IEC 62682

Edition 2.0 2022-12
COMMENTED VERSION

INTERNATIONAL STANDARD

colour inside

Management of alarm systems for the process industries

IEC 62682:2022-12 CMV(en)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC 62682

Edition 2.0 2022-12
COMMENTED VERSION

INTERNATIONAL STANDARD

colour inside

Management of alarm systems for the process industries

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.320; 25.040.40

ISBN 978-2-8322-6270-2

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

MANAGEMENT OF ALARM SYSTEMS FOR THE PROCESS INDUSTRIES

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

This commented version (CMV) of the official standard IEC 62682:2022 edition 2.0 allows the user to identify the changes made to the previous IEC 62682:2014 edition 1.0. Furthermore, comments from IEC SC 65A experts are provided to explain the reasons of the most relevant changes, or to clarify any part of the content.

A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text. Experts' comments are identified by a blue-background number. Mouse over a number to display a pop-up note with the comment.

This publication contains the CMV and the official standard. The full list of comments is available at the end of the CMV.

IEC 62682 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

This second edition cancels and replaces the first edition published in 2014. This edition constitutes a technical revision.

This edition includes minor technical changes with respect to the previous edition, based on changes to ANSI/ISA-18.2:2016. These include the inclusion of packaged systems in the scope (Clause 1), definitions (Clause 3) and alarm system requirements specification (Clause 7). There are changes to improve clarity in wording throughout the document.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65A/1046/FDIS	65A/1064/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

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~~ management life cycle. This document 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 life cycle. Ineffective alarm systems have often been cited as contributing factors in the investigation reports following major process incidents. This document is intended to provide a methodology that will result in the improved safety, quality, and operation in the process industries.

The first edition of this document 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. This second edition has incorporated some changes made in ANSI/ISA-18.2-2016.

This document 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*, with the 2nd edition published in 2007 and the 3rd edition published in 2013. In 2003 the User Association of Process Control Technology in Chemical and Pharmaceutical Industries (NAMUR) issued worksheet NA 102, *Alarm Management*, which was updated in 2008. During the development and maintenance of this document, 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~~ install 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 document 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).~~

The first part (Clause 1 to Clause 3) are normative without any mandatory requirements. Clause 4 contains mandatory requirements. Clause 5 is normative without any mandatory requirements. The main body of the standard (Clause 6 to Clause 18), describes mandatory requirements and non-mandatory recommendations.

Within this document, mandatory requirements are stated with "shall", non-mandatory recommendations are stated with "should", and permissible requirements are stated with "may". The phase "is required" indicates the requirement has been stated previously in the document.

MANAGEMENT OF ALARM SYSTEMS FOR THE PROCESS INDUSTRIES

1 Scope

1.1 General applicability

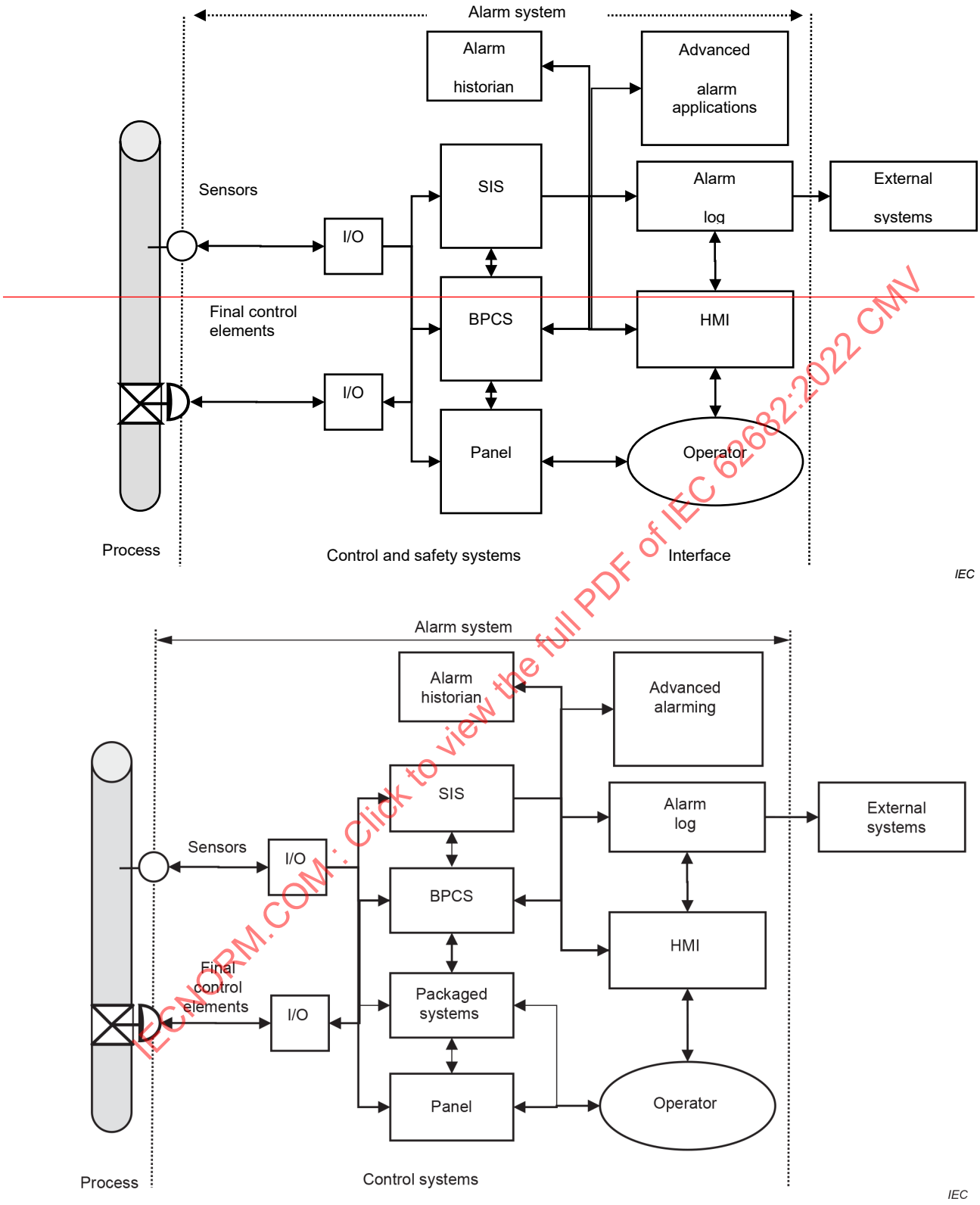
This document specifies general principles and processes for the ~~lifecycle~~ management of alarm systems based on ~~programmable electronic controller and computer-based human-machine interface (HMI) technology~~ controls system and human-machine interfaces (HMI) **1** for facilities in the process industries. It covers all alarms to be presented to the operator through the control system, which includes alarms from basic process control systems, annunciators ~~panels~~, packaged systems, and safety instrumented systems, ~~fire and gas systems, and emergency response systems~~ **2**.

The practices in this document 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.~~ **3**

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.

Figure 1 is not intended to represent physical wiring. **4**



NOTE 1 Packaged systems (e.g., refrigeration machines) can be included in the control system.

NOTE 2 Panel can refer to annunciator panel or other panel types.

NOTE 3 The lines are intended to represent data flow and not physical wiring. 5

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 document. Management of operators is excluded from the scope of this document.

1.2.2 Process sensors and final control elements

The alarms ~~from~~ implemented in sensors and final control elements are included in the scope of this document. ~~Process sensors and final control elements are shown in Figure 1 to indicate alarms can be implemented in these devices.~~ **6** The design and management of process sensors and final control elements are excluded from the scope of this document.

1.2.3 Annunciators

The integration of annunciators into an alarm system is included in the scope of this document. The specification and design of annunciators is excluded from the scope of this document.

1.2.4 Human machine interface

The appearance of alarms in the HMI and functions of alarm related displays are included in the scope of this document. The design and maintenance of the HMI are excluded from this document.

NOTE ANSI/ISA-101.01-2015 provides information on HMI design and maintenance.

1.2.5 Safety instrumented systems

The alarms ~~from~~ implemented in a safety instrumented system are included in the scope of this document. ~~The safety instrumented system (SIS) is shown in Figure 1 to indicate alarms can be implemented in these devices.~~ **7** The design and management of safety instrumented systems are excluded from this document.

NOTE IEC 61511-1 provides information on safety instrumented systems.

~~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.~~

1.2.6 Fire and gas detection and protective systems

The alarms from fire and gas detection and protective systems presented to the operator through the control system are included in the scope of this document. The design and management of fire and gas detection and protective systems is excluded from the scope of this document.

1.2.7 Security systems

The alarms from security systems presented to the operator through the control system are included in the scope of this document. The design and management of security systems is excluded from the scope of this document.

1.2.8 Packaged systems

The alarms from packaged systems presented to the operator through the control system are included in the scope of this document. The design and management of packaged systems is excluded from the scope of this document.

1.2.9 Event data

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

1.2.10 Alarm identification methods

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

1.2.11 Management of change

A specific management of change (MOC) procedure is not included in this document. Some requirements and recommendations for an MOC procedure are included.

1.2.12 Purchase specification

This document is not intended to be used as an alarm system purchase specification.

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.~~

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1 Terms and definitions

3.1.1
absolute alarm
alarm generated when the alarm setpoint is exceeded

EXAMPLE: High-high, high, low, low-low.

3.1.2
acknowledge
operator action that confirms recognition of an alarm

3.1.3
active
alarm state in which the alarm condition is true

Note 1 to entry: Functions such as deadband, on or off delays and latching can allow the alarm to be active when the alarm condition is false or the alarm to not be active when the alarm condition is true.

3.1.4
adaptive alarm
alarm for which the setpoint is changed by an algorithm ~~(e.g., rate based)~~

EXAMPLE: Setpoint calculated based on production rate.

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~~ priority.

3.1.10
alarm banner **8**
graphic element that lists annunciated alarms with selected information

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

Note 2 to entry: Information can include the date, time, priority, and alarm type.

3.1.11
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.

3.1.12
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

EXAMPLE: More than 10 alarms per 10 minutes.

3.1.14
alarm group
set of alarms with common association

EXAMPLE: Grouping alarms by 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

EXAMPLE: Message with operator action or probable cause. **9**

3.1.19
alarm off-delay
debounce
time ~~a process measurement remains in the normal state before the alarm becomes inactive~~ an alarm remains active after the process measurement has returned within the alarm setpoint

3.1.20
alarm on-delay
time ~~a process measurement remains in the alarm state before the alarm is annunciated~~ before an alarm becomes active after the process measurement has exceeded the alarm setpoint

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

EXAMPLE: Priority can use seriousness of consequences and allowable response time to determine urgency.

3.1.23
alarm rate
number of annunciated alarms, per operator, in a specific time interval

3.1.24
~~(~~alarm~~)~~ record
record
set of information which documents an alarm state change

3.1.25
alarm response procedure
guidance for response to an alarm

Note 1 to entry: The guidance can be in many forms and not only in the form of a procedure document.

Note 2 to entry: The guidance can include operator action, probable cause, and other information.

3.1.26
alarm setpoint
alarm limit
alarm trip point
threshold value of a process variable or discrete state that ~~triggers~~ is used to determine the active state of 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.

Note 2 to entry: Information can include the date, time, priority, and alarm type.

3.1.28
alarm system
~~operator support~~ system for generating and handling alarms ~~for managing~~ to help the operator manage abnormal situations **10**

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~~ describes the ~~details~~ functional requirements 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~~ and 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~~ **11**

3.1.31
allowable response time
maximum time between the annunciation of the alarm and when the operator ~~takes~~ must take corrective action to avoid the consequence

3.1.32
annunciator
device or group of devices that call attention to changes in process conditions

3.1.33
assessment
comparison of information from monitoring and additional qualitative (subjective) measurements against stated goals and defined performance metrics

3.1.34
audit <of alarm management>
comprehensive assessment that includes the evaluation of alarm system performance and ~~the effectiveness~~ **12** of the work practices used to administer the alarm system

3.1.35
bad-measurement alarm
alarm generated when the signal for a process measurement is outside the expected range

EXAMPLE: Bad-measurement alarm generated at 3,8 mA for a 4 mA to 20 mA signal.

3.1.36
basic process control system 13
BPCS
system which responds to input signals from the process, its associated equipment, other programmable systems and/or operators and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented function

Note 1 to entry: A BPCS includes all of the devices necessary to ensure that the process operates in the desired manner.

Note 2 to entry: A BPCS typically may implement various functions such as process control functions, monitoring, and alarms.

[SOURCE: IEC 61511-1:2016, 3.2.3, modified – “SIF” has been changed to "safety instrumented function"]

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, the operator console ~~display~~

EXAMPLE: Alarm annunciated via pager or telephone.

3.1.41
chattering alarm
alarm that repeatedly transitions between the ~~alarm~~ active state and the ~~normal~~ not active 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)~~

Note 1 to entry: Requirements can include testing, training, and auditing.

3.1.43
console
~~(~~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~~

hardware, software, and furniture or enclosure at which users monitor and/or control the process, which can include multiple stations, communication devices, and other devices

Note 1 to entry: The span of control of the operator is usually determined by the information available at the operator console.

3.1.44
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~~ one or more basic process control systems (BPCS), safety instrumented systems (SIS).

Note 2 to entry: The control system can include one or more packaged systems.

[SOURCE: IEC 61508-4:2010, 3.3.3, "EUC" has been deleted from the term defined, "from the process" has been changed to "from the equipment under control", "causing" has been changed to "that cause", notes have been modified] **14**

3.1.45
controller-output alarm
alarm generated from the output signal of a control algorithm instead of a direct process measurement

EXAMPLE: Alarm on output on PID controller.

3.1.46
decommission
process to remove an alarm from the alarm system

3.1.47
deviation alarm
alarm generated when the difference between two values exceeds ~~a limit~~ an alarm setpoint

EXAMPLE: Alarm on deviation between primary and redundant instruments or a deviation between process variable and controller setpoint.

3.1.48
discrepancy alarm
mismatch alarm
alarm generated by the difference between the expected plant or device state to its actual state

EXAMPLE: Alarm when a motor fails to start after it is commanded to the on state.

3.1.49
display
visual representation of information used by the operator for monitoring and control

3.1.50
dynamic alarming
automatic modification of alarm attributes based on process state or conditions

3.1.51
enforcement
enhanced alarming technique that can verify and restore alarm attributes in the control system to the values in the master alarm database

3.1.52
event
representation of a solicited or unsolicited fact indicating a state change

~~Note 1 to entry:~~ EXAMPLE: Mode changes and device state changes.

[SOURCE: IEC 62264-2:~~2004~~2013, 3.1.2, modified ~~– a note has been added~~ "in the enterprise" has been deleted and an example has been added.] **15**

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

Note 1 to entry: The first alarm is determined by logic.

3.1.54
fleeting alarm
alarm that transitions between an active alarm state and a not active alarm state in a short period of time without rapidly repeating

3.1.55
highly managed alarm
HMA
alarm belonging to a class with additional requirements above general alarms

Note 1 to entry: Regulatory requirements can be additional requirements.

EXAMPLE: Safety related alarm.

3.1.56
human machine interface
HMI
collection of hardware and software used by the operator and others to monitor and interact with the control system and with the process via the control system

3.1.57
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.

3.1.58
instrument diagnostic alarm
alarm ~~generated by a field device~~ to indicate a field device or signal fault ~~(e.g., sensor failure)~~

EXAMPLE: Out-of-range alarm.

3.1.59
interim alarm
alarm used on a temporary basis to replace an out-of-service alarm

3.1.60
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

3.1.61
master alarm database
authorized list of rationalized alarms and associated attributes

Note 1 to entry: The list can be in many forms and not only in the form of a database.

3.1.62
monitoring
measurement and reporting of quantitative (objective) aspects of alarm system performance

3.1.63
nuisance alarm
alarm that annunciates excessively, unnecessarily, or does not return to normal after the operator ~~response~~ action is taken

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

3.1.64
operator
controller
person who monitors and makes changes to the process

~~**3.1.65**~~
~~**operator station**~~
~~human-machine interface within the operator console~~

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

3.1.65
operator alert 16
audible and/or visible means of indicating to the operator an equipment or process condition for evaluation when time allows which could result in a response

3.1.66
out-of-service
state of an alarm during which the alarm indication is indefinitely suppressed, typically manually, for reasons such as maintenance

3.1.67
packaged system
self-contained combination of hardware and software that can provide alarm, HMI, and control functionality for a specific process function that is part of a facility

3.1.68
plant state
plant mode
defined set of operational conditions for a process plant

EXAMPLE: Shutdown, normal operation.

3.1.69
prioritization
process of assigning a level of operational importance to an alarm

3.1.70
process area
physical, geographical or logical grouping of resources determined by the site

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

3.1.71
rate-of-change alarm
alarm generated when the change in process variable per unit time (dPV/dt) exceeds a defined setpoint

3.1.72
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

3.1.73
re-alarming alarm
re-triggering alarm
alarm that is automatically re-annunciated ~~to the operator~~ **17** under certain conditions

3.1.74
recipe-driven alarm
alarm with setpoints that depend on the recipe that is currently being executed

3.1.75
remote alarm
alarm from a remotely operated facility or directed to a remote interface

3.1.76
reset
operator action that unlatches a ~~latched~~ latching alarm

3.1.77
return to normal
clear
alarm transition from an active ~~annunciated~~ alarm state to a not active ~~annunciated~~ alarm state

3.1.78
safety instrumented system
SIS
instrumented system used to implement one or more safety instrumented functions

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

Note 1 to entry: A SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s). It also includes communication and ancillary equipment (e.g., cables, tubing, power supply, impulse lines, heat tracing).

Note 2 to entry: A SIS may include software.

Note 3 to entry: A SIS may include human action as part of a SIF (see ISA TR 84.00.04:2015, part 1).

[SOURCE: IEC 61511-1:~~2003~~2016, ~~3.2.72~~ 3.2.67, modified – Removed figure from notes and reference to figure from note 1] **18**

3.1.79
safety related alarm
safety alarm
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~~ indicating a potential asphyxiation hazard. **19**

3.1.80
shelve
temporarily suppress an alarm, initiated by the operator, with engineering controls to unsuppress the alarm

Note 1 to entry: Engineering controls can include time limits.

3.1.81
silence
operator action that terminates the audible alarm indication

3.1.82
stale alarm
alarm that remains annunciated for an extended period of time

EXAMPLE: Alarm that remains annunciated for 24 hours.

3.1.83
state-based alarm
mode-based alarms
alarm that has attributes modified or is suppressed based on operating states or process conditions

3.1.84
statistical alarm
alarm generated based on statistical processing of a process variable or variables

3.1.85
suppress
prevent the annunciation of the alarm to the operator when the alarm is active

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

3.1.86
suppress~~ed~~ by design
alarm annunciation to the operator prevented based on plant state or other conditions

3.1.87
system diagnostic alarm
alarm generated by the control system to indicate a fault within the system hardware, software or components

EXAMPLE: Communication error.

3.1.88
tag
control system point
point
unique identifier assigned to a process measurement, calculation, or device within the control system

3.1.89
unacknowledged
alarm state in which the operator has not yet confirmed recognition of an alarm indication

3.1.90
unshelve **20**
transition from the shelved alarm state to the normal or unacknowledged state

3.1.91
unsuppress **20**
transition from a suppressed alarm state to the normal or unacknowledged state

3.2 Abbreviated terms

ACKED	Acknowledged
ASRS	Alarm system requirements specification
BPCS	Basic process control system
CGMP	Current good manufacturing practice
DSUPR	~~Designed suppression~~ Suppressed-by-design
~~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 document

4.1 Conformance guidance

To conform to this document, it shall be shown that each of the mandatory 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 document, 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 document shall be applied to existing systems in a reasonable time as determined by the owner/operator.

4.3 Use of required functionalities

This document requires certain control system functionalities (e.g., shelving) to support the alarm system. Where an alarm system does not have all required functionality, conformance may be achieved if the functionality described in the alarm philosophy is provided.

4.4 Responsibility

Conformance to this document is the responsibility of the owner/operator.

4.5 Local Jurisdictions

Some jurisdictions where the governing authorities (for example national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, in addition to the requirements of this document. **21**

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.

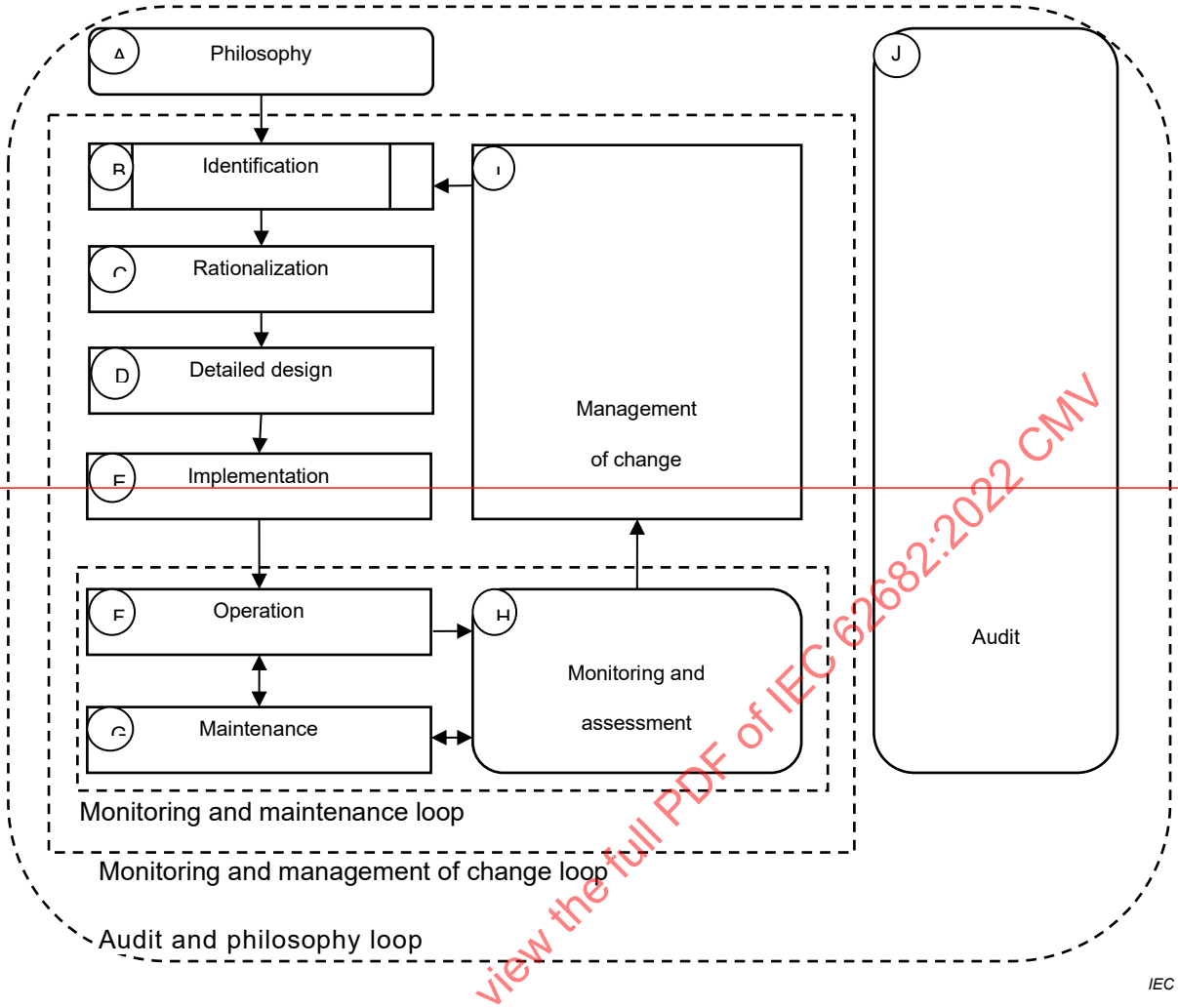
A foundational part of alarm management is the definition of an alarm: an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response. An essential element of this definition is the response to the alarm. This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

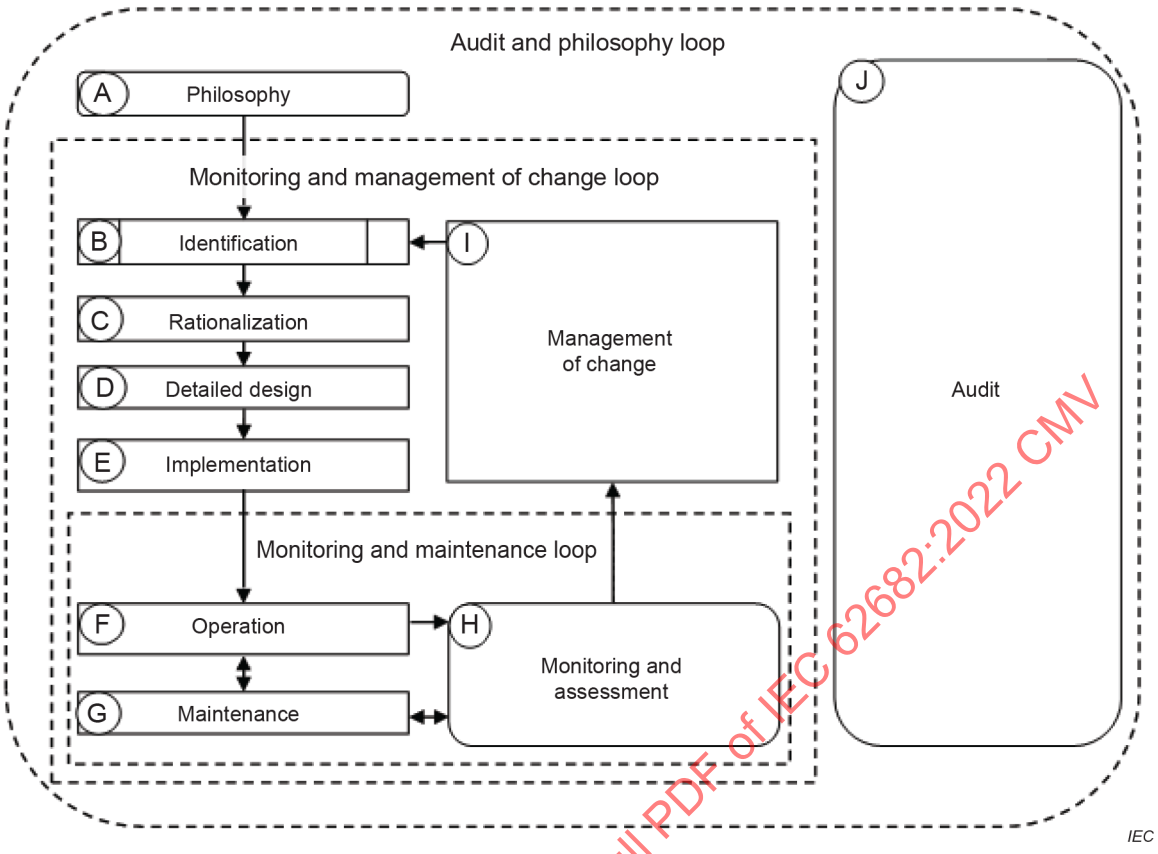
5.2 Alarm management life cycle

5.2.1 Alarm management life cycle model

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

The life cycle model is useful in ~~identifying~~ organizing the requirements and responsibilities for implementing ~~an~~ alarm management ~~system~~. The life cycle 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 document (see 5.2.2.3).

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

NOTE 3 The rounded shapes of stages A, H, and J represent entry points to the life cycle (see 5.2.3).

NOTE 4 The dotted lines represent the loops in the life cycle (see 5.2.5).

Figure 2 – Alarm management life cycle

5.2.2 Alarm management life cycle stages

5.2.2.1 General

The alarm management life cycle 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 Clause 6 to Clause 18 of this document.

5.2.2.2 ~~Alarm philosophy~~ Philosophy (A) 22

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. The alarm philosophy reflects the operations and maintenance work processes and can reference those processes in other documents. 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 life cycle stages, such as the threshold for the MOC process and the specific requirements for change. The philosophy is maintained to ensure consistent alarm management throughout the life cycle of the alarm system.

The development of the ASRS is included in the philosophy stage of the life cycle. 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~~ can 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~~ the methods for determining if an alarm ~~might be~~ is necessary. These methods are defined outside of this document so the identification stage is represented as a predefined process in the life cycle. 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. Information from identification (e.g., alarm setpoint, consequence) should be captured for rationalization. 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 the alarm 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 and definitions 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~~ monitoring, and audit **23** 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 additional 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 state and alarm priority.

Advanced alarming techniques(e.g., state-based alarming) ~~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~~ can 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~~ can 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 over time.

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 life cycle stages from identification to implementation.

5.2.2.11 Audit (J)

In the audit stage, periodic reviews are conducted to evaluate the effectiveness of the alarm management process and 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 management life cycle entry points

5.2.3.1 General

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

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 life cycle stages are only the initial step in managing an alarm system. All stages of the life cycle 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~~ can be used as the basis for the ASRS. This is the life cycle entry point for new ~~installations~~ systems.

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~~ benchmark 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 document. The results of the initial audit can be used in the development of a philosophy.

5.2.4 Simultaneous and encompassing stages

The life cycle diagram (Figure 2) is drawn to represent sequential stages. There are several simultaneous stages which are represented in the life cycle. 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 life cycle are authorized and completed.

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

5.2.5 Alarm management life cycle loops

5.2.5.1 General

In addition to the alarm management life cycle stages, there are three loops in the life cycle. Each loop performs a function during the life 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~~ in compliance with the alarm philosophy. The design might need to be modified or an advanced alarming technique might need to be applied. The alarm could remain in operation while the MOC process is initiated and the stages of the life cycle are repeated.

5.2.5.4 Audit and philosophy loop

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

5.2.6 Alarm management life cycle stage inputs and outputs

The alarm management life cycle stages are connected as the outputs of one stage are often the inputs to another stage. The connections are not fully represented in the life cycle diagram (Figure 2). Table 1 provides more information on the relationships between the inputs and outputs of the life cycle stages.

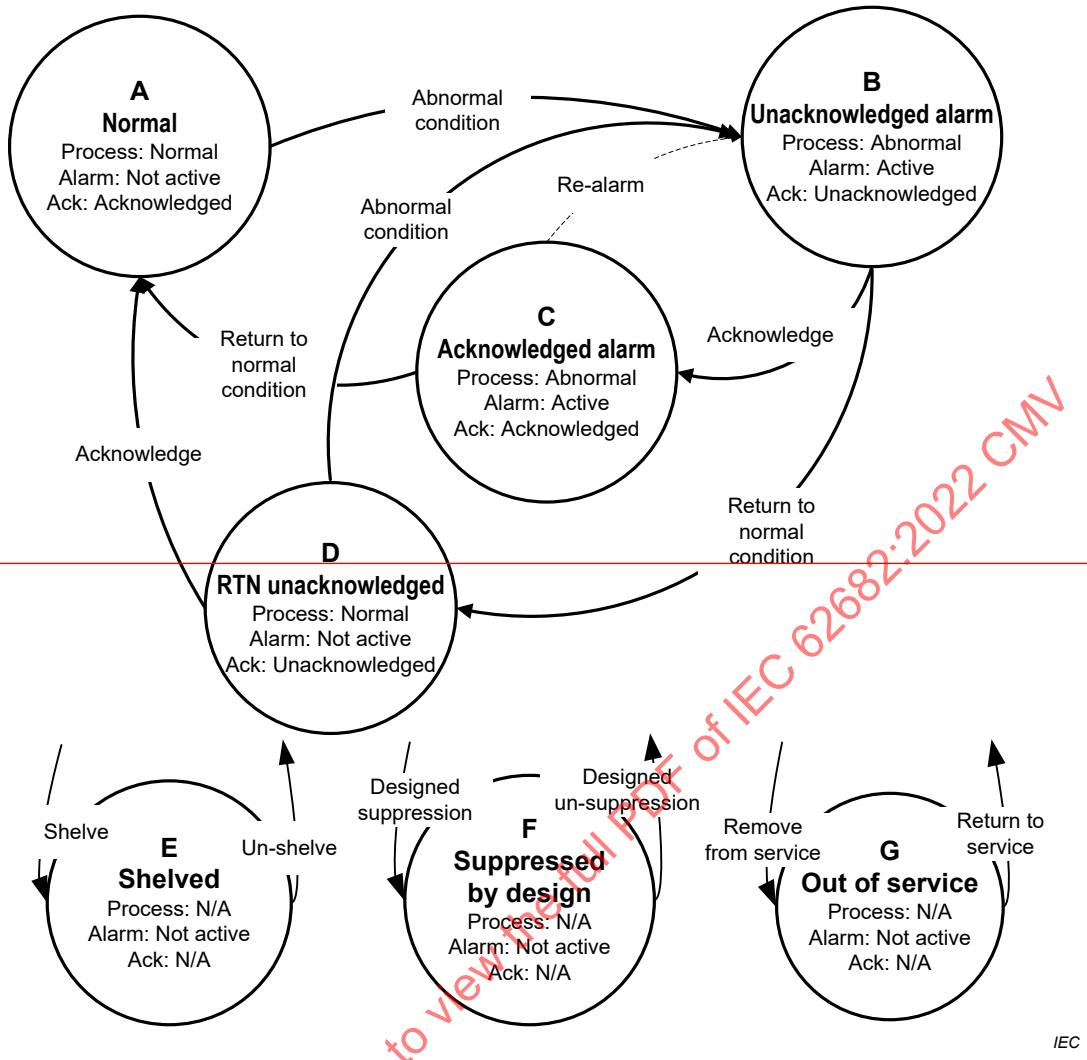
Table 1 – Alarm management life cycle stage inputs and outputs

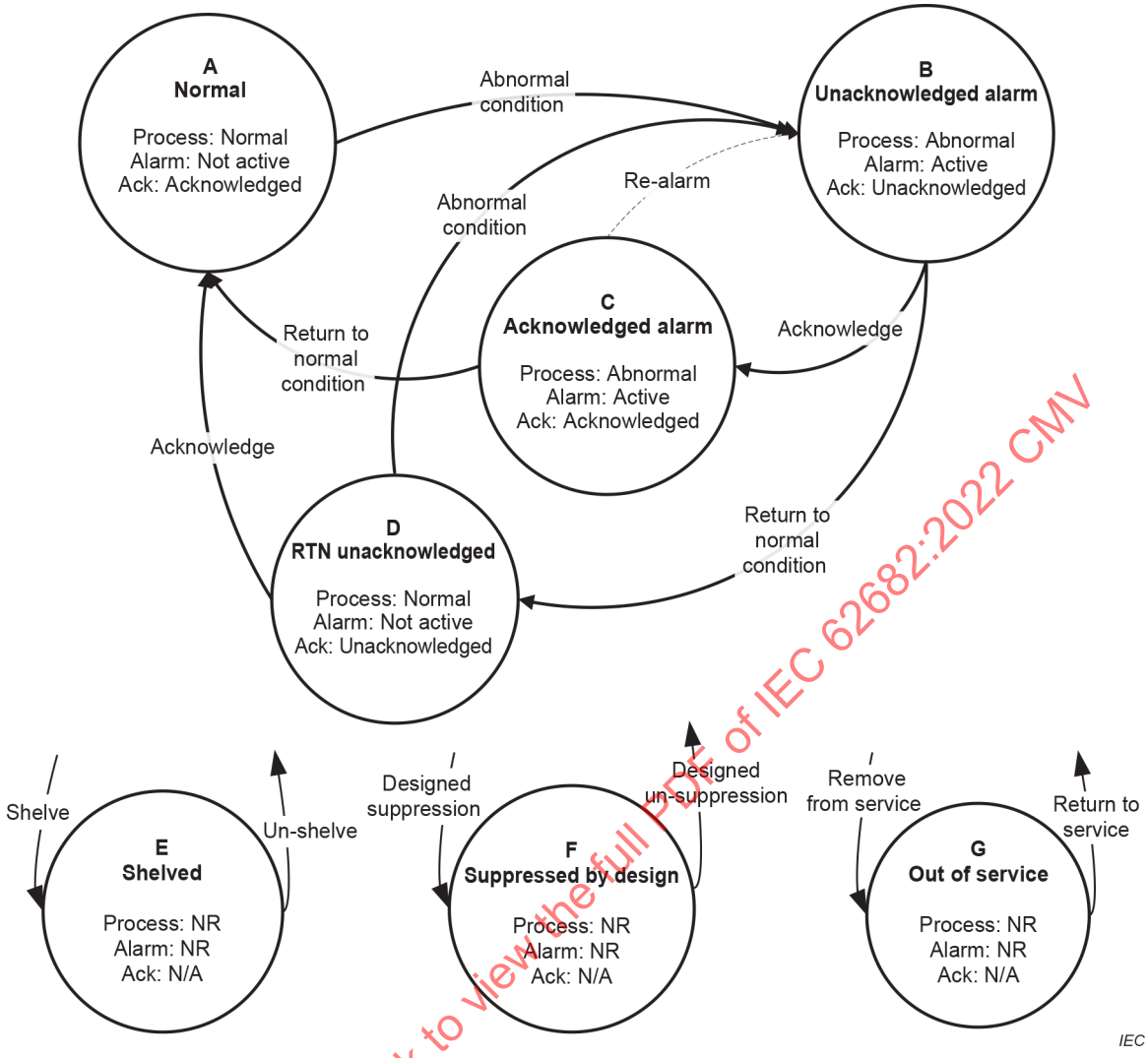
Alarm management life cycle stage		Activities	Clause number	Inputs	Outputs
Stage	Title				
A	Philosophy	Documenting the objectives, guidelines and work processes for alarm management, and ASRS	6, 7	Objectives and standards, audit recommendations	Alarm philosophy and ASRS
B	Identification	Determining 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	Installing alarms, implementation testing, and implementation training	13	Completed alarm design, master alarm database, and ASRS	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, modifications, and deletions of alarms	17	Alarm philosophy and proposed changes	Authorized alarm 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.





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.

NOTE 3 N/A indicates not applicable.

NOTE 4 NR indicates that the state is not relevant (either normal or abnormal, not active or active).

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 not active and previous alarm occurrences 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 not active 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 and not annunciated, typically for maintenance. An alarm in the out-of-service state is ~~under~~ in the ~~control of~~ maintenance stage of the life cycle.

NOTE An alarm in the out-of-service state is not the same as out of service of a unit or equipment. Equipment can be out of service while the associated alarms are not out of service.

5.3.2.9 ~~Alarm status by state~~ Summary of alarm states

The alarm status, annunciation status, and acknowledge status of different alarm states are summarized in Table 2.

Table 2 – Summary of alarm states

ID	Mnemonic	State name	Process condition	Alarm status	Annunciation status	Acknowledge status
A	NORM	Normal alarm state	Normal	Not active	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	Not active	Annunciated	Unacknowledged
E	SHLVD	Shelved state	Normal or abnormal	Not active or active	Suppressed	Not Applicable
F	DSUPR	Suppressed-by-design state	Normal or abnormal	Not active or active	Suppressed	Not Applicable
G	OOS RV	Out-of-service alarm state	Normal or abnormal	Not active or active	Suppressed	Not Applicable

5.3.3 Alarm state transition paths

5.3.3.1 General

The arrows in Figure 3 represent transitions between states. The diagram does not directly illustrate the effects of alarm deadband, on-delay, or off-delay, which can impact the evaluation of alarm status (i.e., active or not active).

5.3.3.2 Transition from normal to unacknowledged (A → B)

The transition from normal to unacknowledged 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~~ make the alarm active.

5.3.3.3 Transition from unacknowledged to acknowledged (B → C)

The transition from unacknowledged to acknowledged 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)

The transition from acknowledged to unacknowledged is the infrequently used option that periodically generates repetitive alarm indications for a single alarm while the alarm remains ~~in the alarm state~~ active.

5.3.3.5 Transition from acknowledged to normal (C → A)

The transition from acknowledged to normal is part of a normal sequence for an alarm. The alarm moves from the acknowledged state to normal and becomes not active.

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

The transition from unacknowledged to return-to-normal unacknowledged occurs when the process returns to normal and the alarm becomes not active before an operator has acknowledged the alarm.

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

The transition from return-to-normal unacknowledged to normal occurs when an alarm has returned to normal and becomes not active. This transition can require operator acknowledgment or can be acknowledged automatically.

5.3.3.8 Transition to shelved (any state → E)

The transition to shelved 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)

The transition from shelved to normal or unacknowledged occurs when an alarm is unshelved, 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.~~ If the alarm is automatically unshelved, the transition should be to the unacknowledged state. If the alarm is manually unshelved, the transition should be to the acknowledged state.

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

The transition to suppressed-by-design 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-design~~ed~~ to normal or unacknowledged (F → A or B)

The transition from suppressed-by-design to normal or unacknowledged occurs when process conditions ~~or states~~ are used to unsuppress alarms when appropriate. Designed unsuppression is typically an automatic operation. If the alarm is active, the transition should be to the unacknowledged state. If the alarm is not active, the transition should be to the normal state.

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

The transition to out-of-service state occurs when an alarm ~~can be~~ is removed from service for maintenance or other reasons. Remove from service is typically a manual operation.

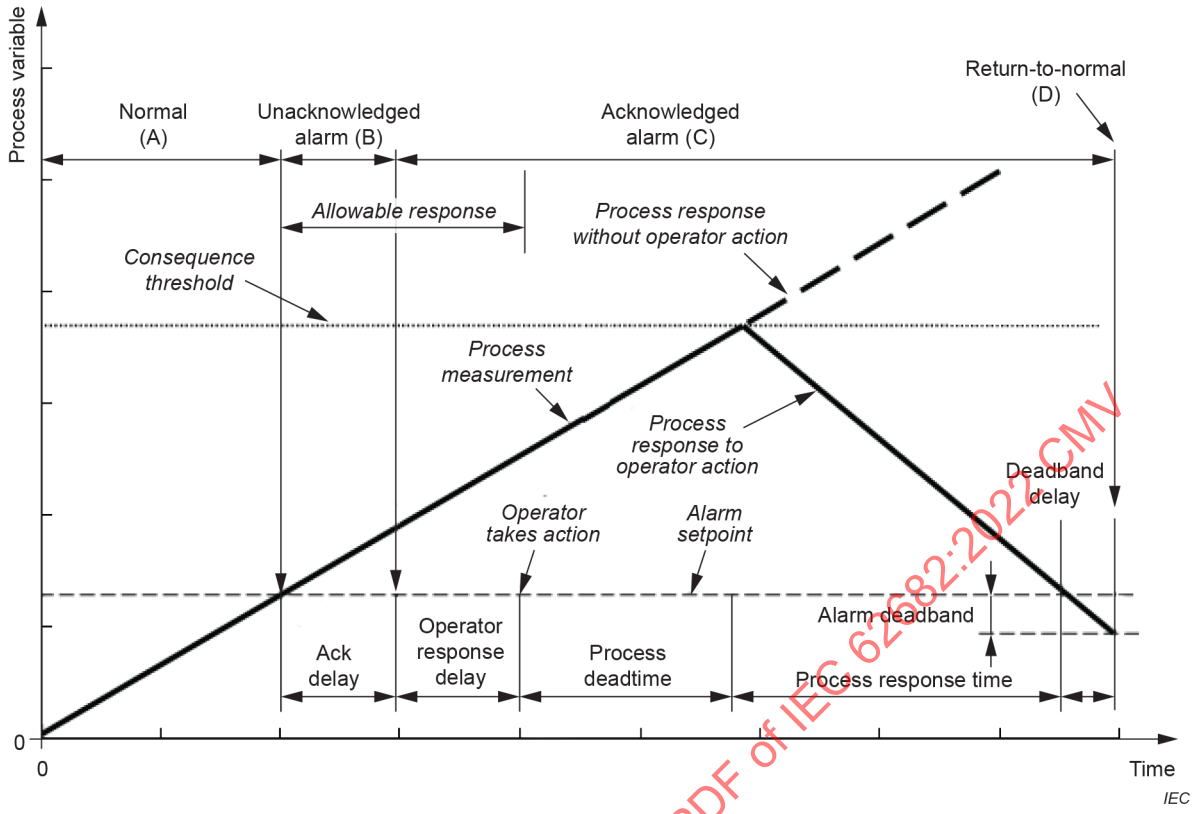
5.3.3.13 Transition from out-of-service to normal or unacknowledged (G → A or B)

The transition from out-of-service to normal or unacknowledged occurs when an alarm ~~can be~~ is returned to service when it is available after maintenance. Return to service is typically a manual operation. If the alarm is active, the transition should be to the unacknowledged state. If the alarm is not active, the transition should be to the normal 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. Figure 4 illustrates only one possible scenario to clarify the definition of terms related to time.



NOTE Ack delay, operator response delay and process deadtime can be zero.

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 not active, and previous alarm occurrences 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

a) measurement accuracy,

b) sampling interval, and

c) 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. The operator can take action before or after acknowledging the alarm. There are several factors that affect the operator response time such as

a) system processing speed,

b) HMI design and clarity,

c) operator awareness and training,

d) operator workload,

e) complexity of determining the operator action, and

f) 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 time until the alarm returns to normal. 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 Allowable response time

The allowable response time is the time beginning with the alarm annunciation and ending at the last moment operator action can prevent the consequence. It can be estimated working backwards from the consequence threshold, considering the process deadtime, the rate of change of the process variable and the separation between the alarm setpoint and the consequence threshold. In Figure 4, the operator response delay is shown within the allowable response time.

5.4.7 Alarm setpoint

The alarm setpoint can be adjusted to increase or decrease the allowable response time. The process for evaluating the alarm setpoint is alarm setpoint determination.

5.4.8 Consequence threshold

The consequence threshold is the value of the process measurement at which the consequence begins to occur. 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.~~

5.4.9 Alarm deadband

The deadband delay shown in Figure 4 illustrates that the alarm does not return to normal immediately after crossing the alarm setpoint.

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~~.

The following three stages of activity occur in the operator sub-system leading to action:

a) the indication of deviation from desired normal operation (i.e., an alarm) is detected,
b) the situation is diagnosed, and the corrective action is determined, and
c) the corrective action is implemented to compensate for the disturbance.

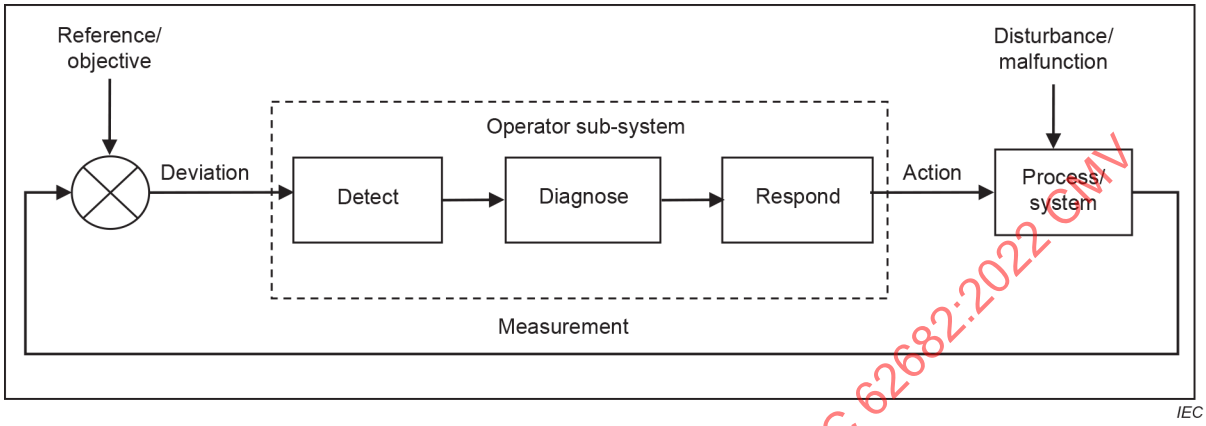


Figure 5 – Feedback model of operator-process interaction

5.5.2 Detect

The operator becomes aware of the deviation from the desired condition by an alarm caused by a disturbance. The design of the alarm system and the operator interface facilitates 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. The alarm response procedures aid the operator's diagnosis.

5.5.4 Respond

The operator takes corrective action in response to the deviation and monitors the process to determine if the deviation is corrected.

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:

a) workload,
b) operator console ergonomics,
c) HMI design, **24**
d) short term or working memory limitations,
e) fatigue,
f) training, and
g) 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 life cycle stages. This is achieved by specifying items, including the methods for alarm identification, rationalization, monitoring, MOC, 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.~~ An alarm philosophy document shall be developed to cover each alarm system. An alarm philosophy may cover more than one alarm system. The alarm philosophy shall include the required contents listed in this clause. The alarm philosophy shall be developed prior to rationalization. **25**

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 contents

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

Alarm philosophy contents	Required / recommended	Subclause
Alarm system maintenance	Required	6.2.21
Testing of alarms	Required	6.2.22
Alarm system performance monitoring	Required	6.2.23
Alarm history preservation	~~Required~~ Recommended	6.2.24
Management of change	Required	6.2.25
Alarm system audit	Required	6.2.26
Related site procedures	Recommended	6.2.27

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 alarm philosophy.

6.2.2 Purpose of alarm system

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

6.2.3 Definitions

The alarm philosophy shall include definitions of terms that will be encountered in the course of design and improvement of an alarm system ~~shall be defined~~ to ensure that all participants share a common understanding. The definition of an alarm shall be documented in the alarm philosophy.

6.2.4 References

The alarm philosophy should include a list of appropriate references ~~for alarm management shall be included~~. References can be internal company documents (e.g., MOC procedure), external standards, or published material.

6.2.5 Roles and responsibilities for alarm management

The alarm philosophy shall establish responsibility by role for the activities of the alarm management life cycle. Specific aspects ~~to cover~~ should include the following:

a) the owner of the alarm system, the philosophy, master alarm database, 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~~ alarms,

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 alarm philosophy shall include the criteria for selection and principles for design of alarms, consistent with the definition of an alarm. The criteria and principles should ~~address~~ include:

a) the role of the alarm system in identifying approaches to unsafe or ~~sub-optimal~~ abnormal 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 Alarm setpoint determination

The alarm philosophy should provide guidance on the methods used for determination of alarm setpoints. Alarm setpoint determination can use several inputs (e.g., consequence thresholds, process dynamics, complexity of the operator response).

6.2.8 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:~~ The alarm philosophy shall address the prioritization, including the following:

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

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

c) the impact of classification on prioritization, if any.

6.2.9 Alarm class definition

Alarm classes are used to set common requirements for managing alarms. An alarm may belong to more than one class. This alarm philosophy ~~should~~ shall include the definition of the alarm classes~~. It should also~~, which can include the following ~~class requirements~~:

a) alarm prioritization considerations,

b) alarm documentation,

c) HMI design,

d) operating procedures associated with the alarms,

e) ~~operator~~ training and training documentation,

f) alarm maintenance,

g) alarm testing,

h) alarm monitoring and assessment,

i) alarm MOC,

j) alarm history retention, and

k) alarm audit.

6.2.10 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,~~ If HMA are used, the alarm philosophy shall define the criteria for assigning alarms to HMA classes. The designation of alarm classes as highly managed should be based upon one or more of the following:

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

6.2.11 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.~~ The alarm philosophy ~~should~~ shall list the criteria to assess alarms and the information to be captured during rationalization. Guidance on the knowledge and experience of the rationalization team should include:

a) operations,

b) process,

c) maintenance,

d) control system, and

e) alarm philosophy.

6.2.12 Alarm documentation

~~Appropriate documentation shall be addressed in the alarm philosophy.~~ The alarm philosophy shall specify the documentation for alarms. This ~~may~~ should include the following:

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

~~b) periodic alarm performance reports,~~

b) specifications for advanced ~~alarm management~~ alarming techniques (e.g., designed suppression).

~~d) specifications for suppress by design.~~

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

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

6.2.13 Alarm design guidance

The alarm philosophy shall provide guidance on the design practices. This guidance should address:

a) alarm deadband,

b) alarm on-delay,

c) alarm off-delay

d) alarm types, and

e) composition of alarm messages.

6.2.14 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.

6.2.15 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:~~

The alarm philosophy shall specify the alarm presentation method to establish principles for consistent display and annunciation.

The following elements should be specified for HMI design:

a) the alarm presentation method (e.g., colour, symbol, and alpha-numeric),

b) the mechanism used (~~e.g., panel, BPCS console screens, etc.~~ for example the HMI) to communicate the alarms to the operator,

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

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

e) the functions that will be available in the HMI, including shelving, suppression, and enhanced and advanced alarming techniques.

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.~~

If enhanced and advanced alarming techniques are used, this section of the alarm philosophy shall be used to identify the approved techniques and related responsibilities and work processes. 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.

6.2.17 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.~~

The alarm philosophy shall specify the methods for initial training, commissioning, and testing of the alarm system.

6.2.18 Alarm response procedures

The alarm philosophy shall address alarm response procedures. Available alarm response procedures can reduce the time it takes the operator to diagnose the problem and determine

the appropriate corrective action, as well as promote consistency between operators. The philosophy should include the following:

a) the information included in the alarm response procedures (e.g., cause, consequence, corrective action), and

b) the method to access the alarm response procedures (e.g., via the operator interface).

6.2.19 Training

The alarm philosophy ~~specifies~~ shall address how plant personnel are to be trained on the use, management, and design of the alarm system, including the training documentation requirements.

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

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

~~b) an outline of the training contents, and~~

b) when training is required.

6.2.20 Alarm shelving

The alarm philosophy should include guidance on how and when alarm shelving can be used, who can perform shelving, as well as authorization and documentation requirements. There are typically limits defined on which alarms can be shelved and shelving duration, based on class or priority.

6.2.21 Alarm system maintenance

The alarm philosophy ~~identifies~~ shall specify the activities necessary to maintain the alarm system. Specific elements ~~that shall be covered in this section~~ for alarm system maintenance shall 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.

6.2.22 Testing of ~~the alarm system~~ alarms

~~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.~~

The alarm philosophy shall address testing based on alarm classes or other methods. Testing documentation may be managed in other systems.

6.2.23 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.~~

The alarm philosophy shall specify methods for assessing alarm system performance. Specific elements ~~that shall be covered in this section~~ for alarm system performance monitoring shall 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.

6.2.24 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.~~

The alarm philosophy should specify the retention of alarm related records (e.g., annunciations, acknowledgements, return to normal, and operator actions). In some industries and regions, regulatory bodies or local statutes might require preservation of this information and tracking of changes to data.

6.2.25 Management of change

The alarm philosophy ~~identifies~~ shall identify the types of changes and the applicable MOC procedures. ~~A management of change procedure shall be documented.~~ Types of changes ~~may~~ can include:

a) temporary changes to alarms (e.g., taking alarms 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~~ The MOC procedure ensures 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,~~ description of each change, and authorization.

6.2.26 Alarm ~~system~~ management audit

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

a) audit frequency, which ~~may~~ can be specified based on alarm class,

b) audit topics, and

c) process for operator interviews.

6.2.27 Related site procedures

~~To avoid inconsistencies between the alarm philosophy and other site procedures,~~ The alarm philosophy should reference 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) MOC procedure, and

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

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. The alarm philosophy should be approved by management. 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) MOC process.

7 Alarm system requirements specification

7.1 Purpose

The alarm system requirements specification (ASRS), which ~~may~~ can also be called an alarm functional requirements specification, is ~~part of the philosophy lifecycle stage~~ developed based on the alarm philosophy and can be an important part of control system procurement. Clause 7 provides guidance on the development and uses of an ASRS. 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 ASRS 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 alarm systems~~,~~ and guide the detailed alarm 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.~~ During implementation, the ASRS can serve as the basis of function testing of the alarm system. The ASRS specifies the alarm system functionality necessary to satisfy the alarm philosophy.

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

7.2 Recommendations

~~Planning~~ An ASRS should be developed for new control systems and major revisions to the alarm functionality of existing control systems. The ASRS 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 management life cycle 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.~~ Modifications to accommodate the alarm system requirements can be necessary to achieve the desired performance. The ASRS should be consistent with the alarm philosophy. 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~~ attribute 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~~ the ASRS 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 Packaged systems

If packaged systems are part of the control system, the ASRS should include guidance on how packaged systems will be interfaced to the alarm system.

7.6 Customization

If important system requirements in the specification are not met by standard commercial products, it ~~may~~ can be necessary to develop custom solutions, or to reconsider the specification. The ASRS facilitates early recognition of the need for customized solutions and ~~can initiate~~ associated cost /benefit analysis.

7.7 Alarm system requirements ~~testing~~ verification

Each alarm system requirement should be ~~tested~~ verified prior to the operations stage of the life cycle.

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 management life cycle for the recommended alarms or alarm changes. Identified alarms are an input to rationalization.

8.2 Alarm identification methods

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

Some common alarm identification methods are:

~~a) allocation of safety layers,~~

a) process hazards analysis (PHA or HAZOP),

b) layer of protection analysis (LOPA),

c) incident investigations,

d) environmental permits,

e) failure mode and effects analysis (FMEA),

f) current good manufacturing practice (cGMP),

g) quality reviews,

h) P&ID reviews,

i) operating procedure reviews, and

j) packaged system 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~~ evaluating alarms.

8.4 Identification documentation

The information related to potential alarms should be documented during identification and used in alarm rationalization if available, including:

a) the consequence threshold (e.g., constraint),

b) the operator response,

c) the consequence of inaction,

d) the probable cause, and

e) the rationale for the consequence threshold.

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~~ documented 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 alarm philosophy. Rationalization produces the detail design information, documented in the master alarm database, necessary for the design stage of the alarm management life cycle.

The activities of rationalization are:

a) alarm justification,

b) alarm setpoint determination,

c) alarm prioritization,

d) alarm classification, and

e) rationalization review.

~~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.~~ Each alarm shall be rationalized and documented as specified in the alarm philosophy, for each applicable plant state. The documentation shall include: **26**

a) alarm type,

b) alarm priority,

c) alarm class,

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

e) operator action,

f) consequence of inaction ~~or incorrect action~~, and

g) plant state.

Additional alarm attributes may be documented during rationalization.

9.2.2 Rationalization documentation recommendations

Rationalization ~~documentation for each alarm~~ should ~~include~~ determine and document the following for every alarm per the alarm philosophy, for each applicable plant state:

a) the maximum allowable response time,
b) the probable cause,
c) the rationale for the alarm setpoint,
d) the identification method, and
e) the need for advanced alarming techniques, if necessary.

9.2.3 Plant states

Plant states can include:

a) start-up,
b) normal operation,
c) operation, step, or phase in batch processes, and
d) shutdown.

9.3 Alarm justification

9.3.1 Alarm justification process

Each 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 alarm include that:

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) include knowledge of the process and the control system, and
c) rely heavily upon operator ~~input~~ knowledge~~, 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~~ and 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~~ can take in response to the alarm;
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.~~
d) the allowable response time.

Those alarms for which the ~~operator's primary response~~ operator action 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 performance

Alarm justification should ~~ensure~~ verify 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 performance from the above listed conditions.

9.4 Alarm setpoint determination

The guidance stated in the alarm philosophy ~~is~~ should be applied to the determination of alarm setpoints.

Effective methods use information including:

a) the allowable response time (see ~~Figure 5~~ Figure 4),

b) the complexity of the operator action,

c) the time necessary to complete the operator action,

d) the normal operating range,

e) other operating or design boundaries, and

f) knowledge of the process operation and history~~, and other factors~~.

For some processes (e.g., batch processes), the alarm setpoint may be modified with plant state.

9.5 Prioritization

Alarm priority is used to aid the operator in determining the order in which to respond to multiple alarms. The method for priority assignment defined in the alarm philosophy is applied to the rationalized alarm and a priority is 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. Alarm priority distribution metrics 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 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.

Alarms in the same class may have different priorities.

9.7 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~~ documented in the alarm philosophy.

9.8 Removal of rejected alarms

Existing alarms that ~~fail~~ are rejected for failing to meet the criteria for ~~alarming provided in the~~ an alarm ~~philosophy~~ shall be documented along with the basis (i.e., criterion it failed to meet) justifying removal. Rejected alarms can be candidates for other forms of notifications (e.g., operator alerts). Those alarms should then be subject to further review by the MOC procedure to remove the alarm from the system.

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~~ is 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 management life cycle,
b) utilization as part of the MOC,
c) alarm response procedures,
d) training of and ~~review~~ use by operators,
e) periodic auditing and reconciliation of the control system alarm settings, and
f) 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 life cycle. ~~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 consideration ~~associated with the triggering of alarms~~ to implement the alarms within a specific control system as specified by the rationalization process. All design considerations related to the presentation of alarms are contained in Clause 11.

10.2 Basic alarm design capabilities

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

10.3 Usage of alarm states

10.3.1 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 devices (e.g., sensors and final control elements),
b) the control ~~and safety~~ system (i.e., BPCS, SIS, packaged system), and
c) the HMI.

10.3.2 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~~ functions (e.g., as an interlock setpoint) in addition to operator notification, then documentation, training and MOC 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~~ and higher access level required). This information should be specifically documented in the alarm philosophy under alarm design principles.

10.3.3 Alarm suppression and other logic functions

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

10.4 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.~~ Alarm type shall be implemented based on the information documented in the master alarm database. The common alarm types ~~may~~ can 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-alarming alarms,
n) statistical alarms,
o) first-out alarms, and
p) bad-measurement alarms.

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

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

10.5 Alarm attributes

10.5.1 General

During the basic design process, the ~~default~~ alarm attributes should be ~~configured~~ selected for each alarm that has been ~~identified during rationalization~~ rationalized and set based on

engineering judgment. Attributes such as alarm 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 description,

~~b) alarm type,~~

b) alarm setpoint or logical conditions,

c) alarm priority,

d) alarm deadband,

e) on-delay or off-delay

f) alarm group, and

g) alarm message.

10.5.2 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~~ should be used in the description.

10.5.3 Alarm setpoints

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

10.5.4 Alarm priority

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

10.5.5 Alarm deadbands

10.5.5.1 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.~~ Alarm deadband is an alarm attribute used to reduce the number of times an alarm is triggered for a given abnormal condition, which ideally would be only once. It prevents an alarm from returning to normal until the alarm is cleared by the deadband, a 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.

10.5.5.2 Alarm deadband requirements

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

10.5.5.3 Alarm deadband recommendations

The engineering basis for 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 100,000) can act as a latch, creating stale alarms. Settings should be documented and then reviewed during commissioning and after significant operating experience.

10.5.6 Alarm on-delay and off-delay

10.5.6.1 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 the alarm setpoint, thus preventing the alarm from ~~being triggered~~ becoming active until the signal remains in the alarm ~~state~~ condition continuously for ~~a specified length of~~ the delay time. The off-delay is used to reduce chattering alarms by ~~locking in the alarm indication for a certain~~ holding the alarm active for the delay period after the process condition has returned to normal.

10.5.6.2 Alarm on-delay and off-delay requirements

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

10.5.6.3 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~~ determination should take into consideration the allowable 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~~ delay on operator response. Settings should be reviewed during commissioning and after ~~significant~~ sufficient operating experience.

10.6 Programmatic changes to alarm attributes

Some sites modify alarm attributes based on conditions such as ~~batch recipe,~~ product type, product grade, plant state, or other conditions. Alarm attributes can typically be programmatically 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);~~

a) control logic (e.g., sequences, phases, state-based logic),

b) advanced alarming techniques,

c) 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~~ the functionality for programmatic changes. For each alarm ~~the user~~, it should ~~identify~~ be identified and ~~clearly~~ documented which programs of the system will have access to modify alarm attributes during operation and which changes will be subject to MOC procedures. Advanced alarming techniques for modifying alarm attributes are covered in Clause 12.

10.7 Review of 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~~ are implemented.

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 life cycle stage. ~~Clause 11 outlines the functionality to provide alarm indications and related functions to the operator and other HMI users.~~ Clause 11 provides requirements and recommendations related to the

presentation of alarms 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.~~

NOTE Guidance for HMI design and maintenance is provided in ANSI/ISA-101.01.

11.2 HMI functions

11.2.1 General

The HMI design for alarms ~~should~~ shall **27** 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) unsuppressed 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) individually 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) support a designed suppression function, and
g) display alarm messages~~, and~~.
~~g) assign alarms to operator stations.~~

11.2.4 HMI functional recommendations

The HMI should provide the ability for the operator to access the alarm response procedures. **28**

11.2.5 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,
e) suppressed-by-design summary displays, and
f) out-of-service summary displays.

11.2.6 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.

11.2.7 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) alarm group or process area,
d) alarm ~~group~~ class(es), 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, text, a combination or shape and 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, text, a combination or shape and text), and should be ~~identical~~ related 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~~ unique. 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~~ unique. 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~~ unique. 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.~~

NOTE 1 "Yes" signifies the indication type is used to indicate the alarm state.

NOTE 2 "No" signifies the indication type is not to be used to indicate the alarm state.

NOTE 3 "Combination" signifies the indication is a combination of visual colour and symbol indications.

NOTE 4 "Optional" signifies the indication is not required.

11.3.4 Audible alarm state indications

The audible alarm indication for unacknowledged alarms may also be 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, 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, except in operating environments where this is not practical.

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, text) should be used to indicate each alarm priority to reinforce colour coding.

NOTE The combination of unique colour and symbol can be used to compensate for colour blindness.

11.4.4.3 Audible alarm priority indications

A distinct 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 message should be structured with consistent information. 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~~ may 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. The displays can 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) suppressed-by-design alarm display, and

i) out-of-service alarm display.

The displays are described with required or recommended functions. The function may be provided through other methods.

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 unsuppressed 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 information for alarms. 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 current process value,
b) the alarm setpoint,
c) the alarm group or process area, and
d) 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 multiple visible alarms, with access-controlled methods as allowed in the alarm philosophy.

11.6.2.6 Functional recommendations

The alarm summary display should provide the following functions:

a) navigational link to the appropriate process display,
b) access to alarm response procedures,

c) filtering of alarms by time of alarm,

d) filtering of alarms by priority,

e) filtering of alarms by alarm type,

f) filtering of alarms by alarm group or 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~~ should be provided. The alarm summary status display provides an indication of the number of unsuppressed 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 state change,

c) filtering by type of alarm state change,

d) filtering ~~of alarms~~ by priority,

e) filtering ~~of alarms~~ by alarm type, and

f) filtering of alarms by alarm group~~, and~~ or 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~~ graphic elements

Other ~~display~~ graphic elements (e.g., alarm banners) may be used to indicate alarm states.

11.7 Alarm shelving

11.7.1 General

The ~~temporary~~ shelving of alarms is a required function. This temporary suppression of alarms by the operator is a ~~function used~~ common practice to keep nuisance alarms from interfering with the effectiveness of the alarm system. Shelving includes a functionality, such as a time limits, 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~~ shelve action with timestamp, and

g) a record of each unshelve event with timestamp.

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~~ unshelving alarm floods by automatically unshelving active alarms too quickly. The state transitions from shelving are:

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.

The shelving function should record the identity of the person that shelved the alarm. **29**

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 alarm 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) unshelving of alarms by group,

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 a required function and a 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 action with timestamp, and

f) a record of each return-to-service event with timestamp. **30**

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 and the approximate anticipated duration of the suppression (e.g., less than an hour, less than a day, less than a week, less than a month). **31**

11.9 Alarms suppressed by design

11.9.1 General

The designed suppression of alarms is a required function and it is common practice to suppress alarms that are not needed due to intended or actual operating conditions. This functionality supports the testing, maintenance, and operator understanding of designed suppression.

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,

~~b) a record of each alarm suppressed bydesign.~~

b) a record of each suppress-by-design event with timestamp, and

c) a record of each unsuppress-by-design event with timestamp. **32**

11.9.3 Designed suppression functional recommendations

The designed 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 if the alarm is active.

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.

11.9.4.5 Functional recommendations

Suppressed-by-design displays should provide the ability for the operator to unsuppress an alarm or disable the designed suppression.

11.10 Alarm annunciator integration

11.10.1 General

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

11.10.2 Alarm annunciator integration recommendations

Alarm annunciators should be integrated in a manner that provides 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 related alarm ~~HMI~~

11.11.1 General

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

11.11.2 Independent safety related alarm HMI

An HMI independent from the BPCS ~~may~~ can be required for the following safety related 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~~ action, communication fault).

NOTE For further guidance, see IEC 61511 series.

12 Detailed design: enhanced and advanced ~~alarm methods~~ alarming

12.1 Purpose

Enhanced and advanced alarming is part of the detailed design life cycle 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~~ Advanced alarming modifies alarm behaviours including logic-based alarming, dynamic alarming, state-based alarming (i.e., mode-based alarming), and adaptive alarms. Most designed suppression ~~methods~~ techniques are included in advanced alarming. In addition to advanced alarming techniques, enhancements to the alarm system also provide enhanced information to the operator or redirect the alarm to the designated responder. ~~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~~ is not ~~be~~ always sufficient to reduce alarm floods or mitigate their effect so enhanced and advanced ~~techniques may~~ alarming can be necessary. The ~~methods~~ techniques 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~~ approved enhanced and advanced alarming ~~methods~~ techniques.

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.~~

Enhanced and advanced alarming techniques add complexity and need additional resources for design, implementation, and maintenance. The MOC procedure should include a review of the impact of changes on the enhanced and advanced alarming techniques as well as risk evaluation of possible failures of the techniques. **33**

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 techniques (e.g., Boolean logic ~~or~~, decision trees) to determine the modifications to be made to alarm systems. This may be implemented in the control system or externally to the control system.

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~~ status 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 attributes (e.g., 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 or prediction 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~~ are often not 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.~~

12.6.2 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~~ responding to an abnormal situation is not in a control room. Such situations can benefit from the availability of a remote alarm system (e.g., paging, e-mail, call-out alarms ~~etc.~~). Where remote alarm systems are used, the alarm philosophy should include these systems.

The reliability of the message delivery is a significant issue in remote alarm systems and should be considered. Periodic test messages should be used to improve reliability. A procedure to ensure response to the alarm should be considered.

It ~~may~~ can be necessary to also provide remote acknowledgement.

12.6.3 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~~ all or part of the functionality of the alarm system within the control system or control system HMI to provide a common interface. Alternatively, supplementary systems can be used, in addition to the ~~existing~~ control system alarm ~~system~~ functions 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 requirements of this document.

12.6.4 Batch process considerations

12.6.4.1 General

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

12.6.4.2 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.

12.6.4.3 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 some advanced alarming techniques is the ability to take calendar time stamps and electronic records indicating when the batch step or phase started and ~~compute and display~~ determine alarms in relative time.

12.6.4.4 Inclusion of lot number and other identifying marks

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

12.7 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 management life cycle, 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~~ verification,

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 requirements for new or modified alarms

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~~ as prescribed in the alarm philosophy or the MOC procedure.

~~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.~~

13.3.3 Training documentation requirements for new or modified highly managed alarms

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

a) the persons trained,
b) a summary of the training material,
c) the method of training, and
d) the date of the training.

13.3.4 Training documentation recommendations for new or modified alarms

Documentation of the training should include:

a) the persons trained,
b) a summary of the training material,
c) the method of training, and
d) the date of the training.

13.3.5 Implementation training requirements for new or modified alarm systems

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

13.3.6 Implementation training recommendations for new or modified alarm systems

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

a) the audible and visual indications for alarms,
b) the methods for silencing an alarm,
c) the distinction of alarm priorities,
d) the use of the alarm HMI features (e.g., alarm summary sorting and filtering),
e) the methods for shelving and suppression, and
f) the methods for removing an alarm from service.

13.4 Implementation testing and ~~validation~~ verification

13.4.1 General

Implementation testing requirements for new alarms and modifications to existing alarms are determined by the ~~classification of the alarm and~~ MOC procedure, the class requirements, or other methods, as detailed in the alarm philosophy.

NOTE Methods can include signal simulation and end-to-end signal function test. **34**

13.4.2 Implementation testing requirements for highly managed alarms

The alarm philosophy shall identify the verification 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 prior to putting the alarms in operation. The testing should include verification of the following:

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 the modified alarm system shall be appropriate to the nature of the change, as determined by ~~site~~ the 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,

d) any designed suppression or enhanced alarming documentation, and

e) test documentation, if required by the alarm philosophy.

NOTE The rationalization documentation and the alarm response procedures can be documented and accessed from the master alarm database.

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~~ can 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,~~
g) method of testing and acceptance criteria, and
h) 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 life cycle. 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 life cycle 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 as specified in the alarm philosophy.

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 priority, **35**
d) the alarm type,
e) the alarm setpoint,
f) the ~~potential~~ probable **36** causes,
g) the consequence of inaction,

h) the operator action,

i) the allowable response time, and

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

14.3.3 Alarm shelving recommendations

Shelved alarms extending beyond a single operating shift should be reviewed. The review ~~requirements~~ procedure 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~~ time limit set in the alarm philosophy:

a) the tag name for alarm,

b) the tag description or alarm description for alarm, and

c) the reason for shelving.

14.3.5 Shift change procedures and alarm review

Written procedures should be developed for the exchange or review of alarm status information at shift change.

14.4 Refresher training for operators

14.4.1 Refresher training requirements for operators

The training requirements for alarms shall be determined by the alarm classification ~~and the class requirements~~ or other methods as detailed in the alarm philosophy.

14.4.2 Refresher training documentation requirements for highly managed alarms

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

a) the persons trained,

b) the method of training, and

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 life cycle. 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~~ classification or other methods 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 and documented **37** 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, including notification to the operator,

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 and documented **38** 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~~ classification or other methods 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,

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

f) the anticipated duration the alarm will be out of service (e.g., longer than a day). **39**

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 and the duration of record retention 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~~ MOC procedure 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~~ Alarm verification may be performed after equipment replacement, 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 specified in the alarm philosophy. ~~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 life cycle. This stage verifies that design, implementation, rationalization, operation, and maintenance are satisfactory. Clause 16 provides ~~guidance~~ requirements and recommendations 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~~ management and improvement of the alarm system. 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.~~

16.2 Performance monitoring requirements

The alarm system shall be monitored. The alarm system performance shall be assessed against the performance targets in the alarm philosophy.

Each alarm transition in Figure 3 should be recorded to provide data for performance monitoring.

16.3 Monitoring and assessment

16.3.1 General

The intent of monitoring and assessment is to identify and correct deviations from expected performance. Monitoring the alarm systems involves analysis of the alarm records to calculate performance and diagnostic metrics. Alarm system assessment is the comparison of performance metrics against the targets specified in the alarm philosophy.

16.3.2 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~~ practical 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.

16.3.3 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~~ 40 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~~ 41 manageable guidelines indicates an alarm system that is annunciating more alarms than an operator ~~can handle, and the likelihood of missing alarms increases~~ is likely able to manage and can impact the probability of operator error.

~~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.~~

16.3.4 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 peak alarm rate is the highest number of alarms annunciated in one interval. 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~~ is a peak alarm rate less than 10.

~~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.~~

Additionally, as a recommended target, less than 1 % of the 10-minute intervals should contain more than 10 alarms.

16.3.5 Alarm floods

Alarm floods are variable-duration periods of alarm activity with annunciation rates likely to exceed the ~~operator response capability~~ ability of the operator to respond. ~~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.~~

The start of an alarm flood is indicated by a high alarm rate (e.g., an alarm rate that exceeds 10 alarms per 10 minutes), and the end of an alarm flood is indicated by a return to a reduced alarm rate (e.g., an alarm rate of less than 5 alarms per 10 minutes). As a recommended target, an alarm system should be in flood for less than 1% of the time. The thresholds for alarm flood should be set in the alarm philosophy.

Improvements to the alarm system and process operation ~~may~~ can 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 be used to mitigate alarm floods. ~~Alarm floods may require advanced methodologies to address.~~ These techniques are described in Clause 12.

16.3.6 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.

16.3.7 Chattering and fleeting alarms

A chattering alarm repeatedly transitions between the ~~alarm~~ active state and the ~~normal~~ not active 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.

16.3.8 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.~~

Alarms that remain annunciated continuously for an extended duration (e.g., longer than 24 hours) can be considered stale. Such alarms provide little valuable information to the operators. Stale alarms should be examined to ensure that they were properly rationalized. Advanced alarming or resolving the root cause can eliminate stale alarms.

There should be few stale alarms per operator console, with action plans to address them. No alarm should be intentionally designed to become stale and there is no long-term acceptable number of stale alarms.

16.3.9 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 as shown in Table 6.

Table 6 – Example 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
NOTE The ~<1 % highest priority is sometimes used for a few alarms with severe consequences.	

~~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.~~

Alarm priority distributions can vary based on process and industry. Significant variance from the target priority distribution can indicate ineffective rationalization or ineffective application of the alarm prioritization methodology.

16.3.10 Rationalization and alarm priority distribution

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

16.4 Unauthorized alarm suppression

The alarm states of shelved, suppressed by design, and out of service are all intended as controlled suppression 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.~~ Uncontrolled alarm suppression increases the potential for mistakes and the resulting risk.

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.~~ The target value for unauthorized alarm suppressions is zero. **42**

16.5 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~~ in a timely manner. The target value for unauthorized changes to alarms is zero.

16.6 Reporting of alarm system analyses

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

16.7 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

MOC is a separate stage of the life cycle. ~~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.~~ MOC for alarm management includes the documentation and authorization of changes to the alarm system, including: the addition of new alarms, the removal of existing alarms, the modification of alarm attributes, and changes to alarm system functions. The purpose of MOC is to ensure that changes are authorized and subjected to the evaluation criteria described in the alarm philosophy. The MOC process ensures that the appropriate life cycle 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 an MOC procedure. ~~Permanent~~ Changes that result in a difference from the authorized values of the alarm setpoint, class, priority, consequence, ~~basis~~ setpoint rationale, 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, including system upgrades, follow all appropriate subsequent alarm management life cycle activities, and
j) implementation of all changes ~~adhere to~~ followed the 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.~~

Documentation requirements shall be determined by the MOC procedure and classification or other methods as detailed in the alarm philosophy.

~~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.~~

17.4 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, as specified in the MOC procedure.

17.5 Alarm ~~attribute modification~~ documentation review recommendations

A list of referencing materials (e.g., graphics, control logic, P&ID, operating procedures, and ~~HAZOP~~ PHA) 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 life cycle 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.~~ Audit verifies the execution of the requirements and work processes against those documented in the alarm philosophy. Audit also includes comparison of the alarm management practices against industry guidelines.

~~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.~~ A benchmark, or initial audit, should be made against a set of documented practices (e.g., the practices listed in this document). 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.

18.3 ~~Initial audit or benchmark~~ Audit 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 or other methods.

Audits shall address all applicable requirements of this document that relate to management processes.

18.4 Audit interviews

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

c) operators have sufficient time to respond to alarms,

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

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

18.5 Audit process recommendations

The alarm philosophy should be audited against industry guidelines and the requirements and recommendations of this document. 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~~ can include:

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

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.

18.6 Action plans

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

Bibliography

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems − Part 4: Definitions and abbreviations*

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~~ application programming requirements*

~~IEC~~EN 62241:2015, *Nuclear power plants – Main control room – Alarm functions and presentation*

IEC 62264-2:2013, *Enterprise-control system integration – Part 2: Object and attributes for enterprise-control system integration*

IEC 62541-9:2020, *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*

ANSI/ISA-18.02-2016, *Management of Alarm Systems for the Process Industries*

ANSI/ISA-101.01-2015, *Human Machine Interfaces for Process Automation Systems*

Engineering Equipment Materials Users' Association, Alarm Systems – A Guide to Design, Management and Procurement, EEMUA Publication No. 191, 3rd Edition, EEMUA, London, UK (~~2007~~2013)

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

ISA-TR84.00.04-2020, Part 1, Guidelines for the Implementation of ANSI/ISA-61511-1-2018

List of comments

1 This change aligns terms with other applicable IEC standards: BPCS is used per IEC 61511 definition, control system is used per the IEC 61508 definition with the modification of packaged systems.

2 This change aligns terms with other applicable IEC standards: BPCS is used per IEC 61511 definition, control system is used per the IEC 61508 definition with the modification of packaged systems.

3 This paragraph relates to conformance and is moved to Clause 4. Provisional statements like should are not allowed in the scope.

4 This addition is to clarify Figure 1.

5 This addition is to clarify Figure 1.

6 This sentence is removed since it was perceived as not clear and introducing ambiguity.

7 This sentence is removed since it was perceived as not clear and introducing ambiguity.

8 Definition of a new term used in this publication.

9 An example is added for clarification.

10 This definition is revised because "operator support system" does not reflect/point to alarm system.

11 This definition is moved to 3.1.65 and changed to "operator alert".

12 This change clarifies that term "audit" has multiple technical contexts that may overlap in practice with alarm management.

13 Definition of a new term used in this publication.

14 This addition aligns notes to source document listed.

15 This change is to correct reference.

16 This definition is moved from 3.1.33 and changed to "operator alert".

17 The phrase "to the operator" is removed from the definition as it is the re- annunciation that is important.

18 This is to align with definition 3.2.67 in IEC 61511-1:2016.

19 An example is added for clarification.

20 Definitions of new terms used in this publication.

21 This paragraph relates to conformance and is moved from Clause 1.1.

22 This change aligns subclause title with Figure 2.

23 This change aligns the text associated with the explanation of alarm class requirements with that used in definition 3.1.11.

24 "Human machine interface design" (operator display design) is also a performance shaping factor which is different for "operator console ergonomics".

25 This change strengthens the alarm philosophy requirement which needs to have one developed before doing any rationalization for existing systems.

26 Every alarm requires rationalization - even those that belong to a group that has common charasterics. As written this subclause implies that one can pick and choose which alarms are to be rationalized. This clause was updated to resolve this issue.

27 HMI design shall be consistent as consistency is a basic requirement in human interface design and ergonomics. See ISO 11064.

28 HMI design shall be consistent as consistency is a basic requirement in human interface design and ergonomics. See ISO 11064.

29 This statement as written was problematic because the shelving function has no control over how many other alarms are annunciating at the same time an active alarm is unshelved. This clause was updated to resolve this issue.

30 The person putting the alarm out of service should indicate the anticipated duration as they cannot be certain of how long it will be out of service, and addition of a new statement that when returning to service the time and date shall be recorded.

31 The person putting the alarm out of service should indicate the anticipated duration as they cannot be certain of how long it will be out of service, and addition of a new statement that when returning to service the time and date shall be recorded.

32 The person putting the alarm out of service should indicate the anticipated duration as they cannot be certain of how long it will be out of service, and addition of a new statement that when returning to service the time and date shall be recorded.

33 The wording as written reflects technology from over 11 years ago and has caveats and thoughts about "extra cost and complexity". In 2020 solutions have been deployed at hundreds of sites and have been working for a decade or so. This clause is updated to reflect that reality.

34 Addition of a note about signal simulation.

35 Alarm priority information shall be included in alarm response procedure recommendation and needs to be added to this list.

36 Changed to "potential causes" to be consistent with definition 3.1.25.

37 Deficiencies and repairs should be documented to determine potential root cause and reduce likelihood of recurrence.

38 Deficiencies and repairs should be documented to determine potential root cause and reduce likelihood of recurrence.

39 The anticipated duration of the alarm being out of service should be documented.

40 "Maximum" is removed as it is not in the EEMUA document.

41 "Maximum" is removed as it is not in the EEMUA document.

42 This sentence is revised to clarify a target value.

IEC 62682

Edition 2.0 2022-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Management of alarm systems for the process industries

Gestion de systèmes d'alarme dans les industries de transformation

IEC 62682:2022-12(en-fr)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

MANAGEMENT OF ALARM SYSTEMS FOR THE PROCESS INDUSTRIES

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62682 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

This second edition cancels and replaces the first edition published in 2014. This edition constitutes a technical revision.

This edition includes minor technical changes with respect to the previous edition, based on changes to ANSI/ISA-18.2:2016. These include the inclusion of packaged systems in the scope (Clause 1), definitions (Clause 3) and alarm system requirements specification (Clause 7). There are changes to improve clarity in wording throughout the document.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65A/1046/FDIS	65A/1064/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

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 management life cycle. This document defines the terminology and models to develop an alarm system, and it defines the work processes recommended to effectively maintain the alarm throughout the life cycle. Ineffective alarm systems have often been cited as contributing factors in the investigation reports following major process incidents. This document is intended to provide a methodology that will result in the improved safety, quality, and operation in the process industries.

The first edition of this document 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. This second edition has incorporated some changes made in ANSI/ISA-18.2-2016.

This document 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*, with the 2nd edition published in 2007 and the 3rd edition published in 2013. In 2003 the User Association of Process Control Technology in Chemical and Pharmaceutical Industries (NAMUR) issued worksheet NA 102, *Alarm Management*, which was updated in 2008. During the development and maintenance of this document, 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 install third-party alarm system software,

c) design or install alarm systems,

d) operate and maintain alarm systems, and

e) audit or assess alarm system performance.

This document is organized in parts. The first part (Clause 1 to Clause 3) are normative without any mandatory requirements. Clause 4 contains mandatory requirements. Clause 5 is normative without any mandatory requirements. The main body of the standard (Clause 6 to Clause 18), describes mandatory requirements and non-mandatory recommendations.

Within this document, mandatory requirements are stated with "shall", non-mandatory recommendations are stated with "should", and permissible requirements are stated with "may". The phase "is required" indicates the requirement has been stated previously in the document.

MANAGEMENT OF ALARM SYSTEMS FOR THE PROCESS INDUSTRIES

1 Scope

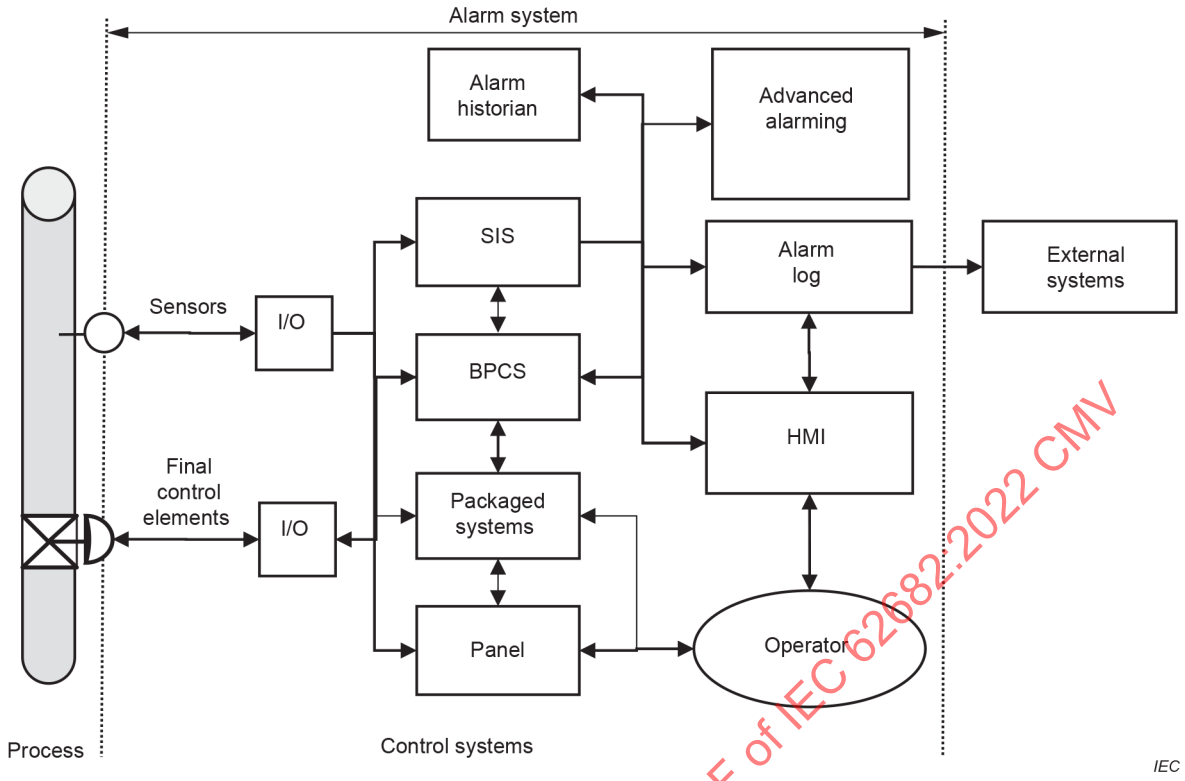
1.1 General applicability

This document specifies general principles and processes for the management of alarm systems based on controls system and human-machine interfaces (HMI) for facilities in the process industries. It covers all alarms to be presented to the operator through the control system, which includes alarms from basic process control systems, annunciators, packaged systems, and safety instrumented systems.

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

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. 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.

Figure 1 is not intended to represent physical wiring.



NOTE 1 Packaged systems (e.g., refrigeration machines) can be included in the control system.

NOTE 2 Panel can refer to annunciator panel or other panel types.

NOTE 3 The lines are intended to represent data flow and not physical wiring.

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 document. Management of operators is excluded from the scope of this document.

1.2.2 Process sensors and final control elements

The alarms implemented in sensors and final control elements are included in the scope of this document. The design and management of process sensors and final control elements are excluded from the scope of this document.

1.2.3 Annunciators

The integration of annunciators into an alarm system is included in the scope of this document. The specification and design of annunciators is excluded from the scope of this document.

1.2.4 Human machine interface

The appearance of alarms in the HMI and functions of alarm related displays are included in the scope of this document. The design and maintenance of the HMI are excluded from this document.

NOTE ANSI/ISA-101.01-2015 provides information on HMI design and maintenance.

1.2.5 Safety instrumented systems

The alarms implemented in a safety instrumented system are included in the scope of this document. The design and management of safety instrumented systems are excluded from this document.

NOTE IEC 61511-1 provides information on safety instrumented systems.

1.2.6 Fire and gas detection and protective systems

The alarms from fire and gas detection and protective systems presented to the operator through the control system are included in the scope of this document. The design and management of fire and gas detection and protective systems is excluded from the scope of this document.

1.2.7 Security systems

The alarms from security systems presented to the operator through the control system are included in the scope of this document. The design and management of security systems is excluded from the scope of this document.

1.2.8 Packaged systems

The alarms from packaged systems presented to the operator through the control system are included in the scope of this document. The design and management of packaged systems is excluded from the scope of this document.

1.2.9 Event data

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

1.2.10 Alarm identification methods

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

1.2.11 Management of change

A specific management of change (MOC) procedure is not included in this document. Some requirements and recommendations for an MOC procedure are included.

1.2.12 Purchase specification

This document is not intended to be used as an alarm system purchase specification.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1 Terms and definitions

3.1.1
absolute alarm
alarm generated when the alarm setpoint is exceeded

EXAMPLE: High-high, high, low, low-low.

3.1.2
acknowledge
operator action that confirms recognition of an alarm

3.1.3
active
alarm state in which the alarm condition is true

Note 1 to entry: Functions such as deadband, on or off delays and latching can allow the alarm to be active when the alarm condition is false or the alarm to not be active when the alarm condition is true.

3.1.4
adaptive alarm
alarm for which the setpoint is changed by an algorithm

EXAMPLE: Setpoint calculated based on production rate.

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 control system

EXAMPLE: Alarm priority.

3.1.10
alarm banner
graphic element that lists annunciated alarms with selected information

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

Note 2 to entry: Information can include the date, time, priority, and alarm type.

3.1.11
alarm class
group of alarms with common set of alarm management requirements

EXAMPLE: Safety related alarm class.

3.1.12
alarm deadband
change in signal from the alarm setpoint necessary for the alarm to return to normal

3.1.13
alarm flood
condition during which the alarm rate is greater than the operator can effectively manage

EXAMPLE: More than 10 alarms per 10 minutes.

3.1.14
alarm group
set of alarms with common association

EXAMPLE: Grouping alarms by 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

EXAMPLE: Message with operator action or probable cause.

3.1.19
alarm off-delay
debounce
time an alarm remains active after the process measurement has returned within the alarm setpoint

3.1.20
alarm on-delay
time before an alarm becomes active after the process measurement has exceeded the alarm setpoint

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

EXAMPLE: Priority can use seriousness of consequences and allowable response time to determine urgency.

3.1.23
alarm rate
number of annunciated alarms, per operator, in a specific time interval

3.1.24
alarm record
record
set of information which documents an alarm state change

3.1.25
alarm response procedure
guidance for response to an alarm

Note 1 to entry: The guidance can be in many forms and not only in the form of a procedure document.

Note 2 to entry: The guidance can include operator action, probable cause, and other information.

3.1.26
alarm setpoint
alarm limit
alarm trip point
threshold value of a process variable or discrete state that is used to determine the active state of the alarm

3.1.27
alarm summary
alarm list
display that lists annunciated alarms with selected information

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

Note 2 to entry: Information can include the date, time, priority, and alarm type.

3.1.28
alarm system
system for generating and handling alarms to help the operator manage 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 describes the functional requirements of the alarm system

3.1.30
alarm type
alarm attribute which gives a distinction of the alarm condition

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

3.1.31
allowable response time
maximum time between the annunciation of the alarm and when the operator must take corrective action to avoid the consequence

3.1.32
annunciator
device or group of devices that call attention to changes in process conditions

3.1.33
assessment
comparison of information from monitoring and additional qualitative (subjective) measurements against stated goals and defined performance metrics

3.1.34
audit <of alarm management>
comprehensive assessment that includes the evaluation of alarm system performance and of the work practices used to administer the alarm system

3.1.35
bad-measurement alarm
alarm generated when the signal for a process measurement is outside the expected range

EXAMPLE: Bad-measurement alarm generated at 3,8 mA for a 4 mA to 20 mA signal.

3.1.36
basic process control system
BPCS
system which responds to input signals from the process, its associated equipment, other programmable systems and/or operators and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented function

Note 1 to entry: A BPCS includes all of the devices necessary to ensure that the process operates in the desired manner.

Note 2 to entry: A BPCS typically may implement various functions such as process control functions, monitoring, and alarms.

[SOURCE: IEC 61511-1:2016, 3.2.3, modified − “SIF” has been changed to "safety instrumented function"]

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, the operator console

EXAMPLE: Alarm annunciated via pager or telephone.

3.1.41
chattering alarm
alarm that repeatedly transitions between the active state and the not active state in a short period of time

3.1.42
classification
process of separating alarms into alarm classes based on common requirements

Note 1 to entry: Requirements can include testing, training, and auditing.

3.1.43
console
operator console
hardware, software, and furniture or enclosure at which users monitor and/or control the process, which can include multiple stations, communication devices, and other devices

Note 1 to entry: The span of control of the operator is usually determined by the information available at the operator console.

3.1.44
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 one or more basic process control systems (BPCS), safety instrumented systems (SIS).

Note 2 to entry: The control system can include one or more packaged systems.

[SOURCE: IEC 61508-4:2010, 3.3.3, "EUC" has been deleted from the term defined, "from the process" has been changed to "from the equipment under control", "causing" has been changed to "that cause", notes have been modified]

3.1.45
controller-output alarm
alarm generated from the output signal of a control algorithm instead of a direct process measurement

EXAMPLE: Alarm on output on PID controller.

3.1.46
decommission
process to remove an alarm from the alarm system

3.1.47
deviation alarm
alarm generated when the difference between two values exceeds an alarm setpoint

EXAMPLE: Alarm on deviation between primary and redundant instruments or a deviation between process variable and controller setpoint.

3.1.48
discrepancy alarm
mismatch alarm
alarm generated by the difference between the expected plant or device state to its actual state

EXAMPLE: Alarm when a motor fails to start after it is commanded to the on state.

3.1.49
display
visual representation of information used by the operator for monitoring and control

3.1.50
dynamic alarming
automatic modification of alarm attributes based on process state or conditions

3.1.51
enforcement
enhanced alarming technique that can verify and restore alarm attributes in the control system to the values in the master alarm database

3.1.52
event
representation of a solicited or unsolicited fact indicating a state change

EXAMPLE: Mode changes and device state changes.

[SOURCE: IEC 62264-2:2013, 3.1.2, modified – "in the enterprise" has been deleted and an example has been added.]

3.1.53
first-out alarm
first-up alarm
alarm determined to be the first in a multiple-alarm scenario

Note 1 to entry: The first alarm is determined by logic.

3.1.54
fleeting alarm
alarm that transitions between an active alarm state and a not active alarm state in a short period of time without rapidly repeating

3.1.55
highly managed alarm
HMA
alarm belonging to a class with additional requirements above general alarms

Note 1 to entry: Regulatory requirements can be additional requirements.

EXAMPLE: Safety related alarm.

3.1.56
human machine interface
HMI
collection of hardware and software used by the operator and others to monitor and interact with the control system and with the process via the control system

3.1.57
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.

3.1.58
instrument diagnostic alarm
alarm to indicate a field device or signal fault

EXAMPLE: Out-of-range alarm.

3.1.59
interim alarm
alarm used on a temporary basis to replace an out-of-service alarm

3.1.60
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

3.1.61
master alarm database
authorized list of rationalized alarms and associated attributes

Note 1 to entry: The list can be in many forms and not only in the form of a database.

3.1.62
monitoring
measurement and reporting of quantitative (objective) aspects of alarm system performance

3.1.63
nuisance alarm
alarm that annunciates excessively, unnecessarily, or does not return to normal after the operator action is taken

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

3.1.64
operator
controller
person who monitors and makes changes to the process

3.1.65
operator alert
audible and/or visible means of indicating to the operator an equipment or process condition for evaluation when time allows which could result in a response

3.1.66
out-of-service
state of an alarm during which the alarm indication is indefinitely suppressed, typically manually, for reasons such as maintenance

3.1.67
packaged system
self-contained combination of hardware and software that can provide alarm, HMI, and control functionality for a specific process function that is part of a facility

3.1.68
plant state
plant mode
defined set of operational conditions for a process plant

EXAMPLE: Shutdown, normal operation.

3.1.69
prioritization
process of assigning a level of operational importance to an alarm

3.1.70
process area
physical, geographical or logical grouping of resources determined by the site

3.1.71
rate-of-change alarm
alarm generated when the change in process variable per unit time (dPV/dt) exceeds a defined setpoint

3.1.72
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

3.1.73
re-alarming alarm
re-triggering alarm
alarm that is automatically re-annunciated under certain conditions

3.1.74
recipe-driven alarm
alarm with setpoints that depend on the recipe that is currently being executed

3.1.75
remote alarm
alarm from a remotely operated facility or directed to a remote interface

3.1.76
reset
operator action that unlatches a latching alarm

3.1.77
return to normal
clear
alarm transition from an active alarm state to a not active alarm state

3.1.78
safety instrumented system
SIS
instrumented system used to implement one or more safety instrumented functions

Note 1 to entry: A SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s). It also includes communication and ancillary equipment (e.g., cables, tubing, power supply, impulse lines, heat tracing).

Note 2 to entry: A SIS may include software.

Note 3 to entry: A SIS may include human action as part of a SIF (see ISA TR 84.00.04:2015, part 1).

[SOURCE: IEC 61511-1:2016, 3.2.67, modified – Removed figure from notes and reference to figure from note 1]

3.1.79
safety related alarm
safety alarm
alarm that is classified as critical for the protection of human life or the environment

EXAMPLE: An alarm indicating a potential asphyxiation hazard.

3.1.80
shelve
temporarily suppress an alarm, initiated by the operator, with engineering controls to unsuppress the alarm

Note 1 to entry: Engineering controls can include time limits.

3.1.81
silence
operator action that terminates the audible alarm indication

3.1.82
stale alarm
alarm that remains annunciated for an extended period of time

EXAMPLE: Alarm that remains annunciated for 24 hours.

3.1.83
state-based alarm
mode-based alarms
alarm that has attributes modified or is suppressed based on operating states or process conditions

3.1.84
statistical alarm
alarm generated based on statistical processing of a process variable or variables

3.1.85
suppress
prevent the annunciation of the alarm to the operator when the alarm is active

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

3.1.86
suppress by design
alarm annunciation to the operator prevented based on plant state or other conditions

3.1.87
system diagnostic alarm
alarm generated by the control system to indicate a fault within the system hardware, software or components

EXAMPLE: Communication error.

3.1.88
tag
control system point
point
unique identifier assigned to a process measurement, calculation, or device within the control system

3.1.89
unacknowledged
alarm state in which the operator has not yet confirmed recognition of an alarm indication

3.1.90
unshelve
transition from the shelved alarm state to the normal or unacknowledged state

3.1.91
unsuppress
transition from a suppressed alarm state to the normal or unacknowledged state

3.2 Abbreviated terms

ACKED	Acknowledged
ASRS	Alarm system requirements specification
BPCS	Basic process control system
CGMP	Current good manufacturing practice
DSUPR	Suppressed-by-design
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
UNACK	Unacknowledged

4 Conformance to this document

4.1 Conformance guidance

To conform to this document, it shall be shown that each of the mandatory requirements has been satisfied.

4.2 Existing systems

For existing alarm systems designed and constructed in accordance with codes, standards, or practices prior to the issue of this document, 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 document shall be applied to existing systems in a reasonable time as determined by the owner/operator.

4.3 Use of required functionalities

This document requires certain control system functionalities (e.g., shelving) to support the alarm system. Where an alarm system does not have all required functionality, conformance may be achieved if the functionality described in the alarm philosophy is provided.

4.4 Responsibility

Conformance to this document is the responsibility of the owner/operator.

4.5 Local Jurisdictions

Some jurisdictions where the governing authorities (for example national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, in addition to the requirements of this document.

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.

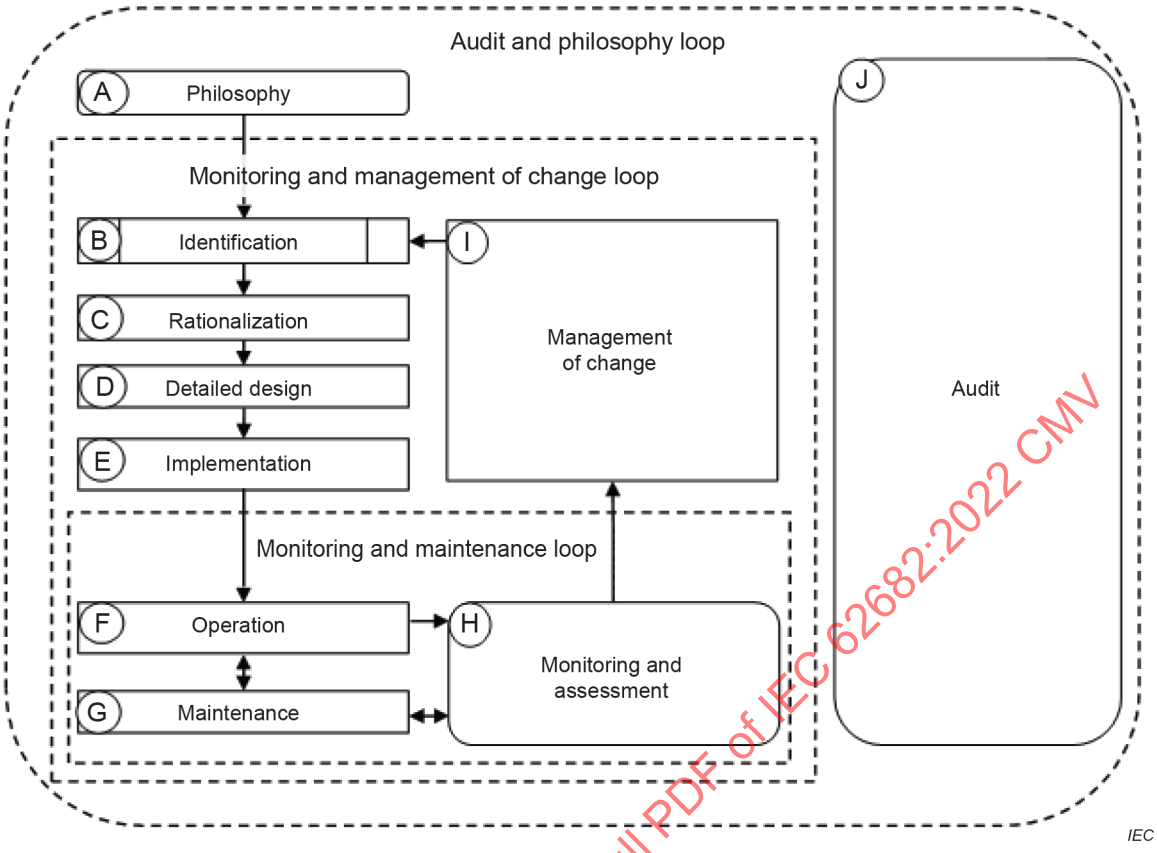
A foundational part of alarm management is the definition of an alarm: an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response. An essential element of this definition is the response to the alarm. This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

5.2 Alarm management life cycle

5.2.1 Alarm management life cycle model

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

The life cycle model is useful in organizing the requirements and responsibilities for implementing alarm management. The life cycle 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 document (see 5.2.2.3).

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

NOTE 3 The rounded shapes of stages A, H, and J represent entry points to the life cycle (see 5.2.3).

NOTE 4 The dotted lines represent the loops in the life cycle (see 5.2.5).

Figure 2 – Alarm management life cycle

5.2.2 Alarm management life cycle stages

5.2.2.1 General

The alarm management life cycle 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 Clause 6 to Clause 18 of this document.

5.2.2.2 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. The alarm philosophy reflects the operations and maintenance work processes and can reference those processes in other documents. 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. The philosophy specifies the processes used for each of the alarm management life cycle stages, such as the threshold for the MOC process and the specific requirements for change. The philosophy is maintained to ensure consistent alarm management throughout the life cycle of the alarm system.

The development of the ASRS is included in the philosophy stage of the life cycle. 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 can provide specific guidance for system design.

5.2.2.3 Identification (B)

The identification stage is a collection point for potential alarms proposed by one of the methods for determining if an alarm is necessary. These methods are defined outside of this document so the identification stage is represented as a predefined process in the life cycle. 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. Information from identification (e.g., alarm setpoint, consequence) should be captured for rationalization. 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 the alarm 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 and definitions 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 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., testing, training, monitoring, and audit 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 additional 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 state and alarm priority.

Advanced alarming techniques (e.g., state-based alarming) improve the effectiveness of the alarm system beyond the basic alarm and HMI design.

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 can 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 can trigger maintenance work or identify the need for changes to the alarm system or operating procedures. Without monitoring an alarm system is likely to degrade over time.

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 life cycle stages from identification to implementation.

5.2.2.11 Audit (J)

In the audit stage, periodic reviews are conducted to evaluate the effectiveness of the alarm management process and maintain the integrity of the alarm system. 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 management life cycle entry points

5.2.3.1 General

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

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 life cycle stages are only the initial step in managing an alarm system. All stages of the life cycle are necessary for complete alarm management.

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 can be used as the basis for the ASRS. This is the life cycle entry point for new systems.

5.2.3.3 Start with monitoring and assessment (H)

The second possible starting point is to begin monitoring an existing alarm system and benchmark 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 document. The results of the initial audit can be used in the development of a philosophy.

5.2.4 Simultaneous and encompassing stages

The life cycle diagram (Figure 2) is drawn to represent sequential stages. There are several simultaneous stages which are represented in the life cycle. 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 life cycle are authorized and completed.

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

5.2.5 Alarm management life cycle loops

5.2.5.1 General

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

5.2.5.2 Monitoring and maintenance loop

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

5.2.5.4 Audit and philosophy loop

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

5.2.6 Alarm management life cycle stage inputs and outputs

The alarm management life cycle stages are connected as the outputs of one stage are often the inputs to another stage. The connections are not fully represented in the life cycle diagram (Figure 2). Table 1 provides more information on the relationships between the inputs and outputs of the life cycle stages.

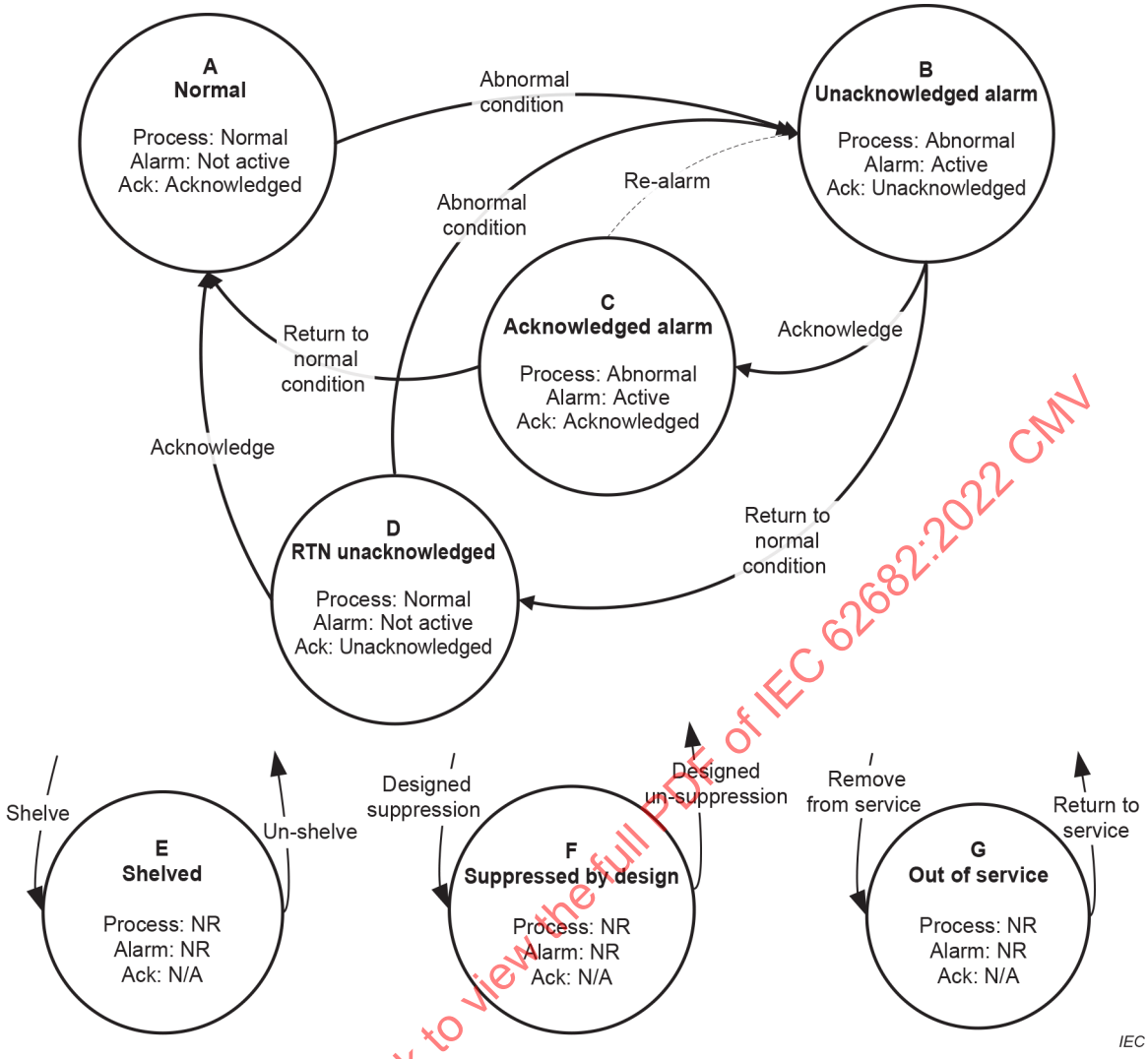
Table 1 – Alarm management life cycle stage inputs and outputs

Alarm management life cycle stage		Activities	Clause number	Inputs	Outputs
Stage	Title				
A	Philosophy	Documenting the objectives, guidelines and work processes for alarm management, and ASRS	6, 7	Objectives and standards, audit recommendations	Alarm philosophy and ASRS
B	Identification	Determining potential alarms	8	PHA report, P&IDs, operating procedures	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	Installing alarms, implementation testing, and implementation training	13	Completed alarm design, master alarm database, and ASRS	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, modifications, and deletions of alarms	17	Alarm philosophy and proposed changes	Authorized alarm 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.



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.

NOTE 3 N/A indicates not applicable.

NOTE 4 NR indicates that the state is not relevant (either normal or abnormal, not active or active).

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 not active and previous alarm occurrences 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 not active before an operator has acknowledged the alarm.

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 and not annunciated, typically for maintenance. An alarm in the out-of-service state is in the maintenance stage of the life cycle.

NOTE An alarm in the out-of-service state is not the same as out of service of a unit or equipment. Equipment can be out of service while the associated alarms are not out of service.

5.3.2.9 Summary of alarm states

The alarm status, annunciation status, and acknowledge status of different alarm states are summarized in Table 2.

Table 2 – Summary of alarm states

ID	Mnemonic	State name	Process condition	Alarm status	Annunciation status	Acknowledge status
A	NORM	Normal alarm state	Normal	Not active	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	Not active	Annunciated	Unacknowledged
E	SHLVD	Shelved state	Normal or abnormal	Not active or active	Suppressed	Not Applicable
F	DSUPR	Suppressed-by-design state	Normal or abnormal	Not active or active	Suppressed	Not Applicable
G	OOS RV	Out-of-service alarm state	Normal or abnormal	Not active or active	Suppressed	Not Applicable

5.3.3 Alarm state transition paths

5.3.3.1 General

The arrows in Figure 3 represent transitions between states. The diagram does not directly illustrate the effects of alarm deadband, on-delay, or off-delay, which can impact the evaluation of alarm status (i.e., active or not active).

5.3.3.2 Transition from normal to unacknowledged (A → B)

The transition from normal to unacknowledged occurs when the process has gone out of the normal range beyond the alarm setpoint and has remained in this state long enough to make the alarm active.

5.3.3.3 Transition from unacknowledged to acknowledged (B → C)

The transition from unacknowledged to acknowledged 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)

The transition from acknowledged to unacknowledged is the infrequently used option that periodically generates repetitive alarm indications for a single alarm while the alarm remains active.

5.3.3.5 Transition from acknowledged to normal (C → A)

The transition from acknowledged to normal is part of a normal sequence for an alarm. The alarm moves from the acknowledged state to normal and becomes not active.

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

The transition from unacknowledged to return-to-normal unacknowledged occurs when the process returns to normal and the alarm becomes not active before an operator has acknowledged the alarm.

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

The transition from return-to-normal unacknowledged to normal occurs when an alarm has returned to normal and becomes not active. This transition can require operator acknowledgment or can be acknowledged automatically.

5.3.3.8 Transition to shelved (any state → E)

The transition to shelved 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)

The transition from shelved to normal or unacknowledged occurs when an alarm is unshelved, manually or automatically. If the alarm is automatically unshelved, the transition should be to the unacknowledged state. If the alarm is manually unshelved, the transition should be to the acknowledged state.

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

The transition to suppressed-by-design occurs when process conditions are used to suppress alarms by design. Designed suppression is typically an automatic operation.

5.3.3.11 Transitions from suppressed-by-design to normal or unacknowledged (F → A or B)

The transition from suppressed-by-design to normal or unacknowledged occurs when process conditions are used to unsuppress alarms when appropriate. Designed unsuppression is typically an automatic operation. If the alarm is active, the transition should be to the unacknowledged state. If the alarm is not active, the transition should be to the normal state.

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

The transition to out-of-service state occurs when an alarm is removed from service for maintenance or other reasons. Remove from service is typically a manual operation.

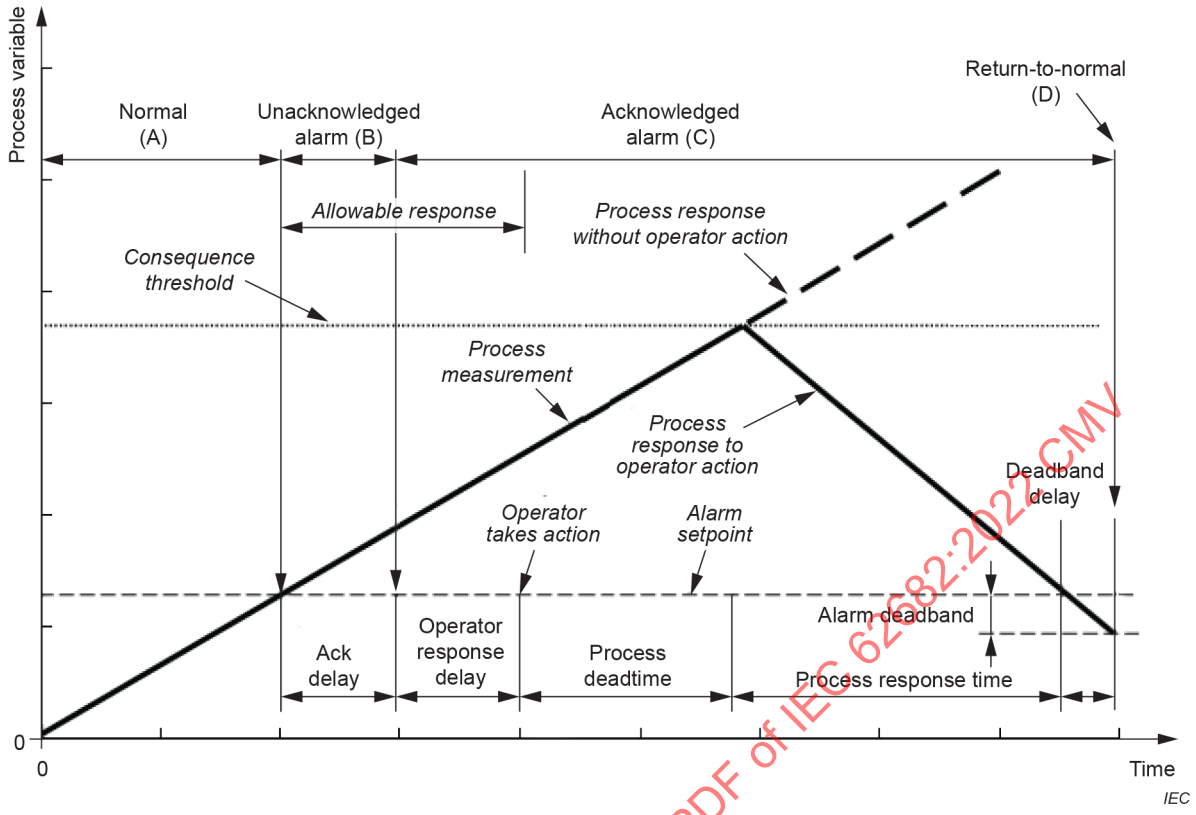
5.3.3.13 Transition from out-of-service to normal or unacknowledged (G → A or B)

The transition from out-of-service to normal or unacknowledged occurs when an alarm is returned to service when it is available after maintenance. Return to service is typically a manual operation. If the alarm is active, the transition should be to the unacknowledged state. If the alarm is not active, the transition should be to the normal 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. Figure 4 illustrates only one possible scenario to clarify the definition of terms related to time.



NOTE Ack delay, operator response delay and process deadtime can be zero.

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 not active, and previous alarm occurrences 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

a) measurement accuracy,

b) sampling interval, and

c) 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, after the acknowledge delay. In this state the alarm is active. The operator can take action before or after acknowledging the alarm. There are several factors that affect the operator response time such as

a) system processing speed,

b) HMI design and clarity,

c) operator awareness and training,

d) operator workload,

e) complexity of determining the operator action, and

f) 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 time until the alarm returns to normal. 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 Allowable response time

The allowable response time is the time beginning with the alarm annunciation and ending at the last moment operator action can prevent the consequence. It can be estimated working backwards from the consequence threshold, considering the process deadtime, the rate of change of the process variable and the separation between the alarm setpoint and the consequence threshold. In Figure 4, the operator response delay is shown within the allowable response time.

5.4.7 Alarm setpoint

The alarm setpoint can be adjusted to increase or decrease the allowable response time. The process for evaluating the alarm setpoint is alarm setpoint determination.

5.4.8 Consequence threshold

The consequence threshold is the value of the process measurement at which the consequence begins to occur. 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.

5.4.9 Alarm deadband

The deadband delay shown in Figure 4 illustrates that the alarm does not return to normal immediately after crossing the alarm setpoint.

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.

The following three stages of activity occur in the operator sub-system leading to action:

a) the indication of deviation from desired normal operation (i.e., an alarm) is detected,
b) the situation is diagnosed, and the corrective action is determined, and
c) the corrective action is implemented to compensate for the disturbance.

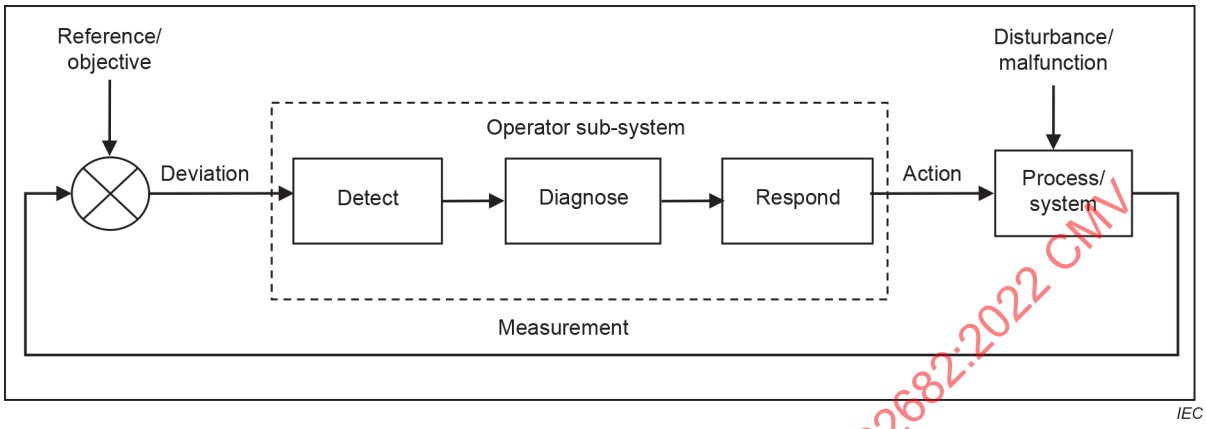


Figure 5 – Feedback model of operator-process interaction

5.5.2 Detect

The operator becomes aware of the deviation from the desired condition by an alarm caused by a disturbance. The design of the alarm system and the operator interface facilitates 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. The alarm response procedures aid the operator's diagnosis.

5.5.4 Respond

The operator takes corrective action in response to the deviation and monitors the process to determine if the deviation is corrected.

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:

a) workload,
b) operator console ergonomics,
c) HMI design,
d) short term or working memory limitations,
e) fatigue,
f) training, and
g) motivation.

6 Alarm philosophy

6.1 Purpose

The alarm philosophy serves as the framework to establish the criteria, definitions, principles, and responsibilities for all of the alarm management life cycle stages. This is achieved by specifying items, including the methods for alarm identification, rationalization, monitoring, MOC, 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

An alarm philosophy document shall be developed to cover each alarm system. An alarm philosophy may cover more than one alarm system. The alarm philosophy shall include the required contents listed in this clause. The alarm philosophy shall be developed prior to rationalization.

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 contents

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

Alarm philosophy contents	Required / recommended	Subclause
Alarm system performance monitoring	Required	6.2.23
Alarm history preservation	Recommended	6.2.24
Management of change	Required	6.2.25
Alarm system audit	Required	6.2.26
Related site procedures	Recommended	6.2.27

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 alarm philosophy.

6.2.2 Purpose of alarm system

The purpose and objectives of an alarm system shall be stated. The purpose and objectives stated serve to orient participants in design and improvement activities and can facilitate the implementation and maintenance of an effective alarm system.

6.2.3 Definitions

The alarm philosophy shall include definitions of terms that will be encountered in the course of design and improvement of an alarm system to ensure that all participants share a common understanding. The definition of an alarm shall be documented in the alarm philosophy.

6.2.4 References

The alarm philosophy should include a list of appropriate references. References can be internal company documents (e.g., MOC procedure), external standards, or published material.

6.2.5 Roles and responsibilities for alarm management

The alarm philosophy shall establish responsibility by role for the activities of the alarm management life cycle. Specific aspects should include the following:

a) the owner of the alarm system, the philosophy, master alarm database, 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 alarms,

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

6.2.6 Alarm design principles

The alarm philosophy shall include the criteria for selection and principles for design of alarms, consistent with the definition of an alarm. The criteria and principles should include:

a) the role of the alarm system in identifying approaches to unsafe or abnormal 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) that the facility will use.

6.2.7 Alarm setpoint determination

The alarm philosophy should provide guidance on the methods used for determination of alarm setpoints. Alarm setpoint determination can use several inputs (e.g., consequence thresholds, process dynamics, complexity of the operator response).

6.2.8 Prioritization method

Consistent priorities aid the operator in deciding the order of response during a period with a high alarm rate. The alarm philosophy shall address the prioritization, including the following:

a) the basis for alarm prioritization (e.g., severity of consequence, time to respond),
b) the metrics for alarm priority (e.g., priority distribution),
c) the impact of classification on prioritization, if any.

6.2.9 Alarm class definition

Alarm classes are used to set common requirements for managing alarms. An alarm may belong to more than one class. This alarm philosophy shall include the definition of the alarm classes, which can include the following:

a) alarm prioritization considerations,
b) alarm documentation,
c) HMI design,
d) operating procedures associated with the alarms,
e) training and training documentation,
f) alarm maintenance,
g) alarm testing,
h) alarm monitoring and assessment,
i) alarm MOC,
j) alarm history retention, and
k) alarm audit.

6.2.10 Highly managed alarms

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

a) alarms critical for the protection of human life (e.g., safety related 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.

6.2.11 Rationalization

The alarm philosophy shall list the criteria to assess alarms and the information to be captured during rationalization. Guidance on the knowledge and experience of the rationalization team should include:

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

6.2.12 Alarm documentation

The alarm philosophy shall specify the documentation for alarms. This should include the following:

a) rationalization information (e.g., a master alarm database), and
b) specifications for advanced alarming techniques (e.g., designed suppression).

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

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

6.2.13 Alarm design guidance

The alarm philosophy shall provide guidance on the design practices. This guidance should address:

a) alarm deadband,
b) alarm on-delay,
c) alarm off-delay
d) alarm types, and
e) composition of alarm messages.

6.2.14 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.

6.2.15 HMI design principles

The alarm philosophy shall specify the alarm presentation method to establish principles for consistent display and annunciation.

The following elements should be specified for HMI design:

a) the alarm presentation method (e.g., colour, symbol, and alpha-numeric),
b) the mechanism used (for example the HMI) to communicate the alarms to the operator,
c) recommendations for the indications on the HMI of the alarm states (e.g., normal, acknowledged, shelved) that will be used at the facility,
d) the types of displays that will be used (e.g., alarm summary, first-out),
e) the functions that will be available in the HMI, including shelving, suppression, and enhanced and advanced alarming techniques.

6.2.16 Approved enhanced and advanced alarming techniques

If enhanced and advanced alarming techniques are used, this section of the alarm philosophy shall be used to identify the approved techniques and related responsibilities and work processes. 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.

6.2.17 Implementation guidance

The alarm philosophy shall specify the methods for initial training, commissioning, and testing of the alarm system.

6.2.18 Alarm response procedures

The alarm philosophy shall address alarm response procedures. Available alarm response procedures can reduce the time it takes the operator to diagnose the problem and determine the appropriate corrective action, as well as promote consistency between operators. The philosophy should include the following:

a) the information included in the alarm response procedures (e.g., cause, consequence, corrective action), and

b) the method to access the alarm response procedures (e.g., via the operator interface).

6.2.19 Training

The alarm philosophy shall address how plant personnel are to be trained on the use, management, and design of the alarm system, including the training documentation requirements.

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

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

b) when training is required.

6.2.20 Alarm shelving

The alarm philosophy should include guidance on how and when alarm shelving can be used, who can perform shelving, as well as authorization and documentation requirements. There are typically limits defined on which alarms can be shelved and shelving duration, based on class or priority.

6.2.21 Alarm system maintenance

The alarm philosophy shall specify the activities necessary to maintain the alarm system. Specific elements for alarm system maintenance shall 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.

6.2.22 Testing of alarms

The alarm philosophy shall address testing based on alarm classes or other methods. Testing documentation may be managed in other systems.

6.2.23 Alarm system performance monitoring

The alarm philosophy shall specify methods for assessing alarm system performance. Specific elements for alarm system performance monitoring shall 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.

6.2.24 Alarm history preservation

The alarm philosophy should specify the retention of alarm related records (e.g., annunciations, acknowledgements, return to normal, and operator actions). In some industries and regions, regulatory bodies or local statutes might require preservation of this information and tracking of changes to data.

6.2.25 Management of change

The alarm philosophy shall identify the types of changes and the applicable MOC procedures. Types of changes can include:

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

b) permanent changes to the master alarm database, alarm attributes, or enhanced and advanced alarming techniques.

The MOC procedure ensures that changes made during design, implementation, operation, or maintenance are appropriately evaluated, authorized, and documented. This typically includes documented assessment of each change, description of each change, and authorization.

6.2.26 Alarm management audit

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

a) audit frequency, which can be specified based on alarm class,

b) audit topics, and

c) process for operator interviews.

6.2.27 Related site procedures

The alarm philosophy should reference relevant procedures. The following documents can be related to the alarm philosophy:

a) standard operating procedures,

b) training policies and guides,

c) safety, health and environmental procedures,

d) maintenance procedures,

e) alarm handling policies,

f) application programming guidelines,

g) commissioning or qualification processes and procedures,

h) MOC procedure, and

i) other site procedures related to the alarm philosophy.

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. The alarm philosophy should be approved by management. 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) MOC process.

7 Alarm system requirements specification

7.1 Purpose

The alarm system requirements specification (ASRS), which can also be called an alarm functional requirements specification, is developed based on the alarm philosophy and can be an important part of control system procurement. Clause 7 provides guidance on the development and uses of an ASRS. 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 ASRS 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 relevant site infrastructure requirements. These requirements are used to help evaluate alarm systems and guide the detailed alarm system design. During implementation, the ASRS can serve as the basis of function testing of the alarm system. The ASRS specifies the alarm system functionality necessary to satisfy the alarm philosophy.

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

7.2 Recommendations

An ASRS should be developed for new control systems and major revisions to the alarm functionality of existing control systems. The ASRS should include 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 management life cycle activities.

There can be new control system projects in which it is determined that an ASRS is not necessary (e.g., replicating existing systems).

7.3 Development

The alarm system is one of the functional systems within a control system. Modifications to accommodate the alarm system requirements can be necessary to achieve the desired performance. The ASRS should be consistent with the alarm philosophy. 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 attribute 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.

7.4 Systems evaluation

Alarm system functionality should be evaluated against the ASRS during control system selection.

7.5 Packaged systems

If packaged systems are part of the control system, the ASRS should include guidance on how packaged systems will be interfaced to the alarm system.

7.6 Customization

If important system requirements in the specification are not met by standard commercial products, it can be necessary to develop custom solutions, or to reconsider the specification. The ASRS facilitates early recognition of the need for customized solutions and associated cost /benefit analysis.

7.7 Alarm system requirements verification

Each alarm system requirement should be verified prior to the operations stage of the life cycle.

8 Identification

8.1 Purpose

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 management life cycle for the recommended alarms or alarm changes. Identified alarms are an input to rationalization.

8.2 Alarm identification methods

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

Some common alarm identification methods are:

a) process hazards analysis (PHA or HAZOP),
b) layer of protection analysis (LOPA),
c) incident investigations,
d) environmental permits,
e) failure mode and effects analysis (FMEA),
f) current good manufacturing practice (cGMP),
g) quality reviews,
h) P&ID reviews,
i) operating procedure reviews, and
j) packaged system manufacturer recommendations.

8.3 Identification training

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

8.4 Identification documentation

The information related to potential alarms should be documented during identification and used in alarm rationalization if available, including:

a) the consequence threshold (e.g., constraint),
b) the operator response,
c) the consequence of inaction,
d) the probable cause, and
e) the rationale for the consequence threshold.

9 Rationalization

9.1 Purpose

During rationalization, existing or potential alarms are systematically compared to the criteria for alarms documented 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 alarm philosophy. Rationalization produces the detail design information, documented in the master alarm database, necessary for the design stage of the alarm management life cycle.

The activities of rationalization are:

a) alarm justification,
b) alarm setpoint determination,
c) alarm prioritization,
d) alarm classification, and

e) rationalization review.

9.2 Rationalization documentation

9.2.1 Rationalization documentation requirements

Each alarm shall be rationalized and documented as specified in the alarm philosophy, for each applicable plant state. The documentation shall include:

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

Additional alarm attributes may be documented during rationalization.

9.2.2 Rationalization documentation recommendations

Rationalization should determine and document the following for every alarm per the alarm philosophy, for each applicable plant state:

a) the maximum allowable response time,
b) the probable cause,
c) the rationale for the alarm setpoint,
d) the identification method, and
e) the need for advanced alarming techniques, if necessary.

9.2.3 Plant states

Plant states can include:

a) start-up,
b) normal operation,
c) operation, step, or phase in batch processes, and
d) shutdown.

9.3 Alarm justification

9.3.1 Alarm justification process

Each alarm is compared to the criteria in the alarm philosophy to justify that it is an alarm.

The criteria from the definition of alarm include that:

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) include knowledge of the process and the control system, and

c) rely heavily upon operator knowledge.

9.3.3 Individual alarm justification

All alarms are systematically reviewed, usually 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, and typically includes:

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

b) the action(s) the operator can take in response to the alarm;

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

d) the allowable response time.

Those alarms for which the operator action 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 performance

Alarm justification should verify that:

a) the alarm will not become a nuisance, and

b) the alarm does not duplicate another alarm.

Advanced alarming techniques (e.g., state-based alarming) can be specified to prevent negative impact on the alarm system performance from the above listed conditions.

9.4 Alarm setpoint determination

The guidance stated in the alarm philosophy should be applied to the determination of alarm setpoints.

Effective methods use information including:

a) the allowable response time (see Figure 4),

b) the complexity of the operator action,

c) the time necessary to complete the operator action,

d) the normal operating range,

e) other operating or design boundaries, and

f) knowledge of the process operation and history.

For some processes (e.g., batch processes), the alarm setpoint may be modified with plant state.

9.5 Prioritization

Alarm priority is used to aid the operator in determining the order in which to respond to multiple alarms. The method for priority assignment defined in the alarm philosophy is applied to the rationalized alarm and a priority is 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. Alarm priority distribution metrics 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 Classification

Alarms shall be assigned to one or more classes as defined in the alarm philosophy. Classification may occur prior to, during, or after the alarm justification and prioritization.

Alarms in the same class may have different priorities.

9.7 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 documented in the alarm philosophy.

9.8 Removal of rejected alarms

Existing alarms that are rejected for failing to meet the criteria for an alarm shall be documented along with the basis (i.e., criterion it failed to meet) justifying removal. Rejected alarms can be candidates for other forms of notifications (e.g., operator alerts). Those alarms should then be subject to further review by the MOC procedure to remove the alarm from the system.

9.9 Documentation

Rationalization shall be documented to become the basis for ensuring the integrity of the alarm system. The documentation (e.g., a master alarm database) is 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 management life cycle,

b) utilization as part of the MOC,

c) alarm response procedures,

d) training of and use by operators,

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

f) 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 life cycle. Clause 10 addresses the design consideration to implement the alarms within a specific control system as specified by the rationalization process. All design considerations related to the presentation of alarms are contained in Clause 11.

10.2 Basic alarm design capabilities

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

10.3 Usage of alarm states

10.3.1 Alarm state triggering

The source for each alarm 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 devices (e.g., sensors and final control elements),
b) the control system (i.e., BPCS, SIS, packaged system), and
c) the HMI.

10.3.2 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 functions (e.g., as an interlock setpoint) in addition to operator notification, then documentation, training and MOC 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 and higher access level required). This information should be specifically documented in the alarm philosophy under alarm design principles.

10.3.3 Alarm suppression and other logic functions

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

10.4 Alarm types

Alarm type shall be implemented based on the information documented in the master alarm database. The common alarm types can 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-alarming alarms,
n) statistical alarms,
o) first-out alarms, and
p) bad-measurement alarms.

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

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

10.5 Alarm attributes

10.5.1 General

During the basic design process, the alarm attributes should be selected for each alarm that has been rationalized and set based on engineering judgment. Attributes such as alarm 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 description,

b) alarm setpoint or logical conditions,

c) alarm priority,

d) alarm deadband,

e) on-delay or off-delay

f) alarm group, and

g) alarm message.

10.5.2 Alarm description

All alarms shall have an informative text provided as a tag description, or alarm description, or both. A structured layout and consistent wording should be used in the description.

10.5.3 Alarm setpoints

Alarm setpoints shall be selected based on the information documented in the master alarm database.

10.5.4 Alarm priority

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

10.5.5 Alarm deadbands

10.5.5.1 General

Alarm deadband is an alarm attribute used to reduce the number of times an alarm is triggered for a given abnormal condition, which ideally would be only once. It prevents an alarm from returning to normal until the alarm is cleared by the deadband, a 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.

10.5.5.2 Alarm deadband requirements

The control system shall provide the functionality to implement deadband.

10.5.5.3 Alarm deadband recommendations

The engineering basis for 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 100,000) can act as a latch, creating stale alarms. Settings should be documented and then reviewed during commissioning and after significant operating experience.

10.5.6 Alarm on-delay and off-delay

10.5.6.1 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 the alarm setpoint, thus preventing the alarm from becoming active until the signal remains in the alarm condition continuously for the delay time. The off-delay is used to reduce chattering alarms by holding the alarm active for the delay period after the process condition has returned to normal.

10.5.6.2 Alarm on-delay and off-delay requirements

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

10.5.6.3 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 determination should take into consideration the allowable 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 delay on operator response. Settings should be reviewed during commissioning and after sufficient operating experience.

10.6 Programmatic changes to alarm attributes

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

a) control logic (e.g., sequences, phases, state-based logic),

b) advanced alarming techniques,

c) 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 the functionality for programmatic changes. For each alarm, it should be identified and documented which programs of the system will have access to modify alarm attributes during operation and which changes will be subject to MOC procedures. Advanced alarming techniques for modifying alarm attributes are covered in Clause 12.

10.7 Review of basic alarm design

A typical control system provides the ability to implement numerous different alarm types for a single process variable. The basic alarm design results should be reviewed against the master alarm database to ensure that only the required alarms are implemented.

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 life cycle stage. Clause 11 provides requirements and recommendations related to the presentation of alarms to the operator and other HMI users. The indication of alarms is only one component of the HMI design, and contributes to effective operator–process interaction (see Figure 5).

NOTE Guidance for HMI design and maintenance is provided in ANSI/ISA-101.01.

11.2 HMI functions

11.2.1 General

The HMI design for alarms shall 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) unsuppressed active alarms,
b) alarm states,
c) alarm priorities, and
d) alarm types.

11.2.3 HMI functional requirements

The HMI shall provide the ability to:

a) silence audible alarm indications (i.e., without acknowledging the alarm),
b) individually 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) support a designed suppression function, and
g) display alarm messages.

11.2.4 HMI functional recommendations

The HMI should provide the ability for the operator to access the alarm response procedures.

11.2.5 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,
e) suppressed-by-design summary displays, and
f) out-of-service summary displays.

11.2.6 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.

11.2.7 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) alarm group or process area,
d) alarm class(es), 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, text, a combination or shape and 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, text, a combination or shape and text), and should be related 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 unique. 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 unique. 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 unique. No audible indication should be used to identify out-of-service alarms.

11.3.3.9 Summary of alarm state indications

The 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

NOTE 1 "Yes" signifies the indication type is used to indicate the alarm state.

NOTE 2 "No" signifies the indication type is not to be used to indicate the alarm state.

NOTE 3 "Combination" signifies the indication is a combination of visual colour and symbol indications.

NOTE 4 "Optional" signifies the indication is not required.

11.3.4 Audible alarm state indications

The audible alarm indication for unacknowledged alarms may also be 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, 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, except in operating environments where this is not practical.

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, text) should be used to indicate each alarm priority to reinforce colour coding.

NOTE The combination of unique colour and symbol can be used to compensate for colour blindness.

11.4.4.3 Audible alarm priority indications

A distinct 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 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 message should be structured with consistent information. The visual alarm message is usually not directly displayed on process displays.

11.5.2.3 Vocalized alarm message indications

A vocalized alarm message may 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. The displays can 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) suppressed-by-design alarm display, and

i) out-of-service alarm display.

The displays are described with required or recommended functions. The function may be provided through other methods.

11.6.2 Alarm summary display

11.6.2.1 Alarm summary display requirements

The alarm summary provides a list of unsuppressed 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 information for alarms. 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 current process value,
b) the alarm setpoint,
c) the alarm group or process area, and
d) 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 multiple visible alarms, with access-controlled methods as allowed in the alarm philosophy.

11.6.2.6 Functional recommendations

The alarm summary display should provide the following functions:

a) navigational link to the appropriate process display,
b) access to alarm response procedures,
c) filtering of alarms by time of alarm,
d) filtering of alarms by priority,
e) filtering of alarms by alarm type,
f) filtering of alarms by alarm group or 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 should be provided. The alarm summary status display provides an indication of the number of unsuppressed 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).

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 by tag name,

b) filtering by time of alarm state change,

c) filtering by type of alarm state change,

d) filtering by priority,

e) filtering by alarm type, and

f) filtering of alarms by alarm group or 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 graphic elements

Other graphic elements (e.g., alarm banners) may be used to indicate alarm states.

11.7 Alarm shelving

11.7.1 General

The shelving of alarms is a required function. This temporary suppression of alarms by the operator is a common practice to keep nuisance alarms from interfering with the effectiveness of the alarm system. Shelving includes a functionality, such as a time limits, 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 shelve action with timestamp, and

g) a record of each unshelve event with timestamp.

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 unshelving alarm floods by automatically unshelving active alarms too quickly. The state transitions from shelving are:

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.

The shelving function should record the identity of the person that shelved the alarm.

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 alarm 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) unshelving of alarms by group,
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 a required function and a 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 out-of-service action with timestamp, and
f) a record of each return-to-service event with timestamp.

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,
c) alarm type,
d) the 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 and the approximate anticipated duration of the suppression (e.g., less than an hour, less than a day, less than a week, less than a month).

11.9 Alarms suppressed by design

11.9.1 General

The designed suppression of alarms is a required function and it is common practice to suppress alarms that are not needed due to intended or actual operating conditions. This functionality supports the testing, maintenance, and operator understanding of designed suppression.

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,
b) a record of each suppress-by-design event with timestamp, and
c) a record of each unsuppress-by-design event with timestamp.

11.9.3 Designed suppression functional recommendations

The designed 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 if the alarm is active.

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 alarm status (i.e., 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.

11.9.4.5 Functional recommendations

Suppressed-by-design displays should provide the ability for the operator to unsuppress an alarm or disable the designed suppression.

11.10 Alarm annunciator integration

11.10.1 General

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

11.10.2 Alarm annunciator integration recommendations

Alarm annunciators should be integrated in a manner that provides 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 related alarm HMI

11.11.1 General

An independent HMI can be required for some safety related alarms by code or standards.

11.11.2 Independent safety related alarm HMI

An HMI independent from the BPCS can be required for the following safety related 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 action, communication fault).

NOTE For further guidance, see IEC 61511 series.

12 Detailed design: enhanced and advanced alarming

12.1 Purpose

Enhanced and advanced alarming is part of the detailed design life cycle 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 are additional layers of logic, programming, or modelling used to modify alarm attributes. Advanced alarming modifies alarm behaviours including logic-based alarming, dynamic alarming, state-based alarming (i.e., mode-based alarming), and adaptive alarms. Most designed suppression techniques are included in advanced alarming. In addition to advanced alarming techniques, enhancements to the alarm system also provide enhanced information to the operator or redirect the alarm to the designated responder.

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

12.2 Basis of enhanced and advanced alarming

12.2.1 General

Enhanced and advanced alarming 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 approved enhanced and advanced alarming techniques.

12.2.2 Effort, manpower requirements and complexity

Enhanced and advanced alarming techniques add complexity and need additional resources for design, implementation, and maintenance. The MOC procedure should include a review of the impact of changes on the enhanced and advanced alarming techniques as well as risk evaluation of possible failures of the techniques.

12.3 Information linking

Alarm systems can be enhanced by linking to information in the master alarm database (e.g., operator action, 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 techniques (e.g., Boolean logic, decision trees) to determine the modifications to be made to alarm systems. This may be implemented in the control system or externally to the control system.

12.4.2 Alarm attribute modification

The functional capability to modify some alarm attributes (e.g., alarm setpoints, 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 status 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 attributes (e.g., setpoint, priority, suppression status) based on defined operating states for equipment or processes. States are often determined through:

a) the status of a 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 or prediction 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 are often not available in the basic alarm system.

12.6.2 Remote alarm systems

Several situations can potentially exist in which the person responding to an abnormal situation is not in a control room. Such situations can benefit from the availability of a remote alarm system (e.g., paging, e-mail, call-out alarms). Where remote alarm systems are used, the alarm philosophy should include these systems.

The reliability of the message delivery is a significant issue in remote alarm systems and should be considered. Periodic test messages should be used to improve reliability. A procedure to ensure response to the alarm should be considered.

It can be necessary to also provide remote acknowledgement.

12.6.3 Supplementary alarm systems

Supplementary alarm systems (e.g., expert system for alarm response) can replace all or part of the functionality of the alarm system within the control system or control system HMI to provide a common interface. Alternatively, supplementary systems can be used, in addition to the control system alarm functions 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 requirements of this document.

12.6.4 Batch process considerations

12.6.4.1 General

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

12.6.4.2 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.

12.6.4.3 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 some advanced alarming techniques is the ability to take calendar time stamps and electronic records indicating when the batch step or phase started and determine alarms in relative time.

12.6.4.4 Inclusion of lot number and other identifying marks

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

12.7 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 management life cycle, 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 verification,

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 requirements for new or modified alarms

Operators shall be trained on the response to all new or modified alarms as prescribed in the alarm philosophy or the MOC procedure.

13.3.3 Training documentation requirements for new or modified highly managed alarms

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

a) the persons trained,
b) a summary of the training material,
c) the method of training, and
d) the date of the training.

13.3.4 Training documentation recommendations for new or modified alarms

Documentation of the training should include:

a) the persons trained,
b) a summary of the training material,
c) the method of training, and
d) the date of the training.

13.3.5 Implementation training requirements for new or modified alarm systems

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

13.3.6 Implementation training recommendations for new or modified alarm systems

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

a) the audible and visual indications for alarms,
b) the methods for silencing an alarm,
c) the distinction of alarm priorities,
d) the use of the alarm HMI features (e.g., alarm summary sorting and filtering),
e) the methods for shelving and suppression, and
f) the methods for removing an alarm from service.

13.4 Implementation testing and verification

13.4.1 General

Implementation testing requirements for new alarms and modifications to existing alarms are determined by the MOC procedure, the class requirements, or other methods, as detailed in the alarm philosophy.

NOTE Methods can include signal simulation and end-to-end signal function test.

13.4.2 Implementation testing requirements for highly managed alarms

The alarm philosophy shall identify the verification 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 prior to putting the alarms in operation. The testing should include verification of the following:

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 the modified alarm system shall be appropriate to the nature of the change, as determined by the 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,

d) any designed suppression or enhanced alarming documentation, and

e) test documentation, if required by the alarm philosophy.

NOTE The rationalization documentation and the alarm response procedures can be documented and accessed from the master alarm database.

Upon completion of the alarm system implementation, the rationalization information shall be updated in accordance with the 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 MOC procedures or the alarm philosophy.

Information used in testing new and modified alarms can 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) method of testing and acceptance criteria, and

h) 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 life cycle. 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 life cycle 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 as specified in the alarm philosophy.

14.2.2 Alarm response procedure recommendations

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 priority,

d) the alarm type,
e) the alarm setpoint,
f) the probable causes,
g) the consequence of inaction,
h) the operator action,
i) the allowable response time, and
j) the alarm class.

14.3 Alarm shelving

14.3.1 Alarm shelving requirements

Alarm shelving shall be allowed as detailed in the alarm philosophy.

14.3.2 Alarm shelving for highly managed alarms

Shelving highly managed alarms shall follow authorization and reauthorization requirements as detailed in the alarm philosophy.

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

14.3.3 Alarm shelving recommendations

Shelved alarms extending beyond a single operating shift should be reviewed. The review procedure 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 time limit set in the alarm philosophy:

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

14.3.5 Shift change procedures and alarm review

Written procedures should be developed for the exchange or review of alarm status information at shift change.

14.4 Refresher training for operators

14.4.1 Refresher training requirements for operators

The training requirements for alarms shall be determined by the alarm classification or other methods as detailed in the alarm philosophy.

14.4.2 Refresher training documentation requirements for highly managed alarms

The following training information on highly managed alarm shall be documented:

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

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

14.4.3 Refresher training content for highly managed alarms

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 life cycle. Clause 15 covers requirements for alarm system testing, replacement, 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 classification or other methods 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

Highly managed alarms shall be periodically tested to ensure performance.

Any deficiencies found during periodic testing of highly managed alarms shall be repaired and documented 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, including notification to the operator,

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 and documented 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 classification or other methods 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,

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

f) the anticipated duration the alarm will be out of service (e.g., longer than a day).

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 and the duration of record retention should be specified.

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 MOC procedure should address replacement equipment (e.g., measurement devices, valves, process equipment) that will change alarm attributes. Alarm verification may be performed after equipment replacement, 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

Personnel shall be periodically trained on the maintenance requirements for all highly managed alarms 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 life cycle. This stage verifies that design, implementation, rationalization, operation, and maintenance are satisfactory. Clause 16 provides requirements and recommendations on the use of alarm system analysis for both on-going monitoring and periodic performance assessment.

Performance monitoring is fundamental to management and improvement of the alarm system. 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.

16.2 Performance monitoring requirements

The alarm system shall be monitored. The alarm system performance shall be assessed against the performance targets in the alarm philosophy.

Each alarm transition in Figure 3 should be recorded to provide data for performance monitoring.

16.3 Monitoring and assessment

16.3.1 General

The intent of monitoring and assessment is to identify and correct deviations from expected performance. Monitoring the alarm systems involves analysis of the alarm records to calculate performance and diagnostic metrics. Alarm system assessment is the comparison of performance metrics against the targets specified in the alarm philosophy.

16.3.2 Alarm system performance metrics

Both initial alarm system assessment and on-going monitoring should include the measures like those shown in Table 7.

The two categories of data in a typical alarm system are alarm records (i.e., dynamic or real-time data) and alarm attributes. 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 practical 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.

16.3.3 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) 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	Manageable
~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 manageable guidelines indicates an alarm system that is annunciating more alarms than an operator is likely able to manage and can impact the probability of operator error.

16.3.4 Peak alarm rate per operator console

For peak alarm rate analysis, annunciated alarms are counted in regular 10-minute intervals (e.g., 13:00 through 13:09). The peak alarm rate is the highest number of alarms annunciated in one interval. The recommended target is a peak alarm rate less than 10.

Additionally, as a recommended target, less than 1 % of the 10-minute intervals should contain more than 10 alarms.

16.3.5 Alarm floods

Alarm floods are variable-duration periods of alarm activity with annunciation rates likely to exceed the ability of the operator to respond. 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 a high alarm rate (e.g., an alarm rate that exceeds 10 alarms per 10 minutes), and the end of an alarm flood is indicated by a return to a reduced alarm rate (e.g., an alarm rate of less than 5 alarms per 10 minutes). As a recommended target, an alarm system should be in flood for less than 1% of the time. The thresholds for alarm flood should be set in the alarm philosophy.

Improvements to the alarm system and process operation can 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 be used to mitigate alarm floods. These techniques are described in Clause 12.

16.3.6 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 %). Substantial performance improvement can be made by addressing the most frequent alarms.

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.

16.3.7 Chattering and fleeting alarms

A chattering alarm repeatedly transitions between the active state and the not active 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.

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.

16.3.8 Stale alarms

Alarms that remain annunciated continuously for an extended duration (e.g., longer than 24 hours) can be considered stale. Such alarms provide little valuable information to the operators. Stale alarms should be examined to ensure that they were properly rationalized. Advanced alarming or resolving the root cause can eliminate stale alarms.

There should be few stale alarms per operator console, with action plans to address them. No alarm should be intentionally designed to become stale and there is no long-term acceptable number of stale alarms.

16.3.9 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 as shown in Table 6.

Table 6 – Example 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
NOTE The ~<1 % highest priority is sometimes used 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.

Alarm priority distributions can vary based on process and industry. Significant variance from the target priority distribution can indicate ineffective rationalization or ineffective application of the alarm prioritization methodology.

16.3.10 Rationalization and alarm priority distribution

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

16.4 Unauthorized alarm suppression

The alarm states of shelved, suppressed by design, and out of service are all intended as controlled suppression methodologies. It is possible for alarms to be suppressed outside of these methodologies. Uncontrolled alarm suppression increases the potential for mistakes and the resulting risk.

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. The target value for unauthorized alarm suppressions is zero.

16.5 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 in a timely manner. The target value for unauthorized changes to alarms is zero.

16.6 Reporting of alarm system analyses

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

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

16.7 Alarm performance metric summary

The alarm performance metrics and example target values previously described 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 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 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 on any day, with action plans to address	
Annunciated priority distribution	3 priorities: ~80 % low, ~15 % medium, ~5 % high or 4 priorities: ~80 % low, ~15 % medium, ~5 % high, ~< 1 % highest Other special-purpose priorities excluded from the calculation	

17 Management of change

17.1 Purpose

MOC is a separate stage of the life cycle. MOC for alarm management includes the documentation and authorization of changes to the alarm system, including: the addition of new alarms, the removal of existing alarms, the modification of alarm attributes, and changes to alarm system functions. The purpose of MOC is to ensure that changes are authorized and subjected to the evaluation criteria described in the alarm philosophy. The MOC process ensures that the appropriate life cycle 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 an MOC procedure. Changes that result in a difference from the authorized values of the alarm setpoint, class, priority, consequence, setpoint rationale, 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, including system upgrades, follow all appropriate subsequent alarm management life cycle activities, and
j) implementation of all changes followed the procedures specified in the alarm philosophy.

17.3 Change documentation requirements

Documentation requirements shall be determined by the MOC procedure and classification or other methods as detailed in the alarm philosophy.

17.4 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, as specified in the MOC procedure.

17.5 Alarm documentation review recommendations

A list of referencing materials (e.g., graphics, control logic, P&ID, operating procedures, and PHA) should be generated and maintained. This reference list should be reviewed prior to making changes to alarms.

18 Audit

18.1 Purpose

Audit is a separate stage of the life cycle 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. Audit verifies the execution of the requirements and work processes against those documented in the alarm philosophy. Audit also includes comparison of the alarm management practices against industry guidelines.

18.2 Benchmark

A benchmark, or initial audit, should be made against a set of documented practices (e.g., the practices listed in this document). 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.

18.3 Audit 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 or other methods.

Audits shall address all applicable requirements of this document that relate to management processes.

18.4 Audit interviews

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

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

b) alarm priority is consistently applied and meaningful,

c) operators have sufficient time to respond to alarms,

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

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

18.5 Audit process recommendations

The alarm philosophy should be audited against industry guidelines and the requirements and recommendations of this document. 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 can include:

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

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.

18.6 Action plans

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

Bibliography

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems − Part 4: Definitions and abbreviations*

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 application programming requirements*

EN 62241:2015, *Nuclear power plants – Main control room – Alarm functions and presentation*

IEC 62264-2:2013, *Enterprise-control system integration – Part 2: Object and attributes for enterprise-control system integration*

IEC 62541-9:2020, *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*

ANSI/ISA-18.02-2016, *Management of Alarm Systems for the Process Industries*

ANSI/ISA-101.01-2015, *Human Machine Interfaces for Process Automation Systems*

Engineering Equipment Materials Users' Association, Alarm Systems – A Guide to Design, Management and Procurement, EEMUA Publication No. 191, 3rd Edition, EEMUA, London, UK (2013)

ISA-TR84.00.04-2020, Part 1, Guidelines for the Implementation of ANSI/ISA-61511-1-2018

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

GESTION DE SYSTÈMES D'ALARME DANS LES INDUSTRIES DE TRANSFORMATION

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses Publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62682 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels. Il s'agit d'une Norme internationale.

Cette deuxième édition annule et remplace la première édition parue en 2014. Cette édition constitue une révision technique.

Cette édition inclut des modifications techniques mineures par rapport à l'édition précédente, en se basant sur les modifications de l'ANSI/ISA-18.2:2016. Elles comprennent l'ajout de systèmes conditionnés dans le domaine d'application (Article 1), de définitions (Article 3) et la spécification des exigences relatives aux systèmes d'alarme (Article 7). Ces modifications ont été apportées pour améliorer la clarté de la formulation dans l'ensemble du document.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
65A/1046/FDIS	65A/1064/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. A cette date, le document sera:

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

INTRODUCTION

La présente Norme internationale traite du développement, de la conception, de l'installation et de la gestion de systèmes d'alarme dans les industries de transformation. La gestion des alarmes inclut plusieurs processus de travail pendant tout le cycle de vie de la gestion d'alarme. Le présent document définit la terminologie et les modèles pour développer un système d'alarme, il définit aussi les processus de travail recommandés pour maintenir efficacement l'alarme tout au long du cycle de vie. Des systèmes d'alarme inefficaces ont souvent été cités dans les rapports d'investigation comme des facteurs ayant contribué à des incidents de processus majeurs. Le présent document vise à fournir une méthodologie qui conduit à une sécurité, qualité et exploitation améliorées dans les industries de transformation.

La première édition du présent document a été adaptée de la norme ISA (International Society of Automation) ANSI/ISA-18.2-2009 *Management of Alarm Systems for the Process Industries*, en tenant pleinement compte d'autres documents d'orientation qui ont été élaborés dans l'ensemble du secteur. La présente deuxième édition incorpore certaines modifications apportées à l'ANSI/ISA-18.2-2016.

Le présent document n'est pas le premier effort visant à définir la terminologie et les pratiques pour des systèmes d'alarme efficaces. En 1999, l'EEMUA (Engineering Equipment and Materials Users' Association) a produit la Publication 191, *Alarm Systems: A Guide to Design, Management and Procurement*, avec la deuxième édition parue en 2007 et la troisième édition parue en 2013. En 2003, la NAMUR (User Association of Process Control Technology in Chemical and Pharmaceutical Industries) a publié la feuille de travail NA 102, *Alarm Management*, qui a été mise à jour en 2008. Au cours du développement et de la maintenance du présent document, tous les efforts ont été faits pour maintenir la terminologie et les pratiques cohérentes avec le travail antérieur de ces organisations et comités respectés.

Le présent document fournit les exigences relatives à la gestion des alarmes et aux systèmes d'alarme. Il est destiné aux personnes et aux organisations qui:

a) fabriquent ou mettent en œuvre des systèmes d'alarme intégrés;

b) fabriquent ou installent des logiciels pour systèmes d'alarme de tiers;

c) conçoivent ou installent des systèmes d'alarme;

d) exploitent et maintiennent des systèmes d'alarme; et

e) auditent ou évaluent les performances des systèmes d'alarme.

Le présent document est organisé en plusieurs parties. La première partie (Article 1 à Article 3) est normative sans aucune exigence obligatoire. L'Article 4 contient des exigences obligatoires. L'Article 5 est normatif sans aucune exigence obligatoire. Le corps de la norme (Article 6 à Article 18) fournit les exigences obligatoires et des recommandations non obligatoires.

Dans le présent document, les exigences obligatoires sont indiquées par "doit", les recommandations non obligatoires sont indiquées par "il convient" et les exigences admissibles sont indiquées par "peut". L'expression "est exigé" indique que l'exigence a été énoncée précédemment dans le document.

GESTION DE SYSTÈMES D'ALARME DANS LES INDUSTRIES DE TRANSFORMATION

1 Domaine d'application

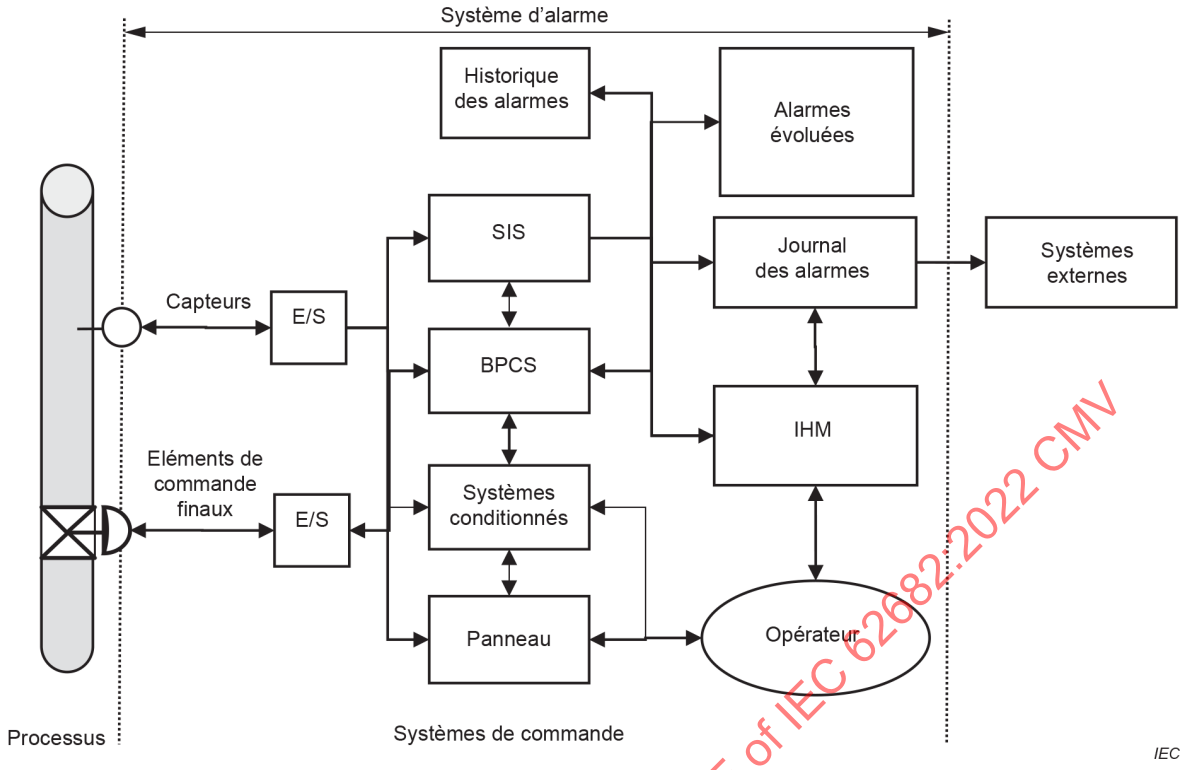
1.1 Applicabilité générale

Le présent document spécifie les principes et les processus généraux pour la gestion de systèmes d'alarme basés sur des systèmes de commande et des interfaces homme-machine (IHM) pour des moyens dans les industries de transformation. Il couvre toutes les alarmes présentées à l'opérateur par le système de commande, qui incluent les systèmes de commande de processus de base, les annonceurs, les systèmes conditionnés et les systèmes instrumentés de sécurité.

Les pratiques dans le présent document sont applicables aux processus continus, aux processus par lots et aux processus discrets. Il peut y avoir des différences de mise en œuvre pour satisfaire aux besoins spécifiques en fonction du type de processus.

La fonction première du système d'alarme est de notifier aux opérateurs les conditions de processus anormales ou les dysfonctionnements du matériel et d'aider à leur résolution. Les systèmes d'alarme peuvent inclure tant le système de commande de processus de base (BPCS) que le système instrumenté de sécurité (SIS), qui utilisent chacun les mesures des conditions de processus et une logique pour produire des alarmes. La Figure 1 représente les concepts d'alarme et de flux de données de réponse dans le système d'alarme. Le système d'alarme inclut également un mécanisme pour communiquer les informations d'alarme à l'opérateur par l'intermédiaire d'une IHM, habituellement un écran de calculateur ou un annonceur. Les fonctions supplémentaires du système d'alarme consistent en un journal des alarmes et des événements, un historique des alarmes et la production d'une métrique de performances pour le système d'alarme. Il existe des systèmes externes qui peuvent utiliser les données issues du système d'alarme.

La Figure 1 ne représente pas le câblage physique.



NOTE 1 Les systèmes conditionnés (par exemple machines frigorifiques) peuvent être inclus dans le système de commande.

NOTE 2 Le terme "tableau" peut faire référence à un tableau annonciateur ou à d'autres types de tableaux.

NOTE 3 Les lignes sont destinées à représenter le flux de données et non le câblage physique.

Figure 1 – Flux de données du système d'alarme

1.2 Exclusions et inclusions

1.2.1 Opérateurs

Les fonctions de l'opérateur recevant des alarmes et y répondant sont incluses dans le domaine d'application du présent document. La gestion des opérateurs est exclue du domaine d'application du présent document.

1.2.2 Capteurs de processus et éléments de commande finaux

Les alarmes mises en œuvre dans des capteurs et des éléments finaux de commande sont incluses dans le domaine d'application du présent document. La conception et la gestion des capteurs de processus et des éléments finaux de commande sont exclues du domaine d'application du présent document.

1.2.3 Annonceurs

L'intégration d'annonceurs dans un système d'alarme est incluse dans le domaine d'application du présent document. La spécification et la conception d'annonceurs sont exclues du domaine d'application du présent document.

1.2.4 Interface homme-machine

L'aspect des alarmes dans l'IHM et les fonctions d'alarme relatives aux affichages sont inclus dans le domaine d'application du présent document. La conception et la maintenance de l'IHM sont exclues du présent document.

NOTE L'ANSI/ISA-101.01-2015 fournit des informations sur la conception et la maintenance de l'IHM.

1.2.5 Systèmes instrumentés de sécurité

Les alarmes mises en œuvre dans un système instrumenté de sécurité sont incluses dans le domaine d'application du présent document. La conception et la gestion des systèmes instrumentés de sécurité sont exclues du présent document.

NOTE L'IEC 61511-1 fournit des informations sur les systèmes instrumentés de sécurité.

1.2.6 Systèmes de détection et de protection contre l'incendie et le gaz

Les alarmes issues des systèmes de détection et de protection contre l'incendie et le gaz présentées à l'opérateur par le système de commande sont incluses dans le domaine d'application du présent document. La conception et la gestion des systèmes de détection et de protection contre l'incendie et le gaz sont exclues du domaine d'application du présent document.

1.2.7 Systèmes de sécurité

Les alarmes issues des systèmes de sécurité présentées à l'opérateur par le système de commande sont incluses dans le domaine d'application du présent document. La conception et la gestion des systèmes de sécurité sont exclues du domaine d'application du présent document.

1.2.8 Systèmes conditionnés

Les alarmes issues des systèmes conditionnés présentées à l'opérateur par le système de commande sont incluses dans le domaine d'application du présent document. La conception et la gestion des systèmes conditionnés sont exclues du domaine d'application du présent document.

1.2.9 Données d'événement

L'indication et le traitement des données analogiques, discrètes et événementielles autres que les indications d'alarme sont exclus du domaine d'application du présent document. Les techniques d'analyse utilisant des données d'alarme et d'événement sont exclues du domaine d'application du présent document.

1.2.10 Méthodes d'identification des alarmes

Des méthodes exigées d'identification d'alarme ne sont pas spécifiées dans le présent document. Des exemples de méthodes d'identification des alarmes sont énumérés.

1.2.11 Gestion des changements

Une procédure spécifique de gestion des changements (MOC) n'est pas incluse dans le présent document. Un certain nombre d'exigences et de recommandations relatives à une procédure MOC sont incluses.

1.2.12 Spécification d'achat

Le présent document n'est pas destiné à être utilisé comme une spécification d'achat de systèmes d'alarme.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes, définitions et termes abrégés

Pour les besoins du présent document, les termes, définitions et acronymes suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1 Termes et définitions

3.1.1
alarme absolue
alarme générée lorsque le point de consigne d'alarme est dépassé

EXEMPLE: Haut-haut, haut, bas, bas-bas.

3.1.2
acquitter
action de l'opérateur qui confirme la reconnaissance d'une alarme

3.1.3
actif
état d'alarme dans lequel la condition d'alarme est vraie

Note 1 à l'article: Des fonctions comme la bande morte, le retard à l'activation d'alarme ou à la désactivation d'alarme et le verrouillage peuvent permettre à l'alarme d'être active lorsque la condition d'alarme est fausse, ou à l'alarme de ne pas être active lorsque la condition d'alarme est vraie.

3.1.4
alarme adaptative
alarme pour laquelle le point de consigne est modifié par un algorithme

EXEMPLE: Point de consigne calculé en fonction du taux de productivité.

3.1.5
alarme réglable
alarme établie par un opérateur
alarme pour laquelle le point de consigne peut être modifié manuellement par l'opérateur

3.1.6
alarmes évoluées
ensemble de techniques qui peuvent aider à gérer des annonces dans des situations spécifiques

EXEMPLE: Alarmes à base d'état.

3.1.7
alarme
moyen sonore et/ou visuel d'indiquer à l'opérateur un dysfonctionnement de matériel, un écart de processus ou un état anormal exigeant une réponse dans les délais

3.1.8
annonce
annonce d'alarme
fonction du système d'alarme pour attirer l'attention de l'opérateur sur une alarme

3.1.9
attribut d'alarme
valeur de réglage pour une alarme au sein d'un système de commande

EXEMPLE: Priorité d'alarme.

3.1.10
bannière d'alarme
élément graphique qui énumère des alarmes annoncées avec des informations sélectionnées

Note 1 à l'article: Des indications de retour à la normale peuvent également apparaître sur le résumé d'alarmes.

Note 2 à l'article: Les informations peuvent inclure la date, l'heure, la priorité et le type d'alarme.

3.1.11
classe d'alarme
groupe d'alarmes avec un ensemble commun d'exigences relatives à la gestion d'alarme

EXEMPLE: Classe d'alarme liée à la sécurité.

3.1.12
bande morte d'alarme
changement dans le signal par rapport au point de consigne d'alarme nécessaire pour que l'alarme retourne à la normale

3.1.13
inondation d'alarmes
état dans lequel la fréquence d'alarme est supérieure à ce que l'opérateur peut gérer efficacement

EXEMPLE: Plus de 10 alarmes toutes les 10 minutes.

3.1.14
groupe d'alarmes
ensemble d'alarmes avec association commune

EXEMPLE: Groupement d'alarmes par unité de processus, zone de processus, ensemble de matériel ou service.

3.1.15
historique des alarmes
dépôt à long terme pour les enregistrements d'alarme

3.1.16
journal des alarmes
dépôt à court terme pour les enregistrements d'alarme

3.1.17
gestion d'alarme
gestion de système d'alarme
ensemble de processus et pratiques pour déterminer, documenter, concevoir, exploiter, surveiller et maintenir des systèmes d'alarme

3.1.18
message d'alarme
chaîne textuelle affichée avec l'indication d'alarme qui fournit des informations supplémentaires à l'opérateur

EXEMPLE: Message avec action de l'opérateur ou cause probable.

3.1.19
retard à la désactivation d'alarme
antirebond
temps pendant lequel une alarme reste active après le retour de la mesure du processus dans les limites du point de consigne d'alarme

3.1.20
retard à l'activation d'alarme
temps avant qu'une alarme devienne active après le dépassement du point de consigne d'alarme par la mesure de processus

3.1.21
philosophie d'alarme
document qui établit les définitions, les principes et les processus de base pour concevoir, mettre en œuvre et maintenir un système d'alarme

3.1.22
priorité d'alarme
importance relative assignée à une alarme au sein du système d'alarme pour indiquer l'urgence d'une réponse

EXEMPLE: La priorité peut utiliser la gravité des conséquences et le temps de réponse admissible pour déterminer l'urgence.

3.1.23
fréquence d'alarme
nombre des alarmes annoncées, par opérateur, dans un intervalle de temps spécifique

3.1.24
enregistrement d'alarme
enregistrement
ensemble d'informations qui documente un changement d'état d'alarme

3.1.25
procédure de réponse aux alarmes
recommandations pour la réponse à une alarme

Note 1 à l'article: Le document d'orientation peut se présenter sous de nombreuses formes et pas seulement sous la forme d'un document de procédure.

Note 2 à l'article: Les recommandations peuvent inclure une action de l'opérateur, la cause probable et d'autres informations.

3.1.26
point de consigne d'alarme
limite d'alarme
point de déclenchement d'alarme
valeur seuil d'une variable de processus ou état discret qui est utilisée pour déterminer l'état actif de l'alarme

3.1.27
résumé d'alarmes
liste d'alarmes
affichage qui énumère des alarmes annoncées avec des informations sélectionnées

Note 1 à l'article: Des indications de retour à la normale peuvent également apparaître sur le résumé d'alarmes.

Note 2 à l'article: Les informations peuvent inclure la date, l'heure, la priorité et le type d'alarme.

3.1.28
système d'alarme
système permettant de générer et traiter les alarmes pour aider l'opérateur à gérer des situations anormales

Note 1 à l'article: L'opérateur est compris dans le système d'alarme. Voir Figure 1.

3.1.29
spécification des exigences de système d'alarme
document qui décrit les exigences fonctionnelles du système d'alarme

3.1.30
type d'alarme
attribut d'alarme qui distingue la condition d'alarme

EXEMPLE: Alarme de variable de processus basse, alarme de variable de processus haute ou alarme "discordance".

3.1.31
temps de réponse admissible
durée maximale entre l'annonce de l'alarme et l'instant où l'opérateur doit entreprendre une action corrective afin de prévenir les conséquences

3.1.32
annonceur
appareil ou groupe d'appareils qui appelle l'attention sur les modifications des conditions de processus

3.1.33
évaluation
comparaison des informations obtenues par la surveillance et par des mesures (subjectives) qualitatives supplémentaires par rapport aux buts énoncés et à la métrique de performance définie

3.1.34
audit <de gestion d'alarme>
évaluation complète qui inclut l'évaluation de la performance du système d'alarme et des pratiques de travail utilisées pour administrer le système d'alarme

3.1.35
alarme "mauvaise mesure"
alarme générée lorsque le signal pour une mesure de processus se situe hors de la plage attendue

EXEMPLE: Alarme "mauvaise mesure" générée à 3,8 mA pour un signal dans la plage comprise entre 4 mA et 20 mA.

3.1.36
système de commande de processus de base
BPCS
système qui répond aux signaux d'entrée provenant du processus, de ses équipements associés, d'autres systèmes programmables et/ou des opérateurs, et qui génère des signaux de sortie faisant fonctionner le processus et ses équipements associés de la manière souhaitée, mais qui n'exécute aucune fonction instrumentée de sécurité

Note 1 à l'article: Un BPCS inclut tous les appareils nécessaires pour s'assurer que le processus fonctionne de la manière souhaitée.

Note 2 à l'article: Un BPCS peut habituellement mettre en œuvre différentes fonctions telles que fonctions de commande de processus, surveillance et alarmes.

[SOURCE: IEC 61511-1:2016, 3.2.3, modifié − "(SIF)" a été supprimé]

3.1.37
référence
audit initial d'un système d'alarme destiné à identifier de façon spécifique les zones à problèmes afin de formuler des plans d'amélioration

3.1.38
alarme "profil binaire"
alarme qui est générée lorsqu'un profil de signaux numériques concorde avec un profil prédéterminé

3.1.39
alarme calculée
alarme générée à partir d'une valeur calculée au lieu d'une mesure directe du processus

3.1.40
alarme par appel
alarme qui avise et informe un opérateur par un moyen différent, ou en plus, de la console d'opérateur

EXEMPLE: Alarme annoncée par téléavertisseur ou téléphone.

3.1.41
alarme oscillante
alarme qui passe sans cesse entre l'état actif et l'état inactif en un bref laps de temps

3.1.42
classification
processus de séparation des alarmes en classes d'alarme basées sur des exigences communes

Note 1 à l'article: Les exigences peuvent inclure les essais, la formation et l'audit.

3.1.43
console
console de l'opérateur
matériel, logiciel et mobilier ou enveloppe permettant de surveiller et/ou commander le processus, qui peut inclure plusieurs stations, appareils de communication et autres

Note 1 à l'article: L'étendue de commande de l'opérateur est généralement déterminée par les informations disponibles sur la console d'opérateur.

3.1.44
système de commande
système qui réagit à des signaux d'entrée provenant de l'équipement commandé et/ou d'un opérateur et produit des signaux de sortie qui font que l'équipement commandé fonctionne de la façon souhaitée

Note 1 à l'article: Le système de commande peut inclure un ou plusieurs systèmes de commande de processus de base (BPCS), des systèmes instrumentés de sécurité (SIS).

Note 2 à l'article: Le système de commande peut comprendre un ou plusieurs systèmes conditionnés.

[SOURCE: IEC 61508-4:2010, 3.3.3, "de l'EUC" a été supprimé du terme défini, "du processus" a été remplacé par "de l'équipement commandé" et les notes ont été modifiées]

3.1.45
alarme de sortie de contrôleur
alarme générée à partir du signal de sortie d'un algorithme de commande au lieu d'une mesure directe du processus

EXEMPLE: Alarme de sortie de contrôleur PID.

3.1.46
mise hors service
processus retirant une alarme du système d'alarme

3.1.47
alarme "écart"
alarme générée lorsque la différence entre deux valeurs excède un point de consigne d'alarme

EXEMPLE: Alarme en cas d'écart entre les instruments principaux et redondants ou d'écart entre la variable de processus et le point de consigne du contrôleur.

3.1.48
alarme "discordance"
alarme désaccord
alarme générée par la différence entre l'état attendu de l'installation ou de l'appareil et son état réel

EXEMPLE: Alarme lorsqu'un moteur électrique ne démarre pas après qu'il a été mis à l'état de marche.

3.1.49
affichage
représentation visuelle des informations utilisées par l'opérateur pour la surveillance et le contrôle

3.1.50
alarmes dynamiques
modification automatique d'attributs d'alarme selon un état ou des conditions du processus

3.1.51
exécution
technique d'alarme améliorée qui peut vérifier et restaurer des attributs d'alarme dans le système de commande aux valeurs contenues dans la principale base de données d'alarme

3.1.52
événement
représentation d'un fait sollicité ou non sollicité indiquant un changement d'état

EXEMPLE: Changements de mode et d'état de l'appareil.

[SOURCE: IEC 62264-2:2013, 3.1.2, modifié – "dans l'entreprise" a été supprimé et un exemple a été ajouté]

3.1.53
alarme "première cause"
première alarme
alarme déterminée pour être la première, dans un scénario à plusieurs alarmes

Note 1 à l'article: La première alarme est déterminée par logique.

3.1.54
alarme fugace
alarme qui passe entre l'état actif de l'alarme et l'état inactif de l'alarme en un bref laps de temps sans répétition rapide

3.1.55
alarme intensément gérée
HMA
alarme appartenant à une classe imposant des exigences supplémentaires par rapport aux alarmes générales

Note 1 à l'article: Les exigences réglementaires peuvent être des exigences supplémentaires.

EXEMPLE: Alarme liée à la sécurité.

3.1.56
interface homme-machine
IHM
ensemble des matériels et logiciels utilisés par l'opérateur et d'autres pour surveiller et interagir avec le système de commande et avec le processus par le biais du système de commande

3.1.57
mise en œuvre
stade de transition entre la conception et l'exploitation pendant lequel l'alarme est mise en service

Note 1 à l'article: La mise en œuvre inclut des activités telles que la mise en service et la formation.

3.1.58
alarme "diagnostic d'instrument"
alarme pour indiquer un défaut d'appareil de terrain ou de signal

EXEMPLE: Alarme "hors service".

3.1.59
alarme intérimaire
alarme utilisée de façon temporaire pour remplacer une alarme "hors service"

3.1.60
alarme à verrouillage
alarme qui reste dans l'état d'alarme après que la condition de processus est revenue à la normale et exige une réinitialisation par l'opérateur avant que l'alarme ne retourne à la normale

3.1.61
principale base de données d'alarme
liste autorisée d'alarmes rationalisées et d'attributs associés

Note 1 à l'article: La liste peut se présenter sous de nombreuses formes et pas seulement sous la forme d'une base de données.

3.1.62
surveillance
mesure et production de rapports relatifs à des aspects (objectifs) quantitatifs de la performance du système d'alarme

3.1.63
alarme perturbatrice
alarme qui s'annonce de manière excessive et inutile ou ne retourne pas à la normale après l'action de l'opérateur

EXEMPLE: Alarme oscillante, alarme fugace et alarme prolongée.

3.1.64
opérateur
contrôleur
personne qui surveille et apporte des changements au processus

3.1.65
alerte d'opérateur
moyen sonore et/ou visuel d'indiquer à l'opérateur d'évaluer un équipement ou une condition de processus lorsque le temps le permet et qui pourrait entraîner une réponse

3.1.66
hors service
état d'une alarme pendant lequel l'indication de l'alarme est supprimée indéfiniment, typiquement manuellement, pour des raisons telles que la maintenance

3.1.67
système conditionné
combinaison autonome de matériel et de logiciel qui peut fournir une fonctionnalité d'alarme, d'IHM et de commande pour une fonction du processus spécifique qui fait partie d'une installation

3.1.68
état d'installation
mode installation
ensemble défini de conditions opérationnelles pour une installation de traitement

EXEMPLE: Arrêt, fonctionnement normal.

3.1.69
priorisation
processus d'assignation d'un niveau d'importance opérationnelle à une alarme

3.1.70
zone de processus
groupement physique, géographique ou logique de ressources, qui est déterminé par le site

3.1.71
alarme "vitesse de variation"
alarme générée lorsque la variation d'une variable de processus par unité de temps ($\mathrm{d}PV/\mathrm{d}t$) dépasse un point de consigne défini

3.1.72
rationalisation
processus pour passer en revue des alarmes potentielles en utilisant les principes de la philosophie d'alarme, pour sélectionner des alarmes en vue de la conception et pour documenter la justification pour chaque alarme

3.1.73
alarme "renouvellement d'alarme"
alarme de redéclenchement
alarme qui est automatiquement annoncée de nouveau dans certaines conditions

3.1.74
alarme pilotée par recette
alarme avec des points de consigne qui dépendent de la recette actuellement exécutée

3.1.75
téléalarme
alarme issue d'une installation exploitée à distance ou dirigée vers une interface distante

3.1.76
réinitialisation
action de l'opérateur qui déverrouille une alarme à verrouillage

3.1.77
retour à la normale
éliminer
passage d'une alarme de l'état actif à l'état inactif

3.1.78
système instrumenté de sécurité
SIS
système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité

Note 1 à l'article: Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unité(s) logique(s) et d'élément(s) terminal(aux). Il inclut également des équipements de communication et auxiliaires (par exemple câbles, tuyauterie, alimentation, lignes d'impulsion, réchauffage des conduites).

Note 2 à l'article: Un SIS peut inclure le logiciel.

Note 3 à l'article: Un SIS peut inclure une action humaine dans le cadre d'une SIF (voir ISA-TR84.00.04:2015, Partie 1).

[SOURCE: IEC 61511-1:2016, 3.2.67, modifié – la figure des notes et la référence à la figure de la Note 1 ont été supprimées]

3.1.79
alarme liée à la sécurité
alarme de sécurité
alarme classée comme étant critique pour la protection de la vie humaine ou de l'environnement

EXEMPLE: Une alarme indiquant un risque potentiel d'asphyxie.

3.1.80
suspendre
supprimer temporairement une alarme, déclenchée par l'opérateur, avec un système de commandes permettant d'annuler la suppression de l'alarme

Note 1 à l'article: Un système de commandes peut inclure des limites temporelles.

3.1.81
silence
action de l'opérateur pour mettre fin à l'indication de l'alarme sonore

3.1.82
alarme prolongée
alarme qui reste annoncée pendant une durée prolongée

EXEMPLE: Alarme qui reste annoncée pendant 24 heures.

3.1.83
alarme basée sur un état
alarmes basées sur un mode
alarme dont les attributs ont été modifiés ou qui est supprimée en fonction des états de fonctionnement ou des conditions de processus

3.1.84
alarme statistique
alarme générée en fonction du traitement statistique d'une ou plusieurs variables du processus

3.1.85
supprimer
empêcher que l'alarme soit annoncée à l'opérateur lorsqu'elle est active

EXEMPLE: Suspendre, supprimer par conception, retirer du service.

3.1.86
supprimer par conception
empêcher l'annonce de l'alarme à l'opérateur en fonction de l'état d'installation ou autres conditions

3.1.87
alarme "diagnostic de système"
alarme générée par le système de commande pour indiquer un défaut au sein de l'équipement matériel, du logiciel ou des composants du système

EXEMPLE: Erreur de communication.

3.1.88
étiquette
point du système de commande
point
identificateur unique assigné à une mesure de processus, à un calcul ou à un appareil au sein du système de commande

3.1.89
non acquitté
état d'alarme dans lequel l'opérateur n'a pas encore confirmé la reconnaissance d'une indication d'alarme

3.1.90
lever la suspension
passage d'une alarme de l'état suspendu à l'état normal ou non acquitté

3.1.91
annuler la suppression
passage d'une alarme de l'état supprimé à l'état normal ou non acquitté

3.2 Termes abrégés

ACKED	Acknowledged (acquitté)
ASRS	Alarm system requirements specification (spécification des exigences des systèmes d'alarme)
BPCS	Basic process control system (système de commande de processus de base)
CGMP	Current good manufacturing practice (bonnes pratiques de fabrication courantes)
DSUPR	Suppressed-by-design (supprimé par conception)
ERP	Enterprise resource planning (planification des ressources de l'organisation)
AMDE	Analyse des modes de défaillance et de leurs effets
HAZOP	Hazard and operability study (études de danger et d'exploitabilité)
HMA	Highly managed alarms (alarmes intensément gérées)
IHM	Interface homme-machine
E/S	Entrée/sortie
LOPA	Layer of protection analysis (analyse des couches de protection)
MES	Manufacturing execution system (système d'exécution de fabrication)
MOC	Management of change (gestion des changements)
NORM	Normale
OOSRV	Out-of-service (hors service)
P&ID	Piping (or process) and instrumentation diagram (schéma de tuyauterie [ou de processus] et d'instrumentation)
PHA	Process hazards analysis (analyse des dangers des processus)
RTNUN	Return to normal unacknowledged (retour à la normale non acquittée)
SHLVD	Shelved (suspendu)
SIS	Système instrumenté de sécurité
UNACK	Unacknowledged (non acquitté)

4 Conformité au présent document

4.1 Recommandations pour la conformité

Pour se conformer au présent document, il doit être démontré que chacune des exigences obligatoires a été satisfaite.

4.2 Systèmes existants

Pour les systèmes d'alarme existants conçus et construits selon des codes, des normes ou des pratiques antérieurs au présent document, le propriétaire/l'opérateur doit déterminer que le matériel est conçu, maintenu, inspecté, soumis à essai et exploité de manière sûre. Les pratiques et les procédures du présent document doivent être appliquées aux systèmes existants dans un temps raisonnable tel que déterminé par le propriétaire/l'opérateur.

4.3 Utilisation des fonctionnalités exigées

Le présent document exige certaines fonctionnalités des systèmes de commande (par exemple suspension) pour prendre en charge le système d'alarme. Si un système d'alarme ne possède pas toutes les fonctionnalités exigées, la conformité peut être obtenue si la fonctionnalité décrite dans la philosophie d'alarme est fournie.

4.4 Responsabilité

Le propriétaire/l'opérateur a la responsabilité de la conformité au présent document.

4.5 Juridictions locales

Dans certaines juridictions, les autorités de régulation (par exemple au niveau national, fédéral, de l'état, provincial, du comté, de la ville) ont établi des exigences relatives à la conception de sécurité de processus, la gestion de la sécurité des processus ou d'autres exigences en plus des exigences du présent document.

5 Modèles de système d'alarme

5.1 Systèmes d'alarme

Les systèmes d'alarme sont utilisés pour communiquer des indications des conditions de processus anormales ou des dysfonctionnements de matériel aux opérateurs, au personnel surveillant et exploitant le processus et d'aider à leur résolution. Les systèmes d'alarme efficaces sont bien conçus, mis en œuvre, exploités et maintenus. La gestion d'alarme est l'ensemble des pratiques et des processus qui assure un système d'alarme efficace.

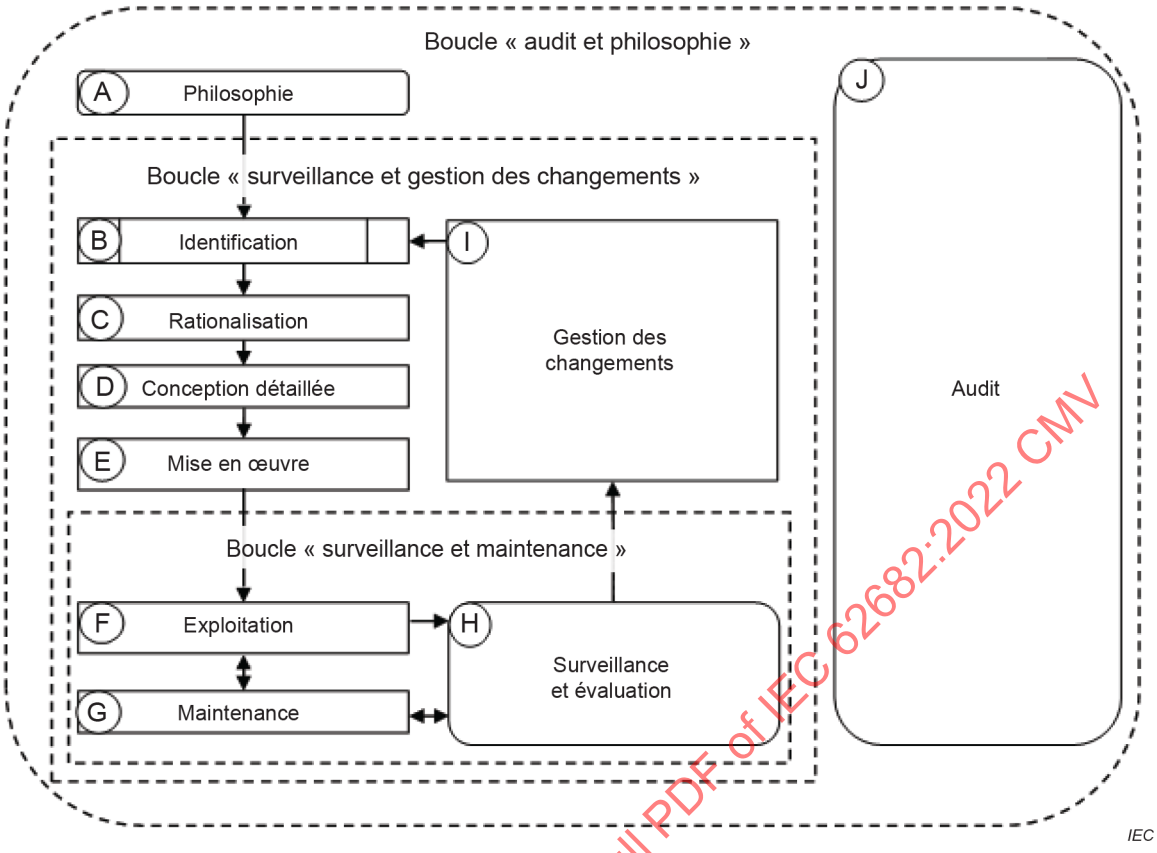
Une partie fondamentale de la gestion d'alarme est la définition d'une alarme, moyen sonore et/ou visuel d'indiquer à l'opérateur un dysfonctionnement de matériel, un écart de processus ou un état anormal exigeant une réponse dans les délais. Un élément essentiel de cette définition est la réponse à l'alarme. Cette définition est renforcée dans les processus de gestion d'alarme décrits dans le présent document.

5.2 Cycle de vie de la gestion d'alarme

5.2.1 Modèle de cycle de vie de la gestion d'alarme

La Figure 2 représente la relation entre les stades du cycle de vie de la gestion d'alarme qui est décrit dans le présent document. Le cycle de vie de la gestion d'alarme couvre la spécification du système d'alarme, la conception, la mise en œuvre, l'exploitation, la surveillance, la maintenance et les activités MOC à partir de la conception initiale jusqu'à la mise hors service.

Le modèle de cycle de vie est utile pour organiser les exigences et les responsabilités pour mettre en œuvre une gestion d'alarme. Le cycle de vie est applicable à l'installation de nouveaux systèmes d'alarme ou pour la gestion d'un système existant.



NOTE 1 La zone utilisée pour le stade B représente un processus défini en dehors du présent document (voir 5.2.2.3).

NOTE 2 Le stade indépendant J représente un processus qui se connecte à tous les autres stades (voir 5.2.2.11).

NOTE 3 Les formes arrondies des stades A, H et J représentent des points d'entrée au cycle de vie (voir 5.2.3).

NOTE 4 Les lignes pointillées représentent les boucles dans le cycle de vie (voir 5.2.5).

Figure 2 – Cycle de vie de la gestion d'alarme

5.2.2 Stades du cycle de vie de la gestion d'alarme

5.2.2.1 Généralités

Les stades du cycle de vie de la gestion d'alarme représentés à la Figure 2 sont brièvement décrits dans les paragraphes suivants. L'étiquette littérale est un identificateur utilisé dans le texte. Les exigences et les recommandations pour chaque stade sont décrites de l'Article 6 à l'Article 18 du présent document.

5.2.2.2 Philosophie (A)

La planification de base est nécessaire avant de concevoir un nouveau système d'alarme ou de modifier un système existant. Généralement, la première étape est le développement d'une philosophie d'alarme qui documente les objectifs du système d'alarme et les processus pour satisfaire à ces objectifs. La philosophie d'alarme reflète les processus de travail liés à l'exploitation et à la maintenance, et peut faire référence à ces processus dans d'autres documents. Pour les nouveaux systèmes, la philosophie d'alarme sert de base pour le document de spécification des exigences du système d'alarme (ASRS).

La philosophie commence par les définitions de base et les étend aux définitions opérationnelles. Les critères pour la priorisation des alarmes et la définition de classes d'alarme, la métrique de performance, les limites de performance et des exigences de rapports sont basés sur les objectifs et les principes pour des systèmes d'alarme. Les schémas pour la présentation des indications d'alarme dans l'IHM, y compris l'utilisation de priorités, sont également établis dans la philosophie d'alarme. La philosophie spécifie les processus utilisés pour chacun des stades du cycle de vie de gestion d'alarme, tels que le seuil pour le processus MOC et les exigences spécifiques pour le changement. La philosophie est maintenue pour assurer une gestion cohérente des alarmes tout au long du cycle de vie du système d'alarme.

Le développement de l'ASRS est inclus dans le stade philosophie du cycle de vie. La spécification peut être spécifique à une installation, en fournissant des détails sur les restrictions ou les options et peut être la base pour sélectionner de nouveaux systèmes de commande ou modifier des systèmes de commande existants. La spécification a généralement un niveau de détail plus approfondi que la philosophie d'alarme et peut fournir des recommandations spécifiques pour la conception de système.

5.2.2.3 Identification (B)

Le stade "identification" est un point de collecte pour les alarmes potentielles proposées par l'une des méthodes pour déterminer si une alarme est nécessaire. Ces méthodes sont définies en dehors du présent document et donc le stade identification est représenté comme processus prédéfini dans le cycle de vie. Les méthodes peuvent être formelles telles que l'analyse des dangers de processus, les spécifications des exigences de sécurité, les recommandations issues d'une investigation d'incidents, les bonnes pratiques de fabrication, les permis environnementaux, le développement P&ID ou les revues de procédures de fonctionnement. Il convient de capturer les informations d'identification (par exemple point de consigne d'alarme, conséquence de l'alarme) en vue de la rationalisation. Les modifications de processus et les essais de fonctionnement peuvent également générer la nécessité pour des alarmes ou des modifications. Un certain nombre de changements d'alarme sont identifiés à partir de la surveillance de routine de la performance du système d'alarme. A ce stade, la nécessité d'une nouvelle alarme ou des modifications d'une alarme existante a été identifiée et l'alarme est prête à être rationalisée.

5.2.2.4 Rationalisation (C)

Le stade "rationalisation" réconcilie la nécessité identifiée d'une alarme ou d'un changement de système d'alarme avec les principes et définitions de philosophie d'alarme. Les étapes peuvent être parachevées en un seul processus ou séquentiellement. Le produit de la rationalisation est la documentation de l'alarme, y compris toutes les éventuelles techniques d'alarmes évoluées, qui peuvent être utilisées pour parachever la conception.

La rationalisation est le processus consistant à appliquer les exigences pour une alarme et à générer la documentation justificative telle que le point de consigne d'alarme, la conséquence et l'action corrective qui peut être entreprise par l'opérateur.

La rationalisation inclut la priorisation d'une alarme basée sur la méthode définie dans la philosophie d'alarme. Souvent, la priorité est basée sur les conséquences de l'alarme et du temps de réponse admissible.

La rationalisation inclut également l'activité de classification pendant laquelle une alarme est assignée à une ou plusieurs classes selon des exigences désignées (par exemple exigences relatives aux essais, à la formation, à la surveillance et à l'audit). Le type de conséquences d'une alarme rationalisée, ou d'autres critères, peut être utilisé pour séparer les alarmes en des classes définies dans la philosophie d'alarme.

Les résultats de la rationalisation sont documentés, typiquement dans la base de données d'alarme principale (c'est-à-dire, un document ou un fichier approuvé) qui est maintenue pendant la vie du système d'alarme.

5.2.2.5 Conception détaillée (D)

Dans le stade "conception", les attributs d'alarme supplémentaires sont spécifiés et conçus selon les exigences déterminées par la rationalisation. Il existe trois domaines de conception: conception d'alarme de base, conception d'IHM et conception de techniques d'alarmes évoluées.

La conception de base pour chaque alarme suit des recommandations en fonction du type de l'alarme et du système de commande spécifique.

La conception d'IHM inclut l'affichage et l'annonce pour les alarmes, y compris les indications de l'état d'alarme et de la priorité d'alarme.

Les techniques d'alarmes évoluées (par exemple alarme basée sur un état) améliorent l'efficacité du système d'alarme au-delà de la conception d'alarme et d'IHM de base.

5.2.2.6 Mise en œuvre (E)

Dans le stade "mise en œuvre", les activités nécessaires pour installer une alarme ou un système d'alarme et l'amener à un statut opérationnel sont parachevées. La mise en œuvre d'une nouvelle alarme ou d'un nouveau système d'alarme inclut l'installation physique et logique et la vérification fonctionnelle du système.

Les opérateurs étant une partie intégrante essentielle du système d'alarme, la formation d'opérateur est une activité importante pendant la mise en œuvre. Les essais de nouvelles alarmes sont souvent une exigence de mise en œuvre. La documentation pour la formation, les essais et la mise en service peut varier avec la classification définie par la philosophie d'alarme.

5.2.2.7 Exploitation (F)

Dans le stade "exploitation", l'alarme ou le système d'alarme est en service et exécute sa fonction prévue. La formation pour la mise à jour des connaissances relatives à la philosophie d'alarme et à l'objectif de chaque alarme est incluse dans ce stade.

5.2.2.8 Maintenance (G)

Dans le stade "maintenance", l'alarme ou le système d'alarme n'est pas opérationnel, mais est soumis à essai ou en cours de réparation. La maintenance périodique (par exemple essais des instruments) est nécessaire pour assurer les fonctions telles que conçues du système d'alarme.

5.2.2.9 Surveillance et évaluation (H)

Dans le stade "surveillance et évaluation", la performance globale du système d'alarme et des alarmes séparées est surveillée en continu par rapport aux objectifs de performance énoncés dans la philosophie d'alarme. La surveillance et l'évaluation des données provenant du stade exploitation peuvent déclencher le travail de maintenance ou identifier la nécessité d'apporter des changements au système d'alarme ou aux procédures de fonctionnement. Sans surveillance, un système d'alarme est susceptible de se dégrader au fil du temps.

5.2.2.10 Gestion des changements (I)

Dans le stade "gestion des changements", des modifications au système d'alarme sont proposées et approuvées. Il convient que le processus de changements suive chacun des stades du cycle de vie de gestion d'alarme et ce, de l'identification jusqu'à la mise en œuvre.

5.2.2.11 Audit (J)

Dans le stade "audit", des revues périodiques sont menées pour évaluer l'efficacité des processus de gestion d'alarme et maintenir l'intégrité du système d'alarme. Les audits de la performance du système peuvent révéler des lacunes non décelées par la surveillance de routine. L'exécution par rapport à la philosophie d'alarme est auditée pour identifier des améliorations du système, telles que des modifications à la philosophie d'alarme. Les audits peuvent également identifier la nécessité d'augmenter la discipline de l'organisation pour suivre la philosophie d'alarme.

5.2.3 Points d'entrée du cycle de gestion d'alarme

5.2.3.1 Généralités

Selon l'approche choisie, il existe trois points d'entrée au cycle de vie de la gestion d'alarme qui sont:

a) la philosophie d'alarme;

b) la surveillance et évaluation; et

c) l'audit.

Ces points d'entrée sont représentés par les zones arrondies à la Figure 2. En tant que points d'entrée, ces stades du cycle de vie constituent seulement l'étape initiale pour gérer un système d'alarme. Tous les stades du cycle de vie sont nécessaires pour un système complet de gestion d'alarme.

5.2.3.2 Commencer par la philosophie d'alarme (A)

Le premier point de départ possible est le développement d'une philosophie d'alarme qui établit les objectifs du système d'alarme et peut être utilisée comme base pour l'ASRS. C'est le point d'entrée du cycle de vie pour de nouveaux systèmes.

5.2.3.3 Commencer par la surveillance et l'évaluation (H)

Le deuxième point de départ possible est de commencer à surveiller un système d'alarme existant et référencer la performance. Des alarmes à problème peuvent être identifiées et traitées par la maintenance ou la gestion des changements. Les données de surveillance peuvent être utilisées dans une évaluation de référence avant le développement de la philosophie d'alarme.

5.2.3.4 Commencer par l'audit (J)

Le troisième point de départ possible est un audit initial, ou référence, de tous les aspects de la gestion d'alarme par rapport à un ensemble de pratiques documentées, telles que celles énumérées dans le présent document. Les résultats de l'audit initial peuvent être utilisés dans le développement d'une philosophie.

5.2.4 Stades simultanés et intégrants

Le schéma de cycle de vie (Figure 2) est tracé pour représenter des stades séquentiels. Il y a plusieurs stades simultanés qui sont représentés dans le cycle de vie. Certains stades englobent les activités d'autres stades.

Le stade surveillance et évaluation (H) est réalisé en même temps que les stades exploitation et maintenance.

Le stade gestion des changements (I) représente le déclenchement du processus de changement par lequel tous les stades du cycle de vie sont autorisés et parachevés.

Le stade audit (J) est une activité intégrante qui peut se produire à n'importe quel point dans le cycle de vie et inclut une revue des activités des autres stades.

5.2.5 Boucles du cycle de vie de la gestion d'alarme

5.2.5.1 Généralités

En plus des stades du cycle de vie de la gestion d'alarme, il y a trois boucles dans le cycle de vie. Chaque boucle accomplit une fonction au cours du cycle de vie.

5.2.5.2 Boucle "surveillance et maintenance"

La boucle "surveillance et maintenance" est la surveillance de routine qui identifie les alarmes à problèmes pour la maintenance. Les alarmes réparées sont renvoyées en fonctionnement.

5.2.5.3 Boucle "surveillance et gestion des changements"

La boucle "surveillance et gestion des changements" est déclenchée lorsque la surveillance de routine indique que la conception d'une alarme n'est pas conforme à la philosophie d'alarme. Il pourrait être nécessaire de modifier la conception ou d'appliquer une technique d'alarmes évoluées. L'alarme pourrait rester en fonctionnement alors que le processus MOC est déclenché et les stades du cycle de vie sont répétés.

5.2.5.4 Boucle "audit et philosophie"

La boucle "audit et philosophie" est le cycle de vie proprement dit et le processus d'amélioration continue du système d'alarme. L'audit identifie des processus dans le cycle de vie à renforcer.

5.2.6 Entrées et sorties du stade de cycle de vie de gestion des alarmes

Les stades du cycle de vie de la gestion des alarmes sont connectés, car les sorties d'un stade sont souvent les entrées d'un autre. Les connexions ne sont pas entièrement représentées dans le schéma du cycle de vie (Figure 2). Le Tableau 1 fournit plus d'informations sur les relations entre les entrées et les sorties des stades du cycle de vie.

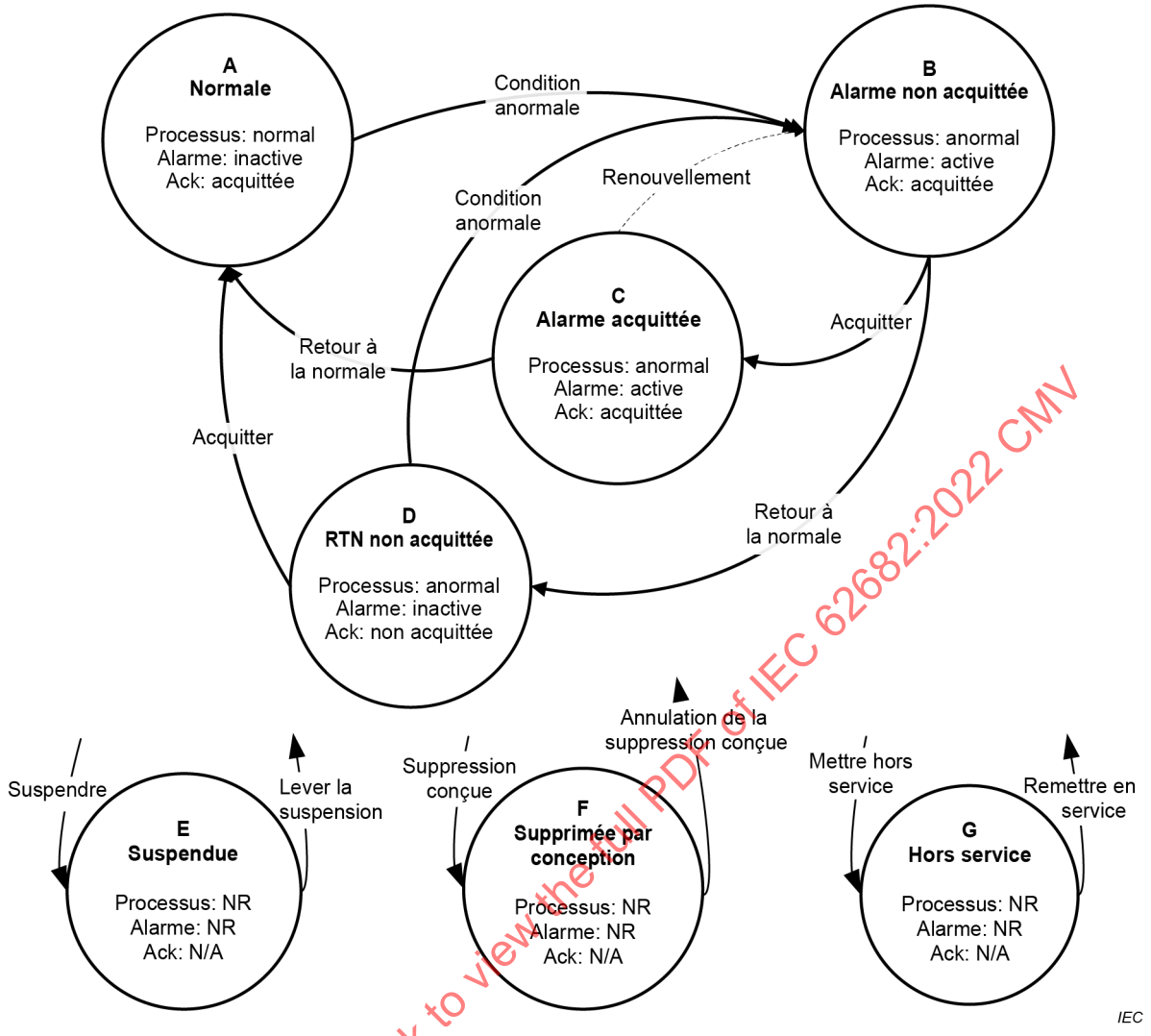
Tableau 1 – Entrées et sorties du stade de cycle de vie de gestion des alarmes

Stade du cycle de vie de la gestion d'alarme		Activités	Numéro d'article	Entrées	Sorties
Stade	Titre				
A	Philosophie	Documenter les objectifs, les lignes directrices et les processus de travail pour la gestion d'alarme et l'ASRS	6, 7	Objectifs et normes, recommandations relatives à l'audit	Philosophie d'alarme et ASRS
B	Identification	Détermination des alarmes potentielles	8	Rapport PHA, P&ID, procédures de fonctionnement	Liste d'alarmes potentielles
C	Rationalisation	Rationalisation, classification, priorisation et documentation	9	Philosophie d'alarme et liste d'alarmes potentielles	Base de données d'alarme principale et exigences relatives à la conception des alarmes
D	Conception détaillée	Conception d'alarme de base, conception d'IHM et conception d'alarmes évoluées	10, 11, 12	Base de données d'alarme principale et exigences relatives à la conception des alarmes	Conception d'alarme complète
E	Mise en œuvre	Installation d'alarmes, essais de la mise en œuvre et formation à la mise en œuvre	13	Conception d'alarme complète, base de données d'alarme principale et l'ASRS	Alarmes opérationnelles et procédures de réponse à des alarmes
F	Exploitation	L'opérateur répond aux alarmes et à la formation de mise à jour des connaissances	14	Alarmes opérationnelles et procédures de réponse à des alarmes	Données d'alarme
G	Maintenance	Maintenance, réparation et remplacement, et essais périodiques	15	Rapports de surveillance d'alarme et philosophie d'alarme	Données d'alarme
H	Surveillance et évaluation	Surveillance des données d'alarme et rapport sur la performance	16	Données d'alarme et philosophie d'alarme	Rapports de surveillance d'alarme et changements proposés
I	Gestion des changements	Processus pour autoriser les ajouts, les modifications et les suppressions d'alarme	17	Philosophie d'alarme et changements proposés	Changements d'alarme autorisés
J	Audit	Audit périodique des processus de gestion d'alarme	18	Normes, philosophie d'alarme et protocole d'audit	Recommandations pour l'amélioration

5.3 États d'alarme

5.3.1 Schéma de transition d'états d'alarme

Le schéma de transition des états d'alarme de la Figure 3 représente les états et les transitions pour des alarmes types. Il y a certes des exceptions, mais ce schéma décrit la majorité des alarmes et sert de référence utile pour la mise au point des principes des systèmes d'alarme et les fonctions IHM.



NOTE 1 Les états E, F et G peuvent connecter à n'importe quel état d'alarme dans le schéma.

NOTE 2 La ligne pointillée indique une option rarement mise en œuvre.

NOTE 3 N/A signifie non applicable.

NOTE 4 NR indique que l'état n'est pas pertinent (normal ou anormal, non actif ou actif).

Figure 3 – Schéma de transition d'états d'alarme

5.3.2 États d'alarme

5.3.2.1 Généralités

Les cercles représentés à la Figure 3 représentent les états d'une alarme. L'étiquette littérale est un identificateur. La deuxième ligne est un nom d'état, souvent abrégé. La troisième ligne décrit des conditions de processus, les quatrième et cinquième lignes énumèrent respectivement le statut de l'alarme et son statut d'acquittement. Les états possibles de suppression d'alarme sont représentés dans la partie inférieure du schéma.

5.3.2.2 État "normale" (A)

L'état d'alarme "normale" (NORM) est défini comme étant l'état dans lequel le processus fonctionne dans les limites de la spécification normale, l'alarme est inactive et les occurrences d'alarmes passées ont été acquittées.

5.3.2.3 État "non acquittée" (B)

L'état d'alarme "non acquittée" (UNACK) est l'état initial lorsqu'une alarme devient active en raison de conditions d'anomalies. Dans cet état, l'alarme est non acquittée. Les alarmes précédemment acquittées peuvent être conçues pour renouveler l'alarme, ce qui entraîne un retour à cet état.

5.3.2.4 État "acquittée" (C)

L'état d'alarme "acquittée" (ACKED) est l'état dans lequel l'alarme est active et l'opérateur a acquitté l'alarme.

5.3.2.5 État "non acquittée avec retour à la normale" (D)

Dans l'état d'alarme "non acquittée et retournée à la normale" (RTNUN), le processus se trouve dans des limites normales et l'alarme devient inactive avant qu'un opérateur n'ait acquitté l'alarme.

5.3.2.6 État "suspendue" (E)

Dans l'état d'alarme "suspendue" (SHLVD), une alarme est temporairement supprimée en utilisant une méthodologie maîtrisée et n'est pas annoncée. Une alarme dans l'état "suspendue" est sous le contrôle de l'opérateur. La fonction de suspension peut automatiquement lever la suspension des alarmes.

5.3.2.7 État "supprimée par conception" (F)

Dans l'état d'alarme "supprimée par conception" (DSUPR), une alarme est supprimée en fonction de conditions de fonctionnement ou d'états d'une installation et n'est pas annoncée. Une alarme dans l'état "supprimée par conception" est sous le contrôle de la logique qui détermine la pertinence de l'alarme.

5.3.2.8 État "hors service" (G)

Dans l'état d'alarme "hors service" (OOSRV), l'alarme est supprimée manuellement (par exemple fonctionnalité de système de commande pour retirer l'alarme du service) lorsqu'elle est retirée du service et n'est pas annoncée, typiquement pour maintenance. Une alarme dans l'état hors service est dans le stade "maintenance" du cycle de vie.

NOTE Une alarme dans l'état hors service n'est pas comparable à la mise hors service d'une unité ou d'un équipement. Le matériel peut être hors service alors que les alarmes associées ne sont pas hors service.

5.3.2.9 Résumé des états d'alarme

Les statuts d'alarme, le statut d'annonce et le statut d'acquittement des différents états d'alarme sont résumés dans le Tableau 2.