

THE ENGINEERING EQUIPMENT AND MATERIALS USERS ASSOCIATION

Alarm systems

A guide to design, management and procurement

PUBLICATION 191

Edition 3

Copyright © 2013 The Engineering Equipment and Materials Users' Association.
A company limited by guarantee. Registered in England. Company number
477838.

ISBN 978-0-85931-192-2

Imprint reference 09-2013

Registered and Trading Address
63 Mark Lane London EC3R 7NQ
Telephone: +44 (0)20 7488 0801
Fax: +44 (0)20 7488 3499
E-mail: 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 governed by a Council of members. This Council is responsible for the policies, financing, membership, and strategy of the Association. Any organisation that is a substantial user or purchaser of engineering products is eligible to 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 organisation 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 by the EEMUA executive directors, 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 enquiries@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 Executive Director. 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 enquiries@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.

Cover photograph, reproduced with kind permission of RWE npower.

Contents

Foreword.....	xiii
About this Guide.....	xv
Core Principles and the Roadmap.....	xxi
1 Introduction	1
1.1 What is an alarm system?	1
1.2 Key design principles.....	2
1.3 Alarm system management philosophy/Company Standard.....	5
1.3.1 Corporate considerations	5
1.3.2 Site considerations	5
1.4 Financial considerations	7
2 Principles of alarm system design	9
2.1 The design process	9
2.2 Where do requirements for alarms come from?	11
2.2.1 Alarms.....	12
2.2.2 Alerts	13
2.2.3 The difference between an alarm, an alert and a prompt.....	14
2.2.4 Alerts as an alternative to control by alarms.....	14
2.2.5 Comparison of alarms, alerts and prompts	15
2.3 Risk assessment	17
2.3.1 The need to identify and minimise risks	17
2.3.2 Risk reduction.....	17
2.3.3 Safety related alarms - principles.....	18
2.3.4 Design and engineering of safety related alarms	19
2.3.5 Proof testing.....	23
2.3.6 Summary	24
2.4 Generation of alarms.....	24
2.4.1 Types of alarms	24
2.4.2 The selection of alarm settings	27
2.5 Structuring of alarms.....	29
2.5.1 Prioritisation	29
2.5.2 Logical processing of alarms.....	32
2.6 User centred design	32
2.6.1 The role of the operator/production staff.....	32
2.6.2 The type of process	34
2.7 Designing for operability	39
2.7.1 Improve the management of alarm overloads.....	40
3 Implementing a system of alarm management	43
3.1 Alarm systems management organisation.....	43
3.1.1 Steering committee	44
3.1.2 Engineering specification	44
3.1.3 Alarm management philosophy document.....	44
3.1.4 The alarm co-ordinator.....	45
3.1.5 Alarm assessments (rationalisation)	45
3.1.6 Alarm database	45
3.1.7 Alarm analysis tools.....	49
3.1.8 Measuring alarm metrics	49
3.1.9 Summary alarm metrics	50
3.1.10 Detailed alarm metrics	50

3.1.11 Operations reporting and feedback action.....	50
3.2 Fostering a culture of improvement	50
3.3 The improvement (rationalisation) process for a specific alarm system	51
3.3.1 System capability	51
3.3.2 Problem identification.....	51
3.3.3 Review team/philosophy document	54
3.3.4 Supporting documentation	54
3.3.5 Plant area categorisation	55
3.3.6 Unit/plant/site review.....	55
3.3.7 Integration	57
3.3.8 Monitor/improvement	57
3.3.9 System tuning	58
3.4 Assessment of existing alarm system status	58
3.4.1 How useful is the alarm system	59
3.4.2 Gaining the opinions of the users.....	60
3.4.3 Understanding the alarm system performance	60
3.4.4 Determine how well alarms are managed.....	60
3.5 Detailed assessment	60
3.6 Initial assessment of individual alarms	61
3.6.1 Assessment of individual alarms on an existing system	61
3.6.2 Assessment of individual alarms for a new system	62
3.6.3 'What if' questioning	63
3.7 Alarm management philosophy document	63
3.7.1 Allocation of roles and responsibilities for design of the alarm system	64
3.7.2 Identification of the alarm system users and their needs	64
3.7.3 Definition of what an alarm should be.....	64
3.7.4 Definition of the safety role of the alarm system	65
3.7.5 Define how any alarms are to be registered.....	65
3.7.6 Definitions of alarm system performance targets.....	65
3.7.7 Rules for prioritisation of alarms	65
3.7.8 Alarm system configuration.....	66
3.7.9 Checklist for designers on the information to be recorded.....	66
3.7.10 Dictionary of terms and abbreviations to be used in alarm messages	66
3.7.11 Guidance to sub-contractors on the design of alarms	66
3.7.12 Guidance on content and structure of alarm response definitions	67
3.7.13 Guidance on interpreting patterns of alarms	67
3.7.14 Guidance on establishing alarm equipment test frequencies	68
3.8 Training.....	68
4 HCI management techniques	71
4.1 Display options.....	71
4.1.1 Alarm annunciator panels	73
4.1.2 Alarm list displays	74
4.1.3 Graphically embedded alarm objects	75
4.2 Overviews.....	75
4.3 Audio/visual assistance to the graphical interface	76
4.4 Alerts.....	78
5 Alarm configuration	81
5.1 Field derivation of alarms	81
5.2 Alarm processing hardware	81
5.2.1 The commercial environment	81
5.2.2 Reliability issues.....	82
5.2.3 Functionality.....	83

5.2.4 Environmental requirements	83
5.3 Alarm response definition.....	84
5.4 Testing of alarms	85
5.4.1 Management of testing.....	85
5.4.2 Example test methodology.....	87
5.5 Suppression	87
5.5.1 Bulk suppression	87
5.5.2 Logical suppression.....	88
5.5.3 General suppression rules.....	88
5.5.4 Implementation of suppression.....	89
5.5.5 Authorisation and control.....	91
6 Performance monitoring/improvement.....	93
6.1 Introduction	93
6.2 Performance metrics	93
6.3 Benchmark values.....	95
6.3.1 Main benchmark values.....	96
6.3.2 Steady state usability benchmarks	96
6.3.3 Abnormal (upset) state usability benchmarks	97
6.3.4 General usability benchmarks.....	98
6.3.5 Summary of metrics and benchmark values	98
6.4 Key performance indicators (KPIs)	99
6.4.1 Primary KPIs.....	100
6.4.2 Secondary KPIs	101
6.5 Performance levels and alarm system states	102
6.5.1 Performance levels	102
6.5.2 Alarm system states	103
6.6 Validation of metrics.....	112
7 Buying a new alarm system.....	113
7.1 Investment appraisal.....	113
7.2 Hardware.....	113
7.3 Specifying alarm functionality	114
7.4 Specifying engineering.....	115
7.4.1 Specification of design procedures	115
7.4.2 Specification of required performance.....	115
7.5 Contractual implications.....	116
7.5.1 Allocation of activities	116
7.5.2 Scheduling of activities.....	116
7.5.3 Contractual tests of acceptability	116
7.6 Ensuring usability	117
Appendix 1 The costs of poor alarm performance	119
A1.1 Three Mile Island	119
A1.2 Milford Haven Refinery.....	119
A1.3 Channel Tunnel Fire.....	119
A1.4 Tosco Avon Accident.....	119
A1.5 Longford Gas Explosion.....	120
A1.6 Grangemouth Refinery Scotland	120
A1.7 First Chemical Corporation	120
A1.8 Texas City.....	121
A1.9 Buncefield Oil Storage Depot	121
A1.10 IChemE accident database.....	121
A1.11 Nuclear power incident database	121

A1.12 HSE accident analysis	121
A1.13 HSE alarm survey.....	122
A1.14 Abnormal Situation Management Consortium	122
A1.15 Refinery study	123
Appendix 2 Pertinent requirements.....	125
Appendix 3 Prioritisation methods	127
A3.1 Potential severity of consequence	127
A3.2 Time to consequence.....	128
A3.3 Priority distribution of alarms.....	129
A3.4 Prioritisation of safety related alarms	130
A3.5 Example methods for setting of priority	131
A3.5.1 Method 1 - Priority matrix evaluation.....	131
A3.5.2 Method 2 - Summating consequence	135
A3.5.3 Method 3 - Taking maximum consequence	137
A3.5.3 Method 4 - General alarm assessment	139
Appendix 4 Logical processing of alarms.....	145
A4.1 General comments	145
A4.2 Grouping	145
A4.3 Suppression	146
A4.3.1 Redundancy logic	146
A4.3.2 Eclipsing.....	146
A4.3.3 Out of service plant	146
A4.3.4 Operating mode	147
A4.3.5 Major event	147
A4.4 Automatic alarm load shedding	148
A4.5 Alarms from equipment under test	149
Appendix 5 Repeating and fleeting alarms.....	151
A5.1 Why repeating alarms occur	151
A5.2 Engineering of signals.....	152
A5.3 Filtering	152
A5.4 Transient suppression	153
A5.5 Deadband	153
A5.6 De-bounce timer	154
A5.7 Counter	155
A5.8 Shelving	156
A5.9 Release ('One-shot' shelving)	157
A5.10 Auto-shelving	157
A5.11 Single line annunciation	158
A5.12 Logging of repeating alarms.....	159
A5.13 Summary	159
Appendix 6 Alarm management in batch plants	161
A6.1 Batch plant operation	161
A6.1.1 Alarm thresholds	162
A6.1.2 Replacement of batch with semi-batch or continuous processes.....	162
A6.2 Operator information	163
A6.3 Alarm rates	163
A6.4 Application of alarm priorities in batch processes	165
A6.5 Design of the alarms	165
A6.6 Generation of alarms	166
A6.7 Management of alarm limits thresholds	166

A6.8 Sources of nuisance alarms	167
A6.9 Sources of alarm floods.....	167
A6.10 Getting information to remote operations	167
Appendix 7 Alarm management in geographically distributed plant.....	169
A7.1 Distributed process operation	169
A7.2 Operator workload	170
A7.3 Alarm system performance and KPIs.....	171
A7.4 Application of alarm priorities in distributed processes.....	171
A7.5 Generation of alarms	172
A7.6 Telemetry issues.....	174
A7.7 Getting information to remote resources	175
Appendix 8 Usefulness questionnaire.....	177
A8.1 How many alarms are useful?	178
Appendix 9 Operator questionnaire.....	181
Appendix 10 Supporting checklists	187
A10.1 Storage and management	187
A10.2 Threshold setting	187
A10.3 Checklist for a good alarm	187
A10.4 Alarm configuration information	188
A10.5 Alarm priority information.....	188
A10.6 HAZOP checklist.....	189
Appendix 11 Design of alarm list displays	191
A11.1 Alarm states	191
A11.2 Content of alarm entry	192
A11.3 Positioning of new alarms	194
A11.4 Alarm acceptance.....	195
A11.5 Movement through the list.....	195
A11.6 Dealing with nuisance alarms	196
A11.7 Display filtering.....	196
Appendix 12 Design of field alarm sensors.....	199
A12.1 Choice of alarm sensor.....	199
A12.2 Measurement of actuator position	200
A12.3 Location of sensors.....	200
A12.4 Sensor range	201
A12.5 Validation of measurements.....	202
A12.6 Signal transmission	203
A12.7 Dependent failures	203
Appendix 13 Example alarm suppression hazard study.....	205
A13.1 Introduction	205
A13.2 Example	205
A13.2.1 Familiarisation.....	206
A13.2.2 Review of operating modes	206
A13.2.3 Review of alarms to be suppressed.....	206
A13.2.4 Reporting	207
A13.2.5 Follow-up	208
Appendix 14 Performance metrics and KPI visualisation	209
A14.1 Operator questionnaires	209

A14.2 Usefulness of alarms.....	209
A14.3 Incident recording	211
A14.4 Number of alarms	211
A14.5 Average alarm rate.....	211
A14.6 Identification of frequent alarms.....	213
A14.7 Number of alarms following a major plant upset	213
A14.8 Number of standing alarms.....	215
A14.9 Priority distribution	216
A14.10 Operator response time.....	217
A14.11 Correlation	217
A14.12 Data analysis tools.....	217
A14.12.1 Specification of alarm logging and analysis tools.....	219
A14.13 KPI improvement visualisation examples.....	220
Appendix 15 Specification checklist - small system.....	223
A15.1 Where dedicated alarm systems are used	223
A15.2 Input handling	223
A15.3 Alarm processing.....	223
A15.4 Alarm display/output	224
A15.5 Environmental	224
Appendix 16 Specification checklist - large system	225
A16.1 Grading of requirements.....	225
Appendix 17 Intelligent fault detection.....	231
A17.1 Pattern recognition	231
A17.2 Neural networks.....	232
A17.3 Fuzzy logic	233
A17.4 Knowledge-based reasoning.....	233
A17.5 Model-based reasoning	234
A17.6 Overview of intelligent fault detection methods.....	235
Appendix 18 Glossary.....	237
Appendix 19 References.....	241
Appendix 20 Bibliography	245

Figures

Figure 1 EEMUA 191 Roadmap selection	xxi
Figure 2 EEMUA 191 Roadmap - Existing system	xxii
Figure 3 EEMUA 191 Roadmap - Conceptual system.....	xxiii
Figure 4 ISA 18.2 Lifecycle model.....	xxiv
Figure 5 HCI, the sensory interface between operator and plant.....	2
Figure 6 Alarm system management overview.....	6
Figure 7 LOPA (Layer of Protection Analysis) diagram.....	18
Figure 8 Safety related alarm reliability requirements.....	21
Figure 9 Operator response stages	21
Figure 10 Proof testing of safety related alarms	23
Figure 11 An effective and ineffective alarm system	27
Figure 12 The setting of a high alarm.....	28
Figure 13 Operator response to an abnormal situation	33
Figure 14 The operator's role in the different plant states.....	36
Figure 15 Batch process conceptual model.....	37

Figure 16 Typical control architecture model	39
Figure 17 Typical form for loop information.....	47
Figure 18 Simple data input form	48
Figure 19 Typical alarm recorded information.....	48
Figure 20 System improvement process	53
Figure 21 Example of Alarm HCI.....	76
Figure 22 Alarm test methodology	86
Figure 23 Alarm suppression implementation	89
Figure 24 Steady state performance levels.....	103
Figure 25 Abnormal condition performance levels	103
Figure 26 Alarm system performance.....	104
Figure 27 Summary of alarm states	105
Figure 28 Typical plot of Key Performance Indicator	123
Figure 29 Productivity histogram	124
Figure 30 The frequency of loss incidents	124
Figure 31 Layer of protection	132
Figure 32 Alarm priority matrix	133
Figure 33 Possible priority bands to achieve required priority distribution	135
Figure 34 Prioritisation using maximum of individual priorities	137
Figure 35 General alarm assessment.....	140
Figure 36 Safety assessment prioritisation	141
Figure 37 Environmental assessment prioritisation	142
Figure 38 Financial (Asset) Loss Assessment Prioritisation.....	143
Figure 39 Repeating alarms generated by noise on a process signal	151
Figure 40 Transfer function of deadband.....	153
Figure 41 The elimination of repeating alarms using deadband	154
Figure 42 Alarm response - batch plant.....	164
Figure 43 S88 Model.....	165
Figure 44 Example of a separate set of alarm thresholds.....	166
Figure 45 Geographically distributed processes.....	173
Figure 46 Alarm state transition diagram for static alarm list display.....	192
Figure 47 Individual alarm quality quadrant	210
Figure 48 Example of alarm frequency analysis	213
Figure 49 Example plot of alarms per minute	214
Figure 50 Initial KPI improvements	221
Figure 51 Initiation of improvements in flood rate	221
Figure 52 Final improvements of all KPIs	221
Figure 53 KPI improvements shown as a radar plot.....	222
Figure 54 Plant system with redundant equipment	231
Figure 55 A simple neural network.....	233
Figure 56 A graphical rule definition.....	234

Tables

Table 1 Characteristics of a good alarm	4
Table 2 Activities to be considered in the design of an alarm system.....	10
Table 3 Content of a typical alarm management philosophy document.....	11
Table 4 Comparison of alarms, alerts/prompts and journal only signals.....	16
Table 5 Human reliability requirements	20
Table 6 Elements of an improvement strategy	51
Table 7 The objectives of an alarm system review.....	52
Table 8 Characteristics of alarm reviews for normal operation and plant upset ..	56
Table 9 Effective techniques for improving alarm systems.....	59
Table 10 Advantages and disadvantages of display options	72
Table 11 Alarm suppression.....	88
Table 12 Example of bulk alarm suppression	90
Table 13 Summary of possible alarm metrics per operator station	94
Table 14 Long term average alarm rate.....	96
Table 15 Major plant upset alarm	97
Table 16 Priority distribution.....	98
Table 17 Standing alarms.....	98
Table 18 Benchmark values for operator usability metric	98
Table 19 Summary of metrics and benchmark values	99
Table 20 Alarm system performance metrics	104
Table 21 Overloaded alarm state	108
Table 22 Reactive alarm state.....	109
Table 23 Stable alarm state	110
Table 24 Robust alarm state	111
Table 25 Alarm system hardware comparisons	114
Table 26 Elements in a user-centred operator interface design	117
Table 27 Priority distribution during system configuration	129
Table 28 Target maximum occurrence rates of alarms of different priorities....	129
Table 29 A proposed Hazard Index grouping	133
Table 30 Priority break points for alarms	137
Table 31 Rules for allocation of safety, environmental and financial priority	138
Table 32 Table of filter time constants.....	153
Table 33 Table of default deadband settings.....	154
Table 34 Table of default de-bounce timer parameters	155
Table 35 Example of weighting of results of usefulness questionnaires	177
Table 36 Proportion of useful alarms	179
Table 37 Attributes of a good alarm message.....	193
Table 38 How system size affects design and management	212
Table 39 Benchmarks for assessing average alarm rates.....	213
Table 40 Guidance on alarm rate following an upset.....	215
Table 41 Alarm pattern array	232

Foreword

The Health and Safety Executive was consulted in the production of this Publication. It endorses the sensible, proportionate, reasonable and balanced advice to owners on the design, management and procurement of alarm systems set out in the guidance.

Peter Baker
Deputy Director and Head of Chemicals Explosives and Microbiological Hazards
Division
Hazardous Installations Directorate
Health & Safety Executive
UK 2013

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.

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 and others. 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 optimisation.
- 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.

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⁽²³⁾ – 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⁽¹⁴⁾ - 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 Australian Longford Refinery incident⁽²⁸⁾ in 1998).

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⁽⁵⁾ 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.

Key Changes in Third Edition, 2013

Edition 3 has been substantially revised and updated. Some Sections in Edition 3 are completely new while others relate to updated versions of Sections in Edition 2 as follows:

Edition 3 Section

Edition 2 Section

Chapter 1	Chapter 1 updated and revised
Chapter 2	Chapter 2 updated and revised
Chapter 3	Chapter 3 updated and revised
Chapter 4	New
Chapter 5	New
Chapter 6	Chapters 4 & 5 updated and revised
Chapter 7	Chapter 6 updated and revised
Appendix 1	Appendix 16 updated and revised
Appendix 2	New
Appendix 3	Appendix 5 updated and revised
Appendix 4	Appendix 8 updated and revised
Appendix 5	Appendix 9 updated and revised
Appendix 6	Appendix 20 updated and revised
Appendix 7	New
Appendix 8	Appendix 15 updated and revised
Appendix 9	Appendix 14 updated and revised
Appendix 10	New
Appendix 11	Appendix 11
Appendix 12	Appendix 10
Appendix 13	New
Appendix 14	Appendix 12
Appendix 15	Appendix 18
Appendix 16	Appendix 17
Appendix 17	New
Appendix 18	Appendix 1 updated and revised
Appendix 19	Appendix 22 updated and revised
Appendix 20	Appendix 23 updated and revised

Relationship between EEMUA 191 and EEMUA 201

Although this guide (EEMUA 191) and the HCI 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 4 as well as 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.

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

This Third Edition has been prepared by a working group of EEMUA's Instrumentation and Control Committee, with input from (in Europe) the HSE, as well as many comments received from readers around the world.

EEMUA gratefully acknowledges the contributions of all who have been involved, in many capacities, during the preparation and production of this Guide.

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.

Notes on use of this Guide

In order to assist readers, the next two pages highlight the core principles underlying the guidance and give a 'roadmap' providing directions to key information.

Chapters 1 to 7 of this Guide concentrate on alarm management philosophy and general principles. Key messages are highlighted in bold.

Much supporting detail is contained in the Appendices

A glossary of terms is given in Appendix 18.

References are listed in Appendix 19. Throughout the text, they are referred to in parentheses, for example⁽⁵⁵⁾.

A bibliography of suggested further reading is given in Appendix 20.

Footnotes are referred to using superscripts, for example¹.

Acronyms used in this Guide

ASCII	American Standard Code for Information Interchange
ASM®	Abnormal Situation Management®
BPCS	Basic Process Control System
CCR	Central Control Room
CRT	Cathode Ray Tube
CSB	US Chemical Safety and Hazard Investigation Board
DCS	Distributed Control System
EMC	Electro-Magnetic Compatibility
ESD System	Emergency Shutdown System
HAZOP	Hazard and Operability Studies
HCI	Human Computer Interface
HSE	Health and Safety Executive
IP	Ingress Protection
IP	Internet Protocol
ISO	International Standards Organization
KPI	Key Performance Indicator
LCD	Liquid Crystal Display
LSH	Level Switch High
LSHH	Level Switch High High
LSL	Level Switch Low
LSLL	Level Switch Low Low
LOPA	Layers of Protection Analysis
MOC	Management of Change
P&ID	Piping and Instrumentation Diagram
PFD	Probability of Failure on Demand
PFD _{avq}	Average Probability of Failure on Demand
PLC	Programmable Logic Controller
SCADA	Supervisory Control And Data Acquisition
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TCP	Transmission Control Protocol
TTC	Time to Consequence
VDU	Visual Display Unit

Core Principles and the Roadmap

This Guide begins with four core principles and a roadmap. The core principles encapsulate the most important ideas presented in this Guide. The roadmap (which is illustrated in Figures 1, 2 and 3) directs different users to the parts of the Guide relevant to their particular needs. It also provides a quick and easy point of reference and an overview of the Guide's advice.

Four core principles run through this Guide:

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; and
- 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 for safety, environmental or business requirements 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.

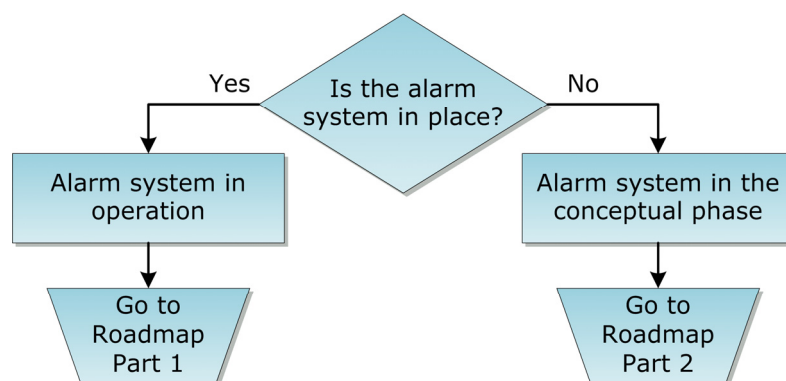


Figure 1 EEMUA 191 Roadmap selection

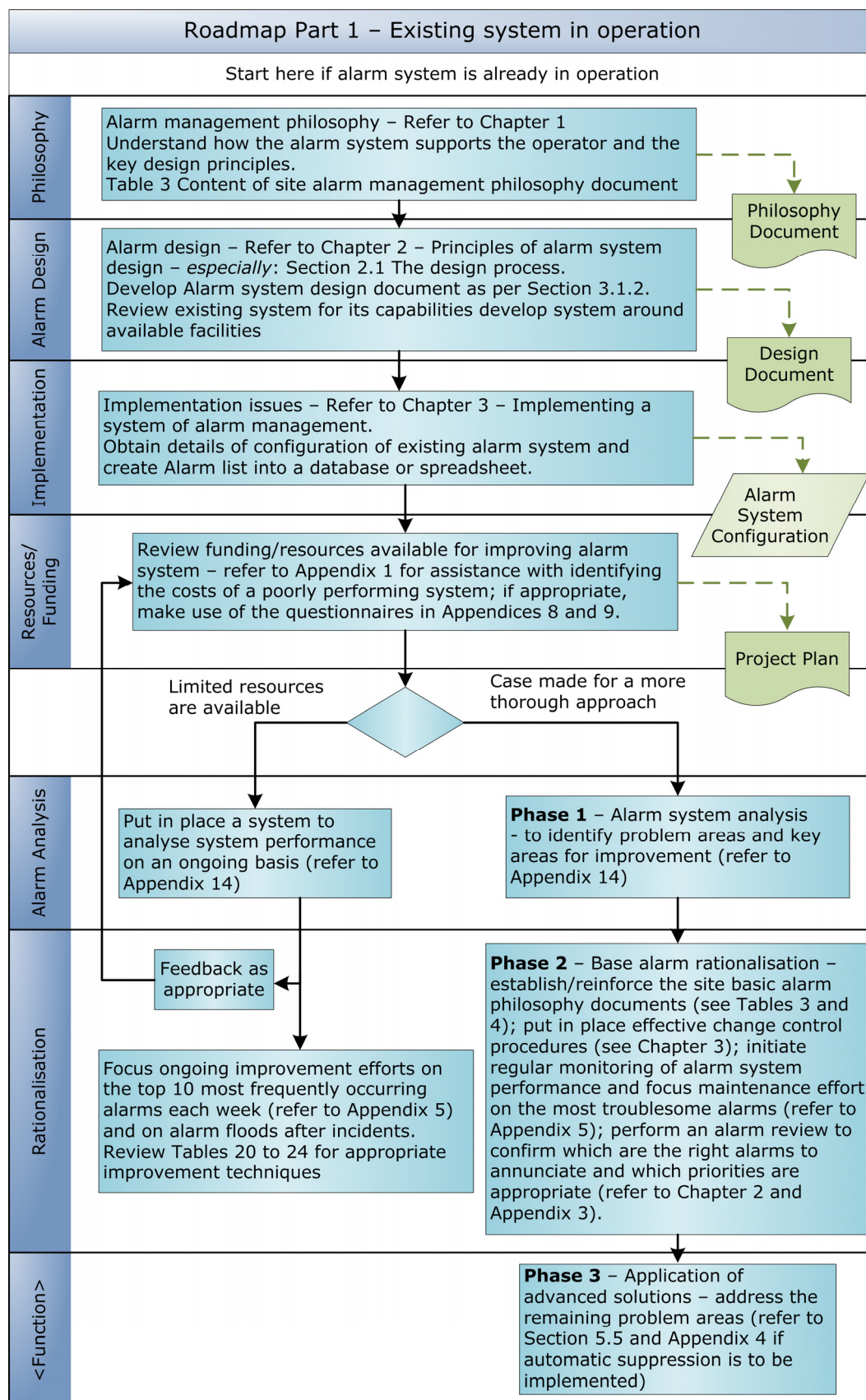


Figure 2 EEMUA 191 Roadmap - Existing system

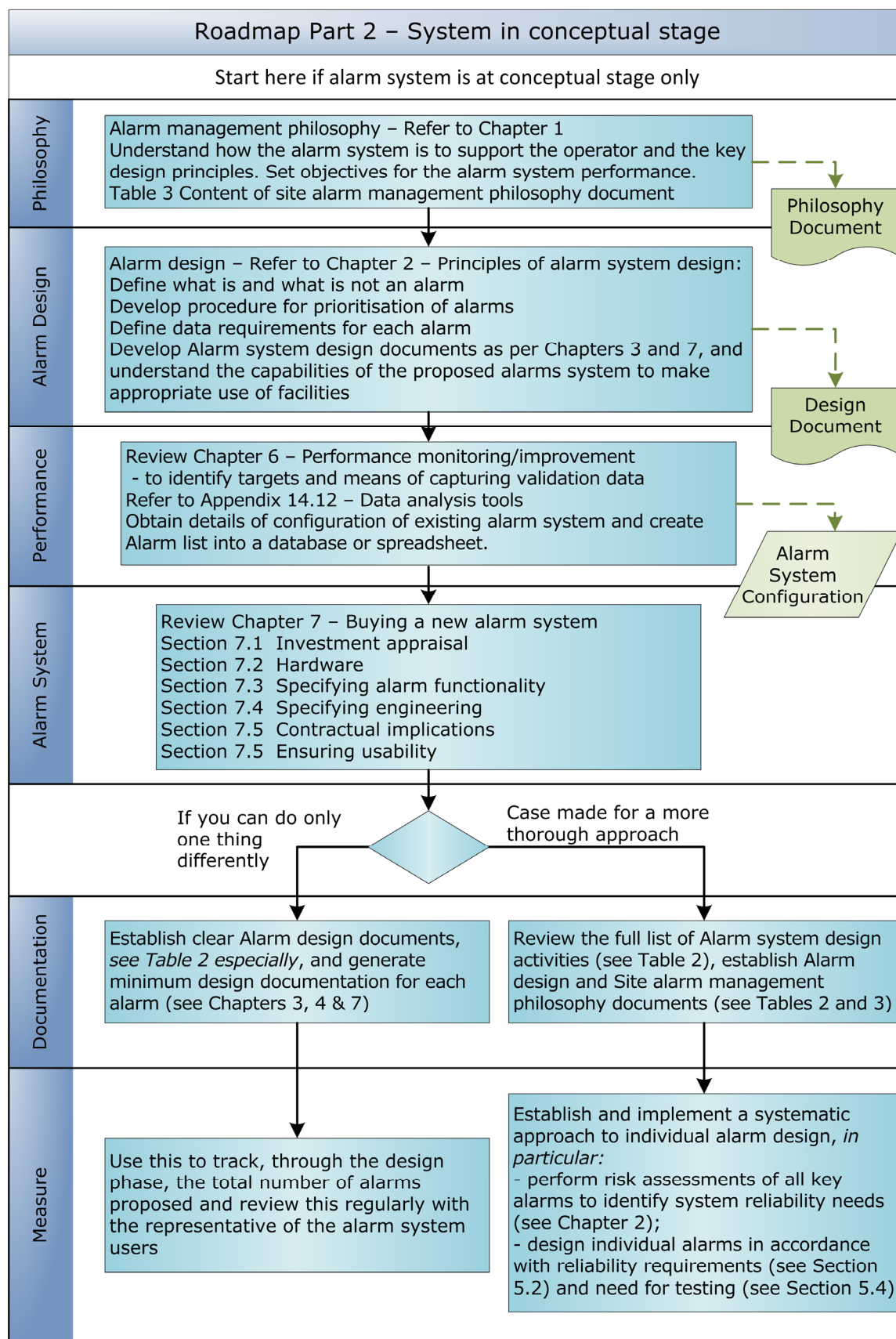


Figure 3 EEMUA 191 Roadmap - Conceptual system

ISA 18.2 Alarm System Lifecycle

Since the issue of the second edition of this Guide, the International Society of Automation has published a standard, ISA 18.2 Management of alarm systems for the process industries⁽¹⁾. Within this standard a lifecycle is defined that covers the alarm system from its specification through design to operation and finally to its eventual decommissioning, see Figure 4.

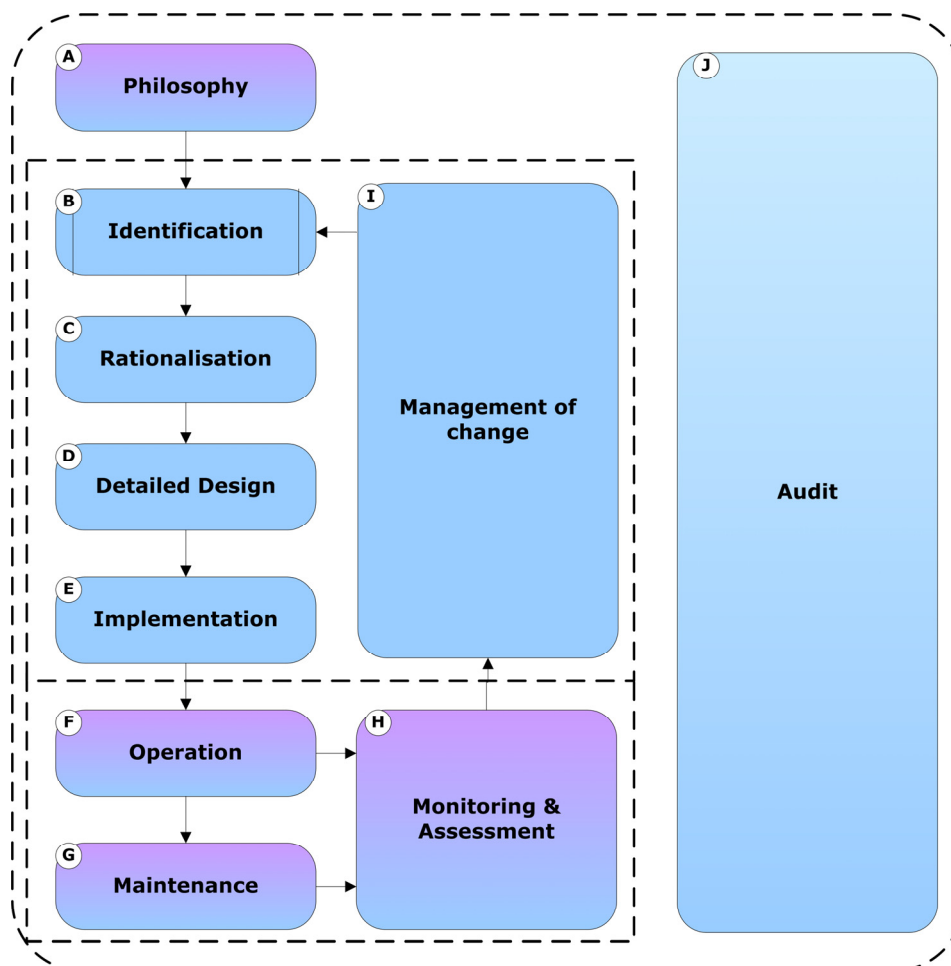


Figure 4 ISA 18.2 Lifecycle model

Details of each phase is described within the standard. In general the ISA 18.2 maps on to the EEMUA 191 guide as follows:

EEMUA 191 Section	ISA 18.2 Process
Chapters 1&2	Philosophy
Chapters 2&3	Identification
Chapters 2&3	Rationalization
Chapters 4&5	Detailed Design
Chapters 5&7	Implementation
Chapter 6	Operation
Chapter 6	Maintenance
Chapter 3	Management of Change
Chapter 6	Audit

1 Introduction

This Chapter provides an introduction to alarm systems and comprises:

- *a basic explanation of what an alarm system is;*
- *a more detailed discussion of the function of an alarm system and of some of the characteristics that a good alarm system should have; and*
- *the need for a clear system management philosophy and organisational structure to support the importance of the alarm system to the plant.*

Key principles identified are that:

- **Every alarm should have a defined purpose.**
- **Every alarm should have a defined response.**
- **Adequate time should be allowed for the operator to carry out this response.**

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

1.1 What is an alarm system?

Alarm systems form a core element of almost all modern operator interfaces to industrial plants including oil refineries, power stations, chemical plants and many others. Traditionally they were based around hard-wired indication lamps and annunciator panels, but most modern systems use computer-driven display devices (e.g. VDUs) to present the operator with graphical representations or text lists of alarms.

Alarms are signals which are annunciated to the operator², typically by an audible sound, some form of visual indication, usually flashing, and by the presentation of a message or some other identifier. An alarm will indicate a problem requiring operator action generally initiated by a process measurement passing a defined alarm setting as it approaches an undesirable or potentially unsafe value. It may also indicate equipment status becoming unhealthy.

Alarm systems are a very important way of automatically monitoring the plant condition and attracting the attention of the process plant operator to significant changes that require assessment or action. They help the operator:

- To maintain the plant within a safe operating envelope. A good alarm system helps the operator to correct potentially dangerous situations before the Emergency Shutdown (ESD) system³ is forced to intervene. This improves plant availability. It also reduces the demand rate on the ESD system and, thus, increases plant safety⁴.
- To recognise and act to avoid hazardous situations. It is the role of the ESD system to intervene before a hazard arises. However, there may be cases, hopefully extremely infrequent, where the plant deviates outside its

²Note that throughout this Guide the term 'operator' should be taken to include the desk operator plus other primary users (e.g. supervisors) assisting in the control of the plant in the control room.

³See Appendix 18.

⁴For automatic protection systems the dangerous failure rate equals the demand rate times the average probability of failure on demand. Reducing the demand rate thus reduces the dangerous failure rate.

design conditions into a state where the ESD system is no longer capable of acting effectively. Also there may be cases where operator action following an alarm has been explicitly identified within the plant Safety Case as a measure of protection.

- To identify deviations from desired operating conditions that could lead to financial loss such as off-specification or overly expensive product.
- To better understand complex process conditions that require a response. Alarms should be an important diagnostic tool and are one of several sources that an operator uses during an upset.

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 term 'alarm processor' refers to the part of the system for processing and displaying alarms. Often this function will be carried out within proprietary electronic annunciator boxes, DCSs or SCADA systems.

The following Figure 5 shows the position of the HCI within a process control system. This of course is where the outputs of the alarm system are made visible to the operator. It is important to develop close integration of the alarm system with the HCI to obtain best operator performance.

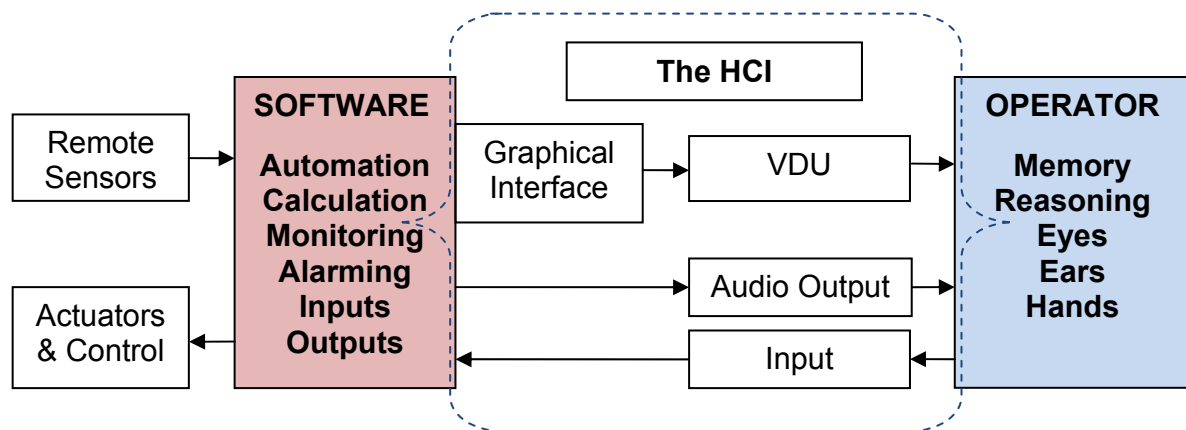


Figure 5 HCI, the sensory interface between operator and plant

1.2 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 plant conditions requiring timely assessment or action.

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 alert, inform and guide.

Thus, when an alarm occurs, the operator should be notified, which typically is done by an audible warning and/or some form of flashing indication. The alarm should present information defining what the problem is, e.g. by displaying a descriptive text message, lighting a labelled annunciator window, or changing a graphic display. Information should also be provided (e.g. hardcopy or operator-selected on-screen help) giving guidance on how to respond to the alarm. Ideally the alarm system should also provide feedback to the operator on the success of actions taken in response to alarms⁵.

For an alarm system to be effective in supporting the operator, 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 can be ignored and ensure that the operator does not adopt a mind frame that the alarms can be ignored⁶. Thus:

Every alarm presented to the operator should be useful and relevant to the operator⁷.

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, this response should be an action (e.g. altering a control set point, changing over to a standby pump, asking a fitter to repair a piece of failed plant equipment). Sometimes the response to the alarm will have to be conditional. For example, the operator might select a graphic display, check the plant condition, and only in certain circumstances carry out any control action. In a few cases the defined response to an alarm will be purely mental. For example, in response to a 'plant tripped' alarm the operator may need only to change the form of plant monitoring the operator is carrying out. There may not be any immediate control action required, but it is important for the operator to make this cognitive switch.

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. A common problem is that such event information often gets mixed in with alarms⁸. If a response is defined for every alarm during the design process, this information provides an excellent starting point for the production of alarm response and training material.

⁵This information will generally have to be provided on supplementary displays, for example, accessed by clicking on an alarm on an alarm list (see Section 4.1.2).

⁶There is experimental evidence⁽³⁾ which shows that there is a 'cry wolf' effect and operators do adapt their response according to the probability of the alarm being useful.

⁷This implies that a change of plant state relevant to the maintenance staff but not relevant to the operator should not be an 'alarm'. Appropriate means should be provided for presenting this information to these staff, and facilities similar to those provided to the operator for presenting alarms may be appropriate. Note, however, that the operator may need to be made aware through alarms of the operational consequences of faults requiring maintenance.

⁸There will be events that occur on plant which are not alarms - such as changes in mode of control loops - which the operator will need to be able to observe. The designer should consider how these are presented. It may be sufficient to show them as status indications on plant mimic formats. Alternatively, an event list display which is similar to but separate from the alarm list display may be appropriate.

Given that the operator is expected to respond to every alarm, it follows that in a usable alarm system:

Adequate time should be allowed for the operator to carry out a defined response.

This implies that:

- The alarm should occur early enough to allow the operator to correct the fault.
- The alarm rate should not exceed that which the operator is capable of handling. A typical operator's role involves many different activities and responsibilities. It is important that the overall role is manageable, and the plant, the control systems and the operator interface should be designed to help achieve this. Furthermore, the time required for other activities often imposes severe limits on what alarm handling workload is acceptable⁹. As will be seen later, this has some very important implications in terms of overall alarm system design.

To ensure that the above objective is achieved:

The alarm system should be explicitly designed to take account of human limitations^{(37),(41),(47),(48)}.

Some of the characteristics that an alarm should have are summarised in Table 1.

Table 1 Characteristics of a good alarm

Characteristics of a good alarm	
Relevant	i.e. not spurious or of low operational value
Unique	i.e. not duplicating another alarm
Timely	i.e. not long before any response is needed or too late to do anything
Prioritised	i.e. indicating the importance that the operator deals with the problem
Understandable	i.e. having a message which is clear and easy to understand
Diagnostic	i.e. identifying the problem that has occurred
Advisory	i.e. indicative of the action to be taken
Focusing	i.e. drawing attention to the most important issues

So far this section has discussed the primary alarm system function of providing notification to the operator. An alarm system may also have a secondary function of providing an alarm log which can be used for optimising plant operation, for

⁹The long term average workload, W, that the alarm system imposes on the operator may be expressed by the equation:

$$W = R \times T$$

where:

R is the average rate at which alarms are presented to the operator, and

T is the average time taken by the operator to respond to the alarm.

For example, if alarms are presented at an average rate of 1 per minute, and the operator takes on average 30 seconds to deal with each alarm, then the alarm system would on average be consuming 50% of the operator's time.

analysis of incidents¹⁰, and for improving the performance of the alarm system. Manufacturers often provide this as part of a broader capability for logging all significant plant events including alarms, plant status changes not included in the alarm list, operator actions, etc. Where this is done it may be necessary to be able to extract alarm logs separate from other events.

1.3 Alarm system management philosophy/Company Standard

It is crucial to ensure that the alarm system is given the correct amount of importance that it rightfully deserves when viewed against other systems used to control and monitor plant. Without active management, the performance of an alarm system will deteriorate due to instrument and actuator faults, changes in process and alterations in the control software functionality. It is important to appreciate that alarm systems have been implicated in many incidents and that regulators are increasingly demanding evidence of good alarm management practice.

1.3.1 Corporate considerations

The importance of alarm systems needs to be recognised by the corporate entity and an overall company philosophy put in place, with the recognition that adequate resources need to be devoted to this issue.

At this level this may simply be appropriate high level documentation raising the status of alarm systems, e.g. an Engineering Principle. There may however also be more detailed documentation e.g. a Technical Procedure, detailing company-wide practice and requirements, which are then appropriately applied at each site.

1.3.2 Site considerations

A high level management sign on to the importance of the alarm system is crucial in ensuring that both human and financial resource is channelled to maintaining and improving alarm system performance. To demonstrate good alarm management practice it is necessary to:

- keep control of the alarm system through configuration management;
- manage the risk of alarms not in service (e.g. shelved or disabled);
- measure performance, communicate and review against KPIs;
- test the alarm system to ensure that it meets the specification; and
- have demonstrably assigned responsibilities and auditable records

The appointment of an 'alarm co-ordinator' as the alarm systems 'champion' can also be an effective way of ensuring that the alarm system obtains the respect it deserves and is not left unmanaged.

Figure 6 below, details a useful hierarchy for alarm system management. Whilst the alarm steering committee, which may only meet a few times a year, gives overall prominence to the management philosophy, the alarm co-ordinator can take a day-to-day role in monitoring and administering the alarm system. When

¹⁰Note that high speed logging of some parameters may be necessary to analyse certain sorts of incidents. Often separate post-incident recorders are used to do this.

and where necessary, the alarm rationalisation team can take on the role of reviewing the system.

Using the alarm data analysis tools and metrics allows on-going monitoring and continuous improvement to be achieved, with help and feedback from the operations teams.

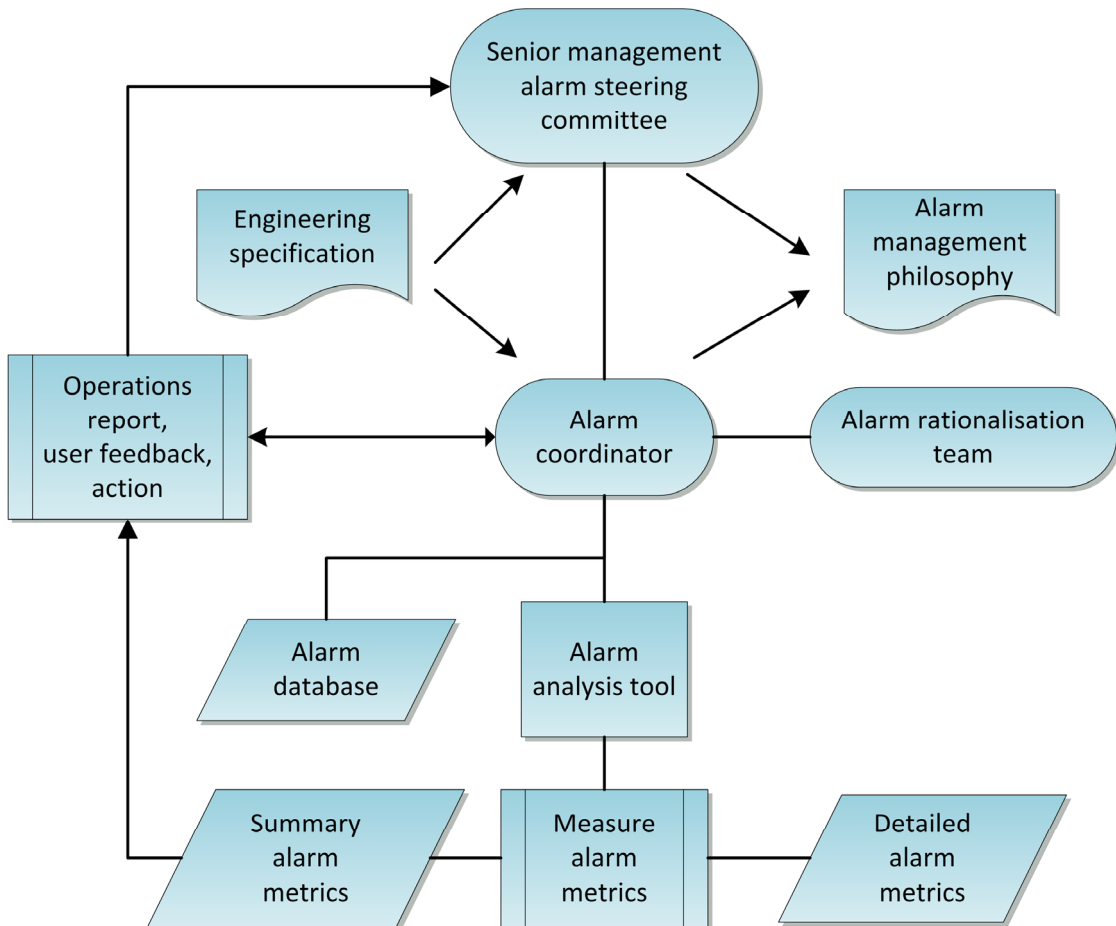


Figure 6 Alarm system management overview

The senior management alarm steering committee should be constituted, and have responsibilities, as detailed below:

- include senior engineering and production managers (Maintenance & Projects);
- chaired by alarm coordinator;
- with the objective to ensure safe and effective operation of alarm systems;
- approve and promote alarm management standards;
- agree upon alarm KPIs and review performance;
- ensure adequate arrangements for specifying new alarms;
- review change management procedure;
- address long standing alarms and testing failures;
- consider training requirements; and
- define requirements for any improvement programme.

Delivery of the full management cycle requires the commitment and dedication of personnel across the process. It needs to engage the management, the operations staff and the full mix of engineers, covering process, instrumentation, control and safety. Chapter 3 gives more detail on implementing a system of alarm management.

1.4 Financial considerations

Financial losses and accidents (sometimes resulting in loss of reputation) occur for a multitude of different reasons at process plants. Often, because designers have tried hard to prevent such incidents, the ones that do happen are due to combinations of several unexpected events occurring together. In addition, it is hard to collect data about all incidents involving financial loss or risk to people or the environment, especially the smaller incidents and the near misses. Because of these difficulties it is hard to make statements like “there have been ‘x’ incidents on process plants in the UK in the last year due to alarm system shortcomings that have cost a total of ‘y’ million pounds”. It is possible, however, to list some of the known incidents that have occurred involving alarm system shortcomings and to quote estimates of the losses involved. Such information is collected together in Appendix 1.

2 Principles of alarm system design

This Chapter provides an introduction to the process of designing an alarm system. It identifies the stages in the process and lays down the principle that the design process should be clearly defined and formally documented. Furthermore, the design of individual alarms should follow a structured procedure.

A fundamental issue when designing each alarm is to consider how important it is and how reliable it should be. To do this it is necessary to go through some form of qualitative or quantitative risk assessment. Important considerations are:

- *Whether the alarm should be classified as safety related according to the definitions given in the international standard IEC 61508⁽²⁹⁾.*
- *Whether the alarm should be implemented in a stand-alone system independent of the process control system.*

The decision whether an alarm is safety related will be influenced by national legislation and by existing practices within the industry sector. Alarms which are safety related should be given special consideration in terms of the design of the operator interface and the operator support provided.

Risk assessment only provides a starting point in the design process. This Chapter goes on to consider broader design issues. This includes how alarm settings are chosen, how priorities should be defined and set, and how alarms should be processed to make them as meaningful as possible. There is also consideration of how an overall alarm system should be designed for operability.

2.1 The design process

The design of an effective operator interface for a modern industrial plant is generally a complex task which should involve consideration of a wide range of human factors issues. It is too broad a topic to be covered in depth in this Guide. Some pointers to the issues involved may be found in various references^{(13), (19), (38), (43)} and in Chapter 4. An in-depth treatment of the topic is provided in EEMUA Publication 201 Process plant control desks utilising Human-Computer Interfaces⁽²⁰⁾, which covers key design principles and practice.

For safe and efficient plant operation it is necessary that the operator's role is designed to be one that the operator can perform effectively and that the operator is provided with suitable tools to support him in doing this. An alarm system is only one of these support tools and, however good it is, the operator will not be able to run the plant safely and efficiently if an operator is being required to carry out a task that is beyond their capabilities, or if the other parts of the operator interface are inadequate. Thus the alarm system should be designed within a framework of considering the complete operator role and support system.

Because of these factors, the design of an alarm system is a complex task. As indicated in Table 2, it may involve a large number of different design activities.

The performance of alarm systems can have a significant safety, environmental and economic impact^{(5), (14), (23), (36)}. Consequently, for all plants where the alarm system is to play a part in preventing or mitigating significant hazards or

economic losses, it is important that good design practices are followed in all the above design activities.

Table 2 Activities to be considered in the design of an alarm system

Considerations for alarm system design
Risk assessment
– Development of the plant safety case – Identification of the safety role of the operator – Risk assessment to identify alarms to protect against safety, environmental or economic risks – Review to identify alarms required to provide significant risk reduction (e.g. safety related alarms)
Ergonomics
– Identification of number of operators and their roles – Overall design of operator interface (e.g. numbers of screens, colour usage, information aids) – Design of the alarm interface (e.g. display methods, annunciation)
Design of individual alarms
– Review of proposed alarms not deriving from risk assessments – Identification of alarms with special integrity or display requirements – Completion of data form for each alarm – Production of alarm response definition (e.g. procedures, task aids, etc.) – Design of plant alarm sensors – Design of hardware for conditioning individual alarm signals – Installation of plant alarm sensors and signal conditioning
Design integration
– Rationalisation of lists of proposed alarms – Review of overall system design to meet Key Design Principles (see Section 1.2) – Identification of required alarm processing functionality
Alarm system configuration
– Installation of alarm system hardware – Configuration of alarm system hardware/software facilities – Construction of alarm information database – Configuration of hardware/software for individual alarms – Configuration of alarm combinatorial logic
Testing and commissioning
– Testing of alarm system facilities – Testing of alarm sensors and signal conditioning – Testing of individual alarm hardware/software configurations – Evaluation of overall ergonomic acceptability – Measurement of alarm system performance – Determination of on-going testing needs – Optimisation of operational performance

In order to ensure that good practice is established and sustained, it is recommended that an alarm system design philosophy document should be defined by a suitably experienced multi-disciplined team. The content of a typical alarm management philosophy document is shown in Table 3. The design of the individual alarms and their configuration in the alarm processor is a complex multi-stage process. To achieve good performance, good design practices should be consistently applied to all alarms. To encourage this:

The design of each alarm should follow a systematic structured procedure in which design decisions are documented.

The overall alarm system design should accord with the Key Design Principles given in Section 1.2.

This will require a review of all proposed alarms, a check that the Key Design Principles are adhered to, and an assessment of whether desired system performance is likely to be met.

Table 3 Content of a typical alarm management philosophy document

Alarm management philosophy document
– Allocation of roles and responsibilities for design of the alarm system, including what user involvement there is to be – Identification of the alarm system users and their needs – A definition of what an alarm should be – A definition of the safety role of the alarm system – Define how any alarms claimed to contribute to safety cases are to be registered (e.g. a list of safety related alarms) – Definitions of alarm system performance targets (e.g. maximum rates) – Rules for prioritisation of alarms – Checklist for designers on the information to be recorded for each alarm – Dictionary of terms and abbreviations to be used in alarm messages – Guidance to sub-contractors on the design of alarms (where appropriate) – Guidance on content and structure of alarm response definitions (e.g. procedures, task aids, etc.) – Guidance on interpreting patterns of alarms, and their grouping, suppressing and acceptance (where appropriate) – Guidance on alarm system configuration – Guidance on establishing alarm equipment test frequencies

2.2 Where do requirements for alarms come from?

Requirements for alarms normally fall into a number of categories:

- process alarms;
- safety related alarms, which can be regarded as a subset of process alarms;
- environmental alarms;
- equipment protection alarms;
- personal safety alarms;
- system alarms; and
- communication alarms, which can be regarded as a subset of system alarms.

Process alarms are initially identified at the process design stage, following a Hazard and Operability assessment. They are used to help keep the process pressures, temperatures, flows, etc., within their design and normal operating limits.

Safety related alarms are usually identified by SIL assessments or Layer of Protection Analysis (LOPA)

Environmental alarms are usually identified by the emissions/pollution limits placed on the process by the regulatory authority. These types of alarms can be problematic as they are often based upon cumulative measurements, which would normally exceed the 'time to consequence' required for an alarm.

Equipment protection alarms are usually specified by the manufacturer to help protect a specific piece of equipment from damage or catastrophic failure and may be a condition of any guarantee.

Personal safety alarms are usually specified by safety audits/reviews with the aim of warning the operator of a possible loss of containment or personal injury e.g. area gas detection, use of a safety shower.

Controls and instrumentation systems alarms are a form of equipment alarm but specifically for the BPCS itself and are usually provided by the manufacturer. This is particularly true of Fail-safe and High-availability systems which have a high degree of self-diagnostics built-in.

Other requirements within these categories may be initiated due to:

- requirements of safety or environmental authorities, insurers, headquarters departments, etc.;
- operating experience/feedback;
- simulator studies;
- incident investigations;
- as an alternative to automation ("It was cheaper than fitting a control system"); and
- task analysis¹¹.

These later requirements can often be informally structured design processes and experience shows that they lead to many poorly justified alarms being proposed. Ideally the whole design processes should be integrated and formally structured, but this may not be completely achievable. However, what is practical is to ensure that every proposed alarm is properly scrutinised. Thus:

Whatever its source, every alarm should be justified (safety, environmental or business needs), properly engineered and be consistent with the overall alarm philosophy and plant risk assessment.

The pertinent requirements for alarms are summarised in Appendix 2.

2.2.1 Alarms

A technical definition for the use of the word 'alarm' throughout this guide is provided in Appendix 18 but in the Concise Oxford English Dictionary it is simply defined as '**a warning of danger**' and it is this awareness of increased risk to personnel, environment or business that an alarm system should try to convey to the operator.

¹¹Task analysis⁽²⁴⁾ is a technique for formally breaking each of the operator's tasks down into a hierarchy of mental and physical actions and identifying the tools and information that the operator needs to perform these. Task analysis can also assist in deciding what tasks should be automated.

It is difficult for a human operator to be fully focused on the control system for an eight or twelve hour shift, especially as much of the work can be mundane and repetitive. Conversely it is difficult to differentiate the importance of individual alarms at a time of high stress.

The important initial result of a new alarm should be that of heightening the operator's awareness of loss potential.

It is for this reason that an alarm system should not be degraded by configuring it to alert operators of trivial state changes or regularly required actions. Therefore one of the most important decisions to be made when designing an alarm system is, at what point does an individual event cease to become an alarm.

As stated above 'The purpose of an alarm system is to direct the operator's attention towards plant conditions requiring timely assessment and action'.

What is meant by timely?

What potential consequences are included?

In the past the 'If in doubt make it an alarm' philosophy made many alarm systems much less effective in abnormal situations.

However, it is now understood that the limitation of an alarm system is the rate at which the operator can analyse and act upon the information being presented and not the rate at which the system can deliver alarms. Consequently, it is necessary to specify clearly which events are to be given the classification of alarm. This is particularly important for process plants, which are able to sustain an abnormal situation condition for some time.

To begin with, it could be reasonably specified that in normal/steady state operation an alarm setting should not be violated.

Any manual changes to an alarm setting should be controlled by a Management of Change system.

Further, a 'lower' limit to any prioritisation calculation method could be set (taking into account reaction time available and possible consequence), beneath which no alarm is required.

Some of the problems with this approach are that a number of events, which could and should in normal operation be annunciated, will not be included. It is for this reason amongst others that 'Alerts' have been developed.

Each user's Alarm Philosophy Document for the company/site should specify at what point an event ceases to become an alarm based upon the operator's ability to act and the possible consequential loss (safety, environmental or financial) and should instead be considered for annunciation as an Alert or Journal only.

2.2.2 Alerts

Operators today are constantly bombarded with a multitude of process-related tasks. Often they must simultaneously:

- monitor multiple process units;

- diagnose and mitigate abnormal situations; and
- recall and perform on-going tasks.

In addition, an operator must integrate alarm system interrupts, radio requests and process control requirements with normal unit monitoring. Such heavy demands can strain, and may even overload, an operator's attention. Process incidents can further tax even the most experienced operators, requiring them to put on-going tasks on hold until the event is mitigated.

In an effort to deal with this complexity and to manage multiple tasks, operators often use their alarm screens to notify them of pre-alarm conditions and to remind them of process events that need attention (prompts). Using the alarm displays in this manner may overload and clutter the system. Instead of resolving a difficult situation, this method often has the opposite effect – creating further difficulties. This situation has developed because operators have not been given tools that adequately keep pace with increasing process unit complexity.

2.2.3 The difference between an alarm, an alert and a prompt

From Section 2.2.1 it is noted that an alarm is used to attract the attention of the operator to significant changes that will require timely assessment and action. It will provide a layer of protection against loss, whether safety, environmental or financial.

An alert is used to attract the attention of the operator to changes that may require assessment or action when time allows.

An alert:

- Is not time critical (as defined by the individual organisation).
- Is not used as a formal layer of protection.
- Will not normally need covering by a Management of Change (MOC) system, if operator configurable.
- May be used as a prompt to alert the operator that a particular noteworthy event has been reached.
- Initiates a condition of heightened watchfulness or preparation for action.

A prompt is defined as a request from the control system that the operator perform some process action that the system cannot perform or that requires operator authority to perform.

2.2.4 Alerts as an alternative to control by alarms

With a screen based system it is possible that one operator will be responsible for more operating units than would have been practical using the control equipment which preceded it. It is also usual for new plants to have many more instruments installed and much more data available. With the classical panel controllers an operator would 'patrol' the panels to ensure that key process variables were within the limits of the operator's 'comfort zone' and that certain indicator lamps were illuminated or not, as required.

With screen based technology it is often tedious for an operator to survey all the variables and events being controlled and monitored by continually scrolling through all of the displays available.

'Alerts' are used to avoid the practice of 'control by alarms' and also to remove from the alarm displays the annunciation of normally expected events. They can be used by the operator to emulate the functionality of patrolling the panels and as an automatic notification of process dependant tasks being required.

The Alert System is a tool which can be used by the operators to alert themselves of a value or position in the process being reached and of which they would like to be notified.

On the continuous process model in Figure 11 an additional 'comfort zone' defined somewhere between the optimum and normal operating zones could be envisaged. The shape of this 'comfort zone' may differ for individual operators and operations and it is at the transition from the comfort zone to the normal operating zone that many of these alerts would be positioned.

In a batch process operation, most alerts would be expected at the transition of stages, operations or actions.

Although alarms and alerts have many similarities they are conceptually different.

- Alarms have limits which should not normally be violated.
- Alerts are a tool to be used by the operator.

The similarities between an alarm and an alert include:

- Operating limits can be defined.
- Violation of operating limits should be annunciated on a display or some other notification device (e.g. a pager, text message, email, etc.).
- The operator responds accordingly.

Differences include:

- Any alarm **should always be acted upon immediately** by the operator unless a higher priority alarm exists. Even if the action is only to decide that the problem does not require resolving immediately.
- 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 MOC or maintenance system.
- When an alert occurs it does not signify that the plant has moved outside of its normal 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.

2.2.5 Comparison of alarms, alerts and prompts

Some examples of the use of alerts are given below:

- An operator may set alerts to monitor a process variable deviation from desired set-point, which will warn them if the controller is failing to control within the limits (comfort zone), which they have defined.
- An operator may wish to set a level value on a vessel they are filling, which when reached by the product, will inform them of the event. This

setting would of course normally be below the fixed High-level alarms for the vessel.

- An alert may be used to inform the operator that a certain point of a process has been reached and a manual task is required or permission is needed to proceed to the next stage of the process.

Alerts, therefore, help the operator to run the plant more efficiently. Alerts should never be safety-related (in the IEC 61508⁽²⁹⁾ sense) or related to some other condition that has a serious impact on the plant or its surroundings – since such conditions are properly dealt with in the alarm or other protective system. 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 ignore them until all alarms have been dealt with. Notice also, that since alerts would often replace some of the low priority alarms that would otherwise have been used, the size of alarm floods are reduced, and can then be much more manageable.

In Table 4 it can be seen that prompts may be normally considered as alerts. An operator prompt which falls into the criteria required for an alarm should be considered for process redesign or automation. An expected event should be signalled to the operator long before it becomes time critical within the alarm definition. If the operator does not respond to the prompt for whatever reason then an alarm may be required as a backup.

Table 4 Comparison of alarms, alerts/prompts and journal only signals

	Display on chronological alarm list	MOC control required	Required to manage abnormal situations	Plant design limit violation	Layer of protection analysis (LOPA)	Operator reminder
Alarms	Yes	Yes	Yes**	Yes	Yes	No
Alerts / Prompts	No	No***	No	No	No	Yes
Journal only	No	No	No	No	No	No

**Unless suppressed.

***Alerts may come under a MOC system if they are not configurable by the operator.

		Action is required and is time critical within alarm priority defined boundaries	
		Yes	No
Expected	No	Alarm	Alert
	Yes	Prompt*	Prompt* Information Journal

*When assessed, the vast majority of prompts should fall outside of the alarm criteria set by the alarm management team although there may be a very few exceptions.

Alerts should not be presented to the operator in the same way as alarms. See Chapter 4 on HCI management techniques.

2.3 Risk assessment

2.3.1 The need to identify and minimise risks

Alarms are provided to reduce the likelihood of sub-optimal plant operation or of plant damage, as these may lead to injury to people, environmental damage and/or economic loss. It follows that the design and engineering of the alarm and alarm system should consider both the functional and integrity requirements relative to the level of risk they are intended to reduce.

In the European Union, national legislation implementing the Framework Directive 89/391⁽¹⁷⁾ requires employers to identify any hazards to people associated with their work activities and to assess the risks from these hazards. Many of the industrial systems covered by this Guide have potential for causing major accidents possibly resulting in multiple fatalities, and for these the assessment of risk will be particularly important.

Having identified potential hazards to people, every employer is also legally obliged to take steps to reduce the risks from these hazards to a tolerable level. In addition, a record of the risk assessment has to be kept, and it has to be reviewed as appropriate. Risk assessment is also a useful (and sometimes necessary) tool for identifying risks of environmental damage and economic loss, and reducing these to a tolerable level.

2.3.2 Risk reduction

Alarms are one of many tools which may be used to reduce risks to a tolerable level. Risk reduction should start with the initial plant design by selecting processes and plant configurations which have appropriate inherent safety and general risk reduction. For example, when designing a chemical plant, a production process might be chosen which avoided generation of hazardous intermediate products. The risk reduction should follow through into the detailed design of the plant where steps should be taken to eliminate hazards, protect against them, reduce their frequency of occurrence and minimise their consequences. These individual layers of risk reduction are brought together to provide a typical layers of protection model as shown below in Figure 7.

As shown, alarms can provide one of these layers of protection against risks, i.e. they sense conditions indicating increases in personal, environmental or economic risk and should result in corrective action being taken. Alarms can also be a significant part of the mitigation layer, where personal protection alarms such as Fire and Gas, may assist in executing the emergency procedures effectively. Where alarms are used, they are usually only one of several layers of protection against the specified risks. For example from Figure 7, there might be:

- **Plant design:** providing inherent safety improvements;
- **BPCS:** automatic control systems (BPCS) which act to maintain process variables within safe bounds;
- **Human Response:** alarms, operator information displays, manual controls and manual trips;
- **Instrument Response:** automatic protection systems;

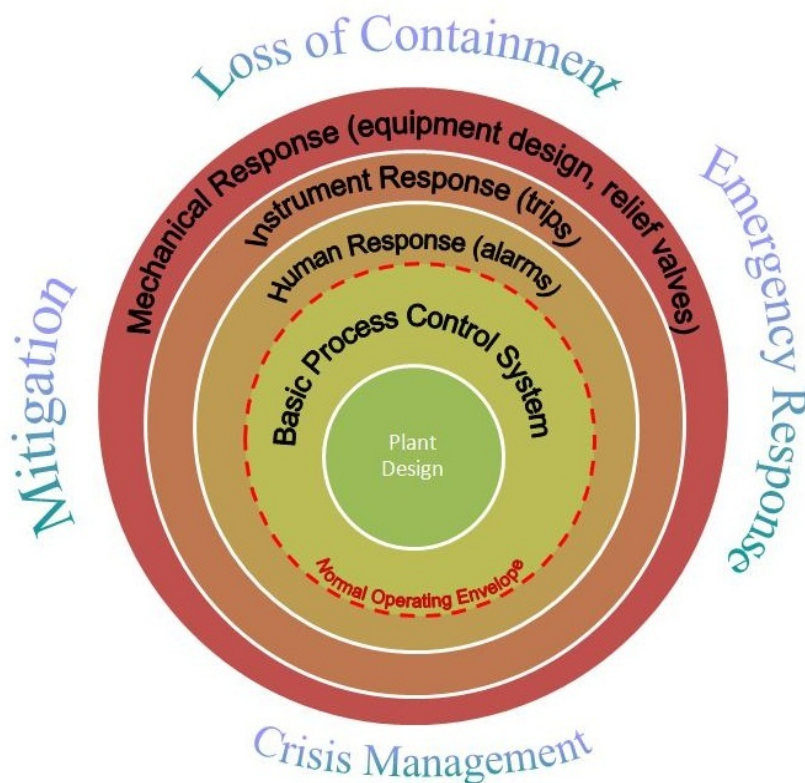


Figure 7 LOPA (Layer of Protection Analysis) diagram

- **Mechanical Response:** e.g. safety relief valves, bursting discs, etc.

And if all else fails, **crisis management, emergency response procedures, etc.** Together these systems should reduce the specified risk to a tolerable level. In this context, the alarm may be used to help avoid the event altogether and therefore reduce demand on the trip system. So although the alarm may not be SIL rated, it should, if properly managed, considerably reduce the demand rate on a demand mode trip system and in consequence reduce the required SIL level for the trip system.

If there is no automatic trip system available and the safety integrity is required to be at Level 1 or above then the alarm will become a **safety related alarm** and therefore the risk graph should not normally use an alarm in the initial SIL determination, as this would involve a common/dependant factor (the operator).

2.3.3 Safety related alarms - principles

Whilst the main focus of this Publication is concerned with non-safety related alarms, there are some situations where an alarm is classified as safety related. However, it should be noted that safety related alarms will be the exception, as the vast majority of alarms on most plant will not be safety related.

IEC 61508⁽²⁹⁾ is the generic international standard for functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems. This standard has been adapted for end users within the Process Industry Sector as IEC 61511⁽³⁰⁾. Many countries recognise such international standards, although there may be no specific legal requirement to apply them. However, in practice, any organisation that follows these standards will usually satisfy their

legal obligations through designing, operating and maintaining their safety related E/E/PE systems to an acceptable standard.

A safety related alarm system is an E/E/PE system under the definitions of IEC 61508 or IEC 61511. An alarm system should be considered to be 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. In such cases the average probability of failure on demand (PFD_{avg}) **of the overall safety function** must be lower than 0.1 and must comply with the requirements of IEC 61508 or IEC 61511. The overall safety function is defined as the means required to detect and rectify the potentially hazardous event and is implicit that **both the equipment delivering the alarm and the operator response are part of the safety related system** and hence they both should be considered within the scope of IEC 61508 or IEC 61511.

Before implementing any safety related alarm, consideration should always be given to providing an automated function:

- Automated response is considered to be higher in the risk control hierarchy since it does not rely upon procedures and instruction/training.
- This is particularly relevant for process alarms that require either fast corrective action or multiple complex actions to prevent the hazardous situation from occurring. In these cases the probability of the operator failing to take the corrective action quickly enough increases significantly to a point at which the criteria for achieving the PFD_{avg} cannot be met.
- Safety related alarms may be an acceptable alternative to an automated action in some instances, for example, where process trips may introduce some form of greater hazard themselves. Where such cases are justified, the design and ergonomics of the alarm and alarm system needs to be considered carefully.

Even where the time to respond is long, or there are multiple alarms or the alarm response is relatively simple, it is recommended that in no circumstances should a PFD_{avg} of less than 0.01 be claimed for any safety function which requires an operator action in response to an alarm.

Where multiple layers of protection require an operator to respond to an alarm, care must be taken to ensure that common/dependent failure modes of the operator are eliminated, for example by only making a single risk reduction claim for the operator.

2.3.4 Design and engineering of safety related alarms

As discussed, any alarm identified as being a safety related alarm must be designed and engineered in line with the requirements of IEC 61508 and/or IEC 61511. EEMUA Publication 222⁽⁵³⁾ also provides guidance on the application of IEC 61511 to safety instrumented systems.

Although this Publication is not intended to supplement the above publications, some general explanation and guidance on the issues surrounding this subject of safety related alarms may be useful.

As discussed above a safety related alarm should not be used for risk reduction factors above 100 (PFD_{avg} of less than 0.01). Therefore, a safety related alarm would normally fall into the category of a SIL 1 function.

SIL 1 requirement criteria has a PFD_{avg} of > 0.01 to < 0.1 , which can be expressed as a risk reduction factor (RRF) of > 10 to < 100 or in more practical terms an availability (reliability) of between 90%-99%. This means that at a minimum availability requirement of 90%, for every 10 alarm initiating events there should not be more than 1 failure of the system to respond correctly. For a maximum availability requirement of 99%, this rises to 1 failure in 100.

For automated equipment, this SIL 1 range of reliability appears to be very reasonable and easily achieved but from a human reliability point of view (see Table 5) a nine fold improvement in performance is significant and therefore any claim made for this type of SIL system much above a RRF of 10 will require a high level of managerial commitment to maintain.

Table 5 Human reliability requirements

Claimed PFD_{avg} of safety function	Alarm and final output system integrity / reliability requirements	Human reliability requirements
1-0.1 (standard alarm)	Alarm and final element systems may be integrated into the process control systems.	No special requirements - however the alarm system should be operated, engineered and maintained to the good engineering standards identified in this Guide.
0.1-0.01 (safety related alarm)	- Alarm and final element systems should be designated as safety related and categorised as implementing SIL 1 safety functions (Safety Integrity Level 1 as defined in IEC 61508). - Alarm and final element systems should be independent from the process control system (unless this has also been designated as safety related).	- The operator should be trained in the management of the specific plant failure that the alarm indicates. - The alarm presentation arrangement should make the claimed alarm very obvious to the operator and distinguishable from other alarms⁽²³⁾. - The alarm should be classified at the highest priority in the system. - The alarm should remain on view to the operator for the whole of the time it is active. - The operator should have a clear written alarm response procedure for the alarm. - The required operator response should be simple, obvious and invariant. - The operator interface should be designed to make all information relevant to management of the specific plant failure easily accessible. - The claimed operator performance should have been audited.
Below 0.01	Alarm and final element systems would have to be designated as safety related and categorised as implementing SIL 2 (or higher) safety functions.	It is recommended that claims for a PFD_{avg} below 0.01 are not made for any safety function which relies upon operator action even if it is multiple alarmed and very simple.

System reliability requirements relate to the whole system and not just the hardware and with this in mind, the safety related alarm system can be broken down into four stages as shown in the conceptual model below, Figure 8.

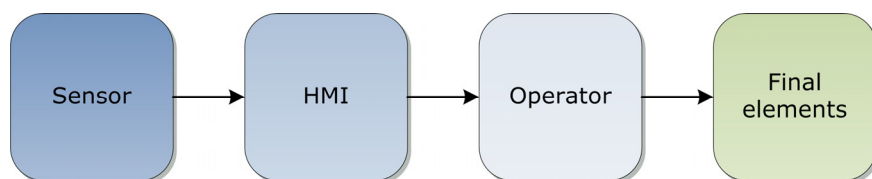


Figure 8 Safety related alarm reliability requirements

From this model it can be seen that for the risk reduction to be achieved, the sensor must detect the event, the HMI must announce the event, the operator must take the correct action in a timely fashion to contain the event and finally the elements required to carry out the actions must work and be independent of other protective layers.

As can be seen, the probability of failure depends both on the reliability and integrity of the equipment, in this case, the sensor, HMI (including alarm processing) and final elements, all of which are relatively straightforward to assess. But it also depends on the reliability and integrity of the operator to see and respond to the alarm with the appropriate action, which is not so easy to assess.

Experience has shown that the majority of failures of alarm systems derive from human errors rather than from hardware failures. The probability of success of the human response can be greatly increased by improving the ergonomics of the operator interface. Although alarm hardware integrity is important, risk reduction benefits are generally more easily derived from improving usability than from improving hardware integrity.

From this perspective, the operator response can itself be further broken down into four stages as shown in Figure 9:-

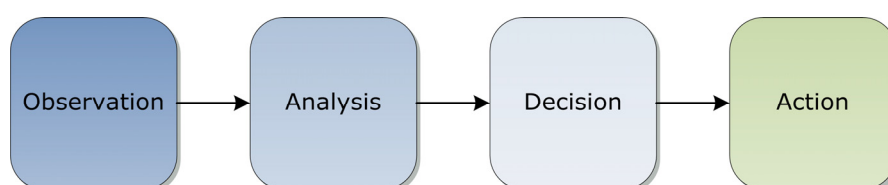


Figure 9 Operator response stages

Again all four stages have to succeed for the operator response to be successfully delivered:

- **Observation (Awareness)** – the timely receipt of information.
- **Analysis** – using the available information (including probably both the alarm and supporting information from the control panel indications) to determine what state the plant and process is in.
- **Decision** – using the results of the analysis to decide what action(s) to take.
- **Action** – delivering the action(s) decided upon.

Taking each of these four stages in turn:-

Stage 1 Observation. The likelihood of the operator failing to observe the alarm on the HMI needs to be assessed. On a small, well managed system with the alarm having the highest priority and always visible to the operator it might be reasonable to expect the alarm to be observed every time. On a large, poorly managed system with poor prioritisation and HMI design, it would be reasonable to expect that the operator might miss the significance of the alarm during periods of high stress.

Success at this stage will primarily depend upon a well-managed working environment, HMI design and alarm rationalisation regime, such that an operator:

- is always present in the control room;
- is aware that the alarm is part of their area of responsibility; and
- will not ignore the alarm at times of high stress.

and that the safety related alarm is:

- of the highest priority;
- is obviously a safety related alarm;
- is not degraded in visibility over time;
- is not degraded by becoming a nuisance alarm; and
- is not shelved/suppressed without authorisation and mitigation.

Stage 2 Analysis. If the level of analysis is simple and no additional data is required the immediate problem should be easily identified. Therefore this and the following stage should have a predetermined written response so that the operator only has to carry out Stages 1 (Observation) and 4 (Action). This will reduce the overall response time and minimise any errors associated with diagnosing and reacting to the potential problem.

Stage 3 Decision. Once the problem is identified, the decision on what action to take should be uncomplicated and well defined.

Stage 4 Action. It should be ensured that, following the alarm, all actions required are easily and safely achievable within the time to consequence and under all reasonably expected operating conditions.

As for any safety instrumented function, the overall assessment of residual risk should include and take into account a common cause failure analysis. The protective equipment should be independent of the control equipment to eliminate common cause failure that could lead directly to a hazardous event through a single failure. Similarly, dependency will exist for a safety related alarm where the operator forms both an integral part of the control function and responds to the alarm.

The independence of the hardware must also be assessed for common cause failure. Sensors that form part of the safety related alarm should be independent from the control sensors including the point or process connection at which the measurement is taken from. The safety related alarm annunciator including power supply must have sufficient integrity in order to prevent a single failure from compromising the control and respective safety function.

2.3.5 Proof testing

Figure 10 summarises the proof testing process for safety related alarms.

Periodic proof testing should cover:

- Confirmation that the plant sensors and alarm system correctly delivers the alarm to the operator interface.
- Confirmation that the operator can be expected to respond in the correct manner through steps such as the provision of documented procedures, refresher training and periodic assessment and accreditation.
- Confirmation that the operator acknowledges the alarm and responds correctly. This can be achieved through scenario testing and checking the operator response against the documented procedures.
- Periodic re-validation that the alarm system is still properly set-up and the overall rate of alarms and the rate of spurious and nuisance is still acceptable.

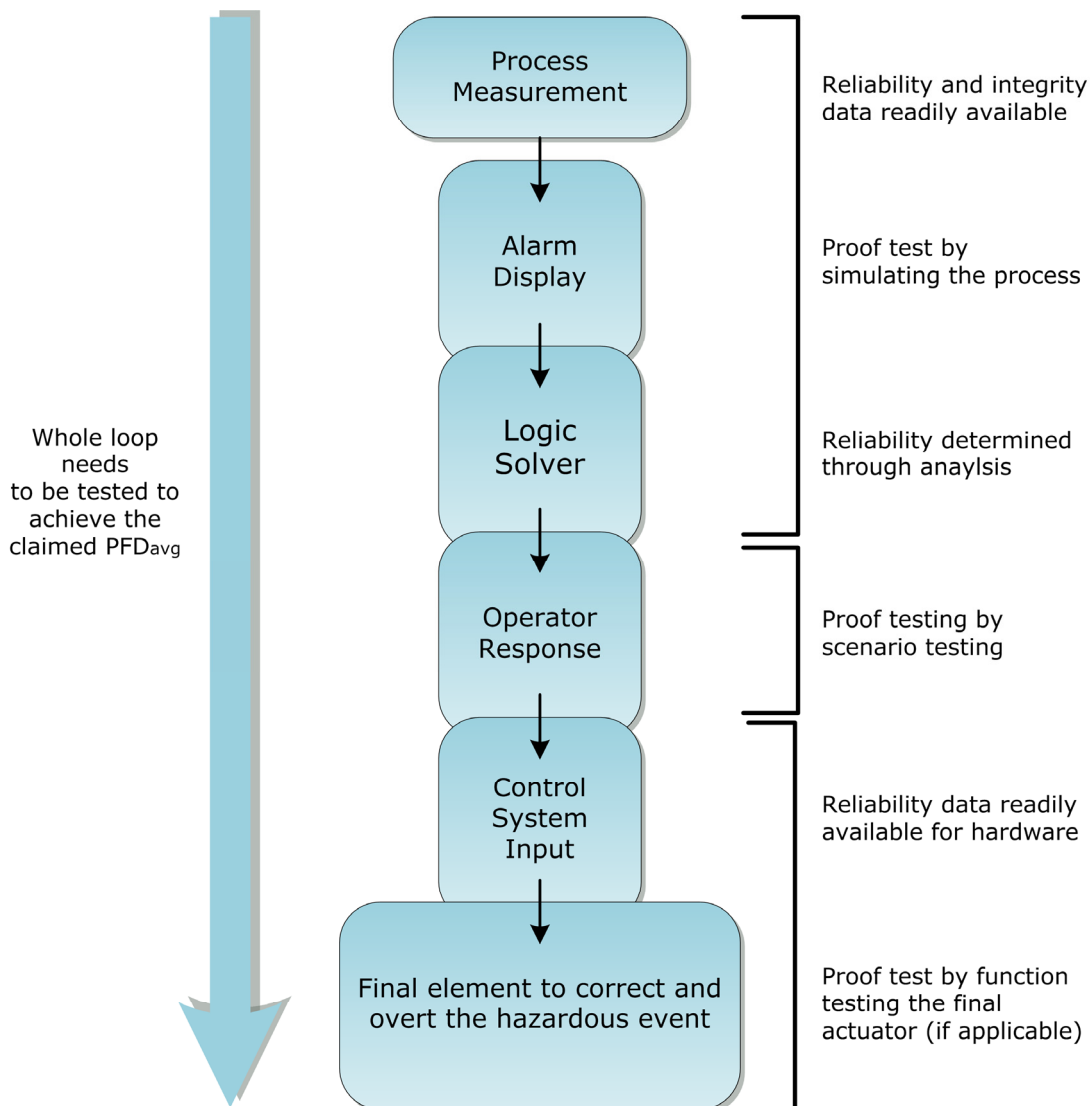


Figure 10 Proof testing of safety related alarms

Unlike automated safety instrumented functions, an alarm complete with response cannot be configured to be fail safe and therefore procedures must be in place to ensure the continued safety of the process plant if a safety related alarm were to fail. For a non-fault tolerant system the requirement is to shut down the system unless an equivalent risk reduction measure can be applied and the repair is carried out in the assumed mean time to repair.

However, there may be other means of protection such as a pressure relief valve and in such cases the unit can continue to operate but should still be shut down if the repair has not been carried out within the mean time to repair.

As for any alarm but particularly relevant for safety related alarms, special effort should be made to avoid spurious alarms as this is likely to reduce credibility and impact the response needed to deal with a genuine demand.

2.3.6 Summary

There are two main ways in which an alarm can be used to reduce risk.

The first is as an aid to reducing the demand on a SIL rated automated trip system and the second is as an alternative to an automated trip system.

The additional human reliability requirements in Table 5, graded by the PFD_{avg} associated with the alarm function, are appropriate for such alarms. It may also be useful to have additional aids such as a reactivation facility which allows the alarm to be repeated if it has not been cleared within a reasonable time following the first alarm. For an alarm providing risk reduction, especially where this is >10 , the following should be considered:

- That the sensor is independent of the SIS and facilities are provided to alert the operator that the SIS has failed.
- That the HMI has high availability and is well (consistently) designed.
- That the alarm system is rationalised.
- The alarm is not a 'nuisance' alarm.
- The analysis and decision stages are well defined.
- The action required is simple to execute and easily achievable within the time constraints available.
- Independent facilities are provided to shutdown such that the hazard can be avoided or which enable all persons to escape to a safe area.
- The time between the operator being alerted and a hazardous event occurring is sufficient for the necessary actions.

2.4 Generation of alarms

2.4.1 Types of alarms

Alarm detection should provide early warning that there is a problem requiring operator intervention whilst minimising unnecessary or nuisance alarms. To achieve this, the most appropriate alarm detection mechanism should be chosen for each parameter. Some methods used for detecting alarms are:

- **Absolute alarms:** generated by comparison of an analogue signal against a defined alarm setting. Typically used to warn of the parameter approaching an absolute limit such as a trip or safety-valve setting. These

are simple to engineer, but tend to cause difficulty in abnormal operational situations. They may need conditioning to take account of plant operating state. The setting of absolute alarms is discussed further in Section 2.4.2.

- **Bit-pattern alarms:** alarms generated when a pattern of digital signals matches a predetermined pattern.
- **Calculated alarms:** generated in software from applications such as modulating controls, batch and sequential controls, efficiency calculations, etc., and often based on logical combinations of several signals. Ideally it should be possible for the application software to dynamically alter alarm settings, priorities, deadbands, etc.
- **Control and instrumentation system alarms:** generated from faults within the control and instrumentation system hardware or software. These can be useful, but care should be taken that they are relevant to the operator and easily understood by the operator. These are commonly misused. Note that it may be desirable to be able to separate the display of these system alarms from the process alarms.
- **Deviation alarms:** generated if the difference between two analogue signals exceeds a certain size. Typically used to compare a controlled variable against the controller set point and to warn that the control system is failing to operate effectively. Care should be taken that the alarm is not generated during large plant disturbances when the control system is doing the best it can, but the control error is large. To avoid this, they may need to incorporate time windows or time delays. The alarms may also need to take account of whether a control loop is selected to automatic or manual operation.
- **Discrepancy alarms:** generated by comparing an expected plant state against an actual plant state.

Discrepancy alarms are often applied to actuators. This requires some model of the expected movement of the actuator in response to movement commands from the operator or from automatic controls or sequences. The model may be fairly crude, e.g. the actuator should always show the correct state (i.e. open or closed) within 10 seconds of a command being sent to it, or may be more sophisticated with actuator slew rate parameters and deadbands in it. A good discrepancy alarm check will identify faults such as stuck actuators or actuator runaway.

In practice, actuators tend to degrade or not perform as modelled and spurious discrepancy alarms can be generated. For example, an actuator may get sluggish and take 12 seconds to close rather than the assumed 10 seconds. Spurious discrepancy alarms can be a nuisance, particularly if there is a large upset affecting the whole plant and many actuators simultaneously generate spurious alarms. Consequently, discrepancy alarms should be designed to be as robust as possible. It is also desirable to have simple procedures for widening tolerance bands in discrepancy alarms on actuators that are slightly degraded and are awaiting maintenance.

- **Rate-of-change alarms:** generated by the rate of change of an analogue signal exceeding a defined setting. These can often provide an early indication of an upset. However, they should be used with great care since noise on the signal tends to be amplified and can result in spurious alarms. Thus, they may need to incorporate time windows or time delays.

Some more advanced alarm detection or modification mechanisms are:

- **Adaptive alarms:** generated using the 'rate-of-change' or 'deviation' principle in combination with absolute thresholds. Where the parameter is well clear of the absolute threshold, the allowable rate-of-change or deviation is relaxed; as the parameter approaches the absolute threshold, the limits on rate-of-change or deviation are tightened.
- **Adjustable alarms:** absolute alarms in which the alarm settings are adjusted to suit operating conditions. This can be done automatically according to some predefined logic. For example, vibration alarm settings on a rotating machine might be made a function of speed, or boiler steam temperatures alarms might be made a function of operating load.
- **Recipe-driven alarms:** alarms that are turned on or off in different plant states, typically by some type of sequence controller. An example might be an alarm for a batch plant that is made active in particular operational phases.
- **Re-triggering alarms:** alarms which are automatically re-annunciated to the operator in certain conditions. This might be when the alarm has been standing for more than a predefined time setting, or when the alarmed variable had moved significantly above its setting. Thus, a high pressure alarm might be set to be raised at 100 bar and to re-annunciate for every 5 bar increase above this (i.e. at 105 bar, 110 bar, etc.).
- **Statistical alarms:** generated by some statistical process to filter out significant changes from process noise.

For the purposes of clarity another term is explained:

- **First-up alarms:** these are not strictly a type of alarm, but are a facility for examining the order of occurrence of alarms. Typically a first-up system would be used to identify the cause of plant item trips. For example, a pump might be tripped by a low flow switch or by loss of power to the motor. If the pump trips, the motor will stop and the flow will drop very quickly, so both a 'motor stopped' and a 'low flow' alarm will be generated. The time difference between them will be fractions of a second, and this will be difficult to resolve with many commercial alarm systems. Fast scanning logic allows the first alarm after the trip to be identified, and hence the cause of the trip to be determined. Some commercial alarm annunciator systems have facilities for displaying first-up alarms built into their hardware functionality. For example, a number of alarms may be put into a first-up group. The first alarm raised in the group might be indicated by a flashing light, the subsequent alarms by a steady light.