

Alarm systems

A Guide to design, management and procurement

Publication 191

Edition 4

Copyright © 2024 The Engineering Equipment and Materials Users Association
A company limited by guarantee. Registered in England. Company number 477838.

ISBN 978-0-85931-243-1

Imprint reference 11-2024
First published 11-2024

Registered Address and Trading Address:
EEMUA, Leytonstone House, 3 Hanbury Drive, London E11 1GA

Telephone: +44 (0)20 7488 0801
Email: sales@eemua.org
Website: www.eemua.org



Engineering Equipment and Materials Users Association

About EEMUA

The Engineering Equipment and Materials Users Association is usually known by its initials, EEMUA. EEMUA is an Association established by the owners and operators of industrial assets. Any organization that is a substantial user or substantial purchaser of engineering products may apply to become a member of EEMUA. Membership is subject to the approval of Council.

EEMUA aims

EEMUA aims to improve the safety, environmental and operating performance of industrial facilities in the most cost-effective way, pursuing and promoting leadership in industrial asset management by sharing engineering experiences and expertise, and by the active, enlightened promotion of the distinct interests of users of engineering products. These aims are achieved by various means, including:

- Providing the organization within which networking, information sharing and collaboration among users on non-competitive technical matters can take place
- Influencing the way written regulations are interpreted and applied in practice
- Promoting and presenting members' views, and encouraging the application of good sound engineering practices
- Developing user guides, specifications, training and competency schemes
- Facilitating members' participation in national and international standards making
- Influencing relevant national and European legislation and regulation.

The income and resources of EEMUA are applied solely towards the promotion of the aims of the Association. No profit is transferred by way of dividend, bonus or otherwise to members. The work of the Association is mainly carried out by members' representatives on EEMUA Technical Committees, Working Groups, and Forums, supported by EEMUA staff.

Incorporation, membership and other information

For the purposes of conducting its business, EEMUA is incorporated in England and Wales as a company, limited by guarantee, not having share capital. All usual aspects of company management and business administration are dealt with through the EEMUA Chief Executive, including policy implementation and leadership of the Executive team (the staff).

A list of EEMUA publications for sale is given at the end of this Publication. The full list is also on the Association's website, including details of on-line shopping facilities.

To enquire about corporate Membership, write to ask@eemua.org or call +44 (0)20 7488 0801.

About this Publication

Legal Aspects

All rights, title and interest in this Publication belong to EEMUA. All rights are reserved. 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 other, without the express prior written agreement of the EEMUA Chief Executive. Infringement of copyright is illegal and also reduces the Association's income thereby jeopardising its ability to fund the production of future publications.

It has been assumed in the preparation of this Publication that: the user ensures selection of those parts of its contents appropriate to the intended application and that such selection and application is correctly carried out by appropriately qualified and competent persons for whose guidance this Publication has been prepared. EEMUA and the individual members of the Work Group that prepared this EEMUA Publication do not, and indeed cannot, make any representation or give any warranty or guarantee in connection with material contained herein. EEMUA and the individual members of the Work Group that prepared this EEMUA Publication expressly disclaim any liability or responsibility for damage or loss resulting from the use or reliance on this Publication. Any recommendations contained herein are based on the most authoritative information available at the time of writing and on current good engineering practice, but it is essential for the user to take account of pertinent subsequent developments and/or legislation.

Any person who encounters an inaccuracy or ambiguity when making use of this Publication is asked to notify EEMUA without delay so that the matter may be investigated and appropriate action taken.

Consultation and feedback

EEMUA encourages constructive comments on this Publication from both Members of the Association and others.

Comments should be sent on the standard feedback form, a copy of which is provided towards the end of this Publication. An electronic version of the feedback form is available from EEMUA - e-mail your request for a copy to ask@eemua.org, telephone your request to +44 (0)20 7488 0801, or download the form from the EEMUA website at www.eemua.org. Submit comments by e-mail (preferred) or post.

Comments are considered by the relevant EEMUA Technical Committees and may be incorporated in future editions of this Publication. New editions are publicised on the EEMUA website.

Contents

Contents	v
List of Tables.....	xiv
List of Figures	xv
Foreword	xvi
About this Guide	1
Aim	1
Scope.....	2
Why this Guide is Important	2
Revised Second Edition 2007	3
Revised Third Edition, 2013.....	3
Revised Fourth Edition, 2024.....	3
Relationship between EEMUA 191 and EEMUA 201	3
Acknowledgements.....	4
Quick overview	4
1 Introduction	8
1.1 What is an alarm?	8
1.2 What is an alarm system?	8
1.3 Why is alarm design important?.....	9
1.4 Key design principles.....	10
1.5 Practical and organizational issues	12
1.5.1 General approach – PDCA.....	12
1.5.2 Resources required	13
1.5.3 Alarm philosophy	13
1.5.4 Project lifecycle	13
1.5.5 Alarm system lifecycle (IEC 62682).....	14
1.5.6 Alarm database	16
1.5.7 Operator response to alarms.....	16
1.5.8 Fostering a culture of improvement.....	17
1.6 Using this guide.....	17
1.7 Supporting documents.....	18

2	Principles of alarm system design.....	19
2.1	Design goals and objectives.....	19
2.1.1	Human / user centred design.....	19
2.1.2	The role of the operator.....	20
2.1.3	The type of process.....	21
2.1.4	Designing for operability.....	23
2.2	Alarm system design.....	24
2.2.1	Hierarchy of risk control.....	24
2.2.2	Alarm system hardware and software.....	24
2.2.3	Designing individual alarms.....	26
2.2.4	When is it appropriate to provide an alarm?.....	26
2.3	Similar, non-alarm functions.....	27
2.3.1	Alerts.....	27
2.3.2	Events.....	28
2.3.3	Prompts.....	28
2.3.4	Non-alarms.....	29
2.4	Alarm classification.....	29
2.5	Highly Managed Alarm (HMA).....	30
2.5.1	Types of HMA.....	30
2.5.2	Protective layer alarms.....	31
2.5.3	HMA management.....	32
2.6	Summary of alarms, alerts, events and prompts.....	33
2.7	Risk management.....	33
2.7.1	The need to identify and control risks.....	33
2.7.2	Risk reduction using alarms.....	34
2.7.3	Taking credit for alarms.....	35
2.7.4	Operator response times.....	36
2.7.5	Alarm systems contribute to controlling risks.....	37
3	Practical considerations for alarm design	38
3.1	Generation of alarms.....	38
3.1.1	Types of alarm.....	38
3.1.2	First-up alarms.....	39
3.1.3	The selection of alarm settings.....	40
3.1.4	Alarm settings by recipe.....	42
3.2	Field derivation of alarms.....	43
3.2.1	Challenges with switch type sensors.....	44
3.2.2	Measurement of actuator position.....	45
3.2.3	Location of sensors.....	45
3.2.4	Analogue sensor range.....	45
3.2.5	Reliability.....	46

3.3	Alarm processing hardware.....	46
3.3.1	BPCS processing of alarms.....	46
3.3.2	High integrity alarm systems.....	47
3.3.3	Combined BPCS and safety systems.....	47
3.3.4	Dedicated alarm systems.....	47
3.3.5	Reliability issues.....	48
3.3.6	Functionality.....	49
3.3.7	Environmental requirements.....	49
3.3.8	Validation of measurements.....	50
3.3.9	Signal transmission.....	50
3.4	Alarm design for unoccupied and remote control rooms.....	51
3.4.1	Getting information to remote operations.....	51
3.4.2	Alarm management in geographically distributed plant.....	52
3.4.3	The role of field personnel in handling alarms.....	53
3.4.4	Telemetry issues.....	54
3.4.5	Getting information to remote resources.....	55
3.5	Alarm identification.....	56
3.5.1	Alarm Tag numbers.....	56
3.5.2	Alarm messages.....	56
4	Implementing an alarm management system.....	57
4.1	Corporate and local arrangements.....	57
4.1.1	Corporate considerations.....	57
4.1.2	Local requirements and considerations.....	58
4.1.3	Corporate and local documents required.....	58
4.2	Alarm systems management organization.....	59
4.2.1	Leadership.....	59
4.2.2	Coordination.....	59
4.2.3	Alarm steering committee.....	60
4.3	Competence.....	60
4.3.1	Operator competence.....	60
4.3.2	Supervisors.....	61
4.3.3	Control and instrument technicians.....	61
4.3.4	Plant managers.....	61
4.3.5	Alarm coordinators.....	62
4.3.6	Human factors engineers.....	62
4.3.7	Non-technical skills.....	62
4.4	Alarm philosophy document.....	62
4.4.1	Requirements for different stages of a plant lifecycle.....	62
4.4.2	Mandatory requirements.....	63
4.4.3	Additional content.....	63
4.5	Testing of alarms.....	64

4.6	Operating with degraded systems	64
4.7	Determining how well alarms are managed.....	65
5	Alarm communication and HMI Design	66
5.1	Human factors	66
5.1.1	Human factors theory in relation to alarms.....	66
5.1.2	Human factors in practice.....	67
5.2	Display options.....	68
5.2.1	Alarm annunciator panels.....	69
5.2.2	Alarm list displays	70
5.2.3	Graphically embedded alarm objects.....	71
5.3	Making sure alarms are noticed.....	72
5.3.1	Audible indications.....	72
5.3.2	Visual indications	73
5.3.3	Alarm priority markers.....	73
5.4	Alerts, events and prompts.....	73
5.5	Design of alarm lists.....	74
5.5.1	Alarm states.....	74
5.5.2	Content of alarm entry	75
5.5.3	Positioning of new alarms on the list	76
5.5.4	Alarm acceptance.....	77
5.5.5	Movement through the list.....	77
5.5.6	Display filtering	77
5.5.7	On screen alarm response definitions	78
5.6	Displaying HMAs	78
5.7	Shelved and suppressed alarms.....	78
5.8	The full alarm list.....	79
6	Practical considerations for alarm system management	80
6.1	Maximising usefulness of alarms	80
6.1.1	Prioritisation.....	81
6.1.2	Special consideration for distributed plant.....	82
6.1.3	Minimising unnecessary and nuisance alarms	83
6.1.4	Avoiding alarm floods.....	84
6.1.5	Logical processing of alarms.....	84
6.1.6	Alarms generated by phase logic or procedure (batch process)	85
6.2	Grouping alarms.....	86
6.3	Alarm suppression.....	86
6.3.1	Bulk suppression	87
6.3.2	Logical suppression.....	87
6.3.3	Implementation of suppression.....	88
6.3.3.1	Specific example of bulk alarm suppression – condition equation.....	90
6.3.3.2	Specific examples of logical suppression.....	90
6.3.4	Authorisation and control	91

6.4	Avoiding repeating alarms	91
6.4.1	Why repeating alarms occur	91
6.4.2	Engineering of signals to minimise noise	92
6.4.3	Filtering	92
6.4.4	Transient suppression	93
6.4.5	Deadband	93
6.4.6	De-bounce timer	94
6.4.7	Counter	95
6.4.8	Single line annunciation	95
6.4.9	Logging of repeating alarms	96
6.4.10	Threshold setting	96
6.5	Alarm shelving	97
6.5.1	Circumstances when shelving is allowable	97
6.5.2	Release ('One-shot' shelving)	98
6.5.3	Alarms from equipment under test	98
6.6	Automatic alarm load shedding	99
6.7	Improving alarms and alarm systems	99
6.7.1	Improving individual alarms (bad actors)	100
6.7.2	Rationalisation to ensure the alarm system is properly configured	100
6.7.3	System replacement	102
6.7.4	General guidance for improving alarms	102
7	Performance monitoring and improvement	104
7.1	Introduction	104
7.2	Measuring what is important	105
7.3	Metrics applied during design	105
7.3.1	Metrics for HMAs	106
7.3.2	Priorities of alarms configured	106
7.3.3	Avoiding standing alarms	106
7.3.4	Performance data generation	107
7.4	Optimizing human Performance Influencing Factors (PIF)	107
7.4.1	Workload and time availability during steady state operation	107
7.4.2	Workload and time availability for non-routine and abnormal operations	107
7.4.3	Clarity of information provided by alarms	107
7.4.4	Benchmark for standing alarms	109
7.4.5	Key Performance Indicators (KPI)	109
7.4.6	Operations reporting and feedback	111
7.4.7	Alarm analysis tools	111
7.4.8	Summary of performance metrics	112
7.4.9	Alarm systems states (robust, stable, reactive, overloaded)	112
7.5	Alarm system audits	119

8 Management of change and projects	120
8.1 Management of change	120
8.1.1 Minor changes.....	121
8.1.2 Significant changes	121
8.1.3 Major projects.....	122
8.1.4 Implementing changes.....	122
8.1.5 Deleting alarms.....	122
8.2 Business case and justifying investment	123
8.2.1 Process improvements	123
8.2.2 Standardisation and consistency	125
8.2.3 Improved operator performance.....	125
8.2.4 Easier training.....	125
8.2.5 Improved security and resilience.....	125
8.2.6 The cost of alarm performance.....	125
Appendix 1 – The costs of poor alarm performance	126
A1.1 Accident summaries.....	126
A1.1.1 Milford Haven refinery.....	126
A1.1.2 Longford gas explosion.....	126
A1.1.3 BP Texas City refinery	126
A1.1.4 Buncefield Oil storage depot.....	127
A1.1.5 Enbridge Incorporated pipeline rupture	127
A1.1.6 Columbia gas pipeline rupture	127
A1.1.7 Pryor Trust well blowout.....	128
A1.1.8 BP-Husky.....	128
A1.2 Costs of poor alarm system performance.....	128
A1.2.1 HSE alarm survey	128
A1.2.2 Abnormal Situation Management (ASM) consortium	129
A1.2.3 Refinery study.....	129
Appendix 2 – Human Factors Integration Plan (HFIP) for alarms	130
A2.1 Purpose of a HFIP	130
A2.2 Project lifecycle.....	130
A2.3 Suggested content for an alarms HFIP.....	130
A2.4 HFIP introduction	131
A2.5 Concept/Select phase	131
A2.5.1 Users and requirements	131
A2.5.2 Constraints	131
A2.5.3 Learning from experience.....	132
A2.5.4 Responsibilities for alarm management	132
A2.5.5 Ensuring end user involvement.....	133
A2.5.6 Draft alarm philosophy	134
A2.5.7 Basis of design.....	131

A2.6 Define phase	134
A2.6.1 Review output from Concept/Select phase	135
A2.6.2 Modes of operation	135
A2.6.3 Layers of protection	135
A2.6.4 Logical processing	135
A2.6.5 Staffing philosophy	135
A2.6.6 Human Machine Interface (HMI) design philosophy	136
A2.6.7 Remote and repeater systems	136
A2.6.8 Working environment considerations	136
A2.6.9 Training requirements and facilities	136
A2.6.10 User preference	136
A2.6.11 Conceptual design	137
A2.6.12 Responsibilities for human factors integration	137
A2.6.13 Basis of design	137
A2.7 Develop/Execute phase	137
A2.7.1 Review output from Define phase	138
A2.7.2 Staffing levels and team working	138
A2.7.3 Creating the final alarm database	138
A2.7.4 HMI design	139
A2.7.5 Plans for commissioning and operation	139
A2.7.6 Project close-out	139
A2.8 Operate phase	140
Appendix 3 – Prioritisation methods	141
A3.1 Potential severity of consequence	141
A3.2 Time to consequence	141
A3.3 Priority distribution of alarms	142
A3.4 Example methods for setting of priority	142
A3.4.1 Method 1 - Priority matrix evaluation	142
A3.4.2 Method 2 - Consequence based prioritisation	144
A3.4.3 Method 3 - Taking maximum consequence	144
Appendix 4 – Example alarm philosophy	147
A4.1 Purpose	147
A4.2 Definitions	147
A4.3 Roles and responsibilities	147
A4.4 Alarm design principles	148
A4.5 Prioritisation methods and metrics	148
A4.6 Alarm class definition	148
A4.7 Criteria for identifying Highly Managed Alarms (HMAs)	149
A4.8 Rationalization criteria to assess alarms	150
A4.9 Alarm documentation	150

A4.10 Alarm design guidance	150
A4.11 Human Machine Interface (HMI) design principles.....	150
A4.12 New or changed system implementation	151
A4.13 Alarm response procedure.....	151
A4.14 Training for operators, managers, designers etc.	152
A4.15 Alarm system maintenance and testing	152
A4.16 Alarm system performance monitoring	152
A4.17 Management of Change (MOC).....	153
A4.18 Alarm system audit.....	153
A4.19 Coverage of non-alarms	153
Appendix 5 – Alarm rationalization procedure	154
A5.1 Introduction.....	154
A5.2 Purpose of alarm rationalization	154
A5.3 Scope of the study.....	154
A5.4 Establish the team.....	155
A5.5 Collect alarm data	155
A5.6 Review the alarm philosophy vs requirements.....	155
A5.7 Conduct rationalization sessions.....	155
A5.8 Document rationalization findings:	156
A5.9 Identify recommended actions.....	156
A5.10 Suggested terms of reference for a rationalization study	157
Appendix 6 – Usefulness questionnaire	158
A6.1 Introduction.....	158
A6.2 How many alarms are useful?	159
Appendix 7 – Operator questionnaire	161
A7.1 Introduction.....	161
Appendix 8 – Alarm Review Checklists	169
A8.1 Alarm threshold setting	169
A8.2 Checklist for a good alarm	169
A8.3 Alarm configuration information	170
A8.4 HAZOP checklist.....	171
A8.5 Alarm sensor design	172
Appendix 9 – Example alarm suppression hazard study.....	173
A9.1 Introduction.....	173
A9.2 Example	173
A9.2.1 Familiarization	174
A9.2.2 Review of operating modes.....	174
A9.2.3 Review of alarms to be suppressed	174

A9.2.4 Reporting	175
A9.2.5 Follow-up.....	175
Appendix 10 – Specification checklist - small system	176
A10.1 Where dedicated alarm systems are used.....	176
A10.2 Input handling.....	176
A10.3 Alarm processing	176
A10.4 Alarm display/output	177
A10.5 Environmental	177
Appendix 11 – Specification checklist - large system	178
A11.1 Grading of requirements.....	178
A11.2 Input handling.....	178
A11.3 Processing of Alarms	179
A11.4 Display of Alarms	180
A11.5 Logging of Alarms.....	181
A11.6 Engineering of Alarm systems.....	182
Appendix 12 – Intelligent fault detection	183
A12.1 Pattern recognition	183
A12.2 Neural networks	184
A12.3 Fuzzy logic.....	185
A12.4 Knowledge-based reasoning.....	186
A12.5 Model-based reasoning.....	187
A12.6 Overview of intelligent fault detection methods.....	187
Appendix 13 – Glossary and abbreviations	189
Appendix 14 – References.....	195
Appendix 15 – Bibliography	198
EEMUA Publication: feedback Form	200
EEMUA Learning Courses	201
EEMUA Publications Catalogue	203

List of Tables

Table 1 Characteristics of a good alarm.....	12
Table 2 Alarm management lifecycle stages (IEC 62682 vs EEMUA 191).....	15
Table 3 How system size affects design and management.....	25
Table 4 Document suggestions.....	58
Table 5 HMI requirements for support of operators.....	67
Table 6 Alarm display options.....	68
Table 7 Alarm suppression.....	88
Table 8 Example of bulk alarm suppression.....	90
Table 9 Table of filter time constants.....	92
Table 10 Table of default deadband settings.....	94
Table 11 Table of default de-bounce timer parameters.....	95
Table 12 Checklist to assist with setting thresholds.....	96
Table 13 Checklist for evaluating an alarm.....	101
Table 14 Effective techniques for improving alarm systems.....	103
Table 15 Priority distribution.....	106
Table 16 Long term average alarm rate.....	107
Table 17 Major process upset alarm.....	108
Table 18 Target maximum occurrence rates of alarms of different priorities.....	108
Table 19 Standing alarms.....	109
Table 20 Summary of possible alarm metrics per operator station.....	112
Table 21 Alarm system performance metrics.....	113
Table 22 Overloaded alarm state.....	115
Table 23 Reactive alarm state.....	116
Table 24 Stable alarm state.....	117
Table 25 Robust alarm state.....	118
Table 26 Hazard Index grouping for use with an alarm priority matrix.....	143
Table 27 Time to Consequence (TTC) grouping for use with an alarm priority matrix.....	143
Table 28 Alarm priority guide when using an alarm priority matrix.....	143
Table 29 Priority break points for alarms.....	144
Table 30 Rules for allocation of safety, environmental and financial priority.....	146
Table 31 Example of weighting of results of usefulness questionnaires.....	158
Table 32 Proportion of useful alarms.....	160
Table 33 Alarm pattern array.....	184

List of Figures

Figure 1 Relationship between Basic Process Control System (BPCS), Safety Instrumented System (SIS) and alarm displays.....	9
Figure 2 PDCA applied to alarm management.....	13
Figure 3 Alarm management activities at project stages.....	14
Figure 4 Lifecycle model (taken from IEC 62682).....	14
Figure 5 Operator response to an abnormal situation	21
Figure 6 Illustration of how alarm settings can vary for batch and continuous processes.....	22
Figure 7 Identifying Alerts, Alarms and Prompts.....	29
Figure 8 Components of an HMA	31
Figure 9 Flowchart guide to decide selection of alarms, alerts, prompts and HMAs.....	33
Figure 10 Layer of Protection model of risk management.....	34
Figure 11 Engineered and human controls for managing risks depending on operational status.....	36
Figure 12 An effective and ineffective alarm system.....	40
Figure 13 The setting of a high alarm with an absolute setpoint.....	41
Figure 14 Example of a separate set of alarm thresholds.....	43
Figure 15 Geographically distributed processes	54
Figure 16 Example of a virtual annunciator panel.....	70
Figure 17 Alarm state transition diagram for static alarm list display.....	75
Figure 18 Example of a flowchart for allocating two levels of prioritisation	82
Figure 19 Typical approach to assigning alarms for batch processes (based on the IEC 61512/ ISA S88 Batch Standard model)	85
Figure 20 Alarm suppression implementation.....	89
Figure 21 Repeating alarms generated by noise on a process signal	91
Figure 22 Transfer function of deadband.....	93
Figure 23 The elimination of repeating alarms using deadband.....	93
Figure 24 Alarm system performance	113
Figure 25 Typical plot of Key Performance Indicator	124
Figure 26 Productivity histogram.....	124
Figure 27 Alarm priority matrix.....	142
Figure 28 Prioritisation using maximum of individual priorities	145
Figure 29 Plant system with redundant equipment	183
Figure 30 A simple neural network.....	185
Figure 31 A graphical rule definition.....	186

Foreword

The Health and Safety Executive was consulted during the revision to this guidance. We endorse the sensible and proportionate approach described in the guidance that supports people with the design, management and procurement of alarm systems.

Max Walker

Acting Head of Chemicals, Explosives and Microbiological Hazards Division
Health and Safety Executive (HSE)
UK 2024

About this Guide

Aim

The aim of this Guide, EEMUA 191, is to assist in the design, development, procurement, operation, maintenance and management of industrial alarm systems. Following the guidance in EEMUA 191 should result in better alarm systems that are more usable and that result in safer and more cost-effective industrial operations.

This Guide has been produced by the users of alarm systems in industry. It is based on what some leading companies are doing, but it is also intended to be challenging and to promote continuous improvement in alarm handling practices from every starting level. It is intended to help both in improving existing systems and in developing new facilities during plant construction or during alarm system refurbishments.

Four core principles have been included in this guide since its early editions.

First – Usability. Alarm systems should be designed to meet user needs and operate within the operator's capabilities. This means that the information alarm systems present should:

- be relevant to the operator's role at the time
- indicate clearly what response is required
- be presented at a rate that the operator can deal with
- be easy to understand.

Second – Safety. The contribution of the alarm system to protecting the safety of people, the environment and the plant equipment should be clearly identified. Any claims made for operator action in response to alarms should be based upon sound human performance data and principles.

Third – Performance monitoring. The performance of the alarm system should be assessed during design and commissioning to ensure that it is usable and effective under all operating conditions. Regular auditing should be continued throughout plant life to confirm that good performance is maintained. This requires a real and continuing commitment from the senior management of the plant.

Fourth – Investment in engineering. Alarm systems should be engineered to suitably high standards. When new alarm systems are developed (or existing systems are modified), the design should follow a structured methodology in which every alarm is justified and properly engineered. The initial investment in system design should be sufficient to avoid the operational problems and the safety, environmental and financial risks that often arise and which result in overall higher lifetime costs. Contract strategies should be chosen to ensure that alarm systems are engineered to good standards.

Scope

This Guide is primarily concerned with alarm systems provided for people operating industrial processes. These include alarm systems in industries such as chemical manufacture, power generation, oil and gas extraction and refining as well as other industries. The Guide has been compiled from the experience gained within such industries, however much of the guidance is generic and with appropriate interpretation can be applied in other sectors. For example, the guide has been used successfully as a basis for training in the rail and transport sectors, in the nuclear industry, and elsewhere.

Guidance is included on:

- The design of alarm processing systems and their functionality.
- The operation of existing alarm systems and performance optimization.
- The specification and purchase of new alarm systems.

Alarm system functionality is now commonly included in computer-based systems used to control and monitor industrial processes, as well as being found in stand-alone dedicated computer-based alarm systems and the more basic annunciator-based or hard-wired 'light box' systems. This Guide is appropriate to alarm systems implemented by any of these methods, wherever a human response may be needed to an alarm condition. The guidance is designed to be practical and usable. There is overview information, and also much detailed guidance on specific issues.

Why this Guide is Important

Alarm systems form an essential part of the operator interfaces to large modern industrial facilities. They provide vital support to the operators by warning them of situations that need their attention and intervention.

Alarm systems thus have an important role in preventing, controlling and mitigating the effects of abnormal situations. If these alarm systems do not work well, the effects can be very serious. The explosion and fires at the Milford Haven Refinery in the UK^[1] – which caused £48 million of plant damage plus major production loss – could have been prevented by the operating staff. They were unable to do this partly because they faced a continuous barrage of alarms for the whole five hour period leading up to the accident. Alarm overload during an abnormal situation is a common problem: it usually means the alarm system is at its least effective when it is needed most. In the England-France Channel Tunnel fire^[2] – which resulted in damage and revenue losses totalling around £200 million – problems with alarms led to slow recognition of the fire and inhibited the effective management of the incident.

In neither of these accidents were people seriously injured or killed. However, there have been serious industrial accidents of a similar nature which have resulted in deaths. There have also been prosecutions and breaches of environmental limits. Whilst the degree to which alarm systems have contributed to these accidents is difficult to establish, alarm information has often been material. Alarm system performance is still being cited in continuing major incidents as a contributory factor (for instance, see the BP-Husky incident^[24] in 2022).

Alarm system shortcomings cause a multitude of smaller avoidable incidents which increase the risks to people and increase operating costs. A survey carried out for the GB Health & Safety Executive in the chemical and power industry^[6] identified many problems with alarm systems and many

cases where inadequacies in alarm system performance had led to financial loss or to equipment or environmental damage. Such incidents are often difficult to identify and quantify precisely. However, the total costs incurred in all such incidents are large and significant savings could be made by eliminating them.

Major accidents that can be attributed to failing alarm systems have continued to happen as exemplified by the Texas City Refinery explosion (2005) and the massive explosion that occurred at the Buncefield Oil Storage Site (2005) in Hertfordshire.

Revised Second Edition 2007

Thousands of copies of this EEMUA 191 Guide have been sold since it was first launched in 1999. Purchasers have included process operating companies, suppliers, engineering contractors, training establishments, regulatory agencies, inspection bodies and individual engineers.

The principles and guidance in EEMUA 191 have been applied worldwide and for many it has become the de facto code of good and best practice. Significant improvements are being seen by those companies investing appropriate time and resources to ensure that their alarm systems meet the requirements of good operational ownership.

From 2007, a revised 2nd Edition was published. It built on the original First Edition, by taking note of feedback from the large body of users of the Guide, updating items as appropriate, especially where knowledge has moved forward.

Revised Third Edition, 2013

Edition 3 was substantially revised and updated. Some Sections in Edition 3 were completely new while others related to updated versions of Sections in Edition 2.

Revised Fourth Edition, 2024

Experience in the use of Edition 3 indicated that there would be value in restructuring the information to be better aligned with how users approach typical alarm management problems. The opportunity was also taken to include more diagrammatic representations of some of the decision trees of importance to users and to add weight to some of the human factors considerations. Terms and definitions have also been revised where necessary to be consistent with the relevant editions of standards published since 2013, principally IEC 62682, IEC 61511 and IEC 61508. Whilst the criteria expressed in previous editions have not changed, in many cases the accompanying explanatory text has been improved. Technological change such as increased use of remote management also needs to be considered and is included in this edition.

Relationship between EEMUA 191 and EEMUA 201

Although this guide (EEMUA 191) and the Control Rooms guide (EEMUA 201) are separate documents, they are very closely related. An alarm system should be viewed as a sub-system of the overall Human-Computer Interface, which the operator uses to monitor and control the plant and the way in which the alarm data is displayed to the operator should be considered as part of the overall HCI design.

More detail on alarm display is given in Chapter 5 as well as in EEMUA 201.

Acknowledgements

The 1st Edition of this Guide was prepared by an EEMUA sub-committee comprising representatives of EEMUA member companies and the GB Health & Safety Executive (HSE). Funding for the Guide was provided by EEMUA member companies and by the Abnormal Situation Management Consortium¹ (ASM®). A large number of comments on the draft Guide were received from EEMUA Member Companies, ASM Consortium members and elsewhere. The development was assisted by the late Matthew Bransby. Tragically Matthew died in a climbing accident in 2000.

This Fourth Edition has been written under the guidance of a working group of EEMUA's Instrumentation and Control committee (INC), but many people have contributed to its production. In particular EEMUA would like to express its thanks to Andy Brazier of ABRisk Limited for his primary author role, to Elaine Skilling of the GB Health and Safety Executive for extensive comments throughout several drafts, to Asger Schliemann Haug of Lloyds Register and Nic Butcher of the Office of the Nuclear Regulator. Further thanks are due to the following members of the industry review group for their insightful and constructive comments which were greatly appreciated.

Martin Anderson	Humanfactors101
Linn Iren Vestly Bergh	Havtil
Marek Bialy	Perenco
Dave Board	Yokogawa
Ian Brown	ProcessVue
Ruud Pikaar	Ergos Human Factors Engineering
Marleen Stieler	NAMUR WG2.9
David Strobhar	Beville
Scott Turner	Emerson Process Management Ltd
Steve Willetts	formerly of British Gas

Any reader is able to make comments or provide suggestions on the current Edition and a feedback form is provided towards the end of this publication for that purpose.

Quick overview

There are many things to consider and be aware of with alarms and alarm management. As a result, despite striving to be clear and concise, this guide is a weighty document. People with a significant role in alarm management should familiarize themselves with the full content. However, many people will have a lesser role and may not know where to start. This quick overview is intended to get you started, highlighting some differences depending on whether you are dealing with an existing or new system.

¹ ASM and Abnormal Situation Management are US registered trademarks of Honeywell International, Inc.

Everyone working with existing or new alarm systems	
Make sure you understand the role of alarms and how poorly design systems cause issues.	- Sections 1.3 and 1.4 give an overview of key points. - Section 2.1 and its sub-sections describe design goals and objectives including the importance of a human / user centred approach to support process operators who have to handle alarms. - Appendix 13 provides a glossary of the terms, including a definition for 'alarm' which will provide a focus on objectives to be achieved.
Make sure you know which regulations, standards and company policies to apply	- Section 1.5.5 gives an overview of IEC 62682. - Section 4.1 and its sub-sections identify corporate and local arrangements that may apply.
Make sure there is a good alarm philosophy document	- Section 2.2 and its sub-sections cover high level design aims for a good system. Section 2.3 covers the use of non-alarms including alerts, events and prompts. - Section 2.5 and its sub-sections describe Highly Managed Alarms (HMA) and associated requirements. - Section 2.7 and its sub-sections covers how alarms should be considered as part of wider risk management for process plant. - Section 4.4 and its sub-sections describe the requirements of a philosophy document. - Appendix 4 presents an example alarm philosophy that you can amend for your own use.
Make sure you have the right resources and competencies in place to manage alarms	- Section 4.2 and its sub-sections describe the organization required for alarm management. - Section 4.3 and its sub-sections describe competency requirements.

Working with an existing system	
Make sure you have ways of evaluating system performance	- Chapter 7 describes how performance can be monitored to drive improvement. It includes benchmarks, Key Performance Indicators (KPI) and how to determine your system status (e.g. robust, reactive). - Section 7.5 discusses audit.
Look at data and ask the operators to determine how well the system works and where it needs to be improved	- Section 4.7 describes what to look at to determine if alarms are being managed well. - Section 6.7.1 describes how bad actors can be rectified. - Section 6.7.4 provides general guidance for improving alarms. - Appendices 6 and 7 present questionnaires that can be used to support evaluation of alarm system performance.
Determine if rationalisation is required and implement	- Section 6.7.2 describes how to carry out alarm rationalisation. - Appendix 5 presents an alarm rationalisation procedure.
Identify the best ways of improving alarm system performance	- Chapter 3 provides detail on alarm design. - Chapter 5 provides detail on interface design and human factors. - Section 6.1 and its sub-sections describe how to make alarms useful. It covers prioritisation, eliminating unnecessary and nuisance alarms, avoiding alarm floods. - Section 6.3 and its sub-sections describe how suppression can be used to reduce alarm rates. - Section 6.4 and its sub-sections describe strategies to reduce repeating alarms including filtering and setting deadbands.
Make the case for change and implement via management of change	- Section 8.1. describes management of change requirements. - Section 8.2 and its sub-sections describe how a business case can be made including process and operator performance, security, cost reduction. - Appendix 1 summarises historical accidents that highlight the cost of poor alarm performance.

Working with a new system	
Put arrangements in place to make sure alarm system performance and human factors are properly considered	• Section 1.5.4 sets out how alarms should be considered over a project lifecycle. • Appendix 2 provides a template for a Human Factors Implementation Plan (HFIP)
Allocate competent resources	• Section 4.3 and its sub-sections describe competencies.
Procure a suitable system	• Section 2.2.2 gives guidance about how to select a system. • Chapter 5 describes the features of the user interface that should be considered when deciding which system to procure. • Appendices 10 and 11 provide specification checklists for small and large systems.
Generate an alarm database	• Section 1.5.6 describes the contents of a database
Conduct a formal rationalisation study	• Section 6.7.2 describes how to carry out alarm rationalisation. • Section 7.3 and its sub-sections describe metrics to be applied during design. • Appendix 5 presents an alarm rationalisation procedure.
Design and implement the system	• Chapter 3 covers alarm design. • Chapter 5 covers design of operator interfaces. • Section 6.1 and its sub-sections describe how to make alarms useful. It covers prioritisation, eliminating unnecessary and nuisance alarms, avoiding alarm floods. • Section 6.3 and its sub-sections describe how suppression can be used to reduce alarm rates communicated to the operator. • Section 6.4 and its sub-sections describe strategies that can reduce repeating alarms including filtering and setting deadbands.

1 Introduction

This Section provides an introduction to alarms and alarm systems. It covers:

- Definition of 'alarm'.
- Basic explanation of what an 'alarm system' is.
- Why alarm design is important.
- Key principles when designing alarm systems.
- Practical and organizational issues of implementing alarm systems.

Key principles identified include:

- **The purpose of an alarm system is to direct the operator's attention and intervention towards process conditions requiring a timely response.**
- **Each alarm should attract, inform and guide.**
- **Every alarm presented to the operator should be useful and relevant to them.**
- **Every alarm should have a defined response.**
- **An alarm's activation point should give the operator adequate time to carry out the defined response.**

These are important principles that underlie much of the thinking in this Guide.

1.1 What is an alarm?

The everyday use of the word alarm refers to a warning of existing or approaching danger, or the device that is used to broadcast that warning. In an industrial setting the following definition applies ^[5]:

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

To achieve its function an alarm must effectively and efficiently prompt the desired response from the operator. It must attract the operator's attention and inform them why an alarm has occurred. The operator must then diagnose what has happened, select an appropriate response and take action. Individual alarms cannot be considered in isolation and the operator interface, which includes the wider alarm system, will affect how the operator performs. Alarms, the alarm system and operator interface must be designed with human capabilities in mind.

1.2 What is an alarm system?

In this Guide the term 'alarm system' refers to the complete system for generating and handling alarms including field equipment, signal conditioning and transmission, alarm processing and alarm display. It also includes hardware, software and supporting information (e.g. alarm response procedures, management controls). The way operators respond to alarms is central to the overall function and so the operator should be viewed as an integral part of the wider system.

The term ‘alarm processor’ refers to the part of the system for processing data from the process, applying logic functions ^[5] to determine if an alarm condition has been met and displaying alarms ^[5]. This is often handled by the Basic Process Control System (BPCS), which uses an electronic Human Machine Interface (HMI) as the display device. This highlights that most alarms are considered to be a Low Integrity Safety Instrumented Alarm Function (LISIAF) ^[6]. Alarms may also be handled by a higher integrity Safety Instrumented Alarm Function (SIAF) or a proprietary electronic annunciator box or panel. These alarms are referred to in this edition of EEMUA 191 as Highly Managed Alarms (HMA).

The following Figure 1 shows the position of the alarm display in relation to the BPCS and Safety Instrumented System (SIS). In a broad sense the display is part of the operator’s HMI and in modern systems is often embedded into its hardware and software. However, functionally alarms are separate from other elements of the HMI. This is especially important for alarms generated by the SIS, which should be handled by a system with high integrity.

Figure 1 highlights that alarms are handled by human operators and so the display has to be consistent with human data handling capabilities. Human factors is an important part of alarm management, which should take into account all aspects of the HMI including process graphics ^[7].

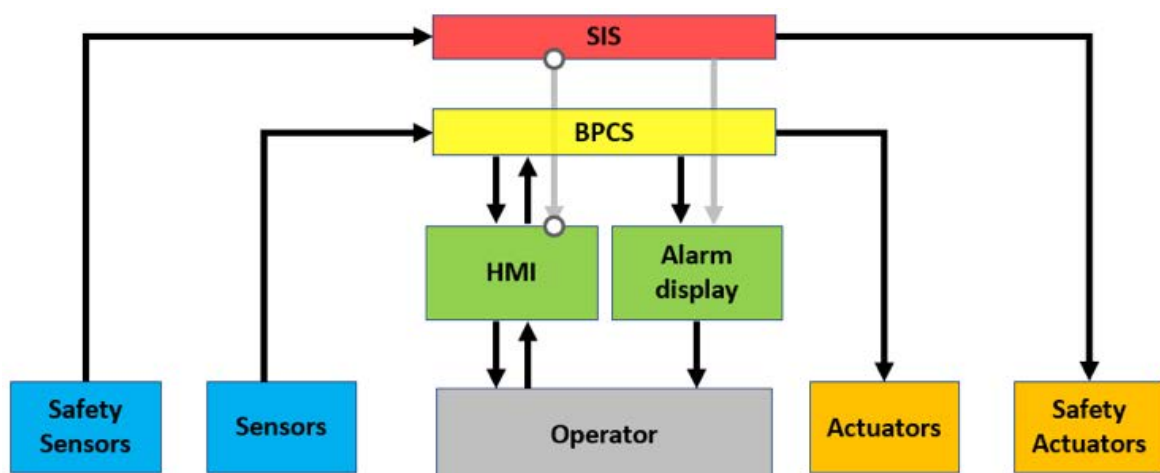


Figure 1 Relationship between Basic Process Control System (BPCS), Safety Instrumented System (SIS) and alarm display

1.3 Why is alarm design important?

We have known for some time that poorly designed alarm systems can contribute to accidents – see Appendix 1 of this guide for examples.

The problem is very rarely a lack of alarms or technical failures of the system’s hardware or software. The main problems are related to human factors - the alarm system does not give operators the information they need in a useful format to allow them to intervene appropriately. Examples of these problems include:

- Unnecessary alarms that do not require an operator response and nuisance alarms during normal operation increase operator workload, reducing their ability to monitor what is happening. They condition operators to assume alarms are not important meaning that situations requiring a response are missed or overlooked

- Floods of alarms during process upsets and planned status changes (start-up and shutdown) overload operators with data so that they cannot diagnose the cause of the problem meaning they are not able to implement an effective response
- Poor alarm descriptions means that operators do not understand what is happening or how they should respond
- Inconsistent prioritisation of alarms means that operators do not know which alarms to respond to first, they may waste time on less critical situations, allowing more critical situations to continue
- Response to alarms is not defined leading to delays whilst operators devise a response in the heat of the moment
- Over-reliance on alarms and failure to adopt inherent safety, making systems prone to failures including human error
- Failure to take into account human strengths and limitations in alarm system design and management leading to acute and chronic stress, which increases the likelihood of human error and leads to physical and mental health issues.

This is important because the frequent occurrence of abnormal situations increases the likelihood of process safety incidents, and serious incidents are often preceded by abnormal situations ^[8].

1.4 Key design principles

The primary function of an alarm system can be defined as:

The purpose of an alarm system is to direct the operator's attention towards process conditions requiring a timely response.

Thus an alarm system is saying to the operator "do something about this urgently", "look at this soon", "don't forget this problem", etc. Thus, it should help the operator to manage tasks and resources, and should focus attention on the most important issues.

To achieve the above:

Each alarm should attract, inform and guide.

Thus the operator should be immediately aware that an alarm has occurred and presented with information that allows them to determine what the problem is and help them to decide how they should respond.

Operators are usually attracted by an audible and/or flashing visible indication. An alarm message informs them about the alarm, either in an alarm banner or list on a screen or by labels on an annunciator panel. Guidance about which alarm to respond to first (if more than one occurs at the same time) is achieved by prioritising alarms and indicating how to respond.

Alarms only direct the operator's attention to a potential issue. The overall HMI is used to collect and display information about the cause of the problem and to provide feedback to the operator about the success of their actions. Procedures defining how to respond, supported by training and experience allow operators to make sense of what is happening and optimize their response. For an alarm system to be effective in supporting the operator's response, every alarm presented to the operator should be a help rather than a hindrance. The objective should be to avoid the operator wasting time on deciding whether the alarm is important and ensure that the operator

does not adopt a mindset that the alarms can be ignored. There is experimental evidence^[9] which shows that there is a 'cry wolf' effect and operators do adapt their response according to the probability of the alarm being useful.

Thus:

Every alarm presented to the operator should be useful and relevant to the operator.

An alarm occurrence that does not require a response from the operator, or the operator is unable to respond to, is a distraction to them. As a minimum it is an annoyance that can cause frustration and may lead them to assume that alarms are of limited value. In some circumstances the distraction caused by dealing with an unnecessary or nuisance alarm can mean a genuine problem is missed.

One way in which the designer can ensure that every alarm is useful is to require that:

Every alarm should have a defined response.

Generally, the response to an alarm should be a process action (e.g. altering a control set point, changing over to a standby pump). The operator receiving the alarm may not perform the action themselves and so their response is to instruct someone else to act (e.g. control room operator uses their radio to instruct a field operator to take action).

To be worthy of an alarm the condition requires a timely response. Actions such as asking a fitter to repair a piece of failed equipment or the operator being informed that a SIS has activated and initiated a change to a safe status are unlikely to satisfy the definition of an alarm. In these cases an 'Alert' may be more appropriate (see Section 2.3) and in many cases the operator should already know about the issue based on data from other sources (e.g. information displayed on an HMI graphic).

The key point is that every alarm (or combination of alarms) should have some response which should have been clearly defined by the designer of that alarm. If a response cannot be defined, then the signal should not be an alarm.

If a response is defined for every alarm during the design process, this information provides an excellent starting point to produce alarm response and training material.

The defined alarm response should be one of the main considerations during any alarm review or rationalisation study. If none has been defined it should be the first thing to be agreed. If one exists it should be reviewed to confirm it is correct and the nature of the response satisfies the definition of an alarm.

Given that the operator is expected to respond to every alarm, it follows that:

An alarm's activation point should give the operator adequate time to carry out the defined response.

This requires that:

- The alarm should occur early enough to allow the operator to correct the fault, taking into account the sub-tasks that need to be completed (detect, diagnose, plan and act).
- The alarm rate should not exceed that which the operator is capable of handling.

Some of the characteristics that an alarm should have (using the 'SMART' acronym) are summarised in Table 1.

Characteristics of a good alarm	
Specific	Unique and not duplicating another alarm
Measurable	Prioritised so that the operator's attention is focussed on the most important issues
Achievable	Understandable, diagnostic and advisory so that the operator knows what has happened, its cause and how to respond
Relevant	Not spurious and indicating an issue that requires a timely response
Time-bound	Operator has enough time to respond but time available is not excessive

Table 1 Characteristics of a good alarm

The primary alarm system function is providing notification to the operator. There may be secondary functions (e.g. providing an alarm log which can be used for optimizing process operation, for analysis of incidents), but these should be set up in a way that does not affect the primary function.

1.5 Practical and organizational issues

One of the key principles of this guidance is that an alarm philosophy (or equivalent) is required to ensure a consistent and effective approach is applied. However, that cannot be developed without some resources.

1.5.1 General approach – PDCA

The classic Plan – Do – Check – Act (PDCA) provides a useful framework for alarm management:

- Plan – Define the philosophy and assign resources for alarm management.
- Do – Implement the philosophy through alarm system design and operational controls.
- Check – Review performance using Key Performance Indicators (KPI), incident reports etc.
- Act – Identify changes required to the philosophy and/or its implementation to address negative aspects of the system and sustain the positive ones.

Figure 2 shows how PDCA can be applied to alarm management.

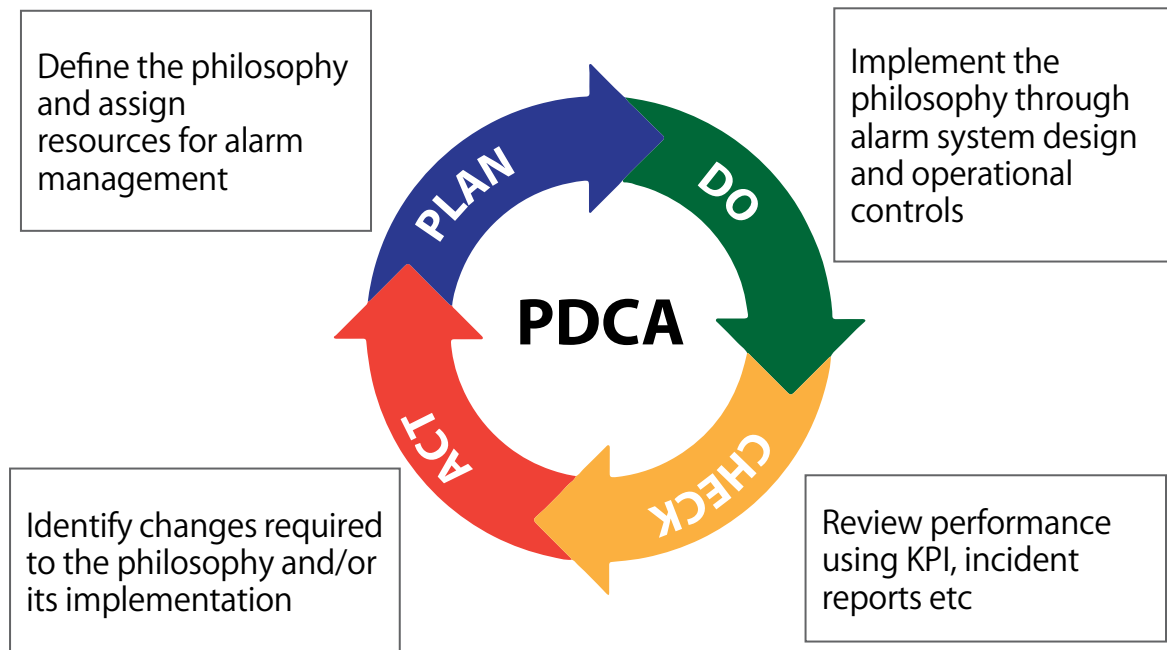


Figure 2 PDCA applied to alarm management

1.5.2 Resources required

The hardware and software that makes up the alarm system will inevitably have a cost. However, achieving an effective alarm system will require a significant human resource. In the first instance this is to generate the alarm philosophy, which then has to be implemented through design. Once operational there is a continuous requirement for maintenance of the system hardware, performance monitoring and management of change. This all requires continual management commitment.

More detail about implementing an alarm management system is provided in Section 4.

1.5.3 Alarm philosophy

The alarm philosophy document is a high level site or business group document that provides the framework for a consistent approach to the specification, design and management of all site alarms irrespective of their origin of design.

More detail about the contents of the philosophy is provided in Section 4.4 and an example is provided in Appendix 4.

1.5.4 Project lifecycle

Whilst this guide is applicable to existing alarm systems, it is often easier to understand what would be done with a brand new system implemented as a standalone project or part of a wider ranging one (e.g. new plant).

All projects follow a lifecycle, which will usually be divided into phases. Organizations use different titles to describe these phases, but the following are typical:

- Concept/Select – Alarm philosophy is developed and a plan is formed to implement through the later stages of the project. It is important to recognize that this is the best opportunity to identify other methods of controlling risk so that alarms are not relied upon.
- Define – Alarm database is generated, based on the philosophy, with reference to safety studies, operational experience etc. Operator response and justification for each alarm are recorded.
- Execute – Detailed alarm assessment or rationalisation takes place to develop an alarm database for implementation. Alarms are installed on the system, tested and commissioned. Alarm responses are handed over to the operations team for immediate and future training and assessment.
- Operate – Alarm management applied as part of the continuous process based on the PDCA cycle.

Figure 3 summarises how alarm management can be implemented during a project.

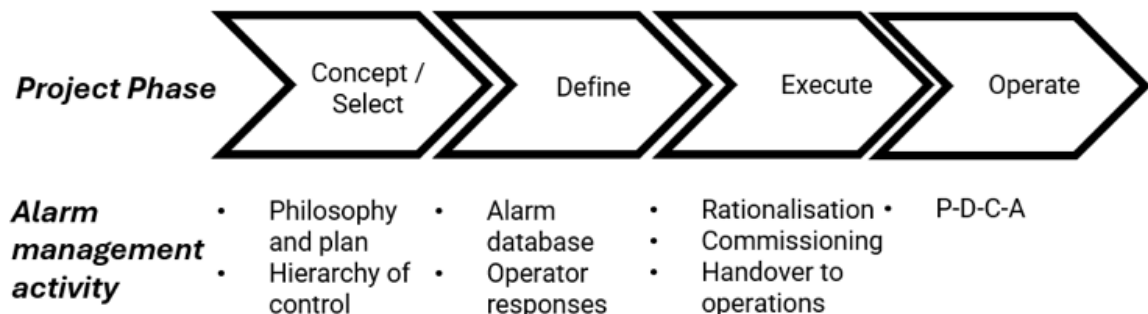


Figure 3 Alarm management activities at project stages

1.5.5 Alarm system lifecycle (IEC 62682)

IEC 62682 ^[5] includes a lifecycle that covers the alarm system from its specification through design to operation and finally to its eventual decommissioning, see Figure 4.

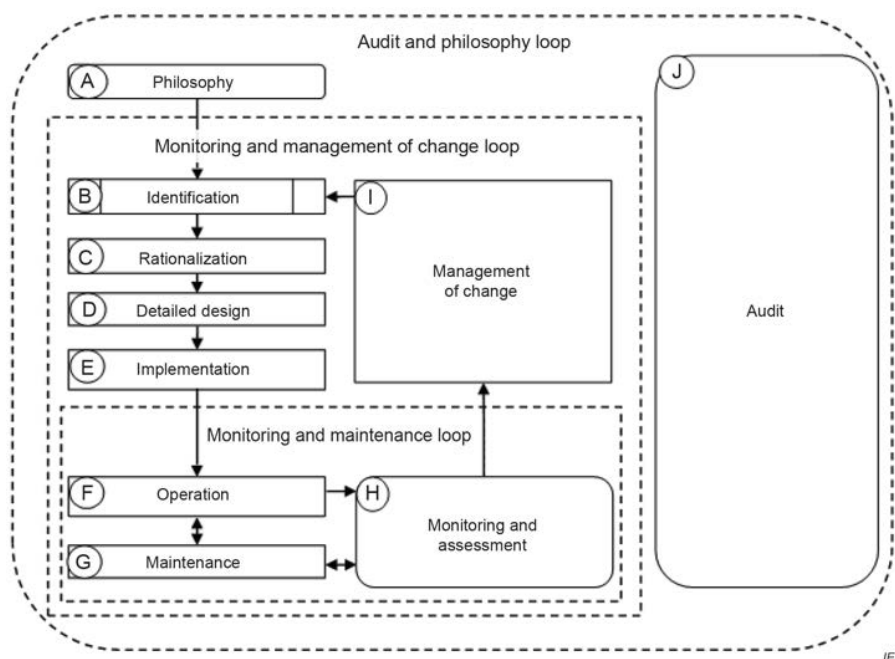


Figure 4 Lifecycle model (taken from IEC 62682)

Details of each lifecycle stage are described within the standard ^[5]. Table 2 below summarizes these, along with the inputs and outputs, mapping them to the content of this edition of EEMUA 191.

IEC 62682					EEMUA 191
Lifecycle stage		Activities	Inputs	Outputs	
A	Philosophy	Documenting objectives, guidelines & work processes for alarm management, and ASRS.	Objectives and standards, audit recommendations.	Alarm philosophy and Alarm System Requirements Specification (ASRS).	Chapters 1, 2, 4
B	Identification	Determining potential alarms	Process Hazard Analysis (PHA) report, Piping and Instrument Diagrams (P&ID), operating procedures.	List of potential alarms	Chapters 2 & 3
C	Rationalisation	Rationalisation, classification, prioritisation, and documentation.	Alarm philosophy, and list of potential alarms.	Master alarm database and alarm design requirements.	Chapters 2, 4 & 6
D	Detailed Design	Basic alarm design, HMI design, and advanced alarming design.	Master alarm database and alarm design requirements.	Completed alarm design.	Chapters 3 & 5
E	Implementation	Installing alarms, implementation testing, and implementation training.	Completed alarm design, master alarm database, and ASRS.	Operational alarms and alarm response procedures.	Chapters 3, 5 & 8
F	Operation	Operator responds to alarms and refresher training.	Operational alarms and alarm response procedures.	Alarm data	Chapter 4, 5 & 7
G	Maintenance	Maintenance repair and replacement, and periodic testing.	Alarm monitoring reports and alarm philosophy.	Alarm data	Chapter 6
H	Monitoring & assessment	Monitoring alarm data and report performance.	Alarm data and alarm philosophy.	Alarm monitoring reports and proposed changes.	Chapter 3
I	Management of change	Process to authorize additions, modifications, and deletions of alarms.	Alarm philosophy and proposed changes.	Authorized alarm changes.	Chapter 4 & 8
J	Audit	Periodic audit of alarm management processes.	Standards, alarm philosophy, and audit protocol.	Recommendations for improvement.	Chapter 7

Table 2 Alarm management lifecycle stages (IEC 62682 vs EEMUA 191)

1.5.6 Alarm database

A site wide database should be used to ensure a consistent approach to alarm management and provide a history trail for changes made. It may be handled via the IO-database if convenient. It can also be used by operators to view the purpose of the alarm and the response that the operator is expected to carry out, should it activate. The database should include every alarm that the operator may receive from every system (i.e. not just alarms handled by the main BPCS).

It is important to record information about each alarm so that if and when conditions change, future reviews can take into account the original objectives and justification. Information that is used to categorize and prioritise each alarm should also be recorded as part of the record for each alarm.

Setting up a database involves a data gathering exercise that will collect together as much information about each alarm as available. For small systems, with very few alarms, spreadsheets have been used. For larger systems proprietary database software may be considered.

The database will typically record:

- Configuration information:
 - Tag information: such as tag reference, description, loop number, P&ID reference.
 - Alarm details: alarm limits, enable/disable status, alarm message text, audible.
 - Measurement details: instrument range, engineering units, plant area, signal type, set point.
 - Alarm parameters: priority setting, hysteresis value (including deviation alarms), timer delays on/off.
- Reason for alarm and alarm settings:
 - Modes of operation for which the alarm is valid.
 - Consequence if alarm is not responded to (e.g. activation of an automated risk control).
 - The hazard being avoided by the alarm, and other risk controls.
 - Time available to respond.
- Expected alarm response.
- Use of logical processing (conditional alarms, advances alarm processing etc.).
- Cross referencing to similar alarms and groups.
- Review information – populated as part of review of individual alarms.
- Recommendations – details of changes to alarm settings and priorities (allows comparison between original and proposed changes).
- Implementation changes – register of all changes to the alarm system.
- Operator response information.

1.5.7 Operator response to alarms

By definition an alarm requires an operator response. Therefore, one of the first questions when reviewing a specific alarm is how should the operator respond? If there is no action to perform then an alarm cannot be justified (it could be an alert or prompt – see Section 2.3).

Defined and documented alarm responses can support the operator when the alarm occurs during operations. They may be presented on the screen or provided in a written alarm response guide that is readily available to the operator when they need it.

The following information should form part of the review of each alarm:

- What the operator should do when the alarm is activated.
- What could have caused the alarm, thus aiding in the diagnostic of the process condition.
- What would be the consequence if no action were taken.

Many alarms may have a very similar response and may be covered by a general definition. However, some, including HMA, require a more detailed response definition (see Section 2.5).

1.5.8 Fostering a culture of improvement

A key aspect to achieving improvement in alarm systems, as in many other things, is for the organization to propagate a culture which encourages improvement. This requires a real commitment by the senior management.

The objective of improving the alarm systems needs to be made clear to all staff involved, and they need to be helped and encouraged to develop a coherent and co-ordinated strategy for achieving this.

A common understanding of the importance of alarms and what constitutes a good system is essential. The key focus should be on supporting the operator to perform their job effectively. If this is not understood it is highly likely that alarms will not be given the importance and resources required. Clear, concise and consistent communication can help foster the culture. On the other hand alarms are usually part of a complex system and continuing to do what has always been done is unlikely to result in good systems. Failure to instigate change because it is difficult is not justification for keeping the status quo.

The results of the survey carried out for the HSE ^[4] indicated that there was a positive correlation between management commitment to improvement and achievement of good results.

1.6 Using this guide

This publication provides guidance. It is not a specification. It is intended to assist you when designing a new alarm system, or evaluating or modifying an existing system. You will need to determine whether other documents (e.g. regulations, standards or in-house guidance) apply to your project and make sure they are complied with. However, this guidance gives an indication of what would be considered good practice in a range of circumstances and sets out an expectation that given the circumstances, appropriate choices will be made to achieve compliance.

The main body of this document (Sections 2 to 8) describes the main guidance for alarm management. The appendices provide resources that you may find useful in your project. In particular:

- Appendix 1 The costs of poor performance. Summary of incidents and studies highlighting the contribution made by alarms to safety.
- Appendix 2 Human Factors Integration Plan (HFIP). Guides you through a project lifecycle, identifying the types of activities to be completed at each key stage. A HFIP should be generated as soon as possible for every new build and modification project, and updated throughout.
- Appendix 3 Prioritisation methods. Examples that you can use and adapt.
- Appendix 4 Alarm Philosophy. Template for generating your own document.
- Appendix 5 Alarm rationalisation procedure. Template for generating your own procedure.

- Appendix 6 Usefulness questionnaire.
- Appendix 7 Operator questionnaire.
- Appendix 8 Alarm review checklists. Selection of checklists you may find useful to support alarm management.
- Appendix 9 Example alarm suppression hazard study.
- Appendix 10 Specification checklist – small system.
- Appendix 11 Specification checklist – large system.
- Appendix 12 Intelligent fault detection.
- Appendix 13 Glossary.
- Appendix 14 References.
- Appendix 15 Bibliography.

1.7 Supporting documents

In addition to the guidance provided in this document people involved in alarm management should be aware of other sources of relevant information. These include

- IEC 62682 Management of alarms systems for the process industries ^[5]
- ISA–18.2–2016 - Management of Alarm Systems for the Process Industries ^[10]

Several Technical Reports have been published by the ISA18 committee, covering topics including basic alarm design (TR3), alarm system monitoring (TR5), enhanced and advanced alarm methods (TR4), and alarm systems for batch and discrete processes (TR6).

2 Principles of alarm system design

This Section introduces the high level principles for designing an alarm system. It covers:

- *Design goals and objectives to maximise operability.*
- *Including alarms in a wider system context.*
- *The role of alerts, events and prompts (alternatives to alarms).*
- *Grouping alarms into classes.*
- *Identifying alarms that are of particularly critical and need to be highly managed.*
- *The role of alarms in managing risks.*

Key principles include:

- ***Understanding human capabilities and limitations is essential if alarms are going to be useful rather than become a hindrance.***
- ***Whatever its source, every alarm should be justified, properly engineered and be consistent with the overall alarm philosophy and risk assessment.***
- ***HMAs create a higher reliance on operator response and their contribution to risk reduction may go beyond simply reducing a demand on engineered layers of protection.***
- ***The alarm philosophy should define the use of alerts, events, prompts, alarms and highly managed alarms.***

One of the most important messages in all of this is that alarms are provided for operators and to be effective the system has to make sure that every alarm received by the operator requires a response. In many cases we have created a self-defeating situation where we overload the operator with alarms so that they cannot respond, and we then address this weakness by implementing additional alarms just in case they do not respond to the first.

This edition of the guide clarifies how alarms are used in conjunction with other similar items including Alerts, Prompts, Events and Highly Managed Alarms (HMA). The combined use of these may be influenced by national legislation and by existing practices within the industry sector. HMA due to safety or the environment are critical risk control measures and will be of concern to regulators. Alerts may be of less interest to operators but useful to others (e.g. maintenance personnel).

2.1 Design goals and objectives

It can be tempting to define an alarm system by its technical capabilities and reliability. However, its purpose is to support operators and so the goals and objectives should focus on the users' requirements.

2.1.1 Human / user centred design

Human centred design is a philosophy that makes the needs, wants, and limitations of the end user the priority focus for design. This is critical for alarm systems that are intended to support operators in their critical role.

Understanding human capabilities and limitations is essential if alarms are going to be useful rather than become a hinderance.

The alarm system is one part of the operator interface, and the whole interface should be designed following ergonomics and human factors good practices to ensure it is usable by the operator. To help achieve this designers should follow a human / user centred philosophy that may include the following elements:

- Task analysis to identify tasks the operator performs and the information and controls required to carry them out.
- Development of design standards for the operator interface covering alarm presentation and graphical display of information.
- Design reviews carried out by a working party comprising designers, operators and ergonomics / human factors specialists that reviews the operator interface design through the various stages of design, construction and commissioning.
- Operator involvement in the testing and evaluation of prototype designs.
- Early ergonomics evaluation of prototype designs by the purchaser.
- Pre-commissioning operator training in use of the operator interface.
- Formal demonstration of the usability of the commissioned operator interface.
- On-going monitoring and improvement of performance.

2.1.2 The role of the operator

The role of an operator for an industrial process encompasses a range of activities including process operation, optimization of production, fault identification, co-ordination of maintenance, etc. Their tasks depend on process state (e.g. normal operation, upset operation, emergency shutdown, planned shutdown, start up, or operating mode change).

Many of the complex processes covered by this Guide do not operate steadily but are subject to constant disturbances (e.g. changes in fuel quality, changes in weather, equipment malfunction, batch operations). Control actions are taken continuously (automatically or manually) to mitigate these disturbances to keep the process close to target operating conditions. The operator's primary role is to monitor and optimize operation by changing control set points, putting equipment under manual control, etc.

If there are significant disturbances (e.g. mechanical failure of equipment, adverse weather, feedstock change), control (manual or automatic) may be lost and the process may enter an 'upset' state. Manual intervention from the operator provides the best opportunity to recover from this situation and this is where alarms should be provided to assist.

If intervention does not take place or is ineffective the process may continue to stray towards a hazardous state where damage, pollution or danger is likely to occur. At this point the safest action is to force the process into a safe or shutdown state. This may be automatic via the BPCS or a SIS, or manually.

The role of the operator during abnormal situations can be very complex. As shown in Figure 5, the operator response may involve several quite different types of task. Furthermore, the operator response required to one abnormal situation may be quite different from that required to an apparently similar situation at another time. Alarms assist operators to detect and diagnose abnormal situations, and to confirm their actions to deal with the situation are successful. However, good HMI design should ensure that they are aware of situations before an alarm is activated.

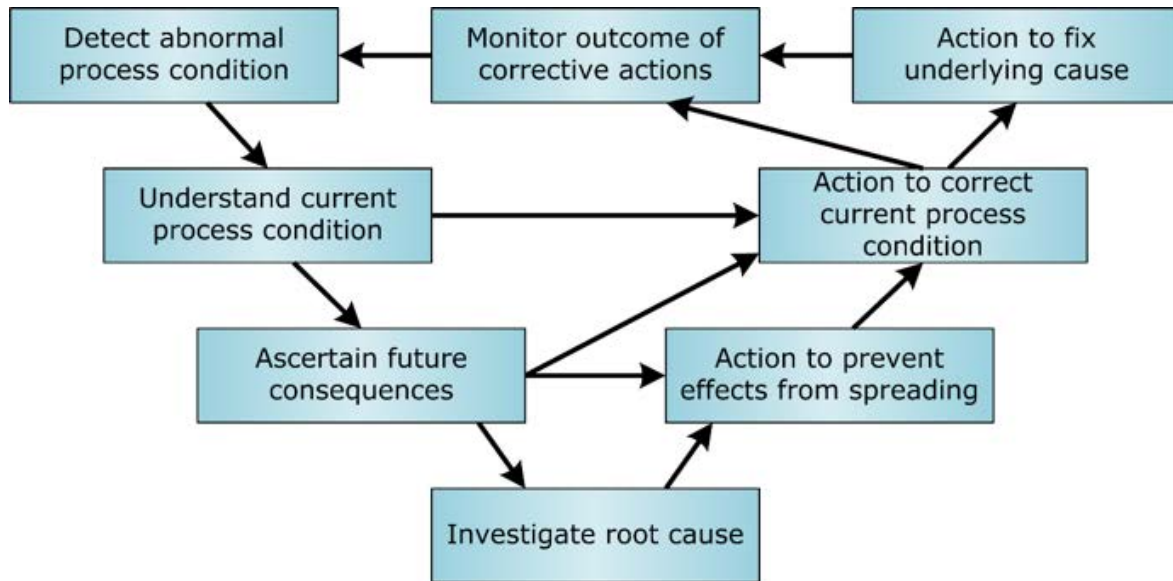


Figure 5 Operator response to an abnormal situation

The operator will often have a lot of data to handle and multiple sub-tasks to complete whilst working under time pressure and stress. It is clear that whilst alarms are a useful tool to help the operator, the need for more general task management during an abnormal situation should be addressed. One key requirement is recognizing when control of a situation is lost and it has to be managed as an emergency or crisis. Operators may be overwhelmed by the situation and fail to recognize its seriousness or signs of escalation. In some cases they may be too proud or concerned about their reputation to ask for assistance.

2.1.3 The type of process

The type of process being controlled will influence the way in which the operators have to react and how alarms are used. Examples include:

- Continuous process
- Batch process
- Hybrid process (this is a mixture of the first two processes)
- Geographically distributed processes.

For continuous processes it is usually quite easy to identify normal ranges for critical parameters. Relatively small deviations can indicate a problem and alarms can quite easily be set to provide early indications to operators.

Alarms for batch processes should be configured so that they are appropriate for all stages of the process. Operating conditions in batch processes vary much more and so it can be more difficult to provide alarms that indicate a problem at one stage of the batch without causing an unnecessary alarm at another stage. Whilst safety limits should be constant (i.e. the design temperature or pressure of a vessel is independent of the operation) the fact that the process is changing towards that limit may be the normal part of the batch and not an indication of a problem.

As an example, consider a process vessel. In a continuous process the level in the vessel may vary between 40% and 60%. Any deviation from this is an indication of a problem and alarms can be set quite close to these values. For a batch process the vessel may cycle between full and empty on a regular basis. In this case it is particularly important to specify the maximum operating level, which would have to be below the high level alarm set point. It is then important to ensure the operator has enough time to respond to the alarm and stop the vessel being over filled. See Figure 6 for an illustration.

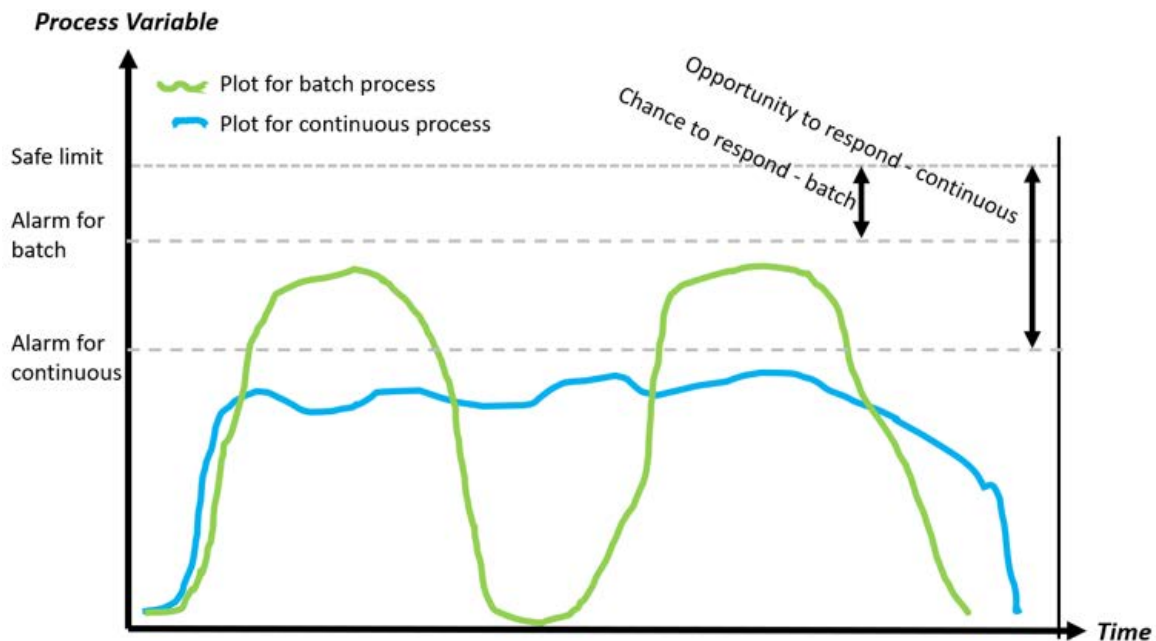


Figure 6 Illustration of how alarm settings can vary for batch and continuous processes

Continuous processes do not operate all of the time. They will be shut down from time to time for maintenance etc. and have to be restarted. Setting alarms for these transitions can be particularly difficult, with the issues discussed above for batch processes being applicable. Decisions need to be made during design about how this will be handled. Whilst in the ideal world the alarms would fulfil requirements for all modes of operation including start-up and shutdown, in the real world it may be acceptable to tolerate a lower standard provided the risks of overloading the operator are recognized, assessed and controlled in some way. Alternatively advanced technology may provide some solutions for adjusting alarms for different modes of operation but can introduce its own problems, which should also be assessed and controlled.

Alarms for geographically distributed processes can cause difficulties for operators who will be remote from the sites and plants they operate. During the design stage each site is often viewed in isolation and the requirements of the operator who is responsible for multiple sites are not considered. Lack of data and time lag due to bandwidth restrictions can mean that data is received late or interventions cannot be made quickly enough. The design should take full account of how operators will handle geographically distributed plants and every site has to be designed to account for the system and operator capabilities and limitations. Many sites will be normally unoccupied or only occupied at certain times of the day. Calling someone to attend introduces additional delays. Events that occur outside of the working day create significant upheaval to the individual (they may be in bed asleep when the event occurs) and can cause knock-on effects the

following day if they are not available to work due to them taking compensatory rest to minimise risks of fatigue.

2.1.4 Designing for operability

Even if each alarm that is generated is operationally useful in its own right it will not be effective if a scenario creates multiple alarms and leads to operator overload.

If an operator is to be effective, it is essential that they can cope with all the tasks demanded of them under both normal and upset conditions. This requires a realistic view of how long it takes for an operator to respond to an alarm and what proportion of the time operators are required to be in a responsive mode.

Observing the physical actions taken by a control room operator responding to an alarm may suggest that it takes less than a minute to deal with the situation. They may press a button to acknowledge the alarm, read the description on the alarm list and click on a graphic to make a process change. This is a highly simplistic assessment of what response to an alarm really involves. To properly diagnose the situation they will need to access multiple pieces of data, consider their options and take action. They then need to wait for their action to be effective and consider whether they need to do more. To achieve all of this on a properly configured system where every alarm relates to a potentially serious event and every occurrence requires a timely response inside 5 minutes would be a challenge, and often impossible due the time lag between an action being made and the process changing. Taking this as an average time to respond, six alarms per hour would occupy the operator for 50% of their time. Do we really want our operators to spend so much time responding and if they are, can we really expect them to ever act proactively? It is noted that operators appear to handle alarms at a greater rate than this, but due to poor system design a lot of the alarms they receive do not require an immediate response.

If an operator is continuously having to respond to alarms they will not have the time or motivation to act proactively.

People may say that evidence shows that operators can handle a great number of alarms without serious problems. This is really a reflection of current poor performance of many alarm systems that mean most alarms do not actually require a response. A key aim is to eliminate these unnecessary alarms so that every alarm does require an effective response.

Alarm overload represents a significant threat to operator effectiveness, so strenuous efforts should be taken to avoid it. This requires all alarms to be justified and properly configured during design. Once a process becomes operational, performance should be audited, overload incidents should be identified and steps should be taken to minimise their frequency.

Overloads are typically due to a small number of spurious or badly designed alarms (often known as 'bad actors'). A review programme should be set up to identify these and to re-engineer them. However, since the alarms that cause overloads tend to vary from incident to incident, the review will ultimately have to cover many different alarms. Techniques to re-engineer alarms range from simple re-tuning through to complex suppression.

2.2 Alarm system design

The discussion about human centred design above illustrates that alarm system design should focus on the operators and their capabilities and limitations; rather than on the process being controlled or the hardware and software provided by the alarm system. Alarms are only one of the items used by the operator to perform their role.

Operators often view alarms as a ‘necessary evil’ rather than something that helps them do their job.

2.2.1 Hierarchy of risk control

Design of any plant should always consider how its objectives can be achieved and balance the risks that may arise. The hierarchy of risk control is recognized as an effective way of managing risks and highlights that alarms are a relatively unreliable solution. Plant design should always aim to apply risk controls as follows:

- Inherent safety – eliminate or minimise hazards so that there is no chance of a hazard occurring. Alarms are not required for inherently safe systems.
- Passive engineering – design and build plant to withstand the maximum possible range of operation conditions. Process excursions will not lead to loss of containment and alarms are not required (provided the plant is properly maintained).
- Active engineering – install devices that will automatically transfer a process to a safe state when activated by an excursion. Examples include SIS and pressure relief valves that operate without any human intervention. Alarms are not part of their operation but have a key role in reducing demand on the safety systems because the operator can intervene before the activation point is reached.
- Administrative controls – competent people working to defined procedures avoid problems and know how to respond if things go wrong, which may be indicated by an alarm.
- Mitigation – arrangements to reduce the consequences of an event. Process alarms are ineffective at this stage because the hazard has already occurred but protective system alarm (e.g. fire and gas detection) may have a role in triggering a response that mitigates the risk (e.g. evacuate the area, active firefighting).

Alarms are low on the hierarchy of risk controls.

2.2.2 Alarm system hardware and software

Some of the components that make up the alarm system will have other uses or be provided almost by default. In particular the sensors that measure conditions, the transmission mechanism (cable or wireless) and the devices that receive the data are likely to be part of the BPCS and/or SIS.

Hardware and software used to communicate alarms to the operator are of most interest and need to be optimized through design. Features to consider when selecting a new system or evaluating and existing system include:

- Number of alarms that can be handled.
- Time taken to process data and activate an alarm.
- Methods of communicating/displaying alarms.
- Options for classifying and prioritising alarms.

- Capability for logical processing of alarms.
- Mechanism for applying and managing suppression, shelving, overrides and inhibits.
- Options for handling non-alarms (e.g. alerts, prompts and events) – see Section 2.3.
- Capability to handle Highly Managed Alarms (HMA) – see Section 2.5.
- Data logging capabilities for problem diagnosis by the operator and monitoring the alarm system performance.
- Security arrangements.

The development of technology over recent decades means that the technical capability of the hardware is less of a concern. The most important consideration when selecting an alarm system is the way alarms are presented to operators and how it fits into the wider HMI.

Table 3 provides a guide for determining the best way of presenting alarms to the operators based on the number of alarms to be configured.

Number of installed alarms per operator	Approach to design and management
Under 100	Simple technology (e.g. annunciators) likely to be acceptable. Operational problems may often be solved by individually tailored solutions, e.g. special electronics. One significant risk is that the operator and the alarm systems may have a safety role that is not fully appreciated. In addition, poor alarm system performance may not be recognized and given management priority.
100-300	If annunciator based alarms are used on their own they need to be very carefully designed to ensure good usability. Mixed annunciator and computer-based alarm displays can be effective. If purely computer-based displays are used, then the alarm system may not have to be sophisticated, but does need good tools for dealing with basic problems, e.g. repeating alarms, alarms from out-of-service plant. Effort should be put into identifying key alarms and ensuring that they are clearly displayed. Management commitment needs to be made to solve operational problems, but much may be achievable with relatively little effort.
301-1000	Sophisticated computer-based alarm handling with powerful tools for logical processing and suppression of alarms is very desirable, possibly in combination with individual displays of critical alarms. Significant effort has to be expended on ensuring a consistent and considered approach to the design of individual alarms. The optimization of operational performance is likely to require involvement of a team of engineering and operational staff for several months.
Over 1000	A major alarm system, which will require significant investment throughout its life cycle and which needs to be developed and maintained to the best practices available within industry if it is to work well.

Table 3 How system size affects design and management

2.2.3 Designing individual alarms

Every alarm configured on a system needs to go through a design process. This should include confirming it is justified and can be configured to support the operator. The specific aspects to design for each alarm include:

- The condition that will activate the alarm. The simplest is normally a static set point but activation may be dynamic (e.g. rate of change, discrepancy between sensors).
- Alarm description.
- Alarm category.
- Alarm priority.
- Logical processing.

Once designed it should be checked to confirm that the alarm will actually support the operator. A particular concern is whether the alarm configured will actually give the operator enough time to respond.

2.2.4 When is it appropriate to provide an alarm?

A number of factors may be considered when deciding if an alarm is required, including:

- Process safety
- Environmental
- Asset protection
- Production
- Product quality or safety
- Personal safety
- Alarm system availability
- Alarm system communication, which can be regarded as a subset of wider system alarms.

Alarms may be proposed as a requirement during a safety study (e.g. Hazard and Operability (HAZOP), Layers of Protection Analysis (LOPA)). However, these tend to look at issues in relative isolation and do not take into account wider considerations. A separate review and rationalisation should take place to confirm the proposed alarms are appropriate with feedback to the original study if this is not the case.

It is common for alarms to be proposed based on custom and practice ('we always have this alarm'), general instructions from interested parties (e.g. insurers, regulators or head office) or incident investigations. In other cases alarms are specified because it is much easier (and cheaper) than applying the hierarchy of risk controls (e.g. inherent safety, passive engineering, SIS). These sources lead to many poorly justified alarms being proposed.

Every proposed alarm should be properly scrutinised to ensure it satisfies the defined requirements. Thus:

Whatever its source, every alarm should be justified, properly engineered and be consistent with the overall alarm philosophy and risk assessment.

The strongest justification will always be related to major accidents with potential to cause harm to people or the environment. Whenever alarms are considered for other types of risk the

potential benefit should be balanced against the negative impact of potential operator overload and distraction. For example, an alarm informing the operator about a potential production interruption without any significant safety or environmental implications would only be justified if the interruption could have a fundamental effect on the business's survival.

2.3 Similar, non-alarm functions

A consistent theme is that alarm systems are only effective when they support the operator and do not cause distraction or overload. Many of the problems encountered occur because unnecessary alarms are provided (i.e. there is no timely operator response required). A root cause of this is that a very wide range of potential alarms can appear to be justified when viewed in isolation.

Failure to keep control of alarm proliferation will quickly lead to distraction and overload for the operator.

Having alternative ways of making data available to operators and others can be a useful way of reducing these problems.

Alerts, prompts and events can be useful alternatives to alarms, helping the system to meet its objective of supporting the operator.

2.3.1 Alerts

Alarms require a timely response. There can be a lot of situations that people may find useful to know about but do not have to respond to in a timely way. There is a temptation to create alarms to inform operators about these situations. An alert is an alternative option.

An alert is used to attract the attention of the operator to situations that may require assessment or action when time allows. They can also be used to inform other people via reports if there is suitable capability (e.g. daily report to maintenance about faults in the last 24 hours).

An alert:

- Is not time critical.
- Is not used as a formal risk control.
- May be operator configurable.
- May be used to inform the operator that a particular noteworthy event has occurred, and
- Initiates a condition of heightened watchfulness or preparation for action.

The similarities between an alarm and an alert include:

- Occurs when a defined operating limit has been exceeded.
- Is shown on a display or some other notification device (e.g. a pager, text message, email, etc.), and
- The person receiving the alert responds accordingly.

Differences include:

- Every alarm occurrence **should always be acted upon immediately** by the operator, or as soon as practicable in accordance with the designated priority and time to respond.

- Alerts are always of lower priority than alarms and ignoring an alert does not normally place a demand on a safety system without first triggering an alarm.
- Many alerts may be configured on an ad-hoc basis by the operator and therefore do not require inclusion in a Management of Change (MOC) or maintenance system.
- When an alert occurs it does not signify that the process has moved outside of its operating envelope or that immediate action is required by the operator to prevent an abnormal situation.
- Alerts can and often should be suppressed in abnormal situations, and
- Alert indications should not be audible.

Alerts can help the operator to run the process more efficiently. During upsets, many alerts might be generated (so 'alert floods' can occur) – but, if alerts have been properly used, the operator knows that they can be ignored until all alarms have been dealt with. Since alerts are used where alarms may otherwise have been used, the size of alarm floods is reduced, and can then be much more manageable.

WARNING: THERE IS A POSSIBILITY OF CONFUSION WHEN DEALING WITH THE AVIATION INDUSTRY, WHICH DEFINES ALERTS AT VARIOUS LEVELS, SOME OF WHICH FALL WITHIN THE IEC DEFINITION OF ALARMS.

2.3.2 Events

An event is any change in process, plant or equipment condition. Examples include a pump starting or stopping, a valve opening or closing. Alarms and alerts are also events. However, it is important to note that most events should not create an alarm because a response from the operator is not required.

Modern systems record events, usually by default. The event record, often captured in a 'historian', creates a valuable data base for analysis after an incident. Because alarms will also be included as events, this database can be useful to put alarms in context with all events occurring at the same time (e.g. "the alarm occurred 5 seconds after the pump stopped").

In most cases events are not particularly interesting to an operator during normal operation (unlike alarms and alerts).

2.3.3 Prompts

A prompt is a request from the BPCS for the operator to perform an action that it cannot perform itself or that requires operator authority. It is normally not time critical and usually requires that the operator either checks the status of one or more items, or performs some manual actions.

Display of prompts should be separate from alarms and alerts and have a different mechanism for drawing the attention of the operator.

The differences between alarms, alerts and operator prompts are that:

- An **alarm** is an **unexpected** event that requires **timely operator action**.
- An **alert** is an **unexpected** event that does not require a response.
- A **prompt** is an **expected** event that may require operator action but is **not time critical**.

Prompts will often be used in batch processes to inform the operator that they need to do something to progress the batch (e.g. manually add a chemical to the reactor, visually check the agitator is turning). Similarly, they are used in automated sequences (e.g. compressor start-up) for continuous processes.

Figure 7 illustrates a decision process for deciding if an event should create an alarm, alert, or prompt, or only requires a record on the event log.

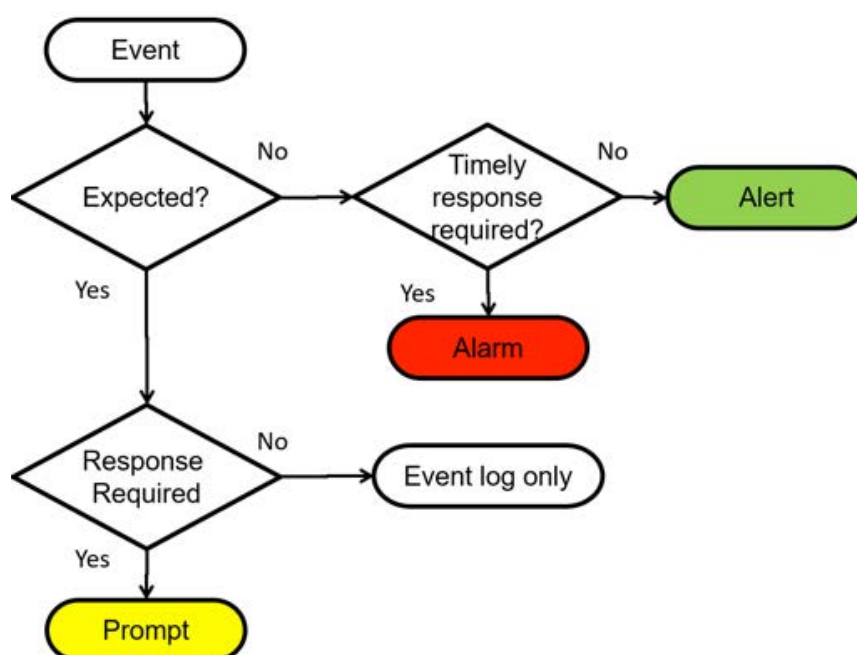


Figure 7 Identifying Alerts, Alarms and Prompts

2.3.4 Non-alarms

It is also useful to re-iterate what signals should not be alarms. They include:

- Signals without a defined operator response.
- Process variable or plant status changes that do not require operator attention.
- Warnings of events which are too fast for the operator to prevent.
- Events that are recorded but which the operator does not need to see.
- Signals which confirm successful operator actions.
- Signals which corroborate or duplicate another alarm (these signals may need to be logically suppressed).

Although these signals are not alarms, they may be recorded as events and may still need to be displayed to the operator as status indications on process graphics.

2.4 Alarm classification

IEC 62682 ^[5] requires that alarms are classified. This involves grouping alarms that have common sets of management requirements. Classes may be determined by the frequency and/or methods used for testing, operator training, monitoring or auditing. Alternatively they may be based on the way alarms are represented on the HMI, covered by management of change or shelved. This is different from alarm prioritisation (see Section 6.1.1 and Appendix 3)

Alarms that are identified as an independent layer of protection from safety studies are likely to require more stringent management and so may be assigned to a separate class (e.g. HMA). There may be a small number of other classes used, with up to four in total being considered appropriate.

Regulations may be the determining factor. For example, alarms associated with environmental monitoring may not be viewed as particularly critical from an operator perspective but may require frequent testing to satisfy permit conditions. Similar examples may be generated by an insurance company, equipment supplier (warranty conditions) or corporate head office (asset protection).

The Alarm Philosophy should identify alarm classes and the method of classifying alarms.

2.5 Highly Managed Alarm (HMA)

HMA is an important class of alarm. HMAs create a higher reliance on operator response to avoid an undesirable outcome (e.g. major accident, significant asset damage). Their contribution to risk reduction may go beyond simply reducing a demand on engineered layers of protection, sometimes because there is no engineered layer in place or those in place are not effective enough to achieve the risk reduction required. This means operator response may be the last line of defence.

HMAs create a higher reliance on operator response and their contribution to risk reduction may go beyond simply reducing a demand on engineered layers of protection.

2.5.1 Types of HMA

It is often useful to classify HMAs according to the party most interested in the associated risk. For example, regulators may be interested in safety or environmental risks. Company owners may want a similar level of scrutiny to be given to avoiding asset damage and customers may be concerned with product quality or service delivery. The following classifications may be used:

- HMA-S: Safety
- HMA-E: Environment
- HMA-A: Asset
- HMA-Q: Quality
- HMA-C: Customer

An additional type of alarm that may be considered as HMAs are those generated by protective systems including fire and gas detection, security systems (physical intruders or cyber-attacks), or environmental discharges. One concern is that these can add considerably to the number of HMAs in a system, although in practice they can usually be managed as groups of alarms. On the other hand it can be beneficial to treat them as HMAs even if they do not meet the exact definition (i.e. multiple gas detectors may automatically activate a process shutdown) because reliable operator response is still expected. There are two options:

1. Treat protective system alarms as a type of HMA (e.g. HMA-PS) and manage accordingly, or
2. Treat protective system alarms as a different type of alarm and generate separate arrangements to manage them.

HMAs for safety reasons (HMA-S) should be avoided through design wherever possible. The majority of alarms on most systems will not need to be highly managed.

2.5.2 Protective layer alarms

The term 'safety related alarm' has been used in previous editions of EEMUA 191 with a quantified explanation that an alarm should be defined as safety related if it is claimed as part of the facilities for reducing the risk from safety or environmental hazards by a factor of ten or more. IEC 62682^[5] currently uses the following definition: "Alarm that is classified as critical for the protection of human life or the environment." In this edition of EEMUA 191 the term used is 'HMA-Safety'.

If a quantified explanation is required to demonstrate the use of a Protective Layer Alarm the appropriate standards (e.g. IEC 61508^[11] and IEC 61511^[12]) should be referred to.

Figure 8 below highlights that the operator is a key component in an HMA if it is intended to provide a layer of protection.

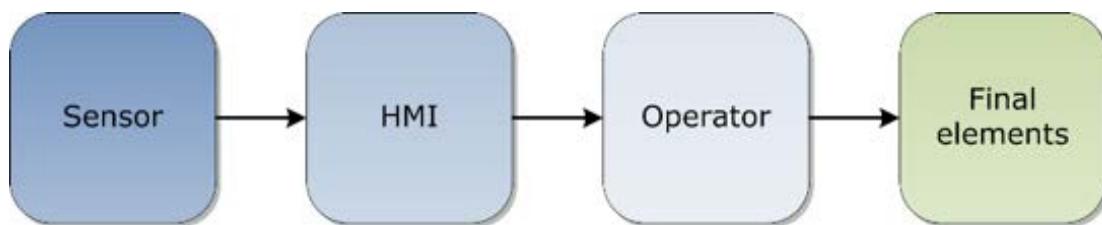


Figure 8 Components of an HMA

The overall reliability of a HMA depends on the reliability and integrity of all the equipment including the sensor, HMI (including alarm processing and communication) and final elements, all of which are relatively straightforward to assess. An alarm system can typically fail in one of two ways:

- i. A technical issue results in an alarm signal being generated.
- ii. An alarm signal is generated but the operator fails to respond in the expected manner.

Both types of failure need to be considered when considering the reliability of the alarm system. Human factors specialists should be employed to assess human reliability (and the factors which affect it).

For the operator to be considered suitably reliable they must, as a minimum:

- Be present to receive the alarm, recognize it is their responsibility and not be inclined to ignore it due to stress or other demands.
- Have immediate access to the information they need to diagnose the cause of the alarm.
- Know how to respond to the alarm.
- Have access to the controls needed to implement the required response, and
- Have adequate time to carry out the required response.

For this to occur the technical system must be configured so that^[13]:

- The alarm is clear and prioritized so that it is unlikely to be overlooked.
- The required action is simple to execute.

- There is sufficient time for the alarm to be detected, diagnosed, and acted upon effectively to prevent the hazard being realised, and
- The credibility of the alarm is not compromised by previous experience or operator perception (e.g., frequent spurious initiation).

Response to an HMA should be identified as a safety critical task for the operator and subject to formal task analysis involving people with suitable human factors competence.

Another way of identifying an alarm as highly managed is to recognize that in an ideal world an automated, engineered layer of protection would be provided but has not been. Reasons for this may include:

- The correct (safe) response is difficult to define and will be affected by a wider range of circumstances. An automated system would be very complicated and would introduce additional risk. A human operator will be better at evaluating the situation.
- Parts of an automated system will not be under the control of the facility and so cannot be relied upon (e.g. generic bulk chemical tanker that can travel to any port worldwide).
- An old system where retrofitting an engineered layer of protection is technically not possible or likely to introduce additional risks.

2.5.3 HMA management

IEC 62682 ^[5] highlights that HMAs require more administration and documentation than most 'normal' alarms. This may result in stricter control of alarm shelving, a more robust approach to dealing with an alarm being out-of-service or increased scrutiny for managing changes.

HMAs may be required to comply with environmental permits, process licence requirements or personal safety, and may be configured to prevent significant asset damage.

For all HMAs there should be:

- An alarm response procedure (more detailed than for most alarms).
- A competence standard for operators who may have to respond.
- A defined proof test method, and
- A defined test frequency.

The content and presentation of operator response definitions for HMAs can have a significant impact on the effectiveness of the operator's response. Response definitions should thus be written in a clear and easy-to-use way which supports the operator and promotes human reliability. They should be instructive, providing step-by-step instructions on actions to be taken by the operator. These should clearly identify variables to be monitored, checks to be made and actions to be taken. Checks should be laid out in a clear fashion, e.g. 'IF level X < 1% THEN ensure valve Y has tripped.'

There is a lot of guidance readily available for writing procedures that may apply to alarm response. Although dated, guidelines^{[14][15]} from the US Nuclear Regulatory Commission for writing and evaluating emergency operating procedures may be particularly relevant.

Task analysis techniques involving people with human factors competence may provide a useful basis for defining alarm response procedures ^{[16][17]}.

2.6 Summary of alarms, alerts, events and prompts

The flowchart in Figure 9 can be used to determine when it is appropriate to use an alarm or when alternatives (e.g. alerts, prompts and HMAs) should be used.

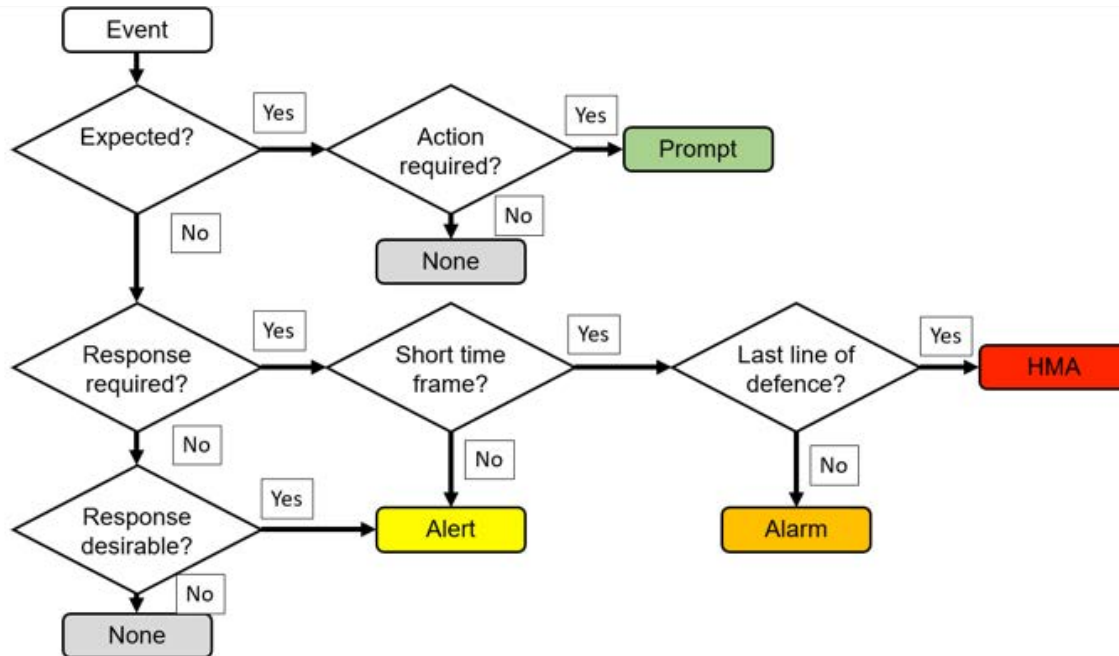


Figure 9 Flowchart guide to decide selection of alarms, alerts, prompts and HMAs

The alarm philosophy should define the use of alerts, events, prompts, alarms and highly managed alarms.

2.7 Risk management

Many of the industrial systems covered by this Guide have potential to cause major accidents that may result in multiple fatalities. For these the assessment of risk will be particularly important. The only way to eliminate the risk is to stop industrial activity, which effectively closes the business. Managing risk is the critical requirement, and alarms can make a valuable contribution to this.

2.7.1 The need to identify and control risks

Where significant regulated risks (e.g. safety, environment) exist there is usually a legal requirement to reduce them. The aim is often to achieve a 'tolerable' or 'acceptable' level of risk, but this can be difficult to achieve in an objective and defensible way. A more useful concept is to set out to reduce risks to As Low As Reasonably Practicable (ALARP).

To demonstrate that risks are ALARP it is necessary to:

- Demonstrate a thorough understanding of hazards and risks of an operation.
- Identify what else could be done to reduce risks, and
- Explain why the additional measures are not required.

Cost Benefit Analysis (CBA) can be used to address the final requirement but in practice a lack of reliable data makes it very difficult. More useful explanations usually refer to a minimal reduction in risk because the existing measures are sufficient (diminishing returns) or highlighting that the investment required to achieve a small risk reduction could be better used somewhere else where a large risk reduction would be achieved.

Problems occur when alarms are identified as an additional risk control measure. They are low cost and in isolation an alarm appears to be an effective way of reducing risk. However, one of the main concerns is operators having to deal with too many alarms, so any additions are likely to increase rather than decrease overall risk. A much better understanding of how alarms contribute to overall risk management is required.

2.7.2 Risk reduction using alarms

Most people would agree that alarms contribute to risk reduction. However, accounting for the reduction achieved is not straightforward. The layers of protection model (Figure 10) is widely accepted as a useful representation and clearly includes reference to alarms.

The layers of protection for a modern process system may include:

- **Plant design:** providing inherent safety improvements.
- **BPCS:** automatic control systems which act to maintain process variables within safe bounds.
- **Human Response:** alarms, operator information displays, manual controls and manual trips.
- **Instrumented Response:** automatic protection systems.
- **Mechanical Response:** e.g. safety relief valves, bursting discs, etc.
- **Mitigation** – Crisis management and emergency response procedures to reduce consequences (e.g. following loss of containment of a hazardous substance).

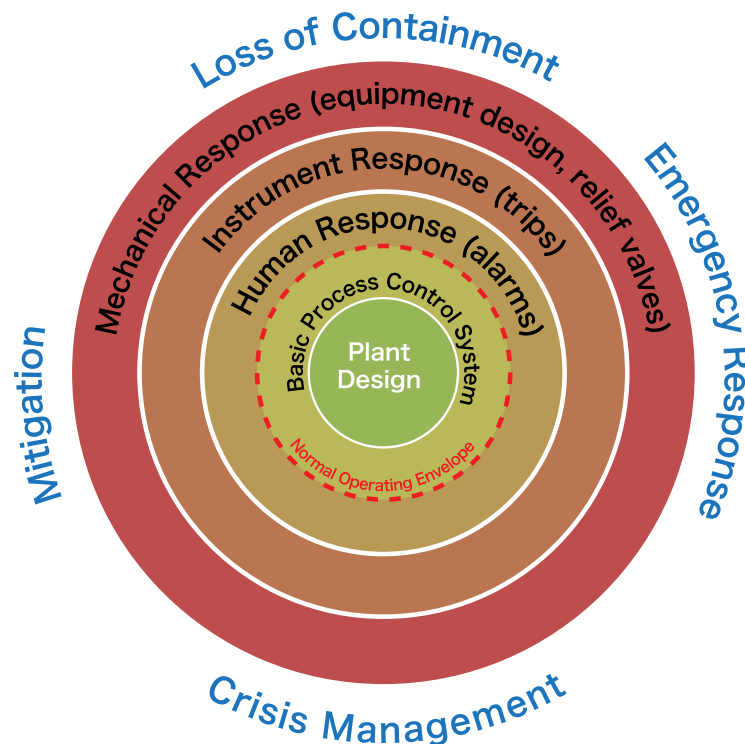


Figure 10 Layer of Protection model of risk management