

BS EN 62682:2015



BSI Standards Publication

Management of alarms systems for the process industries

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 62682:2015. It is identical to IEC 62682:2014.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2015.

Published by BSI Standards Limited 2015

ISBN 978 0 580 79126 0

ICS 13.320; 25.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2015.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

EUROPEAN STANDARD

EN 62682

NORME EUROPÉENNE

EUROPÄISCHE NORM

January 2015

ICS 13.320; 25.040

English Version

**Management of alarms systems for the process industries
(IEC 62682:2014)**

Gestion de systèmes d'alarme dans les industries de
transformation
(IEC 62682:2014)

Alarmmanagement in der Prozessindustrie
(IEC 62682:2014)

This European Standard was approved by CENELEC on 2014-11-19. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

The text of document 65A/704/FDIS, future edition 1 of IEC 62682, prepared by SC 65A "System aspects" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62682:2015.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2015-08-19
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2017-11-19

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62682:2014 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61511 Series	NOTE	Harmonized as EN 61511 Series (not modified).
IEC 61511-1	NOTE	Harmonized as EN 61511-1.
IEC 62541-9	NOTE	Harmonized as EN 62541-9.

CONTENTS

INTRODUCTION.....	11
1 Scope.....	12
1.1 General applicability.....	12
1.2 Exclusions and inclusions.....	13
1.2.1 Operators	13
1.2.2 Process sensors and final control elements	13
1.2.3 Safety instrumented systems.....	13
1.2.4 Event data	13
1.2.5 Alarm identification methods	14
1.2.6 Management of change	14
2 Normative references.....	14
3 Terms, definitions, and abbreviations	14
3.1 Terms and definitions	14
3.2 Abbreviations	22
4 Conformance to this standard	22
4.1 Conformance guidance.....	22
4.2 Existing systems	23
4.3 Responsibility	23
5 Alarm system models.....	23
5.1 Alarm systems	23
5.2 Alarm management lifecycle.....	23
5.2.1 Alarm management lifecycle model.....	23
5.2.2 Alarm management lifecycle stages.....	24
5.2.3 Alarm lifecycle entry points.....	27
5.2.4 Simultaneous and encompassing stages	27
5.2.5 Alarm management lifecycle loops.....	27
5.2.6 Alarm management lifecycle stage inputs and outputs	28
5.3 Alarm states.....	29
5.3.1 Alarm state transition diagram	29
5.3.2 Alarm states.....	30
5.3.3 Alarm state transition paths	31
5.4 Alarm response timeline	32
5.4.1 General	32
5.4.2 Normal (A).....	33
5.4.3 Unacknowledged (B).....	33
5.4.4 Acknowledged (C) and response	33
5.4.5 Return-to-normal (D).....	34
5.4.6 Consequence threshold.....	34
5.5 Feedback model of operator-process interaction	34
5.5.1 General	34
5.5.2 Detect.....	35
5.5.3 Diagnose	35
5.5.4 Respond	35
5.5.5 Performance shaping factors	35
6 Alarm philosophy	35

6.1	Purpose	35
6.2	Alarm philosophy contents.....	35
6.2.1	General	35
6.2.2	Purpose of alarm system	36
6.2.3	Definitions	37
6.2.4	References	37
6.2.5	Roles and responsibilities for alarm management	37
6.2.6	Alarm design principles	37
6.2.7	Rationalization	37
6.2.8	Alarm class definition	37
6.2.9	Highly managed alarms.....	38
6.2.10	HMI design principles.....	38
6.2.11	Prioritization method	38
6.2.12	Alarm setpoint determination	39
6.2.13	Alarm system performance monitoring	39
6.2.14	Alarm system maintenance.....	39
6.2.15	Testing of the alarm system	39
6.2.16	Approved enhanced and advanced alarming techniques	39
6.2.17	Alarm documentation	39
6.2.18	Implementation guidance	40
6.2.19	Management of change	40
6.2.20	Training	40
6.2.21	Alarm history preservation.....	40
6.2.22	Related site procedures	40
6.2.23	Specific alarm design considerations	41
6.2.24	Alarm system audit	41
6.3	Alarm philosophy development and maintenance	41
7	Alarm system requirements specification.....	41
7.1	Purpose	41
7.2	Recommendations.....	42
7.3	Development.....	42
7.4	Systems evaluation	42
7.5	Customization	43
7.6	Alarm system requirements testing	43
8	Identification.....	43
8.1	Purpose	43
8.2	Alarm identification methods.....	43
8.3	Identification training	43
9	Rationalization.....	43
9.1	Purpose	43
9.2	Rationalization documentation	44
9.2.1	Rationalization documentation requirements	44
9.2.2	Rationalization documentation recommendations	44
9.3	Alarm justification.....	44
9.3.1	Alarm justification process.....	44
9.3.2	Justification approach	44
9.3.3	Individual alarm justification	45
9.3.4	Impact on alarm system	45
9.4	Alarm setpoint determination	45

9.5	Prioritization.....	45
9.6	Removal	45
9.7	Classification	46
9.8	Review.....	46
9.9	Use of documentation.....	46
10	Detailed design: Basic alarm design.....	46
10.1	Purpose	46
10.2	Usage of alarm states	46
10.2.1	Alarm state triggering.....	46
10.2.2	Alarm states and other logic functions	46
10.2.3	Alarm suppression and other logic functions	47
10.3	Alarm types.....	47
10.4	Alarm attributes.....	47
10.4.1	General	47
10.4.2	Alarm description	48
10.4.3	Alarm setpoints	48
10.4.4	Alarm priority	48
10.4.5	Alarm deadbands	48
10.4.6	Alarm on-delay and off-delay.....	48
10.5	Programmatic changes to alarm attributes	49
10.6	Review basic alarm design	49
11	Detailed design: Human-machine interface design for alarm systems.....	49
11.1	Purpose	49
11.2	HMI functions.....	49
11.2.1	General	49
11.2.2	HMI information requirements.....	49
11.2.3	HMI functional requirements.....	50
11.2.4	HMI display requirements.....	50
11.2.5	Alarm records requirements	50
11.2.6	Alarm records recommendations	50
11.3	Alarm states indications	50
11.3.1	General	50
11.3.2	Required alarm state indications.....	51
11.3.3	Recommended alarm state indications.....	51
11.3.4	Audible alarm state indications	52
11.4	Alarm priority indications	52
11.4.1	General	52
11.4.2	Alarm priority indication requirements.....	52
11.4.3	Colour alarm priority indications requirements	52
11.4.4	Recommended alarm priority indications.....	53
11.5	Alarm message indications	53
11.5.1	General	53
11.5.2	Recommended alarm message indications	53
11.6	Alarm displays	53
11.6.1	General	53
11.6.2	Alarm summary display	54
11.6.3	Alarm summary status.....	55
11.6.4	Alarm log displays.....	55
11.6.5	Process displays	56

11.6.6	Tag detail displays	56
11.6.7	Other display elements.....	56
11.7	Alarm shelving	56
11.7.1	General	56
11.7.2	Alarm shelving functional requirements.....	56
11.7.3	Alarm shelving functional recommendations.....	57
11.7.4	Shelved alarm displays	57
11.8	Out-of-service alarms	57
11.8.1	General	57
11.8.2	Out-of-service alarm functional requirements	58
11.8.3	Out-of-service alarm displays	58
11.9	Alarms suppressed by design	58
11.9.1	General	58
11.9.2	Designed suppression functional requirements	58
11.9.3	Design suppression functional recommendations	59
11.9.4	Suppressed-by-design displays	59
11.10	Alarm annunciator integration	59
11.10.1	General	59
11.10.2	Alarm annunciator integration recommendations	59
11.10.3	Alarm annunciator display integration recommendations	60
11.11	Safety alarm HMI	60
11.11.1	General	60
11.11.2	Independent safety alarm HMI.....	60
12	Detailed design: Enhanced and advanced alarm methods.....	60
12.1	Purpose	60
12.2	Basis of enhanced and advanced alarming	60
12.2.1	General	60
12.2.2	Effort, manpower requirements and complexity	60
12.3	Information linking.....	61
12.4	Logic-based alarming	61
12.4.1	General	61
12.4.2	Alarm attribute modification	61
12.4.3	Externally enabled systems	61
12.4.4	Logical alarm suppression and attribute modification	61
12.4.5	State-based alarming	61
12.5	Model-based alarming	61
12.6	Additional alarming considerations	62
12.6.1	General	62
12.6.2	Non-control room considerations	62
12.6.3	Remote alarm systems.....	62
12.6.4	Supplementary alarm systems.....	62
12.6.5	Batch process considerations.....	62
12.7	Training, testing, and auditing systems	63
12.8	Alarm attribute enforcement	63
13	Implementation.....	63
13.1	Purpose	63
13.2	Implementation planning	63
13.3	Implementation training	63
13.3.1	General	63

13.3.2	Implementation training	63
13.3.3	Implementation training requirements	64
13.3.4	Training documentation requirements for highly managed alarms	64
13.3.5	Training documentation recommendations	64
13.3.6	Implementation training requirements for new or modified alarm systems	64
13.3.7	Implementation training recommendations for new or modified alarm systems	64
13.4	Implementation testing and validation	64
13.4.1	General	64
13.4.2	Implementation testing requirements for highly managed alarms	64
13.4.3	Implementation testing recommendations for new or modified alarms	65
13.4.4	Implementation testing requirements for new or modified alarm systems	65
13.5	Implementation documentation	65
13.5.1	General	65
13.5.2	Documentation requirements	65
13.5.3	Implementation documentation recommendations	65
14	Operation	66
14.1	Purpose	66
14.2	Alarm response procedures	66
14.2.1	Alarm response procedures requirements	66
14.2.2	Alarm response procedure recommendations	66
14.3	Alarm shelving	66
14.3.1	Alarm shelving requirements	66
14.3.2	Alarm shelving for highly managed alarms	67
14.3.3	Alarm shelving recommendations	67
14.3.4	Alarm shelving record requirements	67
14.4	Refresher training for operators	67
14.4.1	Refresher training requirements for operators	67
14.4.2	Refresher training documentation for highly managed alarms	67
14.4.3	Refresher training content for highly managed alarms	67
14.4.4	Refresher training recommendations for alarms	67
15	Maintenance	68
15.1	Purpose	68
15.2	Periodic alarm testing	68
15.2.1	General	68
15.2.2	Periodic alarm testing requirements	68
15.2.3	Periodic alarm testing for highly managed alarms	68
15.2.4	Periodic alarm test procedure requirements	68
15.2.5	Periodic alarm test procedure recommendations	68
15.2.6	Periodic alarm testing recommendations	69
15.3	Out-of-service alarms	69
15.3.1	General	69
15.3.2	Out-of-service process requirements	69
15.3.3	Out-of-service highly managed alarms	69
15.3.4	Out-of-service process recommendations	69
15.3.5	Requirements for returning alarms to service	69
15.4	Equipment repair	69
15.5	Equipment replacement	70

15.6	Refresher training for maintenance	70
15.6.1	General requirements.....	70
15.6.2	Refresher training requirements for highly managed alarms	70
15.6.3	Refresher training recommendations for alarms	70
16	Monitoring and assessment	70
16.1	Purpose	70
16.2	Requirements.....	70
16.3	Monitoring, assessment, audit, and benchmark.....	70
16.4	Alarm system monitoring	71
16.5	Alarm system performance metrics	71
16.5.1	General	71
16.5.2	Average alarm rate per operator console	71
16.5.3	Peak alarm rate per operator console	72
16.5.4	Alarm floods.....	72
16.5.5	Frequently occurring alarms	73
16.5.6	Chattering and fleeting alarms.....	73
16.5.7	Stale alarms.....	73
16.5.8	Annunciated alarm priority distribution	73
16.5.9	Alarm priority distribution	74
16.6	Unauthorized alarm suppression.....	74
16.7	Alarm attribute monitoring	74
16.8	Reporting of alarm system analyses	74
16.9	Alarm performance metric summary.....	74
17	Management of change.....	75
17.1	Purpose	75
17.2	Changes subject to management of change	75
17.3	Change documentation requirements.....	76
17.4	Change documentation recommendations.....	76
17.5	Alarm removal recommendations	76
17.6	Alarm attribute modification recommendations	76
18	Audit	77
18.1	Purpose	77
18.2	Benchmark.....	77
18.2.1	General	77
18.2.2	Initial audit or benchmark requirements	77
18.3	Audit interviews.....	77
18.4	Audit recommendations	77
18.5	Action plans	78
	Bibliography	79
	Figure 1 – Alarm system dataflow.....	13
	Figure 2 – Alarm management lifecycle	24
	Figure 3 – Alarm state transition diagram	29
	Figure 4 – Alarm response timeline	33
	Figure 5 – Feedback model of operator-process interaction	35
	Table 1 – Alarm management lifecycle stage inputs and outputs	28

Table 2 – Alarm states	31
Table 3 – Required and recommended alarm philosophy content	36
Table 4 – Recommended alarm state indications	52
Table 5 – Average alarm rates	72
Table 6 – Annunciated alarm priority distribution	73
Table 7 – Recommended alarm performance metrics summary	75

INTRODUCTION

Purpose

This International Standard addresses the development, design, installation, and management of alarm systems in the process industries. Alarm 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 adapted from ANSI/ISA-18.2-2009, *Management of Alarm Systems for the Process Industries*, an International Society of Automation (ISA) standard, and 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 1999 the Engineering Equipment and Materials Users' Association (EEMUA) issued Publication 191, *Alarm Systems: A Guide to Design, Management and Procurement*. In 2003 the User Association of Process Control Technology in Chemical and Pharmaceutical Industries (NAMUR) issued worksheet 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, and
- e) audit or assess alarm system performance.

Organization

This standard is organized in two parts. The first part is introductory in nature, (Clauses 1 to 5). The main body of the standard follows (Clauses 6 to 18).

MANAGEMENT OF ALARMS SYSTEMS FOR THE PROCESS INDUSTRIES

1 Scope

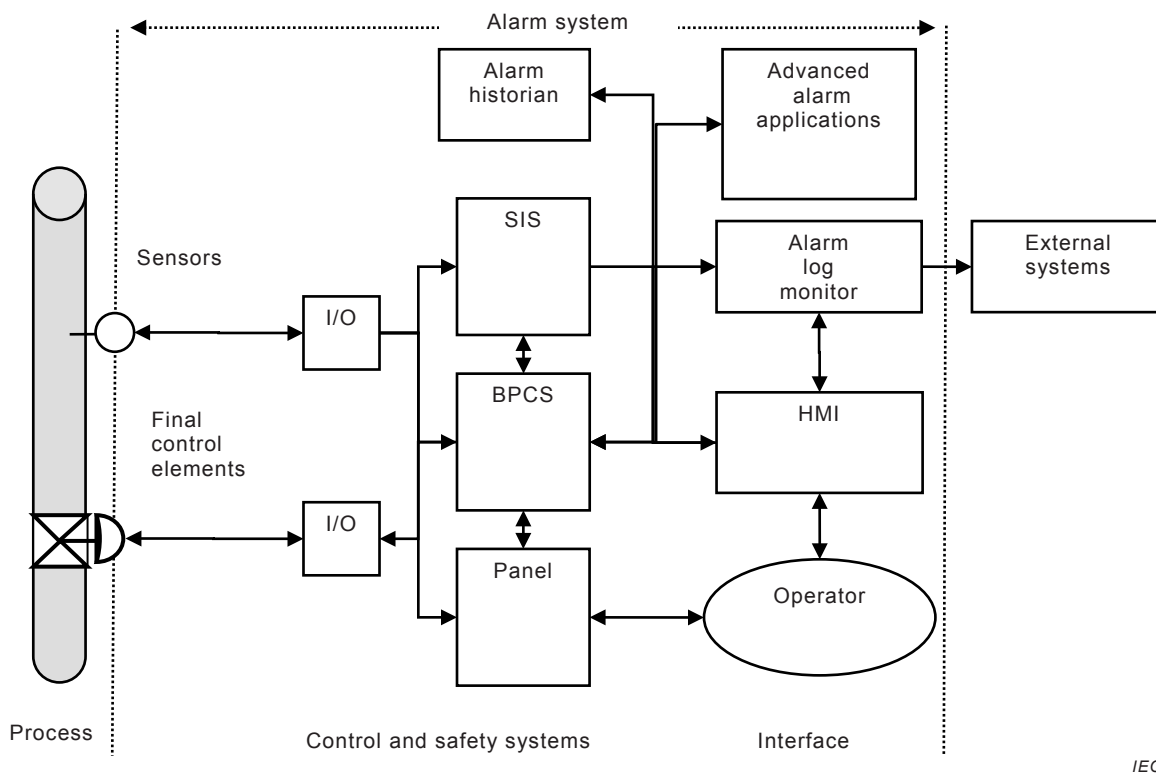
1.1 General applicability

This International Standard specifies general principles and processes for the lifecycle management of alarm systems based on programmable electronic controller and computer-based human-machine interface (HMI) technology for facilities in the process industries. It covers all alarms presented to the operator, which includes alarms from 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 can be differences in implementation to meet the specific needs based on process type.

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, in addition to the requirements of this standard, these should be taken into consideration.

The primary function within the alarm system is to notify operators of abnormal process conditions or equipment malfunctions and support the response. The alarm systems can 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. Figure 1 illustrates the concepts of alarm and response dataflow through the alarm system. The alarm system also includes a mechanism for communicating the alarm information to the operator via an HMI, usually a computer screen or an annunciator panel. Additional functions of the alarm system are an alarm and event log, an alarm historian, and the generation of performance metrics for the alarm system. There are external systems that can use the data from the alarm system.



IEC

Figure 1 – Alarm system dataflow

1.2 Exclusions and inclusions

1.2.1 Operators

The functions of the operator receiving and responding to alarms are included in the scope of this standard. Management of operators is excluded from the scope of this standard.

1.2.2 Process sensors and final control elements

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

1.2.3 Safety instrumented systems

The alarms from safety instrumented systems are included in the scope of this standard. The safety instrumented system (SIS) is shown in Figure 1 to indicate alarms can be implemented in these devices. The design and management of safety instrumented systems are excluded from this standard. Refer to IEC 61511.

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

1.2.4 Event data

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

1.2.5 Alarm identification methods

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

1.2.6 Management of change

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

2 Normative references

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

None.

3 Terms, definitions, and abbreviations

For the purposes of this document, the following terms, definitions and abbreviations apply.

3.1 Terms and definitions

3.1.1

absolute alarm

alarm generated when the alarm setpoint is exceeded

3.1.2

acknowledge

operator action that confirms recognition of an alarm

3.1.3

active

alarm in a state in which the alarm condition is true

3.1.4

adaptive alarm

alarm for which the setpoint is changed by an algorithm (e.g., rate based)

3.1.5

adjustable alarm

operator-set alarm

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

3.1.6

advanced alarming

collection of techniques that can help manage annunciations during specific situations

EXAMPLE: State-based alarming.

3.1.7

alarm

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

3.1.8**annunciation****alarm annunciation**

function of the alarm system to call the attention of the operator to an alarm

3.1.9**alarm attribute**

setting for an alarm within the process control system

EXAMPLE: Alarm setpoint

3.1.10**alarm class**

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

EXAMPLE: Safety related alarm class.

3.1.11**alarm deadband**

change in signal from the alarm setpoint necessary for the alarm to return to normal

3.1.12**(alarm) filtering**

function which selects alarm records to be displayed according to a given element of the alarm record

3.1.13**alarm flood**

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

3.1.14**alarm group**

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

3.1.15**alarm historian**

long term repository for alarm records

3.1.16**alarm log**

short term repository for alarm records

3.1.17**alarm management****alarm system management**

collection of processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems

3.1.18**alarm message**

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

3.1.19**alarm off-delay
debounce**

time a process measurement remains in the normal state before the alarm becomes inactive

3.1.20**alarm on-delay**

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

3.1.21**alarm philosophy**

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

3.1.22**alarm priority**

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)

3.1.23**alarm rate**

number of annunciated alarms, per operator, in a specific time interval

3.1.24**(alarm) record**

set of information which documents an alarm state change

3.1.25**alarm setpoint****alarm limit****alarm trip point**

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

3.1.26**(alarm) sorting**

function which orders alarm records to be displayed according to a given element of alarm record

3.1.27**alarm summary****alarm list**

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

Note 1 to entry: Return to normal indications can also appear on the alarm summary.

3.1.28**alarm system**

operator support system for generating and handling alarms for managing abnormal situations

Note 1 to entry: The operator is included in the alarm system. See Figure 1.

3.1.29**alarm system requirements specification**

document which specifies the details of the alarm system design

3.1.30**alarm type**

alarm attribute which gives a distinction of the alarm condition

EXAMPLE: Low process variable alarm, high process variable alarm, or discrepancy alarm.

3.1.31**alert**

audible and/or visible means of indicating to the operator an equipment or process condition that can require evaluation when time allows

3.1.32**allowable response time**

maximum time between the annunciation of the alarm and when the operator takes corrective action to avoid the consequence

3.1.33**annunciator**

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

3.1.34**assessment**

comparison of information from monitoring and additional qualitative (subjective) measurements, against stated goals and defined performance metrics

3.1.35**audit**

comprehensive assessment that includes the evaluation of alarm system performance and the effectiveness of the work practices used to administer the alarm system

3.1.36**bad-measurement alarm**

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

3.1.37**benchmark**

initial audit of an alarm system designed to specifically identify problem areas for the purpose of formulating improvement plans

3.1.38**bit-pattern alarm**

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

3.1.39**calculated alarm**

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

3.1.40**call-out alarm**

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

3.1.41**chattering alarm**

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

3.1.42**classification**

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

3.1.43**control system**

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 1 to entry: The control system can include both basic process control systems (BPCS) and safety instrumented systems (SIS).

3.1.44**controller-output alarm**

alarm generated from the output signal of a control algorithm (e.g., PID controller) instead of a direct process measurement

3.1.45**decommission**

process to remove an alarm from the alarm system

3.1.46**deviation alarm**

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

3.1.47**discrepancy alarm****mismatch alarm**

alarm generated by the difference between the 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)

3.1.48**display**

visual representation of information used by the operator for monitoring and control

3.1.49**dynamic alarming**

automatic modification of alarm attributes based on process state or conditions

3.1.50**enforcement**

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

3.1.51**event**

representation of a solicited or unsolicited fact indicating a state change

Note 1 to entry: For example, mode changes, device state changes.

[SOURCE: IEC 62264-2:2004, 3.1.2, modified – a note has been added.]

3.1.52**fleeting alarm**

alarm that transitions between an active alarm state and an inactive alarm state in a short period of time

3.1.53**first-out alarm****first-up alarm**

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

3.1.54**highly managed alarm**

alarm belonging to a class with additional requirements above general alarms

EXAMPLE: Safety alarm

3.1.55**human machine interface****HMI**

collection of hardware and software used by the operator to monitor and interact with the control system and with the process via the control system

3.1.56**implementation**

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

Note 1 to entry: Implementation includes activities such as commissioning and training.

3.1.57**instrument diagnostic alarm**

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

3.1.58**interim alarm**

alarm used on a temporary basis to replace an out-of-service alarm

3.1.59**latching alarm**

alarm that remains in alarm state after the process condition has returned to normal and requires an operator reset before the alarm returns to normal

3.1.60**master alarm database**

authorized list of rationalized alarms and associated attributes

3.1.61**monitoring**

measurement and reporting of quantitative (objective) aspects of alarm system performance

3.1.62**nuisance alarm**

alarm that annunciates excessively, unnecessarily, or does not return to normal after the operator response is taken

EXAMPLE: Chattering alarm, fleeting alarm, or stale alarm.

3.1.63**operator****controller**

person who monitors and makes changes to the process

3.1.64**(operator) console**

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

3.1.65**operator station**

human-machine interface within the operator console

Note 1 to entry: Operator station can include multiple screens.

3.1.66**out-of-service**

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

3.1.67**plant state****plant mode**

defined set of operational conditions for a process plant

EXAMPLE: Shutdown, normal operation.

3.1.68**prioritization**

process of assigning a level of operational importance to an alarm

3.1.69**process area**

physical, geographical or logical grouping of resources determined by the site

[SOURCE: IEC 62264-1:2003, 3.1]

3.1.70**rate-of-change alarm**

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

3.1.71**rationalization**

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

3.1.72**re-alarmed alarm****re-triggering alarm**

alarm that is automatically re-announced to the operator under certain conditions

3.1.73**recipe-driven alarm**

alarm with setpoints that depend on the recipe that is currently being executed

3.1.74**remote alarm**

alarm from a remotely operated facility or directed to a remote interface

3.1.75**reset**

operator action that unlatches a latched alarm

3.1.76**return to normal
clear**

alarm transition from an active annunciated alarm state to an inactive annunciated alarm state

3.1.77**safety instrumented system**

instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final elements(s)

Note 1 to entry: This can include either safety instrumented control functions or safety instrumented protection functions or both.

[SOURCE: IEC 61511-1:2003, 3.2.72]

3.1.78**safety related alarm
safety alarm**

an alarm that is classified as critical to process safety for the protection of human life or the environment

EXAMPLE: An alarm with a risk reduction factor greater than 10.

3.1.79**shelve**

temporarily suppress an alarm, initiated by the operator, with engineering controls to unsuppress the alarm

3.1.80**silence**

operator action that terminates the audible alarm indication

3.1.81**stale alarm**

alarm that remains annunciated for an extended period of time (e.g., 24 hours)

3.1.82**state-based alarm
mode-based alarms**

alarm that has attributes modified or is suppressed based on operating states or process conditions

3.1.83**statistical alarm**

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

3.1.84**suppress**

prevent the annunciation of the alarm to the operator when the alarm is active

EXAMPLE: Shelve, suppress by design, remove from service.

3.1.85**suppressed by design**

alarm annunciation to the operator prevented based on plant state or other conditions

3.1.86**system diagnostic alarm**

alarm generated by the control system to indicate a fault within the system hardware, software or components

EXAMPLE: Communication error.

3.1.87**tag
point**

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

3.1.88**unacknowledged**

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

3.2 Abbreviations

ACKED	Acknowledged
ASRS	Alarm system requirements specification
BPCS	Basic process control system
cGMP	Current good manufacturing practice
DSUPR	Designed suppression
EEMUA	Engineering equipment and materials users' association
ERP	Enterprise resource planning
FMEA	Failure mode and effects analysis
HAZOP	Hazard and operability study
HMA	Highly managed alarms
HMI	Human machine interface
I/O	Input/output
LOPA	Layer of protection analysis
MES	Manufacturing execution system
MOC	Management of change
NORM	Normal
OOSRV	Out of service
P&ID	Piping (or process) and instrumentation diagram
PHA	Process hazards analysis
RTNUN	Return to normal unacknowledged
SHLVD	Shelved
SIS	Safety instrumented system
SOP	Standard operating procedure
UNACK	Unacknowledged

4 Conformance to this standard**4.1 Conformance guidance**

To conform to this standard, it shall be shown that each of the requirements in the normative clauses has been satisfied. This is the responsibility of the owner/operator.

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.

4.3 Responsibility

Conformance to this standard is the responsibility of 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, and to support the response. Effective alarm systems are well designed, implemented, operated, and maintained. Alarm management is the set of practices and processes that ensures an effective alarm system.

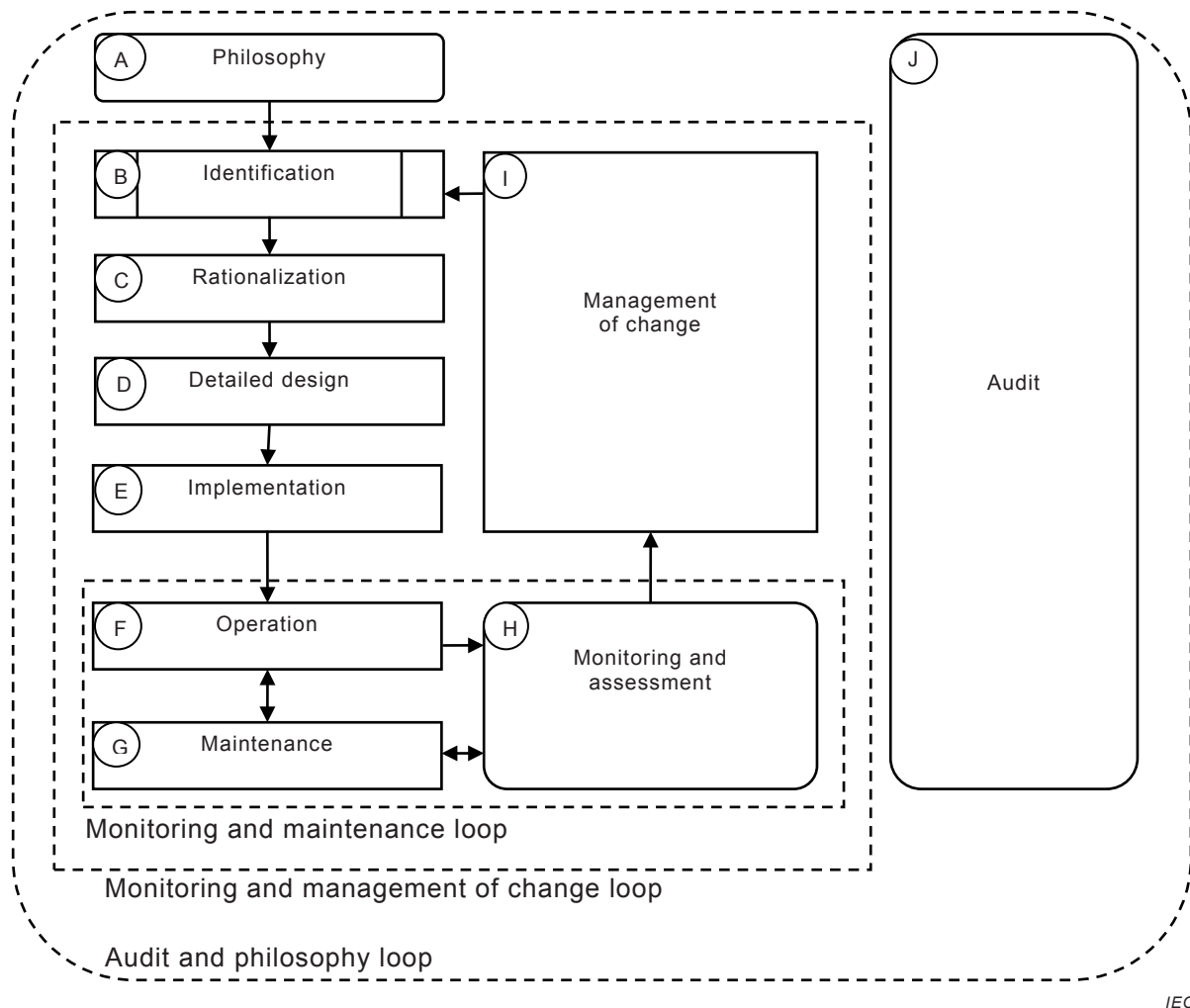
A foundational part of alarm management is the definition of an alarm, an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response. An essential element of this definition is the response to the alarm. This definition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

5.2 Alarm management lifecycle

5.2.1 Alarm management lifecycle model

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 5.2.2.3.

NOTE 2 The independent stage J represents a process that connects to all other stages per 5.2.2.11.

NOTE 3 The rounded shapes of stages A, H, and J represent entry points to the lifecycle per 5.2.3.

NOTE 4 The dotted lines represent the loops in the lifecycle per 5.2.5.

Figure 2 – Alarm management lifecycle

5.2.2 Alarm management lifecycle stages

5.2.2.1 General

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

5.2.2.2 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 criteria for alarm prioritization and the definition of alarm classes, performance metrics, performance limits and reporting requirements are based on the objectives and principles for alarm systems. 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 alarm management 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 ASRS is included in the philosophy stage of the lifecycle. The specification can be plant specific, providing details on restrictions or options, and can be the basis for selecting new or modifying existing control systems. The specification typically goes into more detail than the alarm philosophy and may provide specific guidance for system design.

5.2.2.3 Identification (B)

The identification stage is a collection point for potential alarms proposed by any one of several methods for determining if an alarm might 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 can 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 a new alarm or modifications to an existing alarm has been identified and it is ready to be rationalized.

5.2.2.4 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 output of rationalization is 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.

5.2.2.5 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.

5.2.2.6 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.

5.2.2.7 Operation (F)

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

5.2.2.8 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.

5.2.2.9 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.

5.2.2.10 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 alarm management lifecycle stages from identification to implementation.

5.2.2.11 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 can 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 can also identify the need to increase the discipline of the organization to follow the alarm philosophy.

5.2.3 Alarm lifecycle entry points

5.2.3.1 General

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

- a) alarm philosophy,
- b) monitoring and assessment, and
- c) audit.

These entry points are represented by rounded boxes in Figure 2. 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.

5.2.3.2 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.

5.2.3.3 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 prior to the development of the alarm philosophy.

5.2.3.4 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.

5.2.4 Simultaneous and encompassing stages

The lifecycle diagram (Figure 2) is drawn to represent sequential stages. There are several simultaneous stages which are represented 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.

5.2.5 Alarm management lifecycle loops

5.2.5.1 General

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

5.2.5.2 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.

5.2.5.3 Monitoring and management of change loop

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

5.2.5.4 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.

5.2.6 Alarm management lifecycle stage inputs and outputs

The alarm management 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). Table 1 provides more information on the relationships between the inputs and outputs of the lifecycle stages.

Table 1 – Alarm management lifecycle stage inputs and outputs

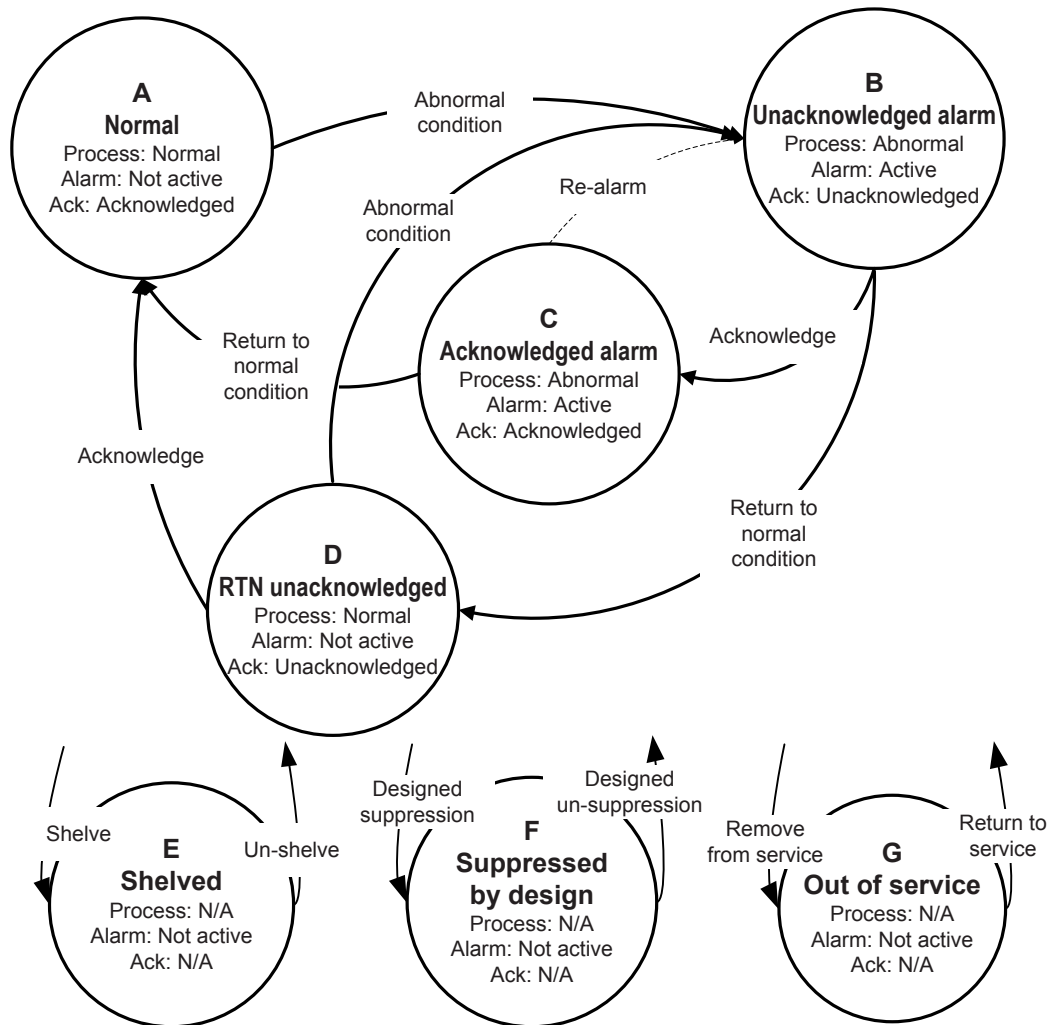
Alarm management lifecycle stage		Activities	Clause number	Inputs	Outputs
Stage	Title				
A	Philosophy	Document the objectives, guidelines and work processes for alarm management, and ASRS.	6,7	Objectives and standards.	Alarm philosophy and ASRS.
B	Identification	Determine potential alarms.	8	PHA report, 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 and alarm design requirements.
D	Detailed design	Basic alarm design, HMI design, and advanced alarming design.	10,11,12	Master alarm database and alarm design requirements.	Completed alarm design.
E	Implementation	Install alarms, implementation testing, and implementation training.	13	Completed alarm design and master alarm database.	Operational alarms and alarm response procedures.
F	Operation	Operator responds to alarms, and refresher training.	14	Operational alarms and alarm response procedures.	Alarm data.
G	Maintenance	Maintenance repair and replacement, and 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 and proposed changes.
I	Management of change	Process to authorize additions,	17	Alarm philosophy and proposed	Authorized alarm changes.

Alarm management lifecycle stage		Activities	Clause number	Inputs	Outputs
Stage	Title				
		modifications, and deletions of alarms.		changes.	
J	Audit	Periodic audit of alarm management processes.	18	Standards, alarm philosophy, and audit protocol.	Recommendations for improvement.

5.3 Alarm states

5.3.1 Alarm state transition diagram

The alarm state transition diagram shown in Figure 3 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.



IEC

NOTE 1 States E, F, and G can connect to any alarm state in the diagram.

NOTE 2 The dotted line indicates an infrequently implemented option.

Figure 3 – Alarm state transition diagram

5.3.2 Alarm states

5.3.2.1 General

The circles in Figure 3 represent the states of an alarm. The letter label is an identifier. 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.

5.3.2.2 Normal state (A)

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

5.3.2.3 Unacknowledged state (B)

The unacknowledged alarm (UNACK) state is the initial state of an alarm becoming active due to abnormal conditions. In this state the alarm is unacknowledged. Previously acknowledged alarms can be designed to re-alarm, causing a return to this state.

5.3.2.4 Acknowledged state (C)

The acknowledged (ACKED) alarm state is the state in which the alarm is active and the operator has acknowledged the alarm.

5.3.2.5 Return to normal unacknowledged state (D)

In the returned to normal unacknowledged (RTNUN) alarm state, the process is within normal limits and the alarm becomes inactive before an operator has acknowledged the alarm condition.

5.3.2.6 Shelved state (E)

In the shelved (SHLVD) alarm state an alarm is temporarily suppressed using a controlled methodology, and not annunciated. An alarm in the shelved state is under the control of the operator. The shelving function can automatically unshelve alarms.

5.3.2.7 Suppressed-by-design state (F)

In the suppressed-by-design (DSUPR) alarm state an alarm is suppressed based on operating conditions or plant states, and not annunciated. An alarm in the suppressed-by-design state is under the control of logic that determines the relevance of the alarm.

5.3.2.8 Out-of-service state (G)

In the out-of-service (OOSRV) alarm state an alarm is manually suppressed (e.g., control system functionality to remove alarm from service) when it is removed from service, typically for maintenance, and not annunciated. An alarm in the out-of-service state is under the control of maintenance.

5.3.2.9 Alarm status by state

The alarm status of different alarm states are summarized in Table 2.

Table 2 – Alarm states

ID	Mnemonic	State name	Process condition	Alarm status	Annunciate status	Acknowledge status
A	NORM	Normal alarm state	Normal	Inactive	Not annunciated	Acknowledged
B	UNACK	Unacknowledged alarm state	Abnormal	Active	Annunciated	Unacknowledged
C	ACKED	Acknowledged alarm state	Abnormal	Active	Annunciated	Acknowledged
D	RTNUN	Returned to normal unacknowledged alarm state	Normal	Inactive	Annunciated	Unacknowledged
E	SHLVD	Shelved state	Normal or abnormal	Active or Inactive	Suppressed	Not Applicable
F	DSUPR	Suppressed-by-design state	Normal or abnormal	Active or Inactive	Suppressed	Not Applicable
G	OOSRV	Out-of-service alarm state	Normal or abnormal	Active or Inactive	Suppressed	Not Applicable

5.3.3 Alarm state transition paths

5.3.3.1 General

The arrows in Figure 3 represent transitions between states. For simplicity, the diagram does not illustrate the effects of alarm deadband and on-delay or off-delay.

5.3.3.2 Transition from normal to unacknowledged (A -> B)

This transition occurs when 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.

5.3.3.3 Transition from unacknowledged to acknowledged (B -> C)

This transition occurs when an operator acknowledges an alarm that is active before the process returns to normal.

5.3.3.4 Transition from acknowledged to unacknowledged (C -> B)

This transition is the infrequently used option that periodically generates repetitive alarm indications for a single alarm while the alarm remains in the alarm state.

5.3.3.5 Transition from acknowledged to normal (C -> A)

This transition is part of a normal sequence for an alarm. The alarm moves from the acknowledged state to normal.

5.3.3.6 Transition from unacknowledged to return-to-normal unacknowledged (B -> D)

This transition occurs when the process returns to normal before an operator has acknowledged the alarm.

5.3.3.7 Transition from return-to-normal unacknowledged to normal (D -> A)

This transition occurs when an alarm has returned to normal and becomes inactive and can require operator acknowledgment, or can be acknowledged automatically.

5.3.3.8 Transition to shelved (any state -> E)

This transition occurs when an operator shelves an alarm to avoid clutter in the active alarm displays. Shelving is a manual operation.

5.3.3.9 Transition from shelved to normal or unacknowledged (E -> A or B)

This transition occurs when an alarm is un-shelved, manually or automatically. If the alarm is not active, the transition should be to the normal state. If the alarm is active, the transition should be to the unacknowledged state.

5.3.3.10 Transition to suppressed-by-design (any state -> F)

This transition occurs when process conditions or states are used to suppress alarms by design. Designed suppression is typically an automatic operation.

5.3.3.11 Transitions from suppressed-by-designed to normal or unacknowledged (F -> A or B)

This transition occurs when process conditions or states are used to un-suppress alarms when appropriate. Designed un-suppression is typically an automatic operation. If the alarm is not active, the transition should be to the normal state. If the alarm is active, the transition should be to the unacknowledged state.

5.3.3.12 Transition to out-of-service state (any state -> G)

An alarm can be removed from service for maintenance or other reasons. Remove from service is typically a manual operation.

5.3.3.13 Transition from out-of-service to normal or unacknowledged (G -> A or B)

An alarm can be returned to service when it is available. Return to service is typically a manual operation. If the alarm is not active, the transition should be to the normal state. If the alarm is active, the transition should be to the unacknowledged state.

5.4 Alarm response timeline

5.4.1 General

Figure 4 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. It is possible to map some alarm states from Figure 3 to the timeline shown in Figure 4, to clarify the definition of terms related to time.

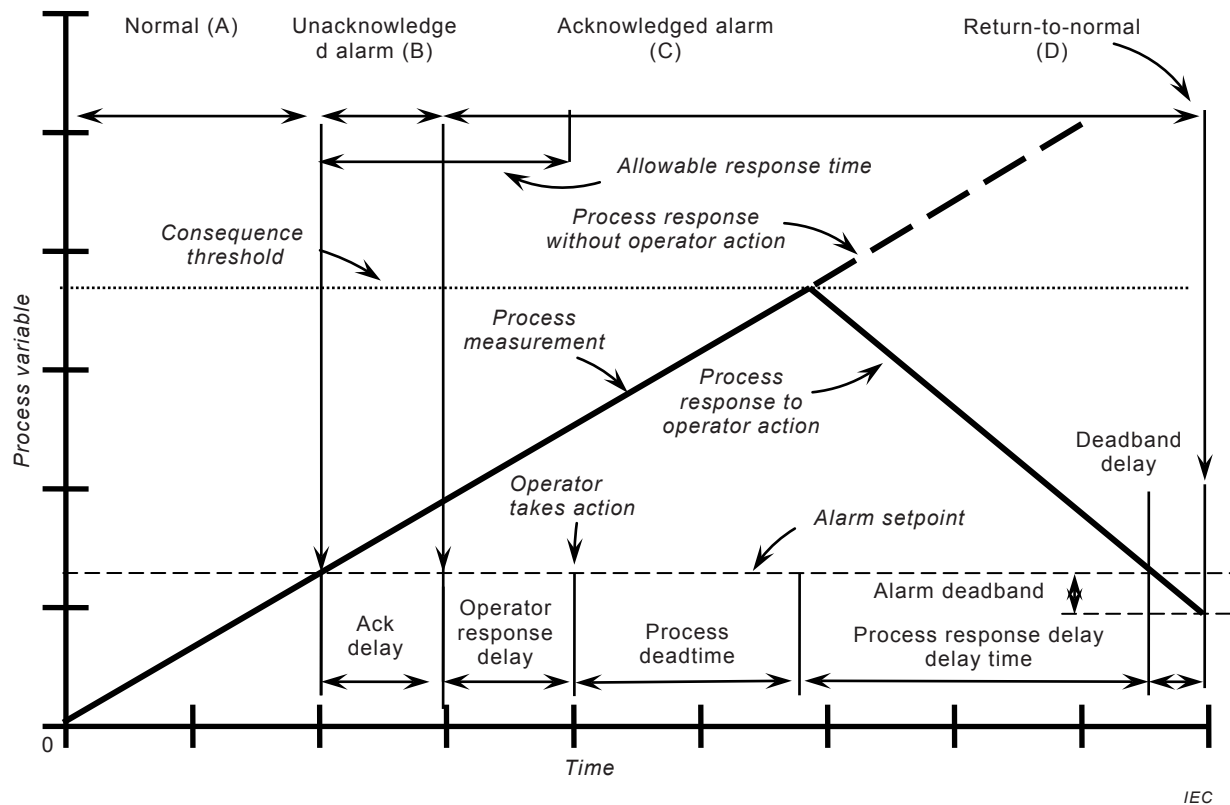


Figure 4 – Alarm response timeline

5.4.2 Normal (A)

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

5.4.3 Unacknowledged (B)

The unacknowledged alarm state results when the measurement crosses the alarm setpoint. There are several factors that affect the alarm annunciation such as

- the measurement accuracy,
- the sampling interval, and
- the alarm on-delay.

The alarm is not always immediately acknowledged by the operator.

5.4.4 Acknowledged (C) and response

The acknowledged alarm state is reached when an operator acknowledges the alarm condition, after the acknowledge delay. In this state the alarm is active. There are several factors that affect the operator response time such as

- the system processing speed,
- the HMI design and clarity,
- the operator awareness and training,
- the operator workload,
- the complexity of determining the operator action, and

- f) the complexity of the operator action.

The actual response time for the alarm is the time beginning when the alarm is annunciated and ending when the operator takes the corrective action. It includes the detection of the alarm, the diagnosis of the situation and determination of the operator 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.

5.4.5 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 return-to-normal time. These include the following:

- a) the operator response delay,
- b) the degree of corrective 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, and
- g) the operational speed of the alarm system.

5.4.6 Consequence threshold

The consequence results when no operator action is taken, 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.

5.5 Feedback model of operator-process interaction

5.5.1 General

A model of operator-process interaction is shown in Figure 5. 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, and
- c) the action is implemented to compensate for the disturbance.

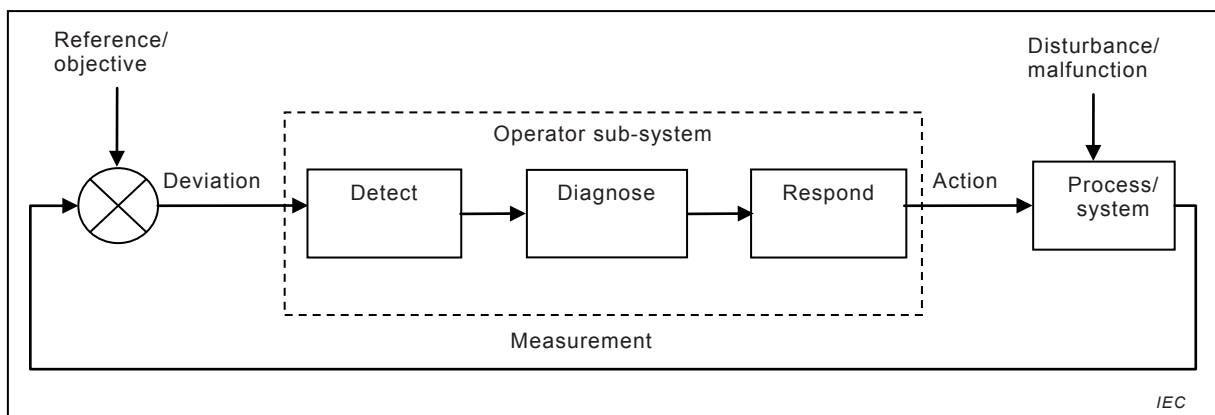


Figure 5 – Feedback model of operator-process interaction

5.5.2 Detect

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

5.5.3 Diagnose

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

5.5.4 Respond

The operator takes corrective action in response to the deviation.

5.5.5 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 management lifecycle. The alarm philosophy serves as the framework to establish the criteria, definitions, principles, and responsibilities for all of the alarm management lifecycle stages. This is achieved by specifying items, including the methods for alarm identification, rationalization, monitoring, management of change and audit to be followed. An alarm philosophy document facilitates:

- a) consistency across the alarm system,
- b) consistency with risk management goals and objectives,
- c) agreement with good engineering practices, and
- d) design and management of the alarm system that supports an effective operator response.

6.2 Alarm philosophy contents

6.2.1 General

Subclause 6.2 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 can vary between industries and from one location to another. The required and recommended contents of the alarm philosophy are listed in Table 3.

Table 3 – Required and recommended alarm philosophy content

Alarm philosophy contents	Required / recommended	Subclause
Purpose of alarm system	Required	6.2.2
Definitions	Required	6.2.3
References	Required	6.2.4
Roles and responsibilities for alarm management	Required	6.2.5
Alarm design principles	Required	6.2.6
Rationalization	Required	6.2.7
Alarm class definition	Required	6.2.8
Highly managed alarms (or site equivalent)	Recommended	6.2.9
HMI design principles	Required	6.2.10
Prioritization method	Required	6.2.11
Alarm setpoint determination	Recommended	6.2.12
Alarm system performance monitoring	Required	6.2.13
Alarm system maintenance	Required	6.2.14
Testing of alarms	Required	6.2.15
Approved enhanced and advanced alarming techniques	Recommended	6.2.16
Alarm documentation	Required	6.2.17
Implementation guidance	Required	6.2.18
Management of change	Required	6.2.19
Training	Required	6.2.20
Alarm history preservation	Required	6.2.21
Related site procedures	Recommended	6.2.22
Specific alarm design considerations	Recommended	6.2.23
Alarm system audit	Required	6.2.24

For alarm 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 alarm rationalization.

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

The required contents of the alarm philosophy can exist in other site procedures. These procedures should be referenced in the philosophy.

6.2.2 Purpose of alarm system

The purpose and objectives of a process plant alarm system shall be defined. Having the purpose and objectives clearly defined serves to orient participants in design and improvement activities. This definition can facilitate the implementation and maintenance of an effective alarm system.

6.2.3 Definitions

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

6.2.4 References

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

6.2.5 Roles and responsibilities for alarm management

Responsibility for the activities of the alarm management lifecycle 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.

6.2.6 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 shall 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, shelved, etc.) that the facility will use.

6.2.7 Rationalization

In order to maximize the functionality of the alarm system it is important that the operator receive only those alarms that require an operator response. Ensuring that an alarm requires a response is done through alarm rationalization. This section of the alarm philosophy should list the criteria to assess alarms and the information to be captured during rationalization.

This section should provide guidance on the knowledge and experience of the rationalization team, which should include:

- a) operations,
- b) process,
- c) control system, and
- d) alarm philosophy.

6.2.8 Alarm class definition

Alarm classes are used to set common requirements for managing alarms. An alarm may belong to more than one class. This section should include the definition of the alarm classes. It should also include the following class 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, and
- k) HMI design.

6.2.9 Highly managed alarms

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

- a) alarms critical to process safety for 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 commercial loss,
- f) alarms for product quality,
- g) alarms for process licensor requirements, and
- h) alarms for company policy.

If HMA classes are used, this section of the alarm philosophy shall document the requirements for these alarm classes.

6.2.10 HMI design principles

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

Specific elements that should be covered in this section include the following:

- 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, shelved, etc.) that will be used at the facility;
- c) the types of displays that will be used (e.g., alarm summary, first-out, etc.);
- d) the functions that will be available in the HMI, including shelving and suppression.

6.2.11 Prioritization method

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

- a) the basis for alarm prioritization (e.g., severity of consequence, time to respond, etc.);
- b) the metrics for alarm configuration (e.g., alarm count and priority distribution);
- c) the impact of classification on prioritization.

6.2.12 Alarm setpoint determination

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

6.2.13 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 shall be covered in this section include the following:

- a) the objective for monitoring and assessment,
- b) the monitoring metrics and target values,
- c) guidance on frequency to review alarm system performance, and
- d) guidance on the approach to improve performance on the metrics.

6.2.14 Alarm system maintenance

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

Specific elements that shall be covered in this section include the following:

- a) alarm maintenance record keeping,
- b) the requirements for out-of-service alarms, and
- c) the policy on the use of interim alarms.

6.2.15 Testing of the alarm system

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

6.2.16 Approved enhanced and advanced alarming techniques

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

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

6.2.17 Alarm documentation

Appropriate documentation shall be addressed in the alarm philosophy. This may include the following:

- a) rationalization information (e.g., a master alarm database),
- b) periodic alarm performance reports,
- c) specifications for advanced alarm management techniques, and
- d) specifications for suppress by design.

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 behaviours to the operator across all modes of operation.

6.2.18 Implementation guidance

Defining the basic approach for initial training, commissioning, and checkout of the alarm system facilitates consistency throughout the plant or company. This assures the effective deployment of the alarm system.

6.2.19 Management of change

This section identifies the types of changes and the applicable procedures. A management of change procedure shall be documented. Types of changes may include:

- a) temporary changes to alarms (e.g., out of service);
- b) permanent changes to the master alarm database, alarm attributes, or enhanced and advanced alarming techniques.

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.

6.2.20 Training

This section specifies how plant personnel are to be trained on the use, management, and design of the alarm system. This section also specifies the training documentation requirements.

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

- a) the job roles or personnel requiring training relating to the alarm system,
- b) an outline of the training contents, and
- c) when training is required.

6.2.21 Alarm history preservation

This section defines what aspects of the alarm history (e.g., annunciations, acknowledgements, return to normal, and operator actions) shall be preserved and the retention period (e.g., incidents, violation of safe operating limits). In some industries and regions, regulatory bodies or local statutes might require preservation of this information.

6.2.22 Related site procedures

To avoid inconsistencies between the alarm philosophy and other site procedures, the alarm philosophy should cite relevant procedures. The following documents can 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) management of change procedure, and

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

6.2.23 Specific 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 and alarms from redundant sensors). Alarm classes may be the source of such specific design considerations.

6.2.24 Alarm system audit

The philosophy document shall specify the requirements of periodic alarm management audits. These requirements may include:

- a) audit frequency, which may be specified based on alarm class,
- b) audit topics, and
- c) process for operator interviews.

6.3 Alarm philosophy development and maintenance

Personnel who apply the alarm philosophy should be involved in developing the alarm philosophy. The team 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,
- b) process instrumentation,
- c) control systems,
- d) process technology,
- e) mechanical/reliability engineering,
- f) safety, health and environmental,
- g) process safety,
- h) human factors,
- i) alarm management, and
- j) management of change process.

7 Alarm system requirements specification

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. Clause 7 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, 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 is to be available when rationalizing, designing, implementing, visualizing and recording individual alarms, and in analysing 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 protocol,
- d) alarm record logging,
- e) alarm record analysis, and
- f) other capabilities that facilitate alarm lifecycle activities.

There can be new control system projects in which it is determined that 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 contains guidance that can be used to generate some of the alarm system requirements specification. The ASRS should include the following:

- a) alarm priorities available,
- b) visible annunciation functionality, such as colours and symbols,
- c) audible alarm annunciation functionality,
- d) alarm summary display functionality,
- e) alarm shelving functionality,
- f) alarm suppression functionality,
- g) alarm configuration functionality, such as deadband and on-delay and off-delay,
- h) alarm log capabilities,
- i) alarm monitoring and assessment functionality,
- j) alarm system audit functionality, and
- k) advanced alarming functionality.

NOTE Some alarm requirements can exist in other documents, such as in a safety requirements specification for SIS applications, as defined in IEC 61511.

7.4 Systems evaluation

Alarm system functionality should be evaluated against requirements during control system selection. The alarm system functionality of 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

If important system requirements in the specification are not met by standard commercial products, it may be necessary to develop custom solutions, or to reconsider the specification. The alarm system requirements specification facilitates early recognition of the need for customized solutions, 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

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) hazard and operability study (HAZOP),
- d) layer of protection analysis (LOPA),
- e) incident investigations,
- f) environmental permits,
- g) failure mode and effects analysis (FMEA),
- h) current good manufacturing practice (cGMP),
- i) quality reviews,
- j) P&ID reviews,
- k) operating procedure reviews, and
- l) packaged equipment manufacturer recommendations.

8.3 Identification training

Personnel using any method for alarm identification should be trained on the alarm philosophy and the criteria for assessing alarms.

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.

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

- a) alarm type,
- b) priority,
- c) class,
- d) alarm setpoint or logical condition (e.g., off-normal),
- e) operator action,
- f) consequence of inaction or incorrect action,
- g) probable cause, and
- h) need for advanced alarming techniques if necessary.

9.2 Rationalization documentation

9.2.1 Rationalization documentation requirements

Rationalization documentation for each alarm shall include the following:

- a) alarm type,
- b) priority,
- c) class,
- d) alarm setpoint or logical condition (e.g., off-normal),
- e) operator action,
- f) consequence of inaction or incorrect action,

9.2.2 Rationalization documentation recommendations

Rationalization documentation for each alarm should include the following:

- a) maximum allowable response time,
- b) probable cause,
- c) identification method, and
- d) need for advanced alarming techniques if necessary.

9.3 Alarm justification

9.3.1 Alarm justification process

Every alarm requiring rationalization is compared to the criteria in the alarm philosophy to justify that it is an alarm.

The criteria from the definition of an alarm include:

- a) the alarm is directed to the operator,
- b) the alarm indicates a process deviation, abnormal condition, or equipment malfunction, and
- c) the alarm requires a timely response.

9.3.2 Justification approach

The alarm justification process should

- a) utilize a team approach,

- b) rely heavily upon operator input, and
- c) focus on the operator action to be prompted.

9.3.3 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 the 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 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.

9.3.4 Impact on alarm system

Alarm justification should ensure that

- a) the alarm will not become a nuisance, and
- b) the alarm does not duplicate another alarm that has the same operator actions.

Advanced alarming techniques (e.g., state based alarming or logic based alarms) can be specified to prevent negative impact on the alarm system.

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 5), 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 (e.g., fire and gas alarms) and the shortest allowable response times. Distribution metrics for priority are provided in Clause 16.

Prioritization may include consideration for alarm classes (e.g., HMA classes) or identification methods, (e.g., LOPA) to set alarm priority.

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 by the MOC procedure to remove the alarm from the system.

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.

Alarms in the same class are not required to have the same priority. 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 Use of 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, and
- e) evaluation of alarm monitoring and effectiveness data.

10 Detailed design: Basic alarm design

10.1 Purpose

Basic alarm design is part of the detailed design stage of the lifecycle. Clause 10 presents the essential requirements to implement the alarms defined by the rationalization process within a specific control system. Clause 10 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

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, and
- c) the HMI.

10.2.2 Alarm states and other logic functions

Clear design guidance should be provided regarding the use of alarm state information with other logic functions, (e.g., 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 can be impacted. Additionally the impact of modifying alarm 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.

10.2.3 Alarm suppression and other logic functions

The alarm suppression functionality shall not bypass other logic functions (e.g., interlock actions).

10.3 Alarm types

An alarm type should be assigned to each alarm defined during rationalization. The alarm type is defined to give the operator a visual distinction of the alarm. The common alarm types may include the following:

- 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-alarmed 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 could 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 abnormal conditions if they are not applied appropriately.

10.4 Alarm attributes

10.4.1 General

During the basic design process the default alarm attributes should be configured for each alarm that has been identified during rationalization and set based on engineering judgment. Attributes such as setpoint and deadband can be different depending upon the specific alarm type that will be implemented. Defining appropriate alarm attributes 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 subclauses. Alarm attributes should include;

- a) alarm setpoint or logical conditions,
- b) alarm type,
- c) alarm priority,
- d) alarm group,
- e) on-delay or off-delay
- f) deadband, and

g) alarm message.

10.4.2 Alarm description

All alarms shall have an informative text provided as a tag description, or alarm description, or both. The use of a structured layout and consistent wording are recommended.

10.4.3 Alarm setpoints

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

10.4.4 Alarm priority

Alarm priority shall be assigned based on the information documented in the master alarm database.

10.4.5 Alarm deadbands

10.4.5.1 General

Alarm deadband is an alarm attribute within the control system that requires the process variable to cross the alarm setpoint into the normal operating range by some defined increment or percentage of the range. 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.

10.4.5.2 Alarm deadband requirements

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

10.4.5.3 Alarm deadband recommendations

The engineering basis for the setting of deadbands should be documented in the alarm philosophy. 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 to 100) can act as a latch, creating stale alarms. Settings should be documented and then reviewed during commissioning and after significant operating experience.

10.4.6 Alarm on-delay and off-delay

10.4.6.1 General

The attributes on-delay and off-delay (i.e., debounce timer) can be used to eliminate nuisance alarms. The on-delay is used to avoid unnecessary alarms when a signal temporarily overshoots its setpoint, 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 the process condition has returned to normal.

10.4.6.2 Alarm on-delay and off-delay requirements

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

10.4.6.3 Alarm on-delay and off-delay recommendations

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 process response time during all modes of operation and whether filtering is being applied to reduce signal noise. On-delay times should be applied only after careful evaluation of potential control system operational effects. Settings should be reviewed during commissioning and after significant operating experience.

10.5 Programmatic changes to alarm attributes

Some sites modify alarm attributes based on conditions such as batch recipe, 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) advanced alarming techniques;
- e) external to the control system (e.g., manufacturing execution system (MES), enterprise resource planning (ERP) system).

The alarm philosophy should detail the use and limitations of this functionality. For each alarm the user should identify and clearly document which programs of the system will have access to modify alarm attributes during operation and which changes will be subject to management of change procedures. Advanced alarming techniques for modifying alarm attributes are covered in Clause 12.

10.6 Review basic alarm design

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 that only the required alarms exist.

11 Detailed design: Human-machine interface design for alarm systems

11.1 Purpose

The HMI design for alarm systems is part of the detailed design lifecycle stage. Clause 11 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 5). Guidance on general HMI design for control systems is outside the scope of this standard.

11.2 HMI functions

11.2.1 General

The HMI design for alarms should be consistent with the alarm philosophy and the overall HMI design philosophy. The capabilities of the control system should be considered in the HMI design.

11.2.2 HMI information requirements

The HMI shall clearly indicate:

- a) active alarms,
- b) alarm states,
- c) alarm priorities, and
- d) alarm types.

11.2.3 HMI functional requirements

The HMI 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,
- e) initiate an alarm shelving function,
- f) display alarm messages, and
- g) assign alarms to operator stations.

11.2.4 HMI display requirements

The HMI shall provide the capability for the following, or equivalent:

- a) alarm summary displays,
- b) alarm indications on process displays,
- c) alarm indications on tag detail display,
- d) shelved alarm summary displays, and
- e) out-of-service summary displays.

11.2.5 Alarm records requirements

An alarm record is a set of information which documents an alarm state change.

An alarm record shall have the following alarm record attributes:

- a) tag name for alarm,
- b) tag description or alarm description for alarm,
- c) alarm state,
- d) alarm priority,
- e) alarm type, and
- f) time and date of occurrence of the alarm state change.

11.2.6 Alarm records recommendations

An alarm record should have the following alarm record elements:

- a) process value at the time when the alarm record is recorded,
- b) alarm setpoint,
- c) process area,
- d) alarm group, and
- e) alarm message.

11.3 Alarm states indications

11.3.1 General

The alarm state transition diagram (see Figure 3) defines the states of alarms.

11.3.2 Required alarm state indications

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

- a) normal,
- b) unacknowledged alarm,
- c) acknowledged alarm,
- d) return-to-normal unacknowledged alarm,
- e) shelved alarm,
- f) suppressed-by-design alarm, and
- g) out-of-service alarm.

11.3.3 Recommended alarm state indications

11.3.3.1 General

The following recommended alarm state indications are common industry practice.

11.3.3.2 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.

11.3.3.3 Unacknowledged alarm state indication

The unacknowledged alarm state should use both an audible indication 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 colours 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.

11.3.3.4 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 colour to the unacknowledged alarm indication. A blinking element should not be used in the visual indication for an acknowledged alarm.

11.3.3.5 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.

11.3.3.6 Shelved alarm state indication

The shelved alarm state 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. No audible indication should be used to identify shelved alarms.

11.3.3.7 Suppressed-by-design alarm state indication

The suppressed-by-design alarm state 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.

11.3.3.8 Out-of-service alarm state indication

The out-of-service alarm state 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.

11.3.3.9 Summary of alarm state indications

The recommended audible and visual alarm state indications for typical alarms are summarized in Table 4.

Table 4 – Recommended alarm state indications

Alarm state	Audible indication	Visual indications		
		Colour	Symbol	Blinking
Normal	No	No	No	No
Unacknowledged alarm	Yes	Yes	Yes	Yes
Acknowledged alarm	No	Yes	Yes	No
Return-to-normal unacknowledged alarm	No	Combination		Optional
Shelved alarm	No	Combination		No
Suppressed-by-design alarm	No	Combination		No
Out-of-service alarm	No	Combination		No
Yes signifies the indication type should be used to indicate the alarm state.				
No signifies the indication type should not be used to indicate the alarm state.				

11.3.4 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

11.4.1 General

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.

11.4.2 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.

11.4.3 Colour alarm priority indications requirements

A separate colour indication shall be used for each alarm priority, except in operating environments where this is not practical. The alarm priority colours shall be reserved and shall not be used for other elements of the HMI.

11.4.4 Recommended alarm priority indications

11.4.4.1 General

The following recommended alarm priority indications are common industry practice.

11.4.4.2 Symbol alarm priority indications

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

11.4.4.3 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

11.5.1 General

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

11.5.2 Recommended alarm message indications

11.5.2.1 General

The following recommended alarm message indications are common industry practice:

- a) visual alarm message indications, and
- b) vocalized alarm message indications.

11.5.2.2 Visual alarm message indications

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

11.5.2.3 Vocalized alarm message indications

A vocalized alarm message, using a voice synthesizer, can be used. The vocalized alarm message should be structured and brief. The vocalized alarm 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

11.6.1 General

Within an HMI there are several types of displays that are effective as part of the alarm system. These include the following:

- a) alarm summary display,
- b) alarm summary status display,
- c) alarm log display,
- d) process display,
- e) tag detail display,
- f) system diagnostic alarm display,

- g) shelved alarm display,
- h) out-of-service alarm display, and
- i) suppressed-by-design alarm display.

11.6.2 Alarm summary display

11.6.2.1 Alarm summary display requirements

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

11.6.2.2 Information requirements

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

- a) tag name for alarm,
- b) tag description or alarm description for alarm,
- c) the alarm state (including acknowledged status),
- d) the alarm priority,
- e) the time/date the alarm became active, and
- f) the alarm type.

11.6.2.3 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, and
- e) the alarm message.

11.6.2.4 Additional information recommendations

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

- a) the number of alarms in the summary list, and
- b) the number of unacknowledged alarms in the summary list.

11.6.2.5 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, and
- d) acknowledgment of visible alarms.

11.6.2.6 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) filtering of alarms by tag name,
- h) time limits for filters, and
- i) sorting of alarms by tag name.

Where filters are used in alarm summary displays the display should clearly indicate when a filter is in use. The time limit is a function that removes the filter when the time period expires.

11.6.3 Alarm summary status

11.6.3.1 General

An alarm summary status display is recommended. The alarm summary status display provides an indication of the number of active alarms by priority for each process area.

11.6.3.2 Information recommendations

The alarm summary 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, and
- c) an indication if all alarms in a priority are acknowledged.

11.6.3.3 Functional recommendations

The alarm summary status display should provide a navigational link to the appropriate process display.

11.6.4 Alarm log displays

11.6.4.1 General

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.).

11.6.4.2 Information recommendations

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

- a) tag name for alarm,
- b) tag description or alarm description for alarm,
- c) the alarm state (including acknowledged status),
- d) the alarm priority,
- e) the date and time of the alarm,
- f) the date and time of acknowledgment,
- g) the date and time of the return to normal, and
- h) the alarm type.

11.6.4.3 Functional recommendations

The alarm log display should provide the following functions:

- a) filtering of alarms by tag name,
- 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, and
- f) filtering of alarms by process area.

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 name (through text or other access methods),
- b) the alarm state, including acknowledge status,
- c) the alarm priority,
- d) the alarm suppression status, and
- e) the alarm type.

11.6.6 Tag detail displays

The tag 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, and
- g) the current value of the process variable or state.

11.6.7 Other display elements

Other display elements may be used to indicate alarm states.

11.7 Alarm shelving

11.7.1 General

The temporary shelving of alarms by the operator is a function used to keep nuisance alarms from interfering with the effectiveness of the alarm system. Shelving includes a functionality to ensure the integrity of the alarm system is maintained.

11.7.2 Alarm shelving functional requirements

The alarm shelving function shall provide the following:

- a) the ability to shelve alarms,
- b) displays of shelved alarms or equivalent list capabilities, to indicate all alarms shelved,
- c) a time limit for shelving,
- d) access control for shelving of individual alarms,
- e) the ability to unshelve alarms, and
- f) a record of each alarm shelved.

The time limit is a function that unshelves the alarm when the time period expires.

11.7.3 Alarm shelving functional recommendations

The alarm shelving function should be designed to prevent alarm floods when active alarms are automatically unshelved.

- a) a manually unshelved alarm should transition to the acknowledged alarm state, and
- b) an automatically unshelved alarm should transition to the unacknowledged alarm state.

11.7.4 Shelved alarm displays

11.7.4.1 General

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

11.7.4.2 Information requirements

Shelved alarm displays shall provide the following information:

- a) tag name for alarm,
- b) tag description or alarm description for alarm,
- c) alarm type,
- d) the alarm status (i.e., active or not active),
- e) the alarm priority, and
- f) the shelved time remaining or the time and date the alarm was shelved.

11.7.4.3 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) sorting of alarms by tag, and
- d) individual unshelving of alarms.

11.7.4.4 Functional recommendations

Shelved alarms displays should provide the following functions:

- a) filtering of alarms by priority,
- b) filtering of alarms by alarm state,
- c) filtering of alarms by process area,
- d) operator entry of the reason the alarm was shelved,
- e) group unshelving of alarms,
- f) navigational link to a process display, and
- g) navigational link to the tag detail display.

11.8 Out-of-service alarms

11.8.1 General

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.

11.8.2 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 alarms out of service,
- d) access control to place alarms out of service if allowed, and
- e) a record of each alarm placed out of service.

11.8.3 Out-of-service alarm displays

11.8.3.1 Out-of-service alarm display requirements

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.

11.8.3.2 Information requirements

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

- a) tag name for alarm,
- b) tag description or alarm description for alarm,
- c) alarm type,
- d) the unsuppressed alarm status (i.e., active or not active),
- e) the alarm priority, and
- f) the time and date the alarm was placed out of service.

11.8.3.3 Functional requirements

Out-of-service alarm displays shall 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 status (i.e., active or not active),
- d) sorting of alarms by process area, and
- e) individual return to service of alarms.

11.8.3.4 Functional recommendations

Out-of-service alarm displays should provide the function for operator entry of the reason the alarm was suppressed.

11.9 Alarms suppressed by design

11.9.1 General

The designed suppression of alarms is common practice to suppress alarms that are not needed due to intended or actual operating conditions.

11.9.2 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, and

b) a record of each alarm suppressed by design.

11.9.3 Design suppression functional recommendations

The design suppression function should be designed to prevent alarm floods when active alarms are automatically unsuppressed.

An automatically unsuppressed alarm should transition to the unacknowledged alarm state.

11.9.4 Suppressed-by-design displays

11.9.4.1 General

Suppressed-by-design displays, or equivalent list capabilities, shall be provided for the alarm system. Suppressed-by-design displays have several required and recommended functions.

11.9.4.2 Information requirements

Suppressed-by-design displays shall provide the following information:

- a) tag name for alarm,
- b) tag description or alarm description for alarm,
- c) alarm type,
- d) the unsuppressed alarm status (i.e., alarm status active or not active),
- e) the alarm priority, and
- f) the time and date the alarm was suppressed.

11.9.4.3 Information recommendations

Suppressed-by-design displays should provide an indication of the suppression method (e.g., designed suppression).

11.9.4.4 Functional requirements

Suppressed-by-design displays shall 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, and
- d) sorting of alarms by process area.

11.10 Alarm annunciator integration

11.10.1 General

Alarm systems may include separate alarm annunciation devices. Subclause 11.10 describes recommendations for integration of independent annunciators into an alarm system.

11.10.2 Alarm annunciator integration recommendations

Alarm annunciators should be integrated to provide the following functions:

- a) communication of alarm state information to the alarm log,
- b) prevention of redundant alarms in the control system, and
- c) prevention of the need for redundant acknowledgement in the control system.

11.10.3 Alarm annunciator display integration recommendations

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

11.11 Safety alarm HMI

11.11.1 General

An independent HMI can be required for some safety alarms by code or standards. The identification methods for safety alarms are outside the scope of this standard.

11.11.2 Independent safety alarm HMI

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

- a) safety related alarms, depending on considerations (e.g., the risk reduction factor), and
- b) system diagnostic alarms from the SIS that indicate dangerous faults, depending on considerations (e.g., the operator response, communication fault).

NOTE For further guidance see IEC 61511.

12 Detailed design: Enhanced and advanced alarm methods

12.1 Purpose

Enhanced and advanced alarming is part of the detailed design lifecycle stage. Clause 12 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 are particularly useful to guide operator action during abnormal process conditions.

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

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

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

12.2 Basis of enhanced and advanced alarming

12.2.1 General

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.

12.2.2 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.

Risk analysis of failure scenarios for enhanced and advanced alarming techniques should be considered before approval and during design.

12.3 Information linking

Alarm systems can be enhanced by linking to 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.

12.4 Logic-based alarming

12.4.1 General

Logic-based alarming is accomplished using Boolean logic or decision trees to determine the modifications to be made to alarm systems.

12.4.2 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.

12.4.3 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.

12.4.4 Logical alarm suppression and 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).

12.4.5 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) the status of a logical variable,
- b) a defined process variable which reaches a specific limit,
- c) logic that looks at many variables and indicators, and
- 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. The state should be clearly displayed to the operator.

12.5 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 can produce a result based on multiple data points, or where an estimation of plant state can be derived from a model.

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

12.6 Additional alarming considerations

12.6.1 General

Some additional enhancements add value to the alarm system. These enhancements can be normally available in the basic alarm system.

12.6.2 Non-control room considerations

Where the operators are expected to respond to alarms while completing non-control room based tasks, remote alarm display and acknowledgement can be considered. Procedures to direct alarms to a back-up operator may be necessary. Where remote alarm systems are used, the alarm philosophy should include these systems.

The use of remote alarm notification practices should include periodic test messages to improve reliability. A procedure to ensure response to the alarm should be considered.

12.6.3 Remote alarm 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 alarm system (e.g., paging, e-mail, etc.).

The reliability of the message delivery is a significant issue in remote alarm systems and should be considered. It may be necessary to also provide remote acknowledgement.

12.6.4 Supplementary alarm systems

Supplementary alarm systems (e.g., expert system for alarm response) can replace the control system alarm notification system or make use of the existing graphics environment to provide a common interface. Alternatively, systems can 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. The system should be designed to ensure alarm availability and reliability are acceptable.

Where a supplementary alarm system is used it shall comply with the all requirements of this standard.

12.6.5 Batch process considerations

12.6.5.1 General

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

12.6.5.2 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 alarming techniques can provide a structure for addressing these types of batch-related alarm problems.

12.6.5.3 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.

12.6.5.4 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 the official batch records of a production run and in comparing records of different production runs. The methods of extracting and attaching such identifying marks should be proven and reliable.

12.7 Training, testing, and auditing systems

The alarm philosophy should specify steps to ensure advanced alarming techniques continue to operate, including training, testing, and auditing. Training, testing, and auditing procedures should include the enhanced and advanced alarming techniques.

12.8 Alarm attribute enforcement

To maintain the designed alarm attribute settings (e.g., alarm setpoints, and alarm priorities) 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 alarming or alarm shelving methodologies.

13 Implementation

13.1 Purpose

Implementation is a separate stage of the alarm lifecycle which is the transition from design to operation. Clause 13 covers general requirements to implement or modify an alarm or alarm system.

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 competent resources,
- c) functional testing or validation,
- d) verification of documentation, and
- e) operator training.

13.3 Implementation training

13.3.1 General

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.

13.3.2 Implementation training

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

13.3.3 Implementation training requirements

The training shall include:

- a) the rationalization information of the alarm (e.g., consequence, causes for alarm, corrective action, etc.), and
- b) the audible and visual indications for the alarm.

13.3.4 Training documentation requirements for highly managed alarms

Documentation of the training for new or modified highly managed alarms shall include

- a) the persons trained,
- b) the method of training, and
- c) the date of the training.

13.3.5 Training documentation recommendations

Documentation of the training should include

- a) the persons trained,
- b) the method of training, and
- c) the date of the training.

13.3.6 Implementation training requirements for new or modified alarm systems

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

13.3.7 Implementation 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 the 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 methods for shelving and suppression, and
- e) the methods for removing an alarm from service.

13.4 Implementation testing and validation

13.4.1 General

Implementation 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.

13.4.2 Implementation 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 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, and
- i) the date the alarm was put into service.

13.4.3 Implementation 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, and
- d) any other functional requirement for the alarm as specified.

13.4.4 Implementation 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 a modified alarm system shall be appropriate to the nature of the change, as determined by site MOC procedures. The testing of new alarm systems shall include:

- a) the audible and visual indications for each alarm priority,
- b) the HMI features, such as alarm messages in the alarm summary or equivalent,
- c) the methods for removing an alarm from service and returning an alarm to service
- d) the methods for shelving,
- e) the methods for alarm suppression,
- f) any additional functions of enhanced or advanced alarming techniques, and
- g) the methods of alarm filtering, sorting, linking of alarms to process displays.

13.5 Implementation documentation

13.5.1 General

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

13.5.2 Documentation requirements

The following documentation shall be provided:

- a) the rationalization information documented,
- b) sufficient information to perform testing of alarms,
- c) the alarm response procedures, and
- d) any designed suppression or enhanced alarming documentation.

Upon completion of the alarm system implementation, the rationalization information shall be updated in accordance with the site MOC procedure.

13.5.3 Implementation documentation recommendations

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

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

Information used in testing new and modified alarms may include the following:

- a) tag name for alarm,
- b) tag description or alarm description for alarm,
- c) alarm type,
- d) priority,
- e) alarm setpoint value or logical condition,
- f) operator action,
- g) consequence of inaction,
- h) date of testing and change,
- i) method of testing and acceptance criteria, and
- j) results of the testing and resolution of any failures or non-compliance.

14 Operation

14.1 Purpose

Operation is a separate stage of the alarm management lifecycle. Clause 14 covers requirements for alarms to remain in and return to the operational state. The operational state is when an alarm is able to indicate an abnormal condition to the operator. The use of tools for alarm handling within the operational state is also described. Operation is the lifecycle stage following implementation and when returning from maintenance.

14.2 Alarm response procedures

14.2.1 Alarm response procedures requirements

Alarm response procedures shall be readily accessible to the operator.

14.2.2 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 tag name for alarm,
- b) the tag description or alarm description for alarm,
- c) the alarm type,
- d) the alarm setpoint,
- e) the potential causes,
- f) the consequence of inaction,
- g) the operator action,
- h) the allowable response time, and
- i) the alarm class.

14.3 Alarm shelving

14.3.1 Alarm shelving requirements

Alarm shelving shall be allowed as documented by the class of the alarm as detailed in the alarm philosophy.

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.

Documentation shall be maintained, including approval, interim alarms and procedures, and reauthorization details.

14.3.3 Alarm shelving recommendations

Shelved alarms extending beyond a single operating shift should be reviewed. Review requirements for shelving alarms should be documented in the alarm philosophy.

14.3.4 Alarm shelving record requirements

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

- a) the tag name for alarm,
- b) the tag description or alarm description for alarm, and
- c) the reason for shelving.

14.4 Refresher training for operators

14.4.1 Refresher training requirements 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.

14.4.2 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, and
- d) the history of 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.

14.4.3 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 rationalization information of the alarm, and
- b) the audible and visual indications for the alarm.

14.4.4 Refresher training recommendations for alarms

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

- a) the rationalization information of the alarm, and
- b) 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 alarm management lifecycle. Clause 15 covers requirements for alarm system testing, replacement-in-kind, and repair. It describes the transition of alarms to the out-of-service state and then return to service. Maintenance also requires refresher training for personnel maintaining the alarm system.

15.2 Periodic alarm testing

15.2.1 General

Periodic alarm testing requirements shall be determined by the alarm class requirements as detailed in the alarm philosophy. The purpose of periodic testing is to ensure that the alarm continues to perform as designed.

15.2.2 Periodic alarm testing requirements

When tests are performed, a record shall be kept for a period specified in the alarm philosophy. The records 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, and equipment number),
- d) result of tests (e.g. the as-found and as-left conditions),
- e) a reference to the testing procedure and methods used, and
- f) cause of test failures.

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

15.2.3 Periodic alarm testing for highly managed alarms

If highly managed alarm classes are used then alarms belonging to these classes shall be periodically tested to ensure performance.

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

15.2.4 Periodic alarm test procedure requirements

Test procedures shall be provided for alarms requiring testing.

15.2.5 Periodic alarm test procedure recommendations

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.

15.2.6 Periodic alarm testing recommendations

Test records should contain the following:

- a) method of testing, and
- b) planned interval before next test.

Any deficiencies found during periodic alarm testing should be repaired in a timely manner.

15.3 Out-of-service alarms

15.3.1 General

Requirements for the out-of-service procedure shall be determined by the alarm class requirements as detailed in the alarm philosophy.

15.3.2 Out-of-service process requirements

Alarms that are placed out of service for extended periods (e.g., days, weeks, or months) shall be examined to determine if an interim alarm or procedure is necessary.

An authorization and documentation process (e.g., permit process) shall be used to take an alarm out of service.

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

15.3.3 Out-of-service highly managed alarms

If a highly managed alarm is taken out of service, appropriate interim alarms or procedures shall be identified considering risk reduction requirements and the plant state.

15.3.4 Out-of-service process recommendations

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

15.3.5 Requirements for 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.

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

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

The site management of change procedures should address replacement equipment (e.g., measurement devices, valves, process equipment) that will change alarm attributes. 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 Refresher training for maintenance

15.6.1 General requirements

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

15.6.2 Refresher training requirements for highly managed alarms

If a highly managed alarm class is used then 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. The documentation of the training shall be retained for the period specified in the alarm philosophy or per company policy.

15.6.3 Refresher training recommendations for alarms

Maintenance personnel should receive refresher 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. Clause 16 provides guidance on the use of alarm system analysis for both on-going monitoring and periodic performance assessment. These activities use many of the same types of measures. Several performance measures are recommended 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 target performance levels in the alarm philosophy.

16.3 Monitoring, assessment, audit, and benchmark

The terms monitoring, assessment, audit, and benchmark are used in the following context.

- Monitoring is the measurement and reporting of quantitative (objective) aspects of alarm system performance.
- Assessment is the comparison of information from monitoring and additional qualitative (subjective) measurements, against stated goals and defined performance metrics.
- Audit is a comprehensive assessment that includes the evaluation of the effectiveness of the work practices used to manage the alarm system.

- Benchmark is an initial audit of an alarm system designed to specifically identify problem areas for the purpose of developing 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 well. The evaluation of work processes relative to the alarm system is covered in Clause 18.

16.4 Alarm system monitoring

Performance monitoring 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. On-going performance measurement can determine when corrective action is needed.

When alarms have been 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 can 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

16.5.1 General

Various types of alarm system analyses, key performance indicators, and methods are possible. Both initial alarm system assessment and on-going monitoring should include the measures like those shown in Table 7. The entire list of chosen analyses should reflect decisions made in the alarm philosophy.

The two categories of data in a typical 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 alarm types, alarm setpoints, priorities, deadbands, and similar items.

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

The target metrics described below 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.

16.5.2 Average alarm rate per operator console

Analysis of alarm rate (i.e. annunciated alarm rate) is a good indicator of the overall health of the alarm system. Recommended targets for the average alarm rate per operator console (i.e., the span of control and alarm responsibility of a single operator) based upon one month of data are shown in Table 5. These rates are based upon the ability of an operator and the time necessary to detect an alarm, diagnose the situation, respond with corrective action(s), and monitor the condition to verify the abnormal condition has been corrected.

Table 5 – Average alarm rates

Very likely to be acceptable	Maximum manageable
~144 alarms per day	~288 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)

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

A period of time that produces more alarms than the operator can handle, increases the likelihood of missed alarms, even if the average for that interval is acceptable.

16.5.3 Peak alarm rate per operator console

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 are not sustainable by an operator for long periods.

For peak alarm rate analysis, annunciated alarms are counted in regular 10-minute intervals (e.g., 13:00 through 13:09). 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 number of intervals exceeding 10 alarms and the magnitude of the highest peaks should be reported.

16.5.4 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 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 time.

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,
- b) duration of each alarm flood,
- c) alarm count in each alarm flood, and
- d) peak alarm rate for each alarm flood.

Advanced alarming techniques can mitigate alarm floods. Alarm floods may require advanced methodologies to address. These techniques are described in Clause 12.

16.5.5 Frequently occurring alarms

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 correctly 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 correct functioning and design.

16.5.6 Chattering and fleeting alarms

A chattering alarm repeatedly transitions between the alarm state and the normal state in a short period of time. Fleeting alarms are similar short-duration alarms that do not immediately repeat. In both cases, the transition is not due to the result of 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 behaviours should be eliminated. There is no long-term acceptable quantity of chattering or fleeting alarms.

16.5.7 Stale alarms

Alarms that remain active continuously for more than 24 hours can be considered as stale alarms. Advanced alarming techniques can be used to eliminate stale alarms.

There should be less than five stale alarms.

16.5.8 Annunciated alarm priority distribution

Effective use of alarm priority can enhance the ability of the operator to manage alarms and provide response. The effectiveness of alarm priority is related to the distribution of the alarm priorities: higher priorities should be used less frequently.

Table 6 – Annunciated alarm priority distribution

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

Some alarm systems use an additional highest priority for a few alarms with severe consequences.

Additional priorities can be useful, such as a lowest priority for instrument diagnostic alarm with very limited operator action. There is no recommended frequency or percentage

distribution for diagnostic alarms, since there is no recommended frequency for instrument failure. Low numbers are better.

Various priorities with limited annunciation (e.g., not audible 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.

16.5.9 Alarm priority distribution

An effective alarm rationalization effort will produce an annunciated alarm priority distribution similar to Table 6. The annunciated alarm priority distribution will not match rationalized alarm priority distributions since all alarms are not equally likely to occur. For alarm systems that do not allow prioritization of instrument or system diagnostic alarms, these alarms can be excluded from the priority distribution calculations to prevent a skewed distribution.

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. Unauthorized suppression of alarms should be detected and reported. The potential for mistakes and the resulting risk are high.

Alarm state transitions to suppressed states and from suppressed states should be recorded. Analysis methods should be used to detect and report any alarms suppressed outside of these methods. There should be no alarms that are suppressed without authorization.

16.7 Alarm attribute monitoring

Unauthorized alarm attribute changes shall be detected and resolved by comparison of actual alarm attributes against rationalization information. Discrepancies shall be identified and resolved quickly. The target value for unauthorized changes to alarms is zero.

16.8 Reporting of alarm system analyses

Alarm system analyses should be reported to personnel (e.g., operators, staff and managers) concerned with the alarm system at the appropriate frequency.

At various phases of an improvement effort, different analyses should be performed at different reporting periods (e.g., providing weekly reports at the start of an effort and monthly reports later on). Weekly analyses can 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. The 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 Table 7.

Table 7 – Recommended alarm performance metrics summary

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 operator console	~144 alarms per day	~288 alarms per day
Annunciated alarms per hour per operator console	~6 (average)	~12 (average)
Annunciated alarms per 10 minutes per operator console	~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 (e.g. system diagnostic alarms) 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.	

17 Management of change

17.1 Purpose

Management of change is a separate stage of the lifecycle. Clause 17 covers requirements for alarm system changes pertaining to the addition of new alarms, removal of existing 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 lifecycle activities are applied to alarm system changes.

17.2 Changes subject to management of change

The addition or removal of alarms and the modification of specified attributes shall require authorization through a management of change procedure. Permanent changes that result in a difference from the authorized values of the alarm setpoint, class, priority, consequence, basis, suppression logic, or response time shall require evaluation through the MOC procedure.

The MOC procedure shall ensure that the following considerations are addressed:

- a) the technical basis for the proposed change,
- b) the 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 activities, and
- j) implementation of all changes adhere to procedures specified in the alarm philosophy.

17.3 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) the reason for the change,
- b) the date the change was made,
- c) the name of the person implementing the change,
- d) the name of the person authorizing the change,
- e) the nature of the change (i.e., the before and after),
- f) the training requirements, and
- g) testing requirements.

17.4 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.

17.5 Alarm removal recommendations

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

17.6 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 the 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 can 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 against procedures and reviewing procedures against 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 Benchmark

18.2.1 General

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.

18.2.2 Initial audit or benchmark requirements

The audit frequency and the specific audit requirements stated in the alarm philosophy shall be followed for all alarms, as required by alarm class.

The audit shall address all applicable requirements of this standard.

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 conditions 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 defined, and
- e) training regarding the 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 all related 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, and
- f) 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.

Bibliography

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

IEC 62241, *Nuclear power plants – Main control room – Alarm functions and presentation*

IEC 62541-9, *OPC unified architecture – Part 9: Alarms and conditions*

Alarm Management, NAMUR-Worksheet NA 102, 3rd Edition, NAMUR-Geschäftsstelle, Leverkusen, Germany (2008)

ANSI/ISA-18.02-2009, *Management of Alarm Systems for the Process Industries*

Engineering Equipment Materials Users' Association, Alarm Systems – A Guide to Design, Management and Procurement, EEMUA Publication No. 191, 2nd Edition, EEMUA, London, UK (2007).

Engineering Equipment Materials Users' Association, *Alarm Systems. – A Guide to Design, Management and Procurement*. EEMUA Publication No. 191, 2nd edition. London: EEMUA, 2007

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards-based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services

Tel: +44 845 086 9001

Email (orders): orders@bsigroup.com

Email (enquiries): cservices@bsigroup.com

Subscriptions

Tel: +44 845 086 9001

Email: subscriptions@bsigroup.com

Knowledge Centre

Tel: +44 20 8996 7004

Email: knowledgecentre@bsigroup.com

Copyright & Licensing

Tel: +44 20 8996 7070

Email: copyright@bsigroup.com



...making excellence a habit.™