



Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

TECHNICAL REPORT

ISA-TR18.2.5-2022

Alarm System Monitoring, Assessment, and Auditing

Approved 3 March 2022

NOTICE OF COPYRIGHT

This is a copyright document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in the *Copyright of ISA Standards* policy. It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.

ISA-TR18.2.5-2022, Alarm System Monitoring, Assessment, and Auditing

ISBN: 978-1-64331-219-4

Copyright © 2022 by the International Society of Automation (ISA). All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of the publisher.

ISA
3252 S. Miami Blvd., Suite 102
Durham, NC 27703 USA
E-mail: standards@isa.org

Preface

This preface is included for information purposes only and is not part of ISA-TR18.2.5-2022.

This technical report has been prepared as part of the service of ISA, the International Society of Automation, toward a goal of helping in the understanding and use of ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA, E-mail: standards@isa.org.

International System of Units (SI) are the preferred units of measurement in ISA standards.

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

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

HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.

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

ISA (www.isa.org) is an international professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used international standards for industrial automation, safety, and cybersecurity; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and events; and provides networking and career development programs for its members and customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content. In addition, through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

The following served as contributing members of ISA18 Working Group 5 in the development of this 2022 technical report:

NAME	AFFILIATION IN 2022
D. Dunn	WS Nelson
B. Hollifield	PAS
K. Brown	Enbridge Inc.
A. Bryant	Oxy Inc.
S. Kandasamy	Chevron
D. Logerot	Emerson
M. Marvan	Shell Canada
N. Sands	DuPont
T. Stauffer	exida Co.
B. Vail	URS
R. Weibel	Tips Inc.

The following served as contributing members of ISA18 Working Group 5 in the development of the original 2012 technical report:

NAME	AFFILIATION IN 2012
J. Brown	WRc Plc
J. Campbell	Consultant
J. Croteau	Biogen Idec
D. Dunn	Aramco Services Co.
L. Farina	Braskem
B. Hollifield	PAS
D. Izara	Invensys Canada
M. Jones	Honeywell
L. Kalra	Chevron
M. Marvan	Shell Canada
J. Mirza	Hendsa
P. O'Donnell	BP
A. Phipps	Eli Lilly
N. Sands	DuPont
F. Szeto	Tar Island Suncor Energy Oil Sands
R. Weibel	Tips Inc.

The following served as voting members of ISA18 during the development of this 2022 technical report:

NAME	AFFILIATION IN 2022
D. Dunn, Co-Chair	WS Nelson
N. Sands, Co-Chair	DuPont
B. Fitzpatrick, Managing Director	Wood

J. Alford	Consultant
J. Bogdan	J Bogdan Consulting LLC
K. Brown	Enbridge Inc.
M. Brown	Matrikon Inc.
M. Carter	Hargrove Controls + Automation
L. Dubois	Manage4U BV
B. Hollifield	PAS
S. Kandasamy	Chevron
D. Logerot	ProSys Inc.
M. Marvan	Shell Canada
D. Metzger	DPM Consulting
L. Myers	Consultant
G. Nasby	City of Guelph Water Services
G. Plowman	Rockwell Automation
D. Rothenberg	D Roth Inc.
T. Stauffer	exida Co.
D. Strobhar	Beville Engineering Inc.
B. Vail	URS
D. Visnich	Burns & McDonnell
R. Weibel	Tips Inc.

This document was approved for publication by the ISA Standards and Practices Board on 3 March 2022.

NAME	AFFILIATION IN 2022
D. Zetterberg, Vice President	Consultant
D. Bartusiak	Collaborative Systems Integration, LLC
D. Brandl	BR&L Consulting, Inc.
P. Brett	Honeywell Inc.
D. Dunn	WS Nelson
J. Federlein	Consultant
B. Fitzpatrick	Wood
S. Fluchs	admeritia GmbH
J.-P. Hauet	KB Intelligence
D. Lee	Emerson
G. Lehmann	AECOM
T. McAviney	Consultant
V. Mezzano	Fluor Corp.
C. Monchinski	Automated Control Concepts Inc.
G. Nasby	City of Guelph Water Services
D. Reed	Rockwell Automation
N. Sands	DuPont
H. Sasajima	FieldComm Asia LLC
I. Verhappen	Willowglen Systems
D. Visnich	Burns & McDonnell
W. Weidman	Consultant
J. Weiss	Applied Control Solutions LLC
M. Wilkins	Yokogawa UK Ltd.

This page intentionally left blank.

Contents

Foreword.....	11
Introduction.....	12
1 Scope	15
2 Purpose	15
3 Definitions.....	15
3.1 Definitions	15
3.2 Abbreviations.....	20
4 Alarm systems and human factors	20
4.1 General	20
4.2 The nature of averages in alarm rate analyses	22
4.3 Specific alarm differences affect operator response	22
4.4 Alarms rates, process types, and operator staffing issues	23
4.5 Operator console assignments and alarm rates	24
5 Periodic alarm system performance reporting.....	25
5.1 General	25
5.2 Performance metrics.....	25
5.3 Diagnostic metrics	25
5.4 Implementation metrics	26
5.5 Scaling metrics	26
5.6 Audit metrics	26
5.7 Class-specific metrics	26
5.8 Analyses related to independent protection layer alarms	27
5.9 Performance overview reports.....	28
5.10 Customized reports for different audiences.....	29
5.11 Levels of alarm performance	31
5.12 Report design	32
6 Alarm system analyses for monitoring and assessment	34
6.1 General	34
6.2 ISA-18.2 Key alarm metrics.....	34
6.3 Annunciated alarm rate per operating position	35
6.4 Annunciated alarm rates per operating position per 10 minutes.....	36
6.5 Alarm floods	37
6.6 Frequently occurring alarms	40
6.7 Chattering and fleeting alarms.....	40
6.8 Alarm rates without chattering alarms.....	43
6.9 Non-annunciated alarms	43
6.10 Alarms by type.....	44
6.11 Stale alarms	44
6.12 Number of pages of alarm summary	45
7 System diagnostic and other analyses	46
7.1 Alarm priority distribution	46
7.2 Redundant, symptomatic, consequential, or correlated alarms	48

7.3	Analysis of specific alarm groupings or classes	49
7.4	Analyses involving alarm acknowledgement	49
7.5	Data gaps.....	50
7.6	Alarms in SCADA systems	50
7.7	Alarms and packaged systems	50
7.8	Actions based on alarm analysis	51
7.9	Alarm system management of change (MOC) monitoring	53
7.10	Improper alarm suppression	53
7.11	Alarm setpoint changes.....	54
7.12	Alarm priority changes	54
7.13	Alarm attributes analysis (alarm settings or configuration).....	54
7.14	Configured alarm priorities by alarm type	54
7.15	Configured alarm ratio	55
7.16	Alarms per I/O type.....	55
7.17	Analysis of operator actions	55
8	Alarm system auditing	58
8.1	General	58
8.2	Audit team.....	58
8.3	Materials for the audit	58
8.4	Audit checklist	59
8.5	Audit interviews	59
8.6	Audit findings.....	59
9	Alarm data	59
9.1	General	59
9.2	Alarm data types.....	60
9.3	Alarm states and alarm occurrence records	60
9.4	Alarm attributes (settings and configuration information)	63
9.5	Operator change events.....	65
10	Methodologies for obtaining alarm occurrence and attribute data.....	65
10.1	General characteristics	65
10.2	Printer port or printer emulation.....	66
10.3	System databases or files	66
10.4	OPC	67
10.5	Custom software	67
11	References	67

Figures

Figure 1 – Alarm management lifecycle (from ISA-18.2)	12
Figure 2 – Feedback model of operator process interaction (ISA-18.2, Figure 5)	21
Figure 3 – Alarm performance dashboard.....	31
Figure 4 – Alarm performance table	32
Figure 5 – Alarm performance chart (one month period)	33
Figure 6 – Alarms per day for a 39-day period.....	36
Figure 7 – Annunciated alarms per 10-minute time period for 10 days.....	37
Figure 8 – Alarm flood analysis for a single operating position.	39
Figure 9 – Alarm flood summary for a single operating position.	39
Figure 10 – Most frequent alarms.....	40
Figure 11 – Chattering alarm analysis graph	42
Figure 12 – Chattering alarm analysis summary	42
Figure 13 – Alarms per day per operator with and without chattering alarms	43
Figure 14 – Alarms by type	44
Figure 15 – Top 10 stale alarms.....	45
Figure 16 – Alarm priority distribution.....	46
Figure 17 – Alarm priority distribution.....	47
Figure 18 – Redundant/symptomatic alarm analysis	48
Figure 19 – Alarm problems and potential solutions.....	52
Figure 20 – Changes of alarm attributes.....	53
Figure 21 – Example table of controller mode changes in one week.....	56
Figure 22 – Chart of controller changes per 10 minutes	57
Figure 23 – Alarm state transition diagram from ISA-18.2	61

Tables

Table 1 – Recommended alarm performance metrics summary from ISA-18.2.....	34
--	----

This page intentionally left blank.

Foreword

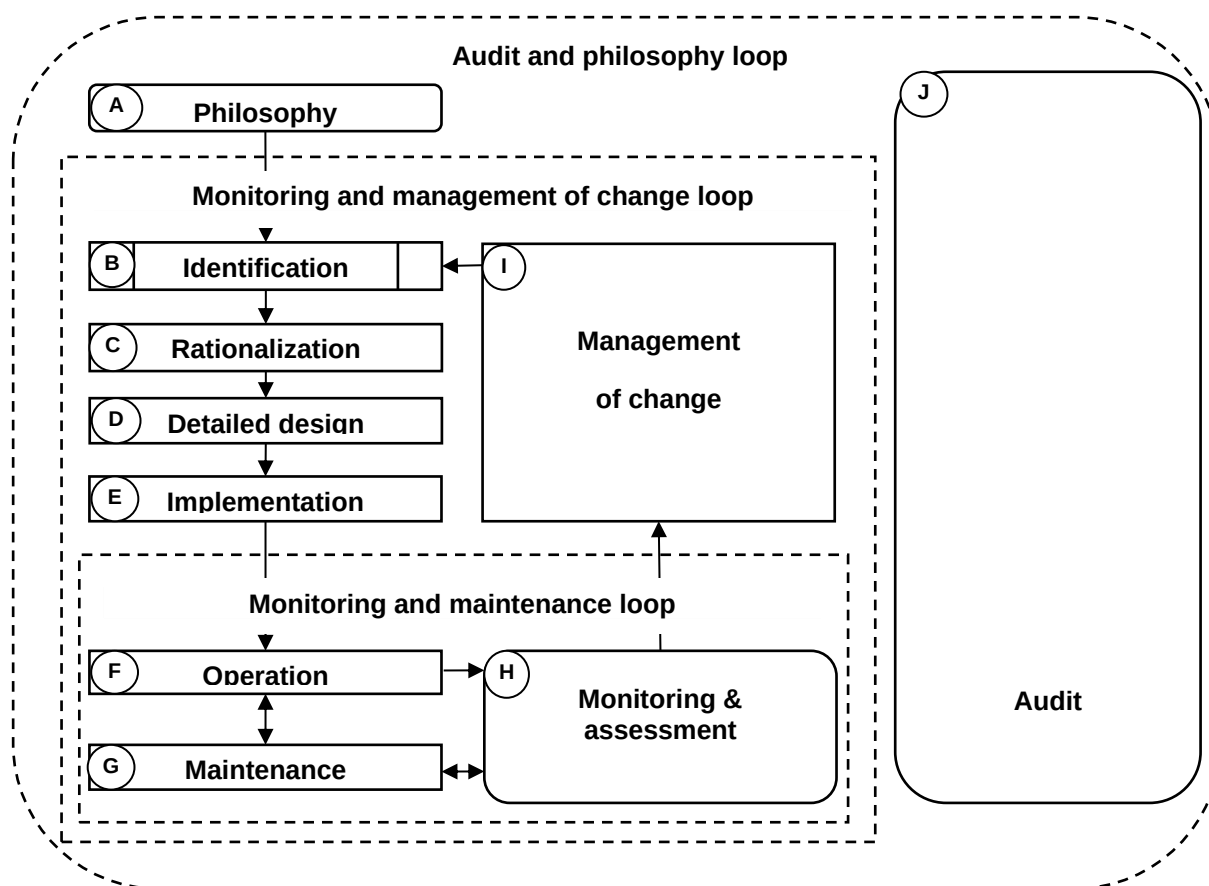
In 2009, ANSI/ISA-18.2-2009, *Management of Alarm Systems for the Process Industries*, commonly referred to as ISA-18.2, was issued, and later updated in 2016. The ISA18 committee established working groups to develop and maintain a series of technical reports with guidance on how to implement the practices outlined in ISA-18.2. The six independent technical reports are described below.

- ISA-TR18.2.1, *Alarm Philosophy* [TR1], provides guidance on the alarm philosophy. TR1 is limited to the scope of Clause 6 in ISA-18.2. The alarm philosophy provides guidance for successful management of the alarm system. It covers the definitions, principles, and activities by providing overall guidance on methods for alarm identification, rationalization, classification, prioritization, monitoring, management of change, and audit.
- ISA-TR18.2.2, *Alarm Identification and Rationalization* [TR2], provides guidance on alarm identification and rationalization. TR2 was limited to the scope of Clauses 8 and 9 in ISA-18.2. Identification and rationalization covers the activities to determine the possible need for an alarm or a change to an alarm; systematically compare alarms to the alarm philosophy; and determine the alarm setpoint, consequence, operator action, priority, and class. Activities include, but are not limited to, identification, justification, prioritization, classification, and documentation.
- ISA-TR18.2.3, *Basic Alarm Design* [TR3], provides guidance on basic alarm design. TR3 focuses on the scope of Clause 10 of ISA-18.2 and may include other clauses as needed (e.g., Clause 14 on operations and Clause 15 on maintenance). Basic alarm design covers the selection of alarm attributes (e.g., types, deadbands, and delay times) and may be specific to each control system.
- ISA-TR18.2.4, *Enhanced and Advanced Alarm Methods* [TR4], provides guidance on advanced and enhanced alarm methods. TR4 focuses on the scope of Clause 12 of ISA-18.2. Enhanced alarm design covers guidance on additional logic, programming, or modeling used to modify alarm behavior. These methods may include: dynamic alarming, state-based alarming, adaptive alarms, logic-based alarming, predictive alarming, as well as most of the designed suppression methods.
- ISA-TR18.2.5, *Alarm Monitoring, Assessment, and Audit* [TR5], provides guidance on monitoring, assessment and audit of alarms. TR5 focuses on the scope of Clauses 16 and 18 in ISA-18.2. Monitoring, assessment, and audit cover the continuous monitoring, periodic performance assessment, and recurring audit of the alarm system.
- ISA-TR18.2.6, *Alarm Systems for Batch and Discrete Processes* [TR6], provides guidance on the application of ANSI/ISA-18.2 alarm life cycle activities to batch and discrete processes, expanding on multiple clauses of ISA-18.2.
- ISA-TR18.2.7, *Alarm Management When Utilizing Packaged Systems* [TR7], provides guidance on how to integrate packaged systems into a BPCS-based centralized alarm system.

The guidance as presented in this technical report is general in nature and should be applied to each system as appropriate by personnel knowledgeable in the manufacturing process and control systems to which it is being applied. This guidance will evolve with experience and technology advancements.

Introduction

ANSI/ISA-18.2, referred to as ISA-18.2 in the technical report, provides the requirements that address alarm systems for facilities in the process industries to improve safety, quality, and productivity. The general principles and processes in ISA-18.2 are intended for use in the lifecycle management of an alarm system based on programmable electronic controller and computer-based human-machine interface (HMI) technology. These requirements are presented in the standard using the alarm management lifecycle shown in ISA-18.2, Figure 1.



NOTE 1 The box used for stage B represents a process defined outside of this standard.

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

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

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

Figure 1 – Alarm management lifecycle (from ISA-18.2)

Clause 16 of ISA-18.2 covers alarm system monitoring and assessment. Clause 18 covers alarm system auditing. Measurement is fundamental to control and improvement. Effective management of the alarm system requires ongoing measurement of its performance. A system designed in accordance with good practices may still have poor performance when brought online.

An alarm system that performs well may experience deterioration over time as sensors and process conditions change, or if a change management policy is not in place and enforced. Ongoing

performance measurement is needed to identify such situations in order to ensure a properly functioning alarm system.

This technical report has been written to aid in the collection of alarm system data, the analysis of that data, and the application of that analysis to improvement in the operation of the process. Sections of the report explain the calculation of the alarm system performance metrics and the basis for performance targets.

The work process of alarm system monitoring, assessment, and audit are the subject of this report. These terms as used herein have specific meanings:

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

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.

This page intentionally left blank.

1 Scope

This technical report was written in support of the widely used ISA international standard, ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*.

This technical report is designed to provide guidance, rationale, and examples of alarm monitoring and assessment, (Clause 16 of ISA-18.2) and audit (Clause 18 of ISA-18.2). This technical report provides guidance and information supplementing ISA-18.2 on the use of alarm system analysis for both ongoing monitoring and periodic performance assessment. Monitoring, assessment, and audit are essential to achieving and maintaining the performance objectives of the alarm system. These activities can identify improvement opportunities in the other lifecycle stages, such as philosophy, rationalization, detailed design, implementation, operation, maintenance, and management of change.

Alarm system performance analysis can also play a part in overall plant performance metrics and be used as an input to process improvement efforts. This is typically in conjunction with process historian data and control loop effectiveness data. However, analyses of control system data, process data, and operator actions are not included in this report except to note the relationship between alarm metrics and other process metrics.

2 Purpose

This technical report has been written to aid in the collection of alarm system data, the analysis of that data, and the application of that analysis to improvement in the operation of the process. Sections of the technical report explain the calculation of the alarm system performance metrics and the basis for performance targets.

3 Definitions

3.1 Definitions

Definitions from ANSI/ISA-18.2-2016 are listed in this section for terms used in this technical report.

3.1.1

absolute alarm

alarm generated when the alarm setpoint is exceeded (e.g., high-high, high, low, low-low)

3.1.2

active

an alarm in a 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.

3.1.3

alarm

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

3.1.4**alarm attribute**

setting for an alarm within the process control system

EXAMPLE: alarm priority

3.1.5**alarm class**

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

3.1.6**alarm deadband**

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

3.1.7**alarm message**

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

3.1.8**alarm off-delay****debounce**

time an alarm remains active after the process measurement has returned within the alarm setpoint

3.1.9**alarm on-delay**

time before an alarm becomes active after the process measurement has exceeded the alarm setpoint

3.1.10**alarm philosophy**

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

3.1.11**alarm priority**

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

3.1.12**alarm setpoint****alarm limit****alarm trip point**

threshold value of a process variable or discrete state that is used to determine if the alarm is active

3.1.13**alarm summary****alarm list**

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

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

3.1.14

alarm type

alarm attribute which gives a distinction of the alarm condition

EXAMPLE: low process variable alarm, high process variable alarm, or discrepancy alarm

3.1.15

allowable response time

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

3.1.16

assessment

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

3.1.17

audit

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

3.1.18

bad-measurement alarm

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

3.1.19

chattering alarm

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

3.1.20

deviation alarm

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

3.1.21

dynamic alarming

automatic modification of alarm attributes based on process state or conditions

3.1.22

enforcement

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

3.1.23

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

3.1.24**highly managed alarm (HMA)**

alarm belonging to a class with additional requirements (e.g., regulatory requirements) above general alarms

EXAMPLE: safety alarm

3.1.25**human machine interface (HMI)**

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

3.1.26**instrument diagnostic alarm**

alarm to indicate a field device or signal fault

EXAMPLE: out-of-range alarm

3.1.27**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.

3.1.28**monitoring**

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

3.1.29**nuisance alarm**

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

EXAMPLE: chattering alarm, fleeting alarm, or stale alarm

3.1.30**operator
controller**

person who monitors and makes changes to the process

3.1.31**(operator) console**

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

3.1.32**out-of-service**

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

3.1.33**plant state
plant mode**

defined set of operational conditions for a process plant

EXAMPLE: shutdown, normal operation

3.1.34

prioritization

process of assigning a level of operational importance to an alarm

3.1.35

process area

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

[SOURCE: IEC 62264-1:2013, 3.1]

3.1.36

rate-of-change alarm

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

3.1.37

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

3.1.38

recipe-driven alarm

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

3.1.39

return to normal

clear

alarm transition from an active alarm state to a not active alarm state

3.1.40

safety alarm

safety related alarm

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

3.1.41

shelve

temporarily suppress an alarm, initiated by the operator, with engineering controls (e.g., time-limited) that unsuppress the alarm

3.1.42

silence

operator action that terminates the audible alarm indication

3.1.43

stale alarm

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

3.1.44

state-based alarm

mode-based alarms

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

3.1.45**suppress**

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

EXAMPLE: shelve, suppress by design, remove from service

3.1.46**suppressed by design**

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

3.1.47**system diagnostic alarm**

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

EXAMPLE: communication error

3.1.48**tag****point**

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

3.1.49**unacknowledged**

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

3.2 Abbreviations

BPCS	Basic process control system
I/O	Input / output
IPL	Independent protection layer
MOC	Management of change

4 Alarm systems and human factors**4.1 General**

Many alarm system performance metrics are designed to incorporate human elements of comprehension and reaction. Display and data processing technologies have rapidly evolved, but the human operator's ability to view, understand, evaluate, and respond has remained relatively unchanged.

This "human constant" allows for the design of metrics that are applicable across industries and control systems, with little need for modification. As a result, many of the metrics in this document are designed to specifically relate to the span of assigned control and alarm responsibility of a single operating position. Therefore, the measurement techniques should be able to isolate the alarm data to that degree.

The human factors issues involved in alarm response are subject to many variables, and firm, fixed performance numbers cannot be established. Alarm response is not an automated process involving deterministic machines; it is a human cognitive process involving thought, analysis, and action.

The derivation of the performance numbers mentioned in this technical report is based on a variety of research studies that have been subsequently published in various articles and publications.

It is worth repeating from ISA-18.2, subclause 16.4.1: “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.”

It is the human factors that limit the alarm rate that can be successfully handled by an operator. To understand and illustrate this, consider the mental and physical steps an operator takes during effective alarm response. These generic steps are the same regardless of industry segment, process type, or control system type.

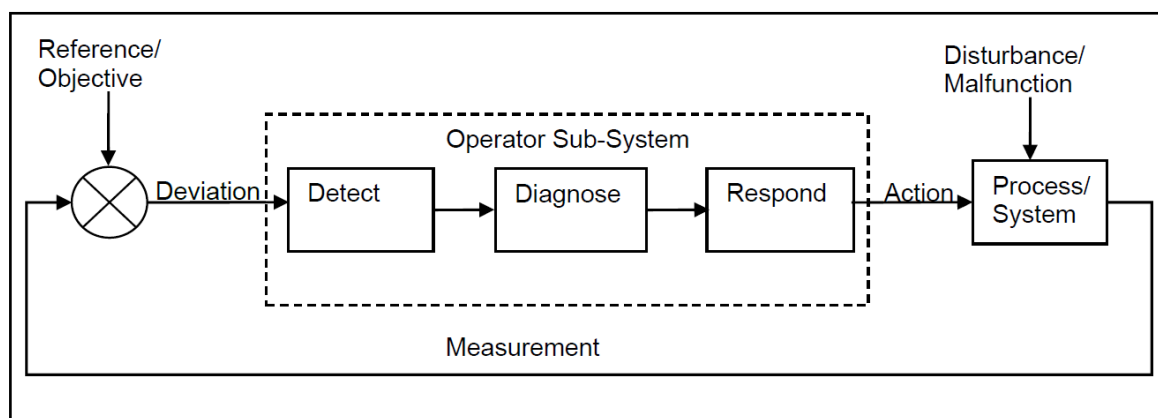


Figure 2 – Feedback model of operator process interaction (ISA-18.2, Figure 5)

Figure 2 is a duplicate of ISA-18.2, Figure 5. The operator steps involved are:

- Detection of the alarm, along with its silencing and/or acknowledgement.
- Diagnosis of the situation, involving:
 - Navigation to the appropriate screen(s) to obtain contextual information from the process of which the alarm is a part.
 - Analysis of the process situation to determine the alarm’s cause.
 - Deciding on the proper action(s) to take in response to the alarm. This may involve consulting reference information or other people.
- Response, the activity of implementing the chosen action(s), generally through manipulation of the control system, contacting and directing other people to perform tasks, leaving the console to take action that cannot be accomplished without doing so, or a combination of all of these.
- Continued system monitoring to ensure that the action(s) performed correct the situation that caused the alarm.

The above sequence of operator steps indicates that alarm response cannot be instantaneous. Several of these steps can only be accomplished sequentially. It is possible to address several alarms at once, and some of the steps for the different alarms can be accomplished in parallel. From consideration of the human factors, it is obvious that an alarm handling rate of one alarm per second is untenable, and one alarm per hour is certainly possible. The maximum rate that can be