to the operations stage of the lifecycle.

8 Identification

NOTE: THIS CLAUSE IS INFORMATIVE AND DOES NOT CONTAIN MANDATORY REQUIREMENTS.

8.1 Purpose

Identification is a separate stage of the alarm lifecycle. Identification is a general term for the different methods that can be used to determine the possible need for an alarm or a change to an alarm. The identification stage is the input point of the alarm lifecycle for the recommended alarms or alarm changes. Identified alarms are an input to rationalization.

8.2 Alarm Identification Methods

This standard does not define or require any specific method for alarm identification. Alarms may be identified by a variety of good engineering practices or regulatory requirements. Some combination of identification methods should be used to determine potential alarms. Where appropriate, alarm identification may be done during alarm rationalization.

Some common alarm identification methods are:

a) allocation of safety layers,

b) process hazards analysis (PHA),

c) layer of protection analysis (LOPA),

d) incident investigations,

e) environmental permits,

f) failure mode and effects analysis (FMEA),

g) current good manufacturing practice (cGMP),

h) ISO quality reviews,

i) P&ID reviews,

j) operating procedure reviews,

k) packaged equipment manufacturer recommendations.

9 Rationalization

9.1 Purpose

Rationalization is a separate stage in the lifecycle. During rationalization, existing or potential alarms are systematically compared to the criteria for alarms set forth in the alarm philosophy. If the proposed alarm meets the criteria, then the alarm setpoint, consequence, and operator action are documented, and the alarm is prioritized and classified according to the philosophy. Rationalization produces the detail design information necessary for the design stage of the alarm lifecycle.

9.2 Objective

Rationalization shall determine and document, at a minimum, the following for every alarm rationalized per the site alarm philosophy for every applicable process state:

a) alarm type,

b) priority,

c) class,

d) alarm setpoint value or logical condition (e.g., off-normal),

e) operator action,

f) consequence of inaction or incorrect action,

g) need for advanced alarm handling techniques if necessary.

9.3 Alarm Justification

During this stage, every alarm requiring rationalization is compared to the criteria set forth in the alarm philosophy for selection to justify that it is an alarm. Initial training of the participants on alarm management and design may improve the effectiveness of the analysis.

9.3.1 Justification Approach

The comparison activity should:

a) utilize a team approach,

b) rely heavily upon operator input,

c) focus on the operator action to be prompted.

9.3.2 Individual Alarm Justification

All alarms to be rationalized are systematically reviewed. This usually is done either by progression through engineering drawings, databases, or HMI displays. The information to be captured for each rationalized alarm should be specified in the alarm philosophy, but typically includes:

a) verification that proposed alarm meets the criteria for an alarm stated in the philosophy,

b) the response action(s) the operator may take,

c) the consequence that will occur if action is not taken or is unsuccessful,

d) the time required between alarm annunciation and the occurrence of the specific consequence.

Those alarms for which the console operator's primary response is simply to relay the information to the appropriate person or group for action (e.g., instrument diagnostic alarms) should be reviewed to determine if an alternate method exists to transfer the information without burdening the operator or the alarm system.

9.3.3 Impact on Alarm System

Alarm justification and prioritization should also consider the functioning of the alarm, together with the alarm attributes, ensuring that:

a) the alarm will not become a nuisance or standing alarm,

b) the alarm does not duplicate another alarm that has the same operator actions.

If either is true, then advanced alarming techniques (e.g., state based alarming or logic based alarms) may need to be specified to prevent this from occurring. Alarms on redundant equipment or redundant instrumentation are often the reasons for either of these to be true.

9.4 Alarm Setpoint Determination

Guidance for the determination of alarm setpoints stated in the alarm philosophy is applied. Effective methods use the allowable response time, (see Figure 6), the complexity of the operator action, knowledge of the process operation and history, and other factors.

9.5 Prioritization

The method for priority assignment defined in the alarm philosophy is applied to the rationalized alarm and a priority assigned. Effective prioritization typically results in higher priorities chosen less frequently than lower priorities. Most of the alarms should be assigned to the lowest alarm priority (least important) and the fewest to the highest alarm priority (most important), with a consistent transition between the two. The resulting priorities should have alignment with the consequence and allowable response time, such that the lowest priority alarms have the least severe consequences and longest allowable response times and the highest priority alarms have the most severe consequences and the shortest allowable response times. Distribution metrics for priority are provided in Clause 16.

9.6 Removal

Existing alarms which fail to meet the criteria for alarming provided in the alarm philosophy shall be documented along with the basis (i.e., criterion it failed to meet) justifying removal. Those alarms should then be subject to further review per the MOC process to remove the alarm attributes from the instrument.

9.7 Classification

Classification is an activity completed in the rationalization stage of the alarm lifecycle. Alarms shall be assigned to one or more classes as defined in the alarm philosophy. Not all alarms in a class need have the same priority.

The classification may occur prior to, during, or after the alarm justification and prioritization.

9.8 Review

Upon completion of the initial justification, prioritization, and classification of all the required alarms, the results should be reviewed to ensure consistent application of the criteria throughout the process. The results should be compared to any targets for number and priority of alarms that might be set forth in the alarm philosophy.

9.9 Documentation

Rationalization shall be documented to become the basis for ensuring the integrity of the alarm system. The documentation (e.g., a master alarm database) delineates the link between each alarm and the alarm philosophy and can be used for several purposes, including:

a) input to the detailed design stage of the alarm lifecycle,

b) utilization as part of the management of change,

c) training of and review by operators,

d) periodic auditing and reconciliation of the control system alarm settings,

e) evaluation of alarm monitoring and effectiveness data.

10 Basic Alarm Design

10.1 Purpose

Basic alarm design is part of the detailed design stage of the lifecycle. This clause presents the essential requirements to implement the alarms defined by the rationalization process within a specific control system. Information in this section addresses the design considerations associated with the triggering of alarms. All design considerations related to the presentation of alarms will be contained in Clause 11.

10.2 Usage of Alarm States

The goal of this activity is to define which alarm states are used during operation of the system. As shown in Figure 5, the possible alarm states are as follows:

a) normal,

b) unack alarm,

c) ack'd alarm,

d) RTN unack,

e) latch unack (optional),

f) latch ack'd (optional),

g) shelved,

h) suppressed by design,

i) out-of-service.

The latching capability represented by latch unack and latch ack'd is optional. This function may not be available in a particular system or users may choose not to utilize these states during operation.

If the alarm latching capability is used, then the scope of implementation (i.e., individual alarms, alarm classes, or the entire system) should be documented.

10.2.1 Alarm State Triggering

The source for each alarm in the system should be documented. Changes in alarm state can be triggered from various sources within a control system as shown in Figure 1, including:

a) the field device (e.g., sensors and final control elements),

b) the control and safety system,

c) the HMI.

10.2.2 Use of Alarm State Information

A clear and consistent philosophy should be documented regarding the use of alarm state information within configuration logic, such as driving interlock actions. If alarm setpoints will be used for purposes in addition to operator notification (e.g., as an interlock setpoint), then documentation, training and management of change may be impacted. Additionally the impact of modifying alarm setpoints and attributes as well as the use of designed suppression should be clearly identified, documented, and potentially restricted (e.g., extra confirmation or higher access level required). This information should be specifically documented in the alarm philosophy under alarm design principles.

10.3 Alarm Types

Alarm types should be designed for each alarm as defined during the rationalization activity. The common alarm types to be considered include:

a) absolute alarms,

b) deviation alarms,

c) rate of change alarms,

d) discrepancy alarms,

e) calculated alarms,

f) recipe-driven alarms,

g) bit-pattern alarms,

h) controller output alarms,

i) systems diagnostic alarms,

j) instrument diagnostic alarms,

k) adjustable alarms,

l) adaptive alarms,

m) re-alarming alarms,

n) statistical alarms,

o) first-out alarms,

p) bad measurement alarms.

The available alarm types that are included within the control system vary. It may be necessary to create a custom alarm type as part of the engineering scope on a project.

Alarm types should be selected carefully based on engineering judgment. Certain types, such as rate-of-change, deviation, bad measurement, and controller output alarms, are common sources of nuisance alarms during process upset conditions if they are not applied appropriately.

10.4 Alarm Attributes

During the basic design process the default alarm attributes should be configured for each alarm that has been identified during rationalization and set according to the master alarm database or based on engineering judgment. Attributes such as setpoint (e.g., limit), deadband or on and off delays, may be different depending upon the specific alarm type that will be implemented. Defining appropriate values can help minimize the number of nuisance alarms that are generated during operation. Recommendations for the design of specific alarm attributes are provided in the following sections.

10.4.1 Alarm Setpoints

Alarm setpoints should be configured based on the information documented in the master alarm database.

10.4.2 Alarm Deadbands

Alarm deadbands are an alarm attribute within the process control system that requires the process variable to cross the alarm setpoint into the normal operating range by some percentage of the range (see Figure 6). Deadbands are typically set based on the normal operating range of the process variable, measurement noise, and the type of process variable. Application of deadbands can be very effective in eliminating nuisance alarms.

10.4.2.1 Alarm Deadband Requirements

The control system shall provide the capability for implementing deadband functionality.

10.4.2.2 Alarm Deadband Recommendations

The engineering basis for setting of deadbands should be documented in the alarm philosophy. Figure 9 provides recommendations which represent a good starting point for common processes. Proper engineering judgment should be employed when setting deadbands in order to minimize nuisance alarms while maintaining process vigilance and plant / personnel safety. Excessive deadband, such as what might be calculated for an instrument with a large scale (e.g., flow of 0 – 100,000) can act as a latch, creating stale alarms. Settings should be documented and then reviewed during commissioning and after significant operating experience.

Signal Type	Deadband (Percent of Operating Range)
Flow Rate	~5%
Level ~5%	
Pressure ~	2%
Temperature ~	1%

Figure 9 – Recommended Starting Point Deadband Based on Signal Type

Reference: ML Bransby, "The Management of Alarm Systems", HSE Books, 1998, pp. 193-195

10.4.3 Alarm On-Delay and Off-Delay

The attributes on-delay and off-delay (i.e., filter timer and debounce timer) can be used to eliminate nuisance alarms. The on-delay is used to avoid unnecessary alarms when a signal temporarily overshoots its limit, thus preventing the alarm from being triggered until the signal remains in the alarm state continuously for a specified length of time. The off-delay is used to reduce chattering alarms by locking in the alarm indication for a certain holding period after it has cleared.

10.4.3.1 Alarm On-Delay and Off-Delay Requirements

The control system shall provide the capability for implementing on-delay and off-delay functionality

10.4.3.2 Alarm On-Delay and Off-Delay Recommendations

Figure 10 provides recommendations which represent a good starting point for common processes. Proper engineering judgment should be employed when setting on and off delays in order to minimize nuisance alarms while maintaining process vigilance and plant or personnel safety. Delay times should consider residence time during all modes of operation and whether PV filtering is being applied to reduce signal noise. On-delay times should be applied only after careful evaluation and potential control system operational effects. Settings should be reviewed during commissioning and after significant operating experience.

Signal Type	**Delay Time (On or Off)**
Flow Rate	~15 Seconds
Level ~60	seconds
Pressure ~1	5 seconds
Temperature ~60	seconds

Figure 10 – Recommended Delay Times Based on Signal Type

Reference: ML Bransby, "The Management of Alarm Systems", HSE Books, 1998, pp. 193-195

10.5 Programmatic Changes to Alarm Attributes

Some sites modify alarm attributes based on conditions such as product type or grade. Alarm attributes can typically be modified from one or more of the following sources:

a) operator interface (e.g., manual changes during operation),

b) engineering interface (e.g., design changes under management of change),

c) control logic (e.g., sequences, phases),

d) external to the control system (e.g., Manufacturing Execution System (MES), Enterprise Resource Planning (ERP) system, or advanced alarming program).

The alarm philosophy should detail the use and limitations of this technology. For each alarm the user should identify and clearly document which sources of the control system will have programmatic access to modify attributes during operation and which sources will be subject to management of change procedures. More advanced techniques for modifying alarm attributes are covered in Clause 12.

10.6 Review Work Product

A typical control system provides the user with the ability to implement numerous different alarm types for a single process variable. To minimize alarm loading on the operator, the basic alarm design results should be reviewed against the master alarm database to ensure than only required alarms are being activated. The methods for activation and deactivation may be different based on the specific functionality provided in the control system.

11 Human-Machine Interface Design for Alarm Systems

11.1 Purpose

The HMI design for alarm systems is part of the detailed design lifecycle stage. This section outlines the functionality to provide alarm indications and related functions to the operator and other HMI users. The indication and display of alarms is only one component of the HMI design, and contributes to effective operator–process interaction (see Figure 7). Guidance on general HMI design for control systems is outside the scope of this standard.

The capabilities of control systems vary widely. Some features described in this section are not available in all systems.

11.2 Overview

The HMI design for alarms follows the alarm philosophy, is consistent with the overall HMI design philosophy, and is within the capabilities of the control system.

11.2.1 HMI Information Requirements

The interface shall clearly indicate:

a) tags in alarm,

b) alarm states,

c) alarm priorities,

d) alarm types.

11.2.2 HMI Functional Requirements

The interface shall provide the ability for the operator to:

a) silence audible alarm indications (i.e., without acknowledging the alarm),

b) acknowledge alarms,

c) place alarms out-of-service through access controlled methods as allowed in the philosophy,

d) modify alarm attributes through access controlled methods only.

11.2.3 HMI Display Requirements

The interface shall provide the capability for the following:

a) at least one alarm summary display,

b) alarm indications on process displays,

c) alarm indications on tag detail display,

d) assignment of alarms to operator stations.

11.2.4 HMI Functional Recommendations

The interface should provide:

a) an alarm shelving function

b) A designed suppression function,

c) display of alarm messages.

11.3 Alarm States Indications

The alarm state transition diagram (see Figure 5) defines the states of alarm in the HMI.

11.3.1 Required Alarm State Indications

A combination of visual indications, audible indications, or both, shall be used to distinguish these alarm states:

a) normal,

b) unacknowledged alarm,

c) acknowledged alarm.

11.3.2 Recommended Alarm State Indications

The following recommended alarm state indications are common industry practice.

11.3.2.1 Normal State Indication

The normal state should not use an audible indication. The normal state visual indication should be the same as indications without alarms.

11.3.2.2 Unacknowledged Alarm State Indication

The unacknowledged alarm state should use an audible and visual indication. The audible indication should be silenced with a silence action or acknowledge action by the operator. The visual indication should be clearly distinguishable from the normal state indication by using colors and symbols, (e.g., shape or text). The visual indication for an unacknowledged alarm should include a blinking element. There are some environments in which an audible indication is not an effective indicator of unacknowledged alarms.

11.3.2.3 Acknowledged Alarm State Indication

The acknowledged alarm state should not use an audible indication. The acknowledged alarm state visual indication should be clearly distinguishable from the normal state indication by using symbols, (e.g. shape or text) and should be identical in color to the unacknowledged alarm indication. A blinking element should not be used in the visual indication for an acknowledged alarm.

11.3.2.4 Return to Normal Unacknowledged State Indication

The return to normal unacknowledged state should not use an audible indication. The return to normal unacknowledged state visual indication may be the same as the normal state or it may indicate an unacknowledged status with a blinking element.

11.3.2.5 Latched Unacknowledged Alarm State Indication

The unacknowledged latched alarm state should use an audible indication, usually the same as the unacknowledged alarm indication. The audible indication should be silenced with a silence action or acknowledge action by the operator. The unacknowledged latched alarm state visual indication may be the same as the unacknowledged alarm indication, or it may be different to indicate the latched status.

11.3.2.6 Latched Acknowledged Alarm State Indication

The acknowledged latched alarm state should not use an audible indication. The latched acknowledged alarm state visual indication should be similar to the acknowledged state indication, but it should be different to indicate the need for operator reset of the latch. The visual indication for a latched acknowledged alarm should not include a blinking element.

11.3.2.7 Shelved Alarm State Indication

Shelved alarms should be visually indicated in the HMI. The visual indication for a shelved alarm should not include a blinking element. The shelved alarm state indication should be distinct from the unacknowledged and acknowledged state indications. No audible indication should be used to identify shelved alarms.

11.3.2.8 Suppressed by Design Alarm State Indication

Alarms suppressed by design should be visually indicated in the HMI. The visual indication for an alarm suppressed by design should not include a blinking element. The suppressed by design alarm state indication should be distinct from the unacknowledged and acknowledged state indications. No audible indication should be used to identify alarms suppressed by design.

11.3.2.9 Out-of-Service Alarm State Indication

Out-of-service alarms should be visually indicated in the HMI. The visual indication for an out-of-service alarm should not include a blinking element. The out-of-service alarm state indication should be distinct from the unacknowledged and acknowledged state indications.. No audible indication should be used to identify out-of-service alarms.

11.3.2.10 Summary of Alarm State Indications

The recommended audible and visual alarm state indications for typical alarms are summarized in Figure 11.

Alarm State	Audible Indication	Visual Indications		
		Color Sy	mbol	Blinking
Normal	**No**	**No**	**No**	**No**
Unacknowledged Alarm	**Yes**	**Yes**	**Yes**	**Yes**
Acknowledged Alarm	**No**	**Yes**	**Yes**	**No**
Return to Normal State Unacknowledged Alarm	**No**	**Optional**	**Optional**	**Optional**
Latched Unacknowledged Alarm	**Yes**	**Yes**	**Yes**	**Yes**
Latched Acknowledged Alarm	**No**	**Yes**	**Yes**	**No**
Shelved Alarm	**No**	**Optional**	**Optional**	**No**
Suppressed by Design Alarm	**No**	**Optional**	**Optional**	**No**
Out-of-Service Alarm	**No**	**Optional**	**Optional**	**No**

Note 1: Yes signifies an indication that is different from the normal state indication.

Figure 11 – Recommended Alarm State Indications

11.3.3 Audible Alarm State Indications

The audible alarm indication for unacknowledged alarms may be also used to indicate the priority, the process area, or the alarm group, depending on the alarm philosophy.

In environments where an audible indication of an unacknowledged alarm is not effective, (e.g., high ambient noise level environments), a clear visual indication of an unacknowledged alarm that is always within view of the operator should be used, (e.g., a light or series of lights).

11.4 Alarm Priority Indications

The alarm philosophy provides a set of alarm priorities used in the HMI to assist the operator in selecting the sequence of alarm response actions.

11.4.1 Alarm Priority Indication Requirements

A unique combination of visual indications, audible indications, or both, shall be used to distinguish the alarm priorities within the alarm system.

11.4.2 Recommended Alarm Priority Indications

The following recommended alarm priority indications are common industry practice.

11.4.2.1 Color Alarm Priority Indications

A separate color indication should be used for each alarm priority. The alarm priority colors should be reserved and should not be used for other elements of the HMI. There are some environments in which colors cannot be reserved for priority indication.

11.4.2.2 Symbol Alarm Priority Indications

A unique symbol, (e.g. shape or text), should be used to indicate each alarm priority to reinforce color coding.

11.4.2.3 Audible Alarm Priority Indications

An audible indication should be used for each alarm priority. In environments where an audible indication is not used as a priority indication, a visual priority indication should be used.

11.5 Alarm Message Indications

The alarm message provides further clarification of the alarm beyond the state and priority indication. It may also include part of the alarm response action or a reference to the alarm response procedure.

11.5.1 Recommended Alarm Message Indications

The following recommended alarm message indications are common industry practice.

11.5.1.1 Visual Alarm Message Indications

A text message should be generated for each alarm and displayed on the alarm summary. The alarm text message is usually not directly displayed on process displays.

11.5.1.2 Vocalized Alarm Message Indications

A vocalized alarm message, using a voice synthesizer, is infrequently used. The vocalized message should be structured and brief. The vocalized message should be silenced with a silence action or acknowledge action by the operator. A visual indication should be used in conjunction with a vocalized alarm message.

11.6 Alarm Displays

Within a control system there are several types of displays that are effective as part of the alarm system. These include:

a) alarm summary display,

b) alarm status display,

c) alarm log display,

d) overview display,

e) process display,

f) tag detail display,

g) first-out display,

h) shelved alarm display,

i) out-of-service alarm display,

j) suppressed by design alarm display.

11.6.1 Alarm Summary Display

At least one alarm summary display is required for each alarm system. The alarm summary provides a list of active alarms within the alarm system. There are several required and recommended functions for alarm summary displays.

11.6.1.1 Information Requirements

The alarm summary display shall list only alarm information. The display shall provide the following information for each alarm:

a) the name and description of the tag in alarm,

b) the alarm state (including acknowledged status),

c) the alarm priority,

d) the time/date the alarm became active,

e) the alarm type.

11.6.1.2 Information Recommendations

The alarm summary display should provide the following information for each alarm:

a) the process value,

b) the alarm setpoint,

c) the process area,

d) the alarm group,

e) the alarm message.

11.6.1.3 Additional Information Recommendations

In addition to the information for each alarm, the header for the alarm summary should display:

a) the number of alarms in the summary list,

b) the number of unacknowledged alarms in the summary list.

11.6.1.4 Functional Requirements

The alarm summary display shall provide the following functions:

a) sorting of alarms by chronological order,

b) sorting of alarms by priority,

c) individual acknowledgment of each alarm.

11.6.1.5 Functional Recommendations

The alarm summary display should provide the following functions:

a) navigational link to the appropriate process display,

b) filtering of alarms by time of alarm,

c) filtering of alarms by priority,

d) filtering of alarms by alarm type,

e) filtering of alarms by alarm group,

f) filtering of alarms by process area,

g) time limits for filters.

Where alarm summary filters are used, the display should clearly indicate when a filter is in use.

11.6.2 Alarm Status Display

An alarm status display is recommended. The alarm status display provides an indication of the number of alarms by priority for each process area, usually in a process flow arrangement.

11.6.2.1 Information Recommendations

The alarm status display should provide the following information for each process area or other grouping:

a) the number of alarms in each alarm priority,

b) the number of unacknowledged alarms in each priority,

c) an indication if all alarms in a priority are acknowledged.

11.6.2.2 Functional Recommendations

The alarm status display should provide the following functions:

a) navigational link to the appropriate alarm status display,

b) navigational link to the appropriate process display,

c) navigational link to the appropriate overview display.

11.6.3 Alarm Log Displays

An alarm log display should be provided. The alarm log display provides access to the alarm log, which contains an alarm record for each alarm state change (e.g., acknowledgment, return to normal), etc…).

11.6.3.1 Information Recommendations

The alarm log display should provide the following information for alarm records:

a) the name and description of the tag,

b) the alarm state (including acknowledged status),

c) the alarm priority,

d) the date and time of the alarm,

e) the date and time of acknowledgment,

f) the alarm type.

11.6.3.2 Functional Recommendations

The alarm log display should provide the following functions:

a) filtering of alarms by tag,

b) filtering of alarms by time of alarm,

c) filtering of alarms by priority,

d) filtering of alarms by alarm type,

e) filtering of alarms by alarm group,

f) filtering of alarms by process area.

11.6.4 Overview Displays

The overview display provides a higher level view of the process than shown on individual process displays. The overview display can assist the operator by providing alarm overview indicators (e.g., show the highest active alarm priority or alarm counts by all priority) for process areas as part of the process overview display.

11.6.5 Process Displays

The process displays provide a process context for the alarms. The process displays should provide the following information:

a) the tag identity (through text or other access methods),

b) the alarm state, including acknowledge status,

c) the alarm priority,

d) the alarm suppression status,

e) the alarm type.

11.6.6 Tag Detail Displays

The detail displays provide a detail for the tag in alarm. A detail display should provide the following information:

a) the alarm state (including acknowledge status),

b) the alarm priority,

c) the alarm group,

d) the alarm type,

e) the alarm setpoint,

f) the alarm suppression status

g) the current value of the tag.

11.6.7 First-out Displays

The first-out display provides the status for a group of alarms and indicates which of the group triggered first. A first-out display should provide the following information:

a) a unique indication of the first-out alarm,

b) all alarms in the first-out group,

c) the state of all the alarms in the first-out group.

11.6.8 Other Display Elements

Other display elements may be used to indicate alarm states, including alarm banners.

11.7 Alarm Shelving

The temporary shelving of alarms by the operator is a common practice to keep nuisance alarms and other alarms from interfering with the effectiveness of the alarm system. Shelving includes a set of functions to ensure the integrity of the alarm system is maintained. Where alarm shelving is provided, the requirements of this clause shall be met.

11.7.1 Alarm Shelving Functional Requirements

The alarm shelving function shall provide the following:

a) displays of shelved alarms or equivalent list capabilities, to indicate all alarm shelved,

b) a time limit for shelving,

c) access control for shelving of highly managed alarms, if allowed,

d) the ability to unshelve alarms,

e) a record of each alarm shelved.

11.7.2 Alarm Shelving Functional Recommendations

The alarm shelving function should be designed to prevent alarm floods when alarms are automatically un-shelved.

11.7.3 Shelved Alarm Displays

Shelved alarm displays, or equivalent list capabilities, for an alarm system with shelving functionality have several required and recommended functions.

11.7.3.1 Information Requirements

Shelved alarm displays shall provide the following information:

a) the tag name and description,

b) alarm type,

c) the unsuppressed alarm state,

d) the alarm priority,

e) the time and date the alarm was shelved or the shelved time remaining.

11.7.3.2 Functional Requirements

Shelved alarm displays shall provide the following functions:

a) sorting of alarms by chronological order of shelving or shelved time remaining,

b) sorting of alarms by priority,

c) individual unshelving of alarms.

11.7.3.3 Functional Recommendations

Shelved alarms displays should provide the following functions:

a) sorting of alarms by chronological order for active alarms,

b) operator entry of the reason the alarm was shelved,

c) filtering of alarms by priority,

d) filtering of alarms by alarm state,

e) filtering of alarms by process area,

f) navigational link to a process display,

g) navigational link to the tag display.

11.8 Out-of-service Alarms

The suppression of alarms by placing an alarm out of service is common practice to remove alarms from service to allow maintenance. There are several required and recommended HMI functions related to out-of-service alarms.

11.8.1 Out-of-service Alarm Functional Requirements

The out-of-service alarm function shall provide the following:

a) a method to individually remove each alarm from service,

b) a method to individually return each alarm to service,

c) displays of out-of-service alarms or equivalent list capabilities, to indicate all alarm out-of-service,

d) access control to place highly managed alarms out-of-service if allowed,

e) a record of each alarm placed out-of-service.

11.8.2 Out-of-service Alarm Displays

Out-of-service alarm display, or equivalent list capabilities, shall be provided for the alarm system. Out-of-service alarm displays have several required and recommended functions. The out-of-service alarm displays may be combined with the shelved alarm displays.

11.8.2.1 Information Requirements

Out-of-service alarm displays shall provide the following information:

a) the tag name and description,

b) alarm type,

c) the unsuppressed alarm state,

d) the alarm priority,

e) the time and date the alarm was placed out-of-service.

11.8.2.2 Information Recommendations

Out-of-service alarm displays should provide an indication of the suppression method (e.g., out-of-service).

11.8.2.3 Functional Recommendations

Out-of-service alarm displays should provide the following functions:

a) sorting of alarms by chronological order of suppression,

b) operator entry of the reason the alarm was suppressed,

c) sorting of alarms by priority,

d) sorting of alarms by alarm state,

e) sorting of alarms by process area,

f) individual return-to-service of alarms.

11.9 Alarms Suppressed by Design

The designed suppression of alarms is common practice to prevent alarms that are not needed due to intended or actual operating conditions. Where alarm designed suppression is provided, the requirements of this clause shall be met.

11.9.1 Designed Suppression Functional Requirements

The designed suppression function shall provide the following:

a) displays of alarms suppressed by design or equivalent list capabilities, to indicate all alarms suppressed by design,

b) a record of each alarm suppressed by design.

11.9.2 Designed Suppression Displays

Designed suppression displays, or equivalent list capabilities, shall be provided for the alarm system. Designed suppression displays have several required and recommended functions. The designed suppression displays may be combined with the shelved alarm displays or out-of-service alarm displays.

11.9.2.1 Information Requirements

Designed suppression displays shall provide the following information:

a) the tag name and description,

b) alarm type,

c) the unsuppressed alarm state,

d) the alarm priority,

e) the time and date the alarm was suppressed.

11.9.2.2 Information Recommendations

Designed suppression displays should provide an indication of the suppression method (e.g., designed suppression).

11.9.2.3 Functional Recommendations

Designed suppression displays should provide the following functions:

a) sorting of alarms by chronological order of suppression,

b) sorting of alarms by priority,

c) sorting of alarms by alarm state,

d) sorting of alarms by process area.

11.10 Alarm Annunciators

Alarm systems may include separate alarm annunciation devices. Alarm annunciators should be integrated into the alarm system. The specification of alarm annunciators is outside the scope of this standard.

Note: For further guidance see ISA-18.1-1979 (R2004).

11.10.1 Alarm Annunciator Functional Recommendations

Alarm annunciators should provide the following functions:

a) The alarm annunciator should communicate alarm state information to the alarm log.

b) The alarm annunciator should be designed so as to prevent redundant alarms in the control system.

c) The alarm annunciator should be designed so as to prevent the need for redundant acknowledgement in the control system.

11.10.2 Alarm Annunciator Display Recommendations

Alarm annunciators should be designed so that the alarm layout on the annunciator follows a consistent methodology.

11.11 Safety Alarm HMI

An independent HMI may be required for some safety alarms. The identification methods for safety alarms are outside the scope of this standard.

11.11.1 Independent Safety Alarm HMI

An HMI independent from the BPCS may be required for the following safety alarms:

a) manual safety function alarms, (depending on considerations, e.g., the risk reduction factor),

b) system diagnostic alarms from the SIS that indicate dangerous faults, (depending on considerations, e.g., the operator response).

Note: For further guidance see ANSI/ISA 84.00.01-2004 Part 1 (IEC 61511 Mod).

12 Enhanced and Advanced Alarm Methods

NOTE: THIS CLAUSE IS INFORMATIVE AND DOES NOT CONTAIN MANDATORY REQUIREMENTS.

12.1 Purpose

Enhanced and advanced alarming is part of the detailed design lifecycle stage. This section provides guidance and consideration for additional alarm management techniques beyond those which are normally employed in control systems. They generally provide added functionality over the basic alarm system design and may be particularly useful to guide operator action during plant upsets or other multiple alarm situations.

Enhanced and advanced alarming methods are additional layers of logic, programming, or modeling used to modify alarm attributes. They methods include dynamic alarming, state-based alarming (i.e., mode-based alarming), adaptive alarms, logic based alarming, and predictive alarming. Most designed suppression methods are included in advanced alarming.

In addition to advanced alarming techniques, enhancements to the alarm system may also provide enhanced information to the operations personnel. This type of information is usually considered necessary to either avoid or mitigate operational problems which may lead to incidents.

The basic alarm design methods may not be sufficient to reduce alarm floods, or mitigate their effect and enhanced and advanced techniques may be necessary. Methods described in this clause can reduce or eliminate flood.

12.2 Basis of Enhanced and Advanced Alarming

Enhanced and advanced alarming methods are often used if the basic alarm design does not achieve the performance goals stated in the alarm philosophy. The alarm philosophy or alarm system requirements specification should include a list of acceptable enhanced and advanced alarming methods.

12.2.1 Effort, Manpower Requirements and Complexity

The additional complexities of enhanced and advanced alarming techniques need additional resources for design, implementation, and maintenance. The management of change process should include a review of the impact of changes on the enhanced and advanced alarming techniques.

The cost of additional alarm system complexity should be compared to the additional benefits of improved alarm system performance.

The consequence failure scenarios for enhanced and advanced alarming techniques should be considered before approval and during design.

12.3 Enhanced and Advanced Alarming Categories

Enhanced and advanced alarming techniques can be categorized by complexity:

12.3.1 Category 1: Information Linking

Information linking techniques, category 1 , in cludes tec hniques that make additional information related to the alarm available to the operator.

12.3.2 Category 2: Logic-based Alarming

Logic-based ala rming, category 2, in cludes t echniques t hat use logic b ased on plant conditions to modify alarm attributes.

12.3.3 Category 3: Model-based Alarming

Model-based ala rming, category 3 , includes tec hniques tha t us e process data a nd process models to provide the operator with information that may include alarms based on analysis or detailed guidance. .

12.3.4 Category 4: Additional Alarming Considerations

Additional alarming consideration category 4, includes those techniques that utilize auxiliary or remote alarm systems.

12.4 Information Linking

Alarm systems can be enhanced by linking information in the master alarm database (e.g., operator action or consequence). Information can also be linked from other sources including: operating procedures, operator logs, maintenance history, or design documents. These links should be easy to manage and maintain.

12.5 Logic-based Alarming

Logic-based alarming is accomplished using Boolean logic or decision trees to determine the modifications to be made to alarm systems. This technique is usually implemented directly in the control system.

12.5.1 Alarm Attribute Modification

The functional capability to modify some alarm attributes (e.g., alarm setpoints or priorities) is necessary for some enhanced and advanced alarming techniques. Some systems may n ot have this functionality and supplementary or externally enabled systems may be considered.

12.5.2 Externally Enabled Systems

Externally enabled systems capture alarm and process data from the control system and use the information to determine plant operating conditions and the corresponding modifications to alarm attributes.

12.5.3 Logical Alarm Suppression/ Attribute Modification

Logical alarm suppression techniques use alarm state conditions from some alarms to modify the alarm attributes of other alarms (e.g., first-out alarms).

12.5.4 State-based Alarming

State-based alarming is an advanced alarm technique that modifies alarm setpoint, priority, or suppression status based on defined operating states for equipment or processes. States are often determined through:

a) status of a logical variable,

b) a defined process variable which reaches a specific limit,

c) logic that looks at many variables and indicators,

d) operator selection.

The state determination and alarm modification can be manual, semi-automated (e.g., some combination of manual and automated), or fully-automated.

12.6 Model-based Alarming

Model-based alarming can be used in areas where a more complex system of annunciating an alarm is desired, where complex process parameters may produce a result based on multiple data points, or where an estimation of plant state can be derived from a model.

Predictive alarms may sometimes be accomplished through the use of process models. Predictive alarms can be used to replace basic alarms and provide additional time to respond.

Model-based alarm systems should not be used as a replacement for the basic alarm system without thorough analysis.

12.7 Additional Alarming Considerations

Some additional enhancements may add value to the alarm system. These enhancements may or may not be normally available in the basic alarm system.

12.7.1 Non-control Room Considerations

Where the operating personnel are expected to respond to alarms while completing non-control room based tasks, consideration may be given to remote alarm display and acknowledgement. Procedures to provide back up to the operator may be necessary.

The use of remote alarm notification practices should include periodic test messages to improve reliability. An alarm escalation procedure should be considered.

12.7.1.1 Paging, e-mailing and Remote Alerting Systems

Several situations can potentially exist in which the person who most needs to know about an abnormal situation and take action on it is not an operator in a control room. Such situations can benefit from the availability of a remote alerting system (e.g., paging, email, etc.).

The reliability of the message delivery is a significant issue in such systems and should be dealt with in the design. Acceptable, if not optimum, results should be achievable even if delivery does fail. It may be necessary to also provide remote acknowledgement.

12.7.2 Supplementary Alarm Systems

Supplementary alarm systems may replace the control system alarm notification system or make use of the existing graphics environment to provide a common interface. Alternatively, system may be used in addition to the existing alarm system to provide additional or alternative alarm information.

Special care should be taken to ensure that the additional information provides value. When these systems are employed to present alarms in place of control system notification techniques, users should design the system to ensure alarm availability and reliability are acceptable.

12.7.3 Batch Process Considerations

The process conditions, states, and phases may be used to modify alarms in batch processes. This is often implemented as state based alarming.

12.7.3.1 Continuously Variable Alarm Thresholds

Alarms for batch processes are often applicable only to specific steps of the process, or associated with changing control loop setpoints, or time varying process data trends. Unless special care is taken, batch processes are especially prone to the generation of nuisance alarms. Advanced alarm methodologies may provide a structure for addressing these types of batch-related alarm problems.

12.7.3.2 Relative Time versus Absolute Time

Data and alarm record time stamps are normally accomplished in computer systems using calendar time. For batch information, relative time (i.e., the time since the beginning of the batch or process step) is more relevant. A feature of advanced alarming is the ability to take calendar time stamps and electronic records indicating when the batch step or phase started and compute and display alarms in relative time.

12.7.3.3 Inclusion of Lot Number and other Identifying Marks

Some sites may specify the functionality to associate identification numbers with alarms. Being able to sort records by the selected identification is also useful in generating official batch records of a production run and in comparing records of different production runs. Methods of extracting and attaching such identifying marks should be proven and reliable.

12.8 Training, Testing, and Auditing Systems

The alarm philosophy should specify steps to ensure advanced alarm functions continue to operate, including training, testing, and auditing. For enhanced and advanced alarming systems, it may be necessary that training, testing, and auditing procedures include the enhanced features of such a system.

12.9 Alarm Attribute Enforcement

To maintain designed alarm attribute settings (e.g., alarm setpoints, alarm priorities, mode-based designed suppression) at authorized values, there should be a regular comparison of the rationalized values with the settings in effect in the control system. Enforcement, the automatic verification and restoration of alarm attributes, is an enhanced alarm technique that performs functions associated with monitoring, assessment, and audit. Enforcement can be initiated on a scheduled basis or on request and should differentiate changes resulting from state-based or alarm shelving methodologies as acceptable so as not to produce false mismatches.

13 Implementation

13.1 Purpose

Implementation is a separate stage of the alarm lifecycle which is the transition from design to operation. This section covers general requirements to install an alarm, an alarm system, or implement a modification to an existing alarm or alarm system, and bring it to operational status. Implementation is the transition from design to operation.

13.2 Implementation Planning

The scope of the project or change will determine the extent of the work necessary. Implementation planning should include the following considerations:

a) disruption to operation,

b) availability of resources,

c) functional testing or validation,

d) verification of documentation,

e) operator training.

13.3 Initial Training

The training requirements for new alarms and modifications to existing alarms are determined by the classification of the alarm and the class requirements as detailed in the alarm philosophy.

13.3.1 Initial Training for Highly Managed Alarms

Operators shall be trained on the response to all new or modified highly managed alarms prior to the operator assuming responsibility for responding to the new or modified alarms.

13.3.1.1 Initial Training Requirements

The training shall include:

a) the technical basis of the alarm (e.g. consequence of inaction, determination of setpoint value, causes for alarm, corrective action, tags used for confirmation, etc),

b) the response or corrective action to the alarm,

c) the audible and visual indications for the alarm.

13.3.1.2 Documentation Requirements

Documentation of the training shall include:

a) the persons trained,

b) the method of training,

c) the date of the training

d) the last time when the personnel were trained.

The minimum retention period is specified in the alarm philosophy document or per company policy.

13.3.2 Initial Training for New or Modified Alarms

Operators should be trained on all new or modified alarms.

13.3.2.1 Training Recommendations

The training should include:

a) the technical basis of the alarm,

b) the response or corrective action to the alarm,

c) the audible and visual indications for the alarm.

13.3.2.2 Documentation Recommendations

Documentation of the training should include:

a) the persons trained,

b) the method of training,

c) the date of the training.

13.3.3 Initial Training Requirements for New or Modified Alarm Systems

Operators shall be trained on all new or modified alarm systems.

13.3.3.1 Initial Training Recommendations for New or Modified Alarm Systems

The training requirements for the modified alarm system should be appropriate for the nature of the change. The training requirements of new alarm system should include:

a) the audible and visual indications for alarms,

b) the distinction of alarm priorities,

c) the use of the alarm HMI features, (e.g., alarm summary sorting and filtering),

d) the proper methods for shelving and suppression,

e) the proper methods for removing an alarm from service.

13.4 Initial Testing and Validation

Initial testing requirements for new alarms and modifications to existing alarms are determined by the classification of the alarm and the class requirements as detailed in the alarm philosophy.

13.4.1 Initial Testing Requirements for Highly Managed Alarms

The alarm philosophy shall identify the testing requirements for highly managed alarms prior to putting the alarms in operation. The initial testing shall be documented including:

a) the alarm setpoint or logical conditions,

b) the alarm priority ,

c) the audible and visual indications for the alarm,

d) any other functional requirement for the alarm as specified ,

e) the persons conducting the testing,

f) the method of testing and acceptance criteria,

g) the results of the testing and resolution of any failures or non-compliance,

h) the date of the testing,

i) the date the alarm was put into service.

13.4.2 Initial Testing Recommendations for New or Modified Alarms

Alarms should be tested during implementation. The testing should include verification of:

a) the alarm setpoint or logical conditions,
b) the alarm priority,
c) the audible and visual indications for the alarm,
d) any other functional requirement for the alarm as specified.

13.4.3 Initial Testing Requirements for New or Modified Alarm Systems

Alarm systems shall be tested during implementation to ensure that appropriate items in the alarm philosophy and ASRS have been met. The testing of modified alarm system shall be appropriate to the nature of the change, as determined by site MOC procedures. The testing of new alarm system shall include:

a) the audible and visual indications for each alarm priority,
b) the HMI features, such as alarm messages displayed in the alarm summary or equivalent,
c) the methods for removing an alarm from service.

13.4.3.1 Initial Testing Recommendations

Initial testing recommendations should include:

a) the methods for shelving,
b) the methods for alarm suppression,
c) any additional functions of enhanced or advanced alarming techniques,
d) method of alarm filtering, sorting, linking of alarms to process displays.

13.5 Documentation

There are several documentation requirements and recommendations for alarm system implementation.

13.5.1 Documentation Requirements

The following documentation shall be provided.

a) Alarm lists from the master alarm database shall be available prior to the implementation of new or modified alarms.
b) Individuals performing alarm testing shall have current and sufficient information to perform the test.
c) The alarm response procedures shall be provided to the operators as a part of placing a new or modified alarm in service.
d) Upon completion of alarm system implementation, the master alarm database shall be updated in accordance with the site MOC procedure.

13.5.2 Documentation Recommendations

The reporting method, documentation format and structure should be in accordance with the project documentation procedures and owners documentation requirements.

The testing methodology and documentation should be appropriate to the nature of change, as determined by site MOC procedures or alarm philosophy.

Information about new and modified alarms that would be useful to both testers and operators can include some of the following:

a) basic process control system alarm source tag,
b) alarm type,

c) priority,

d) alarm setpoint value or logical condition,

e) operator action,

f) consequence of inaction,

g) initial of persons involved,

h) the date of testing and change,

i) the method of testing and acceptance criteria,

j) the results of the testing and resolution of any failures or non-compliance.

14 Operation

14.1 Purpose

Operation is a separate stage of the lifecycle. This section covers requirements for alarms to remain in and return to the operational state. The operational state is when an alarm is on-line and able to indicate an abnormal condition to the operator. This section also describes appropriate use of tools for alarm handling within the operational state. Operation is the lifecycle stage following implementation and when returning from maintenance. Out-of-service alarms are discussed in the maintenance clause.

14.2 Alarm Response Procedures

Alarm response procedures shall be readily accessible to the operator.

14.2.1 Alarm Response Procedure Recommendations

The form of alarm documentation that is deemed most accessible by operating staff should be used. The alarm information recorded during alarm rationalization should also be made readily accessible.

Unless otherwise specified in the alarm philosophy, the alarm response procedures should include:

a) the alarm type,

b) alarm setpoint,

c) potential causes,

d) consequence of deviation,

e) corrective action,

f) allowable response time,

g) alarm class.

14.3 Alarm Shelving

Alarm shelving requirements shall be determined by the classification of the alarm and the class requirements as detailed in the alarm philosophy.

14.3.1 Alarm Shelving Requirements

Shelved alarms shall be reviewed at the beginning of each shift

14.3.2 Alarm Shelving for Highly Managed Alarms

If a highly managed alarm class is used then shelving highly managed alarms shall follow authorization and reauthorization requirements as detailed in the alarm philosophy.

An audit trail shall be maintained recording approval, interim alarms and procedures, and reauthorization details.

14.3.3 Alarm Shelving Recommendations

The operator should be permitted to shelve alarms to prevent unnecessary distraction due to unforeseen alarm system malfunctioning alarms. Shelved alarms extending beyond a single operating shift should be reauthorized. Approval requirements for shelving alarms should be recorded in the site alarm philosophy.

14.3.4 Alarm Shelving Record Recommendations

The following information shall be recorded for each shelved alarm extending beyond a single operating shift:

a) alarm name,

b) the reason for shelving.

14.4 Refresher Training for Operators

The training requirements for alarms shall be determined by the classification of the alarm and the class requirements as detailed in the alarm philosophy.

14.4.1 Refresher Training Documentation for Highly Managed Alarms

If a highly managed alarm class is used then the following training information shall be documented:

a) the persons trained,

b) the method of training,

c) the date of the training.

The frequency of training shall be specified in the alarm philosophy. The documentation of the training shall be retained for the period specified in the alarm philosophy or per company policy.

14.4.2 Refresher Training Content for Highly Managed Alarms

If a highly managed alarm class is used then operators shall be periodically trained on the characteristics of each highly managed alarm. The content of the refresher training shall include:

a) the technical basis of the alarm,

b) the response or corrective action to the alarm,

c) the audible and visual indications for the alarm.

14.4.3 Refresher Training Recommendations for Alarms

Operators should receive periodic training that involves alarm response evaluation. The training should cover a broad range of process scenarios. The training should include:

a) the technical basis of the alarm,

b) the response or corrective action to the alarm,

c) the audible and visual indications for the alarm.

A record of refresher training should be kept indicating who received the training and the time it was received.

15 Maintenance

15.1 Purpose

Maintenance is a separate stage of the lifecycle. This section covers requirements for alarm system testing, replacement-in-kind, and repair. It describes the transition of alarms from the operational state to the out-of-service state and then returning to the operational state. Maintenance also requires refresher training for personnel maintaining the alarm system.

15.2 Periodic Testing

Periodic testing requirements for alarms shall be determined by the classification of the alarm and the class requirements as detailed in the alarm philosophy.

15.2.1 Periodic Testing Requirements

When tests are performed, a record shall be kept for a period specified in the alarm philosophy and shall contain the following:

a) date(s) of testing,

b) name(s) of the person(s) who performed the test or inspection,

c) unique identifier of equipment (e.g., loop number, tag number, equipment number),

d) result of tests.

If the alarm philosophy requires that some alarms be periodically tested then it shall provide guidelines on the frequency and manner of testing.

15.2.2 Periodic Testing for Highly Managed Alarms

If a highly managed alarm class is used then alarms belonging to this class shall be periodically tested to ensure performance.

Any deficiencies found during functional testing of highly managed alarms shall be repaired or else an interim alarm or procedure shall be put in place in a timely manner.

15.2.3 Periodic Test Procedure Recommendations

Test procedures should be provided for alarms requiring testing. Procedures should contain:

a) steps for taking the alarm out-of-service prior to the test and returning the alarm to service after the test,

b) appropriate warnings regarding control loops or final elements that might be affected by the test,

c) steps to address advanced alarming techniques if applicable.

15.2.4 Periodic Testing Recommendations

Test records should contain the following:

a) method of testing,

b) planned interval before next test.

Any deficiencies found during functional testing should be repaired in a safe and timely manner.

15.3 Out-of-service

Out-of-service requirements for alarms shall be determined by the classification of the alarm and the class requirements as detailed in the alarm philosophy.

15.3.1 Out-of-service Process Requirements

Alarms that will be compromised for extended durations (e.g., days, weeks, or months) shall be examined to determine whether an alternative alarm is necessary. If an interim alarm is necessary then it shall adhere to management of change requirements.

An authorization and documentation process (e.g. permit process) shall be used to take an alarm out-of -service. A list of out-of-service alarms shall be available for review on-demand with their corresponding replacements where applicable.

The following information shall be recorded for each out-of-service alarm:

a) the name of the tag in alarm,

b) the alarm type,

c) approval details,

d) details concerning interim alarms or procedures if required,

e) the reason for taking the alarm out-of-service.

15.3.2 Out-of-service for Highly Managed Alarms

If a highly managed alarm is taken out-of-service for longer than one shift, appropriate interim alarms or procedures shall be identified unless the process is in a state where the consequence has been eliminated.

15.3.3 Out-of-service Process Recommendations

Approval requirements for taking alarms out-of-service should be specified in the site alarm philosophy. The duration of record retention should be defined in the site alarm philosophy.

15.4 Equipment Repair

Information related to an alarm malfunction should be available to the operator. Alarms affected by non-functioning equipment (e.g., equipment that is taken out-of-service for repair or preventative maintenance) should be placed out-of-service if the condition will not be resolved within a reasonable time as specified in the alarm philosophy.

15.5 Equipment Replacement

If replacement equipment (e. g., measurement devices, valves, process equipment) will change operating conditions or alarm attributes, then site management of change procedures should be followed. Replacements that do not result in such changes do not require management of change. If a replacement is made then alarm validation may be required depending on the class of the alarm as specified in the alarm philosophy.

15.6 Returning Alarms to Service

Prior to returning out-of-service alarms to the operational state, operators shall be notified to ensure they are aware of the returning alarm and the removal of the interim methods.

15.6.1 Recommendations for Returning Alarms to Service

Interim alarms and procedures should be removed, where applicable, when the original alarms are returned to service.

15.7 Refresher Training for Maintenance

The training requirements for the maintenance of alarms shall be determined by the classification of the alarm and the class requirements as detailed in the alarm philosophy.

15.7.1 Refresher Training Requirements for Highly Managed Alarms

If a highly managed alarm class is used then the appropriate personnel shall be periodically trained on the maintenance requirements for all highly managed alarms. The frequency of training shall be specified in the alarm philosophy. Documentation of the training shall include the persons trained, the method of training, and the date of the training. The record shall be retained for the period specified in the alarm philosophy document or per company policy.

15.7.2 Refresher Training Recommendations for Alarms

Maintenance personnel should receive periodic training on the maintenance requirements of alarms. A record of refresher training should be kept indicating who received the training and the time it was received. Evaluations should be conducted to ensure site maintenance procedures are clearly understood.

16 Monitoring and Assessment

16.1 Purpose

Monitoring and assessment is a separate stage of the lifecycle. This stage verifies that design, implementation, rationalization, operation, and maintenance are satisfactory. This clause provides guidance on the use of alarm system analysis for both ongoing monitoring and periodic performance assessment. These activities use many of the same types of measures. This clause recommends several performance measures that should be considered for inclusion in the alarm philosophy.

Problems identified via alarm system monitoring may be resolved in several different parts of the lifecycle (e.g., design, maintenance, or management-of-change) depending upon the nature of the problem.

16.2 Requirements

Alarm system performance shall be monitored. Monitoring and assessment of the alarm system performance shall be made against the goals in the alarm philosophy.

16.3 Monitoring, Assessment, Audit, and Benchmark

The usage of these terms is in the following context:

a) Monitoring is the measurement and reporting of quantitative (objective) aspects of alarm system performance.

b) Assessment is the comparison of information from monitoring and additional qualitative (subjective) measurements, against stated goals and defined performance metrics.

c) Audit is a comprehensive assessment that additionally includes the evaluation of the effectiveness of the work practices used to administer the alarm system.

d) Benchmark is an initial audit of an alarm system designed to specifically identify problematic areas for the purpose of formulating improvement plans.

Monitoring typically occurs at a higher frequency than assessment. The monitoring of some aspects of the alarm system performance is based upon continuous measurement. The intent of monitoring is to identify problems and take corrective actions to fix them.

The focus of the assessment process is to apply engineering judgment and review to determine whether the system is performing properly. The evaluation of work processes relative to the alarm system is covered in the audit section.

16.4 Alarm System Measurement

Performance measurement is fundamental to control and improvement. An alarm system will likely experience performance deterioration over time, as sensors age and process conditions change, or if an alarm change management policy is not in place. Ongoing performance measurement can determine when corrective action is needed.

When alarms have been properly rationalized and designed, and nuisance alarms (e.g., chattering alarms) eliminated, the resulting alarm rate reflects the control system's ability to keep the process within bounds without requiring manual operator intervention. The solutions to high alarm rates may include improvements to the control system or to the process rather than adjustments to the alarm system. Enhanced or advanced alarm techniques may be necessary.

16.5 Alarm System Performance Metrics

Various types of alarm system analyses, key performance indicators, and methods are possible. Both initial alarm system assessment and ongoing monitoring should include the measures in this section. The entire list of chosen analyses should reflect decisions made in the alarm philosophy.

The two categories of data in a typical control system alarm system are alarm records (i.e., dynamic or real-time data) and alarm attributes (i.e., alarm settings or configuration data). Both categories are valuable in alarm system performance measurement and are subject to different analyses.

a) Alarm records contain alarm-related information and are produced by the system when alarms occur.
b) Alarm attributes make up the underlying structure which is necessary in order that alarm records are produced, including the decisions about alarm types, alarm setpoints, priorities, deadbands, and similar items.

In general, at least 30 days of data is desirable for calculating the metrics in this section. For batch operations, data corresponding to several similar batches is more applicable.

The target metrics in the following sections are approximate and depend upon many factors, (e.g. process type, operator skill, HMI, degree of automation, operating environment, types and significance of the alarms produced). Maximum acceptable numbers could be significantly lower or perhaps slightly higher depending upon these factors. Alarm rate alone is not an indicator of acceptability.

16.5.1 Average Annunciated Alarm Rate per Operating Position

Analysis of annunciated alarm rates is a good indicator of the overall health of the alarm system. Recommended targets for the average annunciated alarm rate per operating position (i.e., the span of control and alarm responsibility of a single operator) based upon one month of data are shown in Figure 12. These rates are based upon the ability of an operator and the time necessary to detect an alarm, navigate within the control system to the relevant data, analyze the situation, determine and perform proper corrective action(s), and monitor the situation to ensure the alarmed condition is successfully handled.

Very Likely to be Acceptable	Maximum Manageable
~150 Alarms per day	~300 Alarms per day
~6 Alarms per hour (average)	~12 Alarms per hour (average)
~1 Alarm per 10 minutes (average)	~2 Alarms per 10 minutes (average)

Figure 12 – Average Alarm Rates

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

The use of averages 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.

16.5.2 Peak Annunciated Alarm Rates per Operating Position

Alarm rates of 10 alarms or more in a 10 minute time period may exceed the operator capability for effective alarm response, or result in missed alarms. Rates approaching 10 alarms in 10 minutes may not be reliably sustainable by an operator for long periods.

For peak alarm rate analysis, annunciated alarms are counted in regular 10-minute intervals (e.g. 1:00 pm through 1:09 pm). The recommended target corresponding to one month of data is that less than ~1% of the 10-minute intervals should contain more than 10 alarms.

Both the peak and average alarm rates should be taken into account simultaneously because either measurement individually could be misleading. The quantity of intervals exceeding 10 alarms, and the magnitude of the highest peaks should be reported.

16.5.3 Alarm Floods

Alarm floods are variable-duration periods of alarm activity with annunciation rates likely to exceed the operator response capability. In an alarm flood, the alarm system is likely to be ineffective in assisting the operator.

Alarm flood calculations involve the determination of adjacent time periods where the alarm generation rate is high, thus producing an overall flood event.

The start of an alarm flood is indicated by the first regular 10 minute interval with an alarm rate that exceeds 10 alarms per 10 minutes. The end of an alarm flood is indicated by the first regular 10 minute interval with an alarm rate of less than 5 alarms per 10 minutes. Alarm floods should be of short duration and low total alarm count. As a recommended target, an alarm system should be in flood for less than ~1% of the reporting period.

16.5.3.1 Alarm Flood Analysis

Improvements to the alarm system and process operation may be indicated by the analysis of alarm floods. No targets are provided for these metrics. Alarm flood analysis should include:

a) number of alarm floods per reporting period,

b) duration of each alarm flood,

c) alarm count in each alarm flood,

d) peak alarm rate for each alarm flood.

Alarm floods may require advanced methodologies to address. Some methods are described in Clause 12.

16.5.4 Frequently Occurring Alarms

A relatively few individual alarms (e.g., 10 to 20 alarms) often produce a large percentage of the total alarm system load (e.g., 20% to 80%). 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 analysis methodology is to use at least several weeks of data and rank alarm records from most to least frequent. The most frequent alarms are likely not working properly or as designed. High frequency alarms often have major skewing effects on other performance measurements.

The top 10 most frequent alarms should comprise a small percentage of the overall system load (e.g., 1% to 5%). Action steps based on this analysis include review for proper functioning and design.

16.5.5 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 operator action.

A threshold for chattering of an alarm that repeats three or more times in one minute is often used as a first pass identification of the worst chattering alarms. Other values may be used.

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 operators. Chattering alarms are often high in the listing of the most frequent alarms. Chattering and fleeting alarm behaviors should be eliminated. There is no long-term acceptable quantity of chattering or fleeting alarms.

16.5.6 Stale Alarms

Alarms that remain in effect continuously for more than 24 hours may be considered as stale. Some alarms remain in the alarm state continuously for days, weeks, or months. Such alarms provide little valuable information to the operators. They clutter the alarm displays and often represent conditions that are not truly abnormal. 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.

There should be less than five stale alarms on any given day, with action plans to address them. No alarm should be intentionally designed to become stale and there is no long-term acceptable number of stale alarms.

16.5.7 Annunciated Alarm Priority Distribution

Effective use of alarm priority can enhance the ability of the operator 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.

Priority Designation	Percentage Distribution
3 priorities: Low, Medium, High	~80% Low, ~15% Medium, ~5% High
4 priorities: Low, Medium, High, Highest	~80% Low, ~15% Medium, ~5% High, ~<1% Highest

Figure 13 – Annunciated Alarm Priority Distribution

Four priority systems often include an additional highest priority for a very few selected alarms.

Additional special-purpose priorities may be useful, such as a lowest priority for instrument malfunction or diagnostic alarms with very limited and prescribed operator action. There is no recommended frequency or percentage distribution for such diagnostic alarms, since there is no recommended frequency for instrument failure. Low numbers are better.

Various priorities with limited annunciation (e.g., silent alarms) are sometimes used for special circumstances. There is no recommended distribution for limited annunciation priorities.

Distributions at wide variance to these percentages can compromise the value of prioritization and generally indicate alarm priority settings that did not result from a consistent alarm rationalization methodology. Effective rationalization is the usual solution.

16.5.8 Alarm Attributes Priority Distribution

An effective alarm rationalization effort will produce annunciated alarm record priority distributions similar to Figure 13. It is useful to measure the priority distribution of the underlying alarm attribute structure. The distribution of alarm priority attributes should be similar to Figure 13. Annunciated alarm record distributions will not match alarm attribute distributions since all alarms are not equally likely to occur. Diagnostic-type alarms are excluded from the priority attribute distribution percentage calculations due to their skewing effect.

16.6 Unauthorized Alarm Suppression

The alarm states of shelved, suppressed by design, and out-of-service are all intended as controlled methodologies. It is possible for alarms to be suppressed outside of these methodologies. 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 to detect and report any alarms suppressed outside of proper methods. There should be no alarms that are improperly suppressed.

16.7 Alarm Attribute Monitoring

Unauthorized alarm attribute changes shall be detected and resolved. Periodic monitoring at the frequency specified in the alarm philosophy shall be made of the actual alarm attributes in effect on the control system, compared to the rationalized attributes in a master alarm database or to allowable alarm attribute changes specified in the alarm philosophy. Discrepancies shall be identified and resolved quickly. The target value for improperly changed alarms is zero.

16.8 Reporting of Alarm System Analyses

Alarm system analyses should be properly reported. Reporting should:

a) include personnel (e.g., operators, staff, managers) concerned with the alarm system,

b) be at a frequency appropriate to the nature of the data contained and the needs of the recipients.

At various phases of an improvement effort, different analyses should be performed at different frequencies (e.g., providing weekly reports at the start of an effort and monthly reports later on). Weekly analyses may still cover the prior 30 days of data to produce meaningful trends. The alarm philosophy should specify analysis and reporting frequencies.

Action should be taken on problems identified by the alarm analyses. Progress and status of actions should be regularly reported.

16.9 Alarm Performance Metric Summary

The alarm performance metrics and example target values previously described, with the same qualifications, are summarized in the Figure 14.

Alarm Performance Metrics Based upon 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 Operating Position	~150 alarms per day	~300 alarms per day
Annunciated Alarms Per Hour per Operating Position	~6 (average)	~12 (average)
Annunciated Alarms Per 10 Minutes per Operating 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 10 alarms	~<1%	
Maximum number of alarms in a 10 minute period	≤10	
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 Priority Distribution	3 priorities: ~80% Low, ~15% Medium, ~5% High or 4 priorities: ~80% Low, ~15% Medium, ~5% High, ~<1% "highest" Other special-purpose priorities excluded from the calculation	
Unauthorized Alarm Suppression	Zero alarms suppressed outside of controlled or approved methodologies	
Unauthorized Alarm Attribute Changes	Zero alarm attribute changes outside of approved methodologies or MOC	

Figure 14 – Alarm Performance Metric Summary

17 Management of Change

17.1 Purpose

Management of change is a separate stage of the lifecycle. This section covers requirements for alarm system changes pertaining to the addition of new alarms, alarm attribute modification, authorization, and documentation. The purpose of management of change is to ensure that changes are authorized and subjected to the evaluation criteria described in the alarm philosophy. The management of change process ensures that the appropriate stages of the alarm management lifecycle are applied to alarm system changes.

17.2 Changes Subject to Management of Change

Alarm addition and removal shall require authorization through MOC. Permanent changes that result in a difference from the designed values of the alarm setpoint, class, priority, consequence, basis, suppression logic, or response time shall require evaluation through MOC.

17.3 Change Review Process Requirements

The MOC process shall ensure the following considerations are addressed:

a) the technical basis for the proposed change,

b) impact of change on health, safety and the environment,

c) modifications are in accordance with the alarm philosophy,

d) modifications for operating procedures,

e) time period for which change is valid,

f) authorization requirements for the proposed change,

g) the degree of safety is maintained if the alarm is implemented for safety reasons,

h) personnel from appropriate disciplines are included in the review,

i) changes to the alarm system follow all appropriate subsequent alarm management lifecycle stages,

j) implementation of all changes adhere to procedures specified in the alarm philosophy.

17.4 Change Documentation Requirements

Documentation requirements shall be determined by the classification of the alarm and the class requirements as detailed in the alarm philosophy.

The following information shall be recorded for approved changes:

a) reason for the change,

b) date the change was made,

c) the name of the person implementing the change,

d) the name of the person authorizing the change,

e) nature of the change,

f) training requirements,

g) testing requirements.

17.5 Change Documentation Recommendations

Changes required to related system components and documentation as a consequence of alarm changes should be recorded as part of the change record. Records should:

a) be protected against unauthorized modification, destruction, or loss,

b) be revised, amended, reviewed, and approved under the control of an appropriate document control procedure,

c) be stored for a duration determined by the site record retention policy,

d) be maintained per the alarm philosophy class requirements.

17.6 Alarm Decommissioning Recommendations

If an alarm is no longer needed then it should be decommissioned from the alarm system. Displays and related documentation should be modified within a reasonable time.

17.7 Alarm Attribute Modification Requirements

When changes to alarm attributes are necessary then the proposed modifications, including the addition and deletion of alarms, shall follow the MOC process specified in the alarm philosophy.

17.8 Alarm Attribute Modification Recommendations

A list of referencing materials (e.g., graphics, control logic, P&ID, operating procedures, and HAZOP) should be generated and maintained. This reference list should be reviewed prior to making changes to alarms. This prevents introducing incorrect information into documentation and helps prevent interim automation logic and graphic errors.

18 Audit

18.1 Purpose

Audit is a separate stage of the lifecycle which is conducted periodically to maintain the integrity of the alarm system and alarm management processes. Audit of system performance may reveal gaps not apparent from monitoring. Execution against the alarm philosophy is audited to identify any requirements for system improvements, such as modifications to the alarm philosophy or the work process defined therein.

An audit reviews the managerial and work practices associated with the alarm system. It determines whether those practices are sufficient to adequately administer the system by reviewing practices vs. procedures and procedures vs. policy or requirements. Audit also includes comparison of the alarm management practices against industry guidelines.

The frequency of the audit process is lower than monitoring and assessment.

18.2 Initial Audit or Benchmark

All aspects of alarm management should be audited at the start of an improvement effort. An initial audit or benchmark should be made against a set of documented practices, (e.g., the practices listed in this standard). A benchmark includes an initial iteration of the audit process, in order to capture any work practice concerns. The results of the initial audit can be used in the development of a philosophy.

18.2.1 Initial Audit or Benchmark Requirements

The audit frequency and the specific audit requirements stated in the alarm philosophy shall be followed for highly managed alarms.

18.3 Audit Interviews

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

a) alarms occur only on events that require operator action,

b) alarm priority is consistently applied and meaningful,

c) alarms occur in time for effective action to be taken,

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

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

18.4 Audit Recommendations

The alarm philosophy should be audited against industry guidelines and the requirements and recommendations of this standard. 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 which may include:

a) verification that alarms require operator action to avoid a defined consequences,

b) documentation of alarm attributes and rationalization,

c) MOC documentation of modifications to alarm attributes in the master alarm database,

d) alarm performance monitoring reports,

e) documentation of repairs to malfunctioning alarms,

a) documentation for out-of-service alarms.

18.5 Action Plans

Action plans should be developed for problems identified during the audit processes. When defining an action plan, timelines, accountabilities, and review of results obtained should be assigned to each item.

Developing and promulgating technically sound consensus standards and recommended practice is one of ISA's primary goals. To achieve this goal the Standards and Practices Department relies on the technical expertise and efforts of volunteer committee members, chairmen and reviewers.

ISA is an American National Standards Institute (ANSI) accredited organization. ISA administers United States technical Advisory Groups (USTAGs) and provides secretariat support for International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) committees that develop process measurement and control standards. To obtain information on the Society's standards program, please write:

ISA
Attn: Standards Department
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

ISBN: -1-936007-19-6