

Draft ISA – 18.02 – 2009.04.01

Management of Alarm Systems for the Process Industries

Approved << Insert Date>>

Draft: Not Approved

This document is a draft that represents work being done by an ISA Standards Committee leading to the development of an ISA Standard. ISA grants permission to anyone to reproduce and distribute copies of this draft ISA standard, in whole or in part, but only for the following purposes and only as long as the recipient is not charged any fee for the copy (nor may the copy be included as part of a package with other materials or presentations for which a fee is charged):

Review of and comment on the draft standard;

Provide to others for review and comment;

Promotion of the standard; or

Informing and educating others about the standard.

In addition, all copies must reproduce a copyright notice as follows:

Copyright © 2009 ISA. All rights reserved. Reproduced and distributed with permission of ISA.

ISA reserves all other rights to the draft standard. Any other reproduction or distribution without the prior written consent of ISA is prohibited.

The reader is cautioned that this document has not been approved and cannot be presumed to reflect the position of ISA or any other committee, society, or group. Although every effort has been made to ensure accuracy, neither ISA, members of the S&P Department, nor their employers shall be held liable for errors or limitations.

ISA – 18.02 – 2009, Management of Alarm Systems for the Process Industries

ISBN: <<Insert ISBN Number Here>>

Copyright © 2009 by the International Society of Automation. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of the publisher.

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709

E-mail: standards@isa.org

Draft: not approved

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 ISA 18.02-2009.

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 acted as active members of ISA Committee ISA18:

NAME	COMPANY
------	---------

Committee list (to be inserted later)

This published standard was approved for publication by the ISA standards and practices board on <<date>>

NAME	COMPANY
------	---------

<< List of S&P board members>>

Contents

Introduction	9
Purpose	9
Organization	9
1 Scope	10
1.1 General Applicability	10
1.2 The Alarm System.....	10
1.3 Exclusions	11
2 Normative References.....	12
2.1 References	12
3 Definition of Terms and Acronyms.....	12
3.1 Definitions.....	12
3.2 Acronyms.....	18
4 Conformance to this Standard.....	18
4.1 Conformance Guidance.....	18
4.2 Existing Systems.....	18
5 Alarm System Models	19
5.1 Alarm Systems.....	19
5.2 Alarm Management Lifecycle	19
5.3 Process Condition Model	25
5.4 Alarm States	27
5.5 Alarm Response Timeline	31
5.6 Feedback Model of Operator – Process Interaction	33
6 Alarm Philosophy	33
6.1 Purpose	33
6.2 Alarm Philosophy Contents	34
6.3 Alarm Philosophy Development and Maintenance	39
7 Alarm System Requirements Specification	40
7.1 Purpose	40
7.2 Recommendations	40
7.3 Development.....	41
7.4 Systems Evaluation.....	41
7.5 Customization and Third-Party Products	41
7.6 Alarm System Requirements Testing.....	41
8 Identification	41
8.1 Purpose	41
8.2 Alarm Identification Methods	42
9 Rationalization	42
9.1 Purpose	42
9.2 Objective	42
9.3 Alarm Justification.....	42
9.4 Alarm Setpoint Determination.....	43
9.5 Prioritization.....	43

9.6	Removal	44
9.7	Classification	44
9.8	Review.....	44
9.9	Documentation.....	44
10	Basic Alarm Design	44
10.1	Purpose	44
10.2	Usage of Alarm States	44
10.3	Alarm Types.....	45
10.4	Alarm Attributes	46
10.5	Programmatic Changes to Alarm Attributes	47
10.6	Review Work Product.....	47
11	Human-Machine Interface Design for Alarm Systems	48
11.1	Purpose	48
11.2	Overview.....	48
11.3	Alarm States Indications	49
11.4	Alarm Priority Indications	50
11.5	Alarm Message Indications	51
11.6	Alarm Displays.....	51
11.7	Alarm Shelving.....	54
11.8	Out-of-service Alarms	55
11.9	Alarms Suppressed by Design	56
11.10	Alarm Annunciators.....	57
11.11	Safety Alarm HMI	57
12	Enhanced and Advanced Alarm Methods	58
12.1	Purpose	58
12.2	Basis of Enhanced and Advanced Alarming	58
12.3	Enhanced and Advanced Alarming Categories	59
12.4	Information Linking	59
12.5	Logic-based Alarming	59
12.6	Model-based Alarming	60
12.7	Additional Alarming Considerations.....	60
12.8	Training, Testing, and Auditing Systems	61
12.9	Alarm Attribute Enforcement	61
13	Implementation	61
13.1	Purpose	61
13.2	Implementation Planning.....	62
13.3	Initial Training.....	62
13.4	Initial Testing and Validation	63
13.5	Documentation.....	64
14	Operation	65
14.1	Purpose	65
14.2	Alarm Response Procedures.....	65
14.3	Alarm Shelving.....	65
14.4	Refresher Training for Operators.....	66

15	Maintenance	67
15.1	Purpose	67
15.2	Periodic Testing	67
15.3	Out-of-service	68
15.4	Equipment Repair	68
15.5	Equipment Replacement	68
15.6	Returning Alarms to Service.....	68
15.7	Refresher Training for Maintenance	69
16	Monitoring and Assessment	69
16.1	Purpose	69
16.2	Requirements	69
16.3	Monitoring, Assessment, Audit, and Benchmark.....	69
16.4	Alarm System Measurement	70
16.5	Alarm System Performance Metrics	70
16.6	Unauthorized Alarm Suppression	73
16.7	Alarm Attribute Monitoring.....	73
16.8	Reporting of Alarm System Analyses	73
16.9	Alarm Performance Metric Summary	74
17	Management of Change	74
17.1	Purpose	74
17.2	Changes Subject to Management of Change.....	74
17.3	Change Review Process Requirements.....	75
17.4	Change Documentation Requirements	75
17.5	Change Documentation Recommendations	75
17.6	Alarm Decommissioning Recommendations	75
17.7	Alarm Attribute Modification Requirements.....	75
17.8	Alarm Attribute Modification Recommendations.....	76
18	Audit	76
18.1	Purpose	76
18.2	Initial Audit or Benchmark	76
18.3	Audit Interviews	76
18.4	Audit Recommendations	76
18.5	Action Plans.....	77

Figures

Figure 1 – Alarm System Dataflow.....	10
Figure 2 – Alarm Management Lifecycle	20
Figure 3 – Alarm Management Lifecycle Stage Inputs and Outputs.....	25
Figure 4 – Process Condition Model	26
Figure 5 – Alarm State Transition Diagram	28
Figure 6 – Alarm Timeline.....	31
Figure 7 – Feedback Model of Operator Process Interaction.....	33
Figure 8 – Required and Recommended Alarm Philosophy Content.....	35
Figure 9 – Recommended Starting Point Deadband Based on Signal Type.....	46
Figure 10 – Recommended Delay Times Based on Signal Type	47
Figure 11 – Recommended Alarm State Indications.....	50
Figure 12 – Average Alarm Rates.....	71
Figure 13 – Annunciated Alarm Priority Distribution	72
Figure 14 – Alarm Performance Metric Summary	74

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 SP18 and SP67 committees, ISA-18.1-1979 (R2004) *Annunciator Sequences and Specifications*. In 1992 Amoco, Chevron, Exxon, Shell and Honeywell formed the Abnormal Situation Management Consortium (ASM) to develop a vision for better response to process incidents, with additional support in 1994 from the 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.

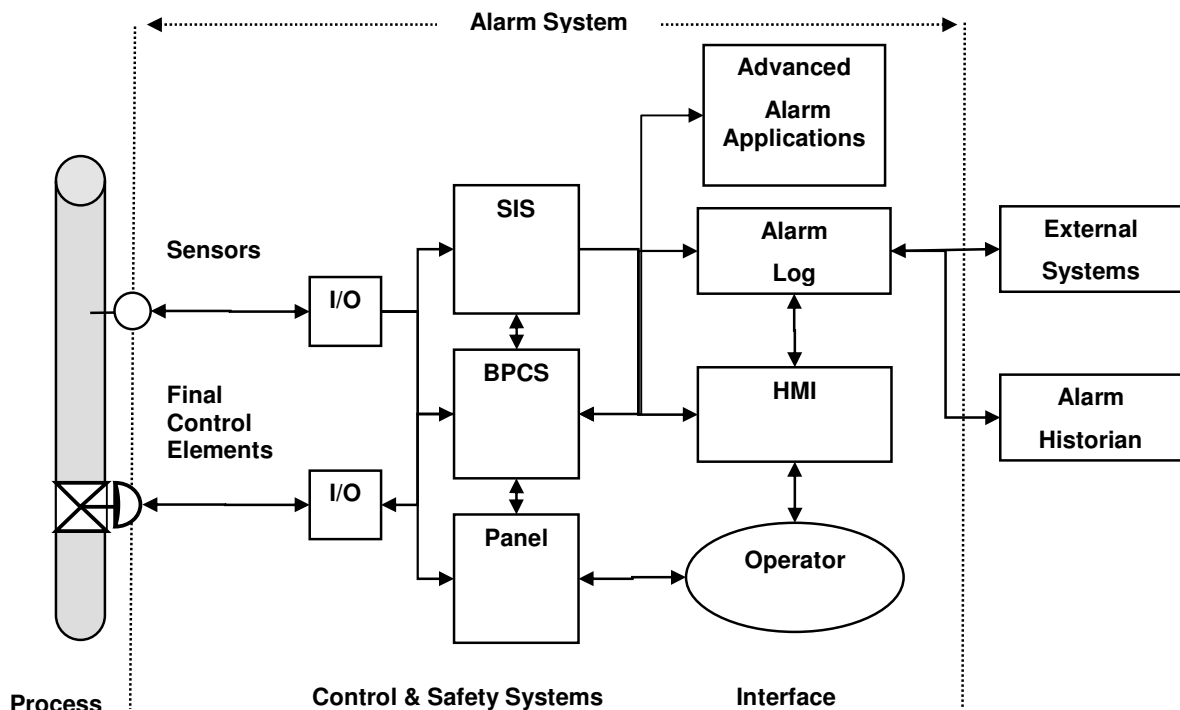


Figure 1 – Alarm System Dataflow

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 is 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* [S84]

ANSI/ISA-91.00.01-2001 *Identification of Emergency Shutdown Systems and Controls That Are Important to Maintaining Safety in Process Industries* [S91]

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 alarm 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 takes 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 method, in a multiple-alarm scenario, of determining which alarm occurred first.

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-alarmed 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

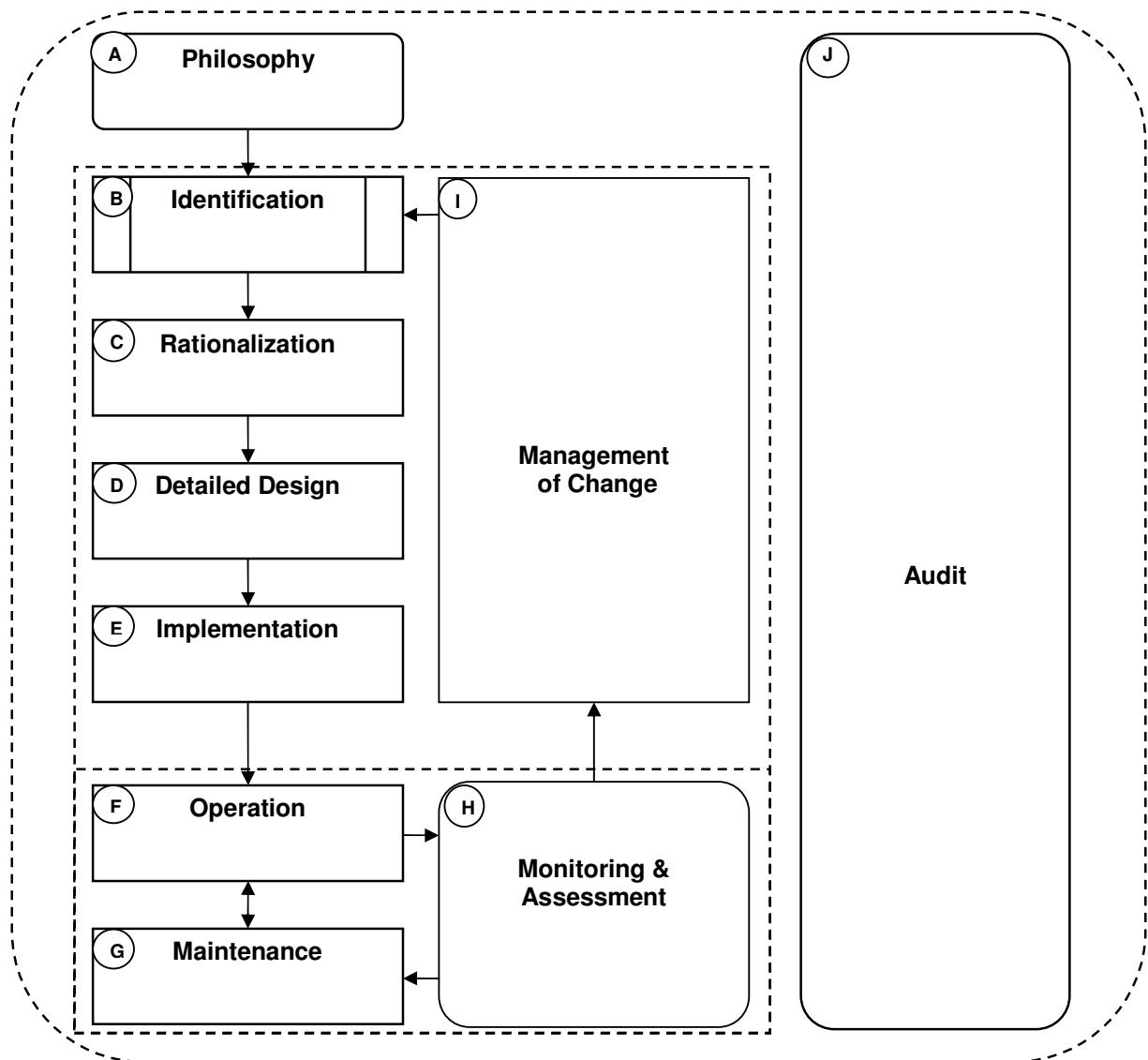
Alarm systems are used to communicate indications of abnormal process conditions or equipment malfunctions to the operators, the personnel monitoring and operating the process. Effective alarm systems are well designed, implemented, operated, and maintained. Alarm management is the set of practices and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