

Contents

About the Author	vii
Foreword	xxix
Acknowledgments	xxxix
Credits	xxxix
Introduction	xxxix
Not a Handbook	xxxix
Audience	xxxix
Usefulness	xxxix
Contents	xxxix
Part I: The Alarm Management Problem	xxxix
Part II: The Alarm Management Solution	xxxix
Part III: Implementing Alarm Management	xxxix
Book Deliverables	xxxvii
Important Word	xxxvii
Note	xxxvii

<i>Part 1: The Alarm Management Problem</i>	1
---	---

Chapter 1: Meet Alarm Management	3
1.1 Key Concepts	4
1.2 Alarm Performance Problems	5
Symptoms	5
Evidence	5
1.3 Reasons for Alarm Improvement	6
How Alarms Fit into Process Operating Situation	6
Alarm Management	8
Benefits	8

1.4 A Brief History of Alarm Management	10
1.5 The “Management” in Alarm Management	11
1.6 Alarm Design Roadmap	12
1.7 Audience for this Book	13
1.8 Importance of Alarm Management	13
1.9 Fundamentals of Alarm Management	15
Bottom Line of Alarm Management	15
Fundamentals	15
Operator Action	17
Importance of the Fundamentals	18
1.10 Design for Human Limitations	19
1.11 Alarm Management and Six Sigma	19
1.12 Controls Platforms	21
PLC versus DCS	21
PLC Special Considerations	22
1.13 Continuous versus Discrete and Batch	22
1.14 Application Effect on Alarm Design	23
1.15 Time and Dynamics	24
1.16 Historical Incidents	27
Three Mile Island	27
Milford Haven	28
Texas City	29
Why Now?	30
1.17 The New Design	31
Not by Subtraction Alone	31
Starting Alarm Improvement	32
Alarm Philosophy	32
Data Gathering and Analysis	32
Alarm Conventions and Redesign Guidelines	36
1.18 Example Alarm Redesign (Rationalization) Results	38
1.19 Completing the Design	39
Advanced Techniques	39
Situation Awareness	39
Operator Screen Design	40
Operational Integrity Improvement	40
Condition Monitoring	41

1.20 Alarm Improvement Projects	41
1.21 Lessons for Successful Alarm Management	42
1.22 Important Design and Safety Notice	43
1.23 Conclusion	43
1.24 Notes and Additional Reading	44
Notes	44
Recommended Additional Reading	44
Chapter 2: Abnormal Situations	47
2.1 Key Concepts	48
2.2 Introducing Abnormal Situations	49
Two Scenarios	49
The Two Sides of Abnormal Situations	50
2.3 Observing Abnormal Situations	51
2.4 Understanding Abnormal Situations	53
2.5 Understanding Incidents	55
General Concepts Learned	55
Your Plant Data	55
2.6 General Lessons from Incidents	56
Examination for Cause	57
Hazards Defined by the FAA	60
Two Events	61
2.7 Critical Contributors to Incidents	61
Subtle Abnormalities	61
The Human Nature of Operators	62
Stop in Time	63
2.8 The Importance of Time	63
An Example	63
Process Safety Time	65
SUDA	66
Alarm Activation Point and Time	67
2.9 Why Abnormal Situations Are Important	67
2.10 Message of Abnormal Situations	69
State of Control Loops	70
The Magic in a Control Loop	71
Abnormal Situations in Perspective	72

2.11 Notes and Additional Reading	73
Notes	73
Recommended Additional Reading	73
Chapter 3: Strategy for Alarm Improvement	75
3.1 Key Concepts	76
3.2 How We Got Ourselves into Trouble	76
Controls Technology Evolution	77
How We Think	78
The Way Forward	79
3.3 The Alarm Management Problem	80
Symptoms	80
Root Causes	81
A Good Alarm	81
So Many Alarms, So Little Time	81
Benefits of Rationalization	82
3.4 Alarm Activation Path	83
3.5 The Geography of Alarm Management	84
Plant Area Model	84
Smallest Area of Rationalization	86
3.6 Alarm Improvement Teams	87
Representation	87
Local Teams	88
Site Team	89
Large Corporate Team	90
3.7 Alarm Improvement Projects	90
3.8 Standards and Regulations Overview	92
Best Practices Summary	92
Key Messages	93
Guides, Standards, and Regulations	93
3.9 Proposed Regulations	94
Department of Transportation (United States)	94
3.10 Standards and Guides	94
EEMUA 191	95
NAMUR (Germany)	96
ISA 18	98

OSHA (United States)	99
HSE (UK)	100
EPRI (United States)	100
Remarks	101
3.11 Conclusion	101
3.12 Notes and Additional Reading	101
Notes	101
Recommended Additional Reading	102
Chapter 4: Alarm Performance	103
4.1 Key Concepts	104
4.2 Alarm Problems	104
4.3 Alarm Performance Assessment	105
4.4 Alarm Metrics and Benchmarks	105
Why Have Metrics?	106
Plant Area of Focus—A Single-Operator Area	107
Basic Configuration Metrics	107
Basic Activation Metrics	109
4.5 Alarm Assessment Tools	110
Why Use a Tool?	111
Characteristics of Good Tools	111
Tool Providers	111
Getting the Data In	113
Configuration Data	113
Activation Data	114
4.6 Configuration Analysis	116
4.7 Activation Analysis	118
Activation Analysis across Industrial Segments	119
Deriving Implications from Activation Analyses	119
Acknowledgment Ratio	121
Time to Acknowledge	121
Time to Clear	122
Alarm Flood	122
Chattering and Repeating	122
Related and Consequential	123
Standing and Stale	123

Nuisance Alarms (Bad Actors)	123
4.8 Advanced Activation Analysis	126
4.9. Alarm Correlation Analyses	126
Situations	126
General Comments	128
4.10 One Day in the Life of an Alarm System— Configuration	128
Number of Tags and Tags with Alarms	129
Number of Alarms by Alarm Type	129
Priority of Configured Alarms	129
Duplicate Alarms	130
4.11 One Day in the Life of an Alarm System—Activation	132
The Raw Data	132
Amount of Data Produced in One Day	134
Alarm Activations	134
Time in Alarm	135
Time to Acknowledge	137
Operator Actions	137
4.12 Alarm System Performance Levels	139
4.13 Conclusion	140
4.14 Notes and Additional Reading	140
Notes	140
Recommended Additional Reading	141
 <i>Part 2: The Alarm Management Solution</i>	 143
Chapter 5: Permission to Operate	145
5.1 Key Concepts	146
5.2 Management's Role	146
5.3 Operating Situations	147
Operating in Uncertainty	147
Unique Events	147
Explosive Events	148
Definitions	149
5.4 How Permission to Operate Came to Be	149
5.5 How Permission to Operate Works	150

5.6 Permission to Operate	150
5.7 Alternative Methods for Granting Permission	151
De Facto Decisions	151
Operating Modality Decisions	152
5.8 Managing the Operator's Permission	153
Qualifying Abnormal	153
No Help at Hand	153
Observer Evaluation	154
Operator Evaluation	154
Putting It All Together	156
5.9 Shut Down and Safe Park	156
Operator-Initiated Shutdown	157
Automated Shutdown	157
Safe Park	158
5.10 Special Technology	158
Detection and Warning of Abnormal Conditions	159
Conditions Related to the Plant	159
Conditions Related to the Operator	159
5.11 Operator Redeployment	160
5.12 Process Complexity	163
Linearly Related Complexity	164
Integrated/Complex Related	164
5.13 Training and Skills	165
Industrial Manufacturing	165
Military Training	166
5.14 Other Key Principles of Operation	167
Additional Operating Principles	167
Field Principles	168
Safety System Principles	168
Design and Inspection Principles	168
Management Principles	168
5.15 What Is Being Done by Others	169
Technology in Development	169
5.16 Conclusion	169
5.17 Notes	170

Chapter 6: Alarm Philosophy	171
6.1 Key Concepts	172
6.2 Caveats	172
A Foundation Is at the Bottom	172
Owner versus Designer	173
Reliance on Philosophy	173
Completeness	173
6.3 Getting Started	173
Operator Survey	174
Advice to the Reader on Timing of This Topic	174
6.4 Special Alarm Issues	175
Types of Alarms and Their Recommended Use	175
Smart Field Devices	176
Light Boxes	176
Special Cases of Redundant Alarms	176
About Alerts	177
Classes of Alarms	178
6.5 Overview of Alarm Philosophy	178
Philosophy 101	178
Operator-Centric Items	179
Plant-Centric Items	179
Alarm System Purpose	180
Philosophy Intent	181
Elements in the Philosophy	182
6.6 Alarm Priority	183
Priority Levels	184
Priority Names	186
Humorous Illustration of Priority	187
Consequence and Severity	187
Urgency	190
Priority Assignment	192
Alarm Priority Assignment Setup Review	192
6.7 Enterprise Philosophy Framework	193
Overview	194
Framework Philosophy Document	196
At the Enterprise Level	196

Factoring It All into the Philosophy	198
6.8 Site-Level Philosophy	198
Site Personality	199
The Rest of the “Bases”	200
6.9 Alarm Design Principles	200
Fundamental Principles	201
Functional Principles	202
Key Performance Indicators	202
Critical Success Factors	203
Approved Management of Change Requirements	204
Procedure for Rationalization	204
Alarm Configuration: Specific Issues	204
Alarm Activation Point Determination	205
Priority Assignment	205
Alarm Presentation	205
Operator Roles	205
Interplay with Procedures	206
Training	207
Escalation	207
Maintenance	208
6.10 Example Procedure: To Silence or to Acknowledge	208
6.11 Philosophy Hit List	211
6.12 Alarm Philosophy Workshop	212
Workshop Details	212
Facilitation	216
Preparation	216
6.13 Enterprise Philosophy Framework	218
6.14 Conclusion	218
6.15 Notes	219
Chapter 7: Rationalization	221
7.1 Key Concepts	221
7.2 Introduction	222
Basic Approaches	223
Cornerstone Concepts of Alarm Management	224
7.3 About the Word “Rationalization”	226

7.4 Checklist	226
7.5 Getting Ready to Rationalize	227
Housekeeping	227
Bad Actors	228
Filters and Deadbands	229
The Data	231
Alarm Documentation and Rationalization Tools	231
Rationalization Is Not Just About Numbers	232
7.6 Alarm Response Manual	233
Header Information	233
Configuration Data	234
Causes	234
Confirmatory Actions	236
Consequences of Not Acting	236
Automatic Actions	237
Manual Corrective Actions	237
Safety-Related Testing Requirements	237
Example Online Alarm Response Sheet	237
Additional Items	239
7.7 Rationalization Methods	239
Alarms Are Not the Important Part	239
Rationalization Approaches	240
“Starting from Where You Are” Rationalization	240
“Starting from Zero” Rationalization	241
7.8 Required Alarms and Common Elements	243
Required Alarms	243
Common Elements	243
7.9 “Starting from Where You Are” Rationalization	244
Work Process	244
7.10 “Starting from Zero” Rationalization	246
Work Process	247
Wrap-Up	249
7.11 Only Four Alarms	249
7.12 Identifying Subsystem Boundaries	251
Decomposition	251
7.13 “Starting from Zero” Examples	256

Furnace	256
Heat Exchanger	257
7.14 Working Through the Database	259
Method of Flows	260
Method of Elements	261
Choosing a Method	262
7.15 The Alarm Activation Point	263
Alarm Activation Point Determination	264
A Digression in Setting Alarm Activation Points	266
The Limit of Alarm Limits	267
Generalizing Alarm Activation Point Calculations	269
Too Much Time; Just Enough Time	270
Alarm “Pick-Up” Order	271
7.16 Determining Alarm Priority	275
Assigning Priority	276
Calibrating the Alarm Priority Assignment Process	278
Nonweighted Maximum Severity with Urgency Direct to Priority	280
7.17 Alarm Priority Assignment Examples	283
Sum of All Severities	283
Sum of All Severities Weighted by Urgency	284
Maximum Severity	285
Urgency Only	285
Maximum Severity Weighted by Urgency	286
Summary of Examples	286
7.18 Rationalization Working Sessions	287
Teams	287
Participant Preparation	289
Work Areas	289
Work Sessions	290
Events Schedule	291
7.19 Partial Rationalizations	293
Concepts and Experience	293
Bad Actors	294
Rationalize Only Important Parts of the Operator’s Area	294

Rationalize Only Alarms that Activate	295
Bottom Line	296
7.20 Conclusion	297
7.21 Notes and Additional Reading	297
Notes	297
Recommended Additional Reading	297
Chapter 8: Enhanced Alarm Methods	299
8.1 Key Concepts	300
8.2 Beginning	300
8.3 The Situation	302
8.4 Safety Notice	303
Operator Awareness	303
Monitoring	304
Unsafe Operations	304
8.5 Enhanced Alarm Functions	304
8.6 Enhanced Alarm Infrastructure	306
General Considerations	306
Alarm Processors	306
Basic Infrastructure	306
Enhanced Infrastructure	307
Alarm Integrity Monitoring	307
8.7 Operator Consent	307
Implement Automatically	308
Implement Unless Cancelled	309
Suggest with Positive Response Required	309
Suggest Only	310
8.8 Operator-Controlled Suppression Techniques	310
8.9 Preconfigured, Simplified Suppression Techniques	312
8.10 Informative Assistance	314
When Informative Assistance Is Useful	314
How to Do It	315
Examples	316
More Examples	318
8.11 Knowledge-Based	319
Pattern Recognition	320
Neural Networks	321

Fuzzy Logic	322
Knowledge-Based Reasoning	323
Model-Based Reasoning	324
8.12 Keeping Track of Plant State	325
Explicit Plant States	326
Implicit Plant States	326
8.13 Alarm Information without Alarm Activation	327
Plant Area Model	328
Conditional Alarming Facilitators	329
8.14 Alarm Activation Permissions	330
Category I Alarms	331
Category II Alarms	332
Category III Alarms	332
8.15 Conclusion	332
8.16 Notes and Additional Reading	333
Notes	333
Recommended Additional Reading	333
 <i>Part 3: Implementing Alarm Management</i>	 335

Chapter 9: Implementation	337
9.1 Key Concepts	337
9.2 Beginning	338
9.3 Implementation Steps	339
Approvals	339
Configuration	340
Enhanced Alarm Features	340
Process Graphics and Other Displays	341
Procedures	341
Training	341
Documentation	341
Infrastructure	342
Operability Review	342
Final Approval	342
9.4 Implementation	343
Simulators and Training	343
Cutover and Testing	343

Moving On	343
9.5 Conclusion	343
Chapter 10: Life Cycle Management	345
10.1 Key Concepts	345
10.2 Assess Alarm Performance	346
Initial Assessment	347
Periodic Assessment	347
Timing of Assessments	347
Collection of Data	348
Every Alarm Activation Points to Opportunity	348
10.3 Interpretation of Periodic Assessments	349
Evaluate	349
Look for Added Benefits	349
Modify and Repair	350
Monitor and Enforce	350
Nuisance Alarms	350
Alarm Creep	351
Adding and Removing Alarms	352
10.4 Advanced Interpretation of Periodic Assessments	352
Nomenclature and Design	352
Value	354
Cases	354
10.5 Statistical Process Control and Alarm Management	364
Background	364
Relevance to Alarm Management	365
Guidance	366
10.6 Enforcement	367
Enforcement by Shift	368
Periodic Enforcement	369
Aperiodic Enforcement	369
10.7 Notes	369
Chapter 11: Project Development	371
11.1 Key Concepts	372

11.2 The Fit of Alarm Improvement	372
11.3 The Business Case	373
Percentage of Daily Losses	374
Direct Calculation	375
Negotiation	375
Bottom Line	376
11.4 Project Design Approaches	376
Alarm Improvement by Starting from Where You Are	377
Alarm Improvement by Starting from Zero	378
Usefulness of Stages	381
11.5 Project Construction Alternatives	381
Sitewide, Comprehensive	382
Sitewide, Staged	383
Sitewide, Unit-by-Unit, Comprehensive	383
Review	384
11.6 Why Some Projects Fail	385
11.7 “Low-Hanging” Fruit	386
11.8 Conclusion	387
Chapter 12: Situation Awareness	389
12.1 Key Concepts	390
12.2 Operator Support Needs	390
The Hat	390
The Disaster Chain	391
Need for Situation Awareness	393
Visualizations	394
12.3 The Deviation Diagram	394
12.4 User-Centered Design—Human Factors	396
Human Factors Details	396
Environment	396
Scaling	397
Compensation	398
Understandability	398
Implementability	398
Unified Feel	399

12.5 Our Biological Clock	399
12.6 Other Operator Support Issues	400
Intent Recognition	401
Operator Vigilance	401
To Push or to Pull	402
12.7 Operator Displays	403
Physical Display Architecture	403
Modern Displays	405
Hierarchical Display Architecture	406
The Overview Level	409
The Secondary Level	410
The Tertiary Level	411
12.8 Navigation	413
12.9 Notifications Instead of Alarms	415
12.10 Perception Problems with Video Displays	416
Relationships and Size	417
Coding Conflicts	418
Color	420
Comments	426
12.11 New Operator Display Design	427
Coding Schemes and Icons	427
Overview Level	429
Secondary Level	430
Tertiary Level	433
Do ASM-Style Displays Work?	434
12.12 Wrap-Up	435
12.13 Notes and Additional Reading	436
Notes	436
Recommended Additional Reading	436
Appendix 1: Definitions of Terms, Abbreviations, and Acronyms	439
Appendix 2: Twenty-Four Hours of Alarms	452
Appendix 3: Operator Alarm Usefulness Questionnaire	501
A3.1 Operator Alarm Usefulness Questionnaire	502

Explanation	502
Purpose	502
General Instructions	502
Confidentiality	502
Surveyors	503
Additional Information If You Have Questions	503
Where Questionnaire Is to Be Returned	503
Operator Alarm Usefulness Questionnaire	504
Normal Steady Operation	506
Plant Faults and Trips	508
General	515
A3.2 Quiet Period Alarm Usefulness Questionnaire	517
Explanation	517
Instructions	517
Column Definitions	517
Survey Data Table	518
Summary	519
Appendix 4:	
Alarm Philosophy from Honeywell European Users	521
Appendix 5:	
Overview of <i>Alarm Management for Process Control</i>	537
A5.1 The Chapters	538
Part I: The Alarm Management Problem	538
Part II: The Alarm Management Solution	541
Part III: Implementing Alarm Management	544
Appendix 6: Alarm Response Sheet	547
Appendix 7: Metrics and Key Performance Indicators	549
Part I: Recommended Requirements for Analysis Tools	549
A7.1 Purpose	549
A7.2 Background	549
A7.3 Analysis Types	550
A7.4 Queries	551
A7.5 Alarm Remediation Analyses	555
A7.6 Tools and Key Features	558

Part II: Metrics	561
A7.7 Introduction	561
A7.8 Static (Configuration) Metrics	562
A7.9 Dynamic (Activation) Metrics	564
Appendix 8: Alarm Management Pioneers	567
A8.1 Opening Notes	567
Father of Modern Alarm Management	567
A8.2 Alarm Management Taskforce	567
Pioneering Members	568
Objectives for Work	570
A8.3 Abnormal Situation Management Consortium	570
Key Players	571
Objectives for Work	572
A8.4 Additional Credits	572
Standards and Practice Organizations	572
Trainers and Consultants	572
Services Providers	572
Technology Providers	572
Industrial Controls Providers	572
Personalities at Large	573
A8.5 Note	573
Appendix 9: Qualitative Risk Method for Priority Assignment	575
Acknowledgment	575
A9.1 Qualitative Risk	575
A9.2 Porter's Discussion on the Rationales for the Qualitative Risk Matrix for Alarm Prioritization	576
Goal	576
Scope	576
A9.3 Description of Matrix	576
Probability Axis	576
Severity Axis	578
A9.4 Definition of Priorities	578

Appendix 10:	
Manufacturing Modalities and Alarm Management	583
A10.1 Introduction	583
A10.2 Characteristics of Manufacturing Modalities	583
A10.3 Comparison Matrix	585
Appendix 11: Notifications Management	589
A11.1 Introduction	589
A11.2 Points to Consider	590
A11.3 Questions and Issues	591
Index	593

Foreword

The control room of a process plant is by turns either a boring or terrifying place, much like the cockpit of a fighter jet or a large passenger aircraft: “hours of boredom punctuated by moments of sheer terror,” as the old aphorism goes. The boredom comes from processes running properly. The terror comes when they do not. And, as the litany of process plant disasters shows, after the terror sometimes comes picking through the ruins, looking for bodies.

What we’ve learned in a generation of studying those horrifying days after plant disasters is that more often than not, the final straw has been the plant operators consistently making wrong decisions based on the information they think they have about what is going on in the process. Many of these disasters have been blamed on cascades of alarms that made it impossible for operators to figure out which alarms actually were important and what they meant.

Safety instrumented systems are designed to be emergency shutdown systems, and often they work properly. There are specific standards worldwide that define how a safety-instrumented system should work. What does not exist is the same kind of standard for alarms and alarm management.

Doug Rothenberg has been in the forefront of research and standards making for alarm management in the process industries for many years. He did the pioneering work in the development and deployment of distributed control system (DCS) alarm management technology from 1989 through the present. He also was a founding member of the Alarm Management Task Force and the ASM Consortium and is a voting member of ISA 18, the Alarm Management Standards Committee.

His book is a comprehensive treatment of the current best practices in industrial process control alarm management. Doug covers the entire alarm management process from how to recognize the level of performance of existing systems through the methodology and procedures for redesigning (or designing new) state-of-the-practice alarm systems. You do not need any special or detailed experience in the configuration or specification of process control equipment. The ability to appreciate technical issues is important, but no prerequisite exists for any specific technical, educational, or experiential background.

In this book, Doug elevates alarm management from a fragmented collection of procedures, metrics, and trial and error to the level of a technology discipline. This is the

first book about alarm management to do so. Doug gives you the fundamental underpinnings that will provide a level of understanding that is independent of opinion and partial experiences. All critical tasks are explained, with examples and insight into what they mean. Alternatives are everywhere to enable industrial users to tailor-make their solutions for their particular sites.

Using this book, you will be able to understand how to rationalize alarms and how to work toward the same sort of human-factors engineering that has revolutionized cockpit design but is now applied to control rooms in industrial process plants.

If you work in a process plant, design process plants, or design, operate, or maintain control systems, this is your indispensable reference book.

Walt Boyes
Fellow, International Society of Automation
Editor in Chief, *Control* magazine

Acknowledgments

The author gratefully acknowledges the contributions of the following friends and colleagues:

Ari Bar-on—for his unflagging friendship, unrelenting constructive advice, and lending more ear than one ear might bear, all with compassion and class

Ian Nimmo—for believing in alarm management, steadfast friendship, and advice along the way

Steve Apple, Walt Boyes, Steve Elwart, Alan Phipps, and Chris Wilson—for their unrelenting push to write this book and make it a best of class and their guidance to help make it so

Greg Morris—for believing that alarm training is empowering

Jack Pankoff—for teaching me the business of running a business

Angela Stump—for reviewing drafts of this work with such heart and mind

David Gaertner, John Bogdan, and Diego Izarra—for believing in alarm management as a vital service

Joel Stein—for being as much a colleague as a publisher

Rachel Paul McGrath—for preparing the design and page layout with care and talent that brought words in files into visual life

There are a large number of professionals who took up the challenge of better production through better alarm systems. These pioneers are to be found in appendix 8 of this book, as their enumeration would take much more space than a simple acknowledgment might allow.

Douglas H. Rothenberg
Shaker Heights, Ohio, USA

Credits

The author wishes to thank the generosity of the following organizations for permission to use copyright materials that they own and may have previously published.

ControlGlobal.com, Itasca, IL, for Figure 3.3.2

Chevron NA, New Orleans, LA, for appendix 9

Ergon Refining, Vicksburg, MS, for Figure 7.6.2

Honeywell, Inc., Phoenix, AZ, for Figures 2.3.1, 2.4.1, 2.6.1, 2.9.1, 2.9.2, 4.10.2, 5.3.1, 11.3.1, 12.6.4, 12.6.5, 12.6.8, 12.6.9, 12.8.1, and 12.10.1 to 12.10.8

Henry Holt, Inc., New York, for Figure 12.4.2

Human Centered Solutions, for Figure 12.10.9

PAS, Inc., Houston, TX, for Figure 10.3.1

Power Engineering, Tulsa, OK, for Figure 1.3.2

TiPS, Inc., Austin, TX, for use of ACE and LogMate software to prepare numerous alarm configuration and operational graphs

The author and publisher gratefully acknowledge the license granted by Matrikon, Inc., Edmonton, Alberta, to reproduce in this book, Table 4.7.3 and Figures 4.7.1 to and including 4.7.3 taken from Matrikon. For further information about Matrikon, Inc., and its Alarm Manager product, please see <http://www.matrikon.com>.

Introduction

We warm ourselves by fires we did not build and drink from wells we did not dig.

—Ancient Semitic wisdom

This book embodies the current best practices of process control alarm systems for industrial manufacturing facilities. It is a comprehensive guide developed to help you understand, design, evaluate, and use alarm systems. The coverage is accurate and complete and, at the same time, easy to grasp. The book contains all the “what is” information about alarm management so that you will fully understand. There is an extensive “how to” that you can use to perform every aspect of alarm system redesign. The style is low key. The technology is down to earth, solid, and based on strong design fundamentals.

Some of you have experience with alarm projects. You’ve done work before others even knew alarm improvement was such an extraordinary opportunity to better operations. No doubt when you read this, you will find differences in what is suggested here in comparison to what you’ve done for your site. Please understand that this situation does not mean to imply that either of us might be wrong. It is just that now we understand the methodology better and have some very powerful and useful tools and procedures at our disposal. We do not have to do as much trial and error. New standards and practices are in place. We better understand how alarm management really works.

Right about now others might be asking, how in the world can a topic as obscure as alarm management possibly lead to an entire book? What can be so important and useful? It just so happens that alarm improvement is a powerful means toward a valuable end. It provides a useful way to better plant operations. Alarm management is one of those lucky finds that yields wonderful prizes. Let me tell you why. Think about a time, many years ago, when travel was done mostly on foot, without maps, on dusty roads with forks and no signposts or mile markers. There were a number of ways to try to get to a town or village. One could simply follow a road and watch to see if it were becoming more traveled as one went along. One might be fortunate enough to happen upon a fellow traveler and inquire. If there were no traveler or no road, one might follow a stream to see what could be found. Depending on the lay of the land, it might be possible to

head down into an inviting valley, or in the direction of chimneys smoking, or follow the hubbub to a busy market.

Like the stream, road, or fellow traveler, alarm management leads to the village—but in our case the village is significantly improved plant operations. There are, of course, other roads to better operation. Examples would be a desire to reduce long-term costs, a need to improve product quality or delivery schedules, a requirement to manage environmental exposure, or the need to provide a significantly safer enterprise. Choose any one. Along the way, you will touch most of the same aspects you are going to touch by taking the alarm improvement path. Much of the benefits will be similar. But a most important difference will be that the alarm improvement road, this road, is traveled enough so that there are good maps, effective signposts, and lots of fellow travelers. This road has also been carefully planned with good restaurants and comfortable motels. Enjoy the trip.

NOT A HANDBOOK

This is not a handbook.

Handbooks may deal with any topic, and are generally compendiums of information in a particular field or about a particular technique. They are designed to be easily consulted and provide quick answers in a certain area. (Wikipedia)

This book is not a handbook because alarm management is not about affirming business as usual. Nothing is wrong with business as usual, except that is how process control systems (PCS) alarm capabilities drifted away from their intended purpose and into the center stage of poor operations performance. Getting better is less about tinkering and polishing and more about rethinking and redesign. Alarm management now has a foundation and a body of implementation experiences. This text covers the entire alarm management process from recognition to action. The reader learns how to recognize the level of performance of existing systems as well as how to take action through the methodology and procedures for designing new state-of-the-practice alarm systems. To do this job well, you will need to know more than the highlights and have more than lots of lists and procedures.

AUDIENCE

This book was created for individuals with a general familiarity of modern process control systems and how operators use them to manage their plants. Readers need not have any special or detailed experience in the configuration or specification of process control equipment. The ability to appreciate technical issues is important, but no prerequisite exists for any specific technical, educational, or experiential background. The book is a comprehensive treatment of the current best practices. The text covers the entire alarm management process from how to recognize the level of performance of existing systems through the methodology and procedures for redesigning (or designing new) state-of-the-practice alarm systems.

You will find the style and content useful and understandable. The majority of the material has been presented around the world to a wide audience in a variety of formats as industrial and professional short courses and workshops. Audiences have included plant operators, operations supervisors and managers, process controls technicians, instrument and control technicians and engineers, health and safety personnel, process engineers and engineering supervisors, all manner of support staff, and notably senior plant management. The material of this book has met with enthusiastic reception. If you are interested in alarm management, this is your source!

USEFULNESS

This work elevates alarm management from a fragmented collection of procedures, metrics, and trial and error to the level of a technology discipline. Fundamental underpinnings provide a level of understanding that is independent of opinion and partial experiences. All critical tasks are explained, with examples and insight into what they mean. Alternatives are everywhere to enable industrial users to tailor-make their solutions for their particular sites.

Many of the leading power, chemical, mining, pharmaceuticals, and petroleum manufacturing companies contributed to this best practice. There are a growing number of alarm management applications and improvement programs. They serve to excite the industrial community with the importance of good alarm system design. This text is a one-stop shop for alarm management practices from start to finish. It includes important material for understanding and managing abnormal plant operations. It illustrates the serious importance of process control graphics in the management of plants.

Redesigning alarms will ensure that plant operators have an improved notification system to provide warning of abnormal operation. However, alarm improvement cannot stand alone. Warning alone fails to ensure operational success. This broad coverage exposes the practitioner to all the additional key aspects and practices that work together. The value of this treatment derives from the combination of the delivery of a clear, workable, comprehensive alarm system design and the coverage of intimately related “enablers” that empower the operator to fully leverage the improved alarm system.

CONTENTS

This book is organized in three parts. Part I covers the alarm management problem. Part II lays out the solution. Part III provides the pathway to make it all real. There are twelve chapters. There is a natural progression of the work, with each chapter covering a specific area. It is suggested that the reader cover the material in that order. However, each chapter has value if read separately. This can be especially useful for those with a working knowledge of the technology who are looking for more detail or greater depth in selected topics. The book provides a working guide for project planning and execution. Certain chapters work especially well as stand-alone treatments. Chapter 2, “Abnormal Situations,” chapter 5, “Permission to Operate,” and chapter 12, “Situation Awareness,” are designed with this in mind. These topics bring out aspects of enterprise management that go beyond

alarm systems in their overall importance. They elevate alarm improvement effectiveness to a level of value capable of delivering demonstrable benefit.

Each chapter begins with the mention of the key concepts that underlie the topic.¹ These key concepts are provided to assist the reader to clearly separate the concepts from the explanatory discussion. Taken as a whole, the set of key concepts could make up a shorthand bible of alarm management.

Part I: The Alarm Management Problem

Chapter 1, “Meet Alarm Management,” explores the basic reasons for considering improving your alarm system, introduces the four fundamental concepts that guides the process, and bridges the implementation over the distributed control system (DCS) and programming logic controllers (PLC) controls platforms and the process types: continuous, discrete, and batch. Chapter 2, “Abnormal Situations,” links process operation abnormalities to alarm performance requirements. Along the way we pick up the important concept of how to use time in setting alarm activation levels. Chapter 3, “Strategy for Alarm Improvement,” brings us up to speed with the who, what, when, and how to effect alarm system redesign. The existing standards and best practices are also covered. Chapter 4, “Alarm Performance,” covers the useful scales for measuring both alarm system design and operational performance.

Part II: The Alarm Management Solution

Chapter 5, “Permission to Operate,” provides a framework to cover an important need in plant operational protocol to ensure that unmanageable situations are avoided. Chapter 6, “Alarm Philosophy,” covers how each enterprise will specify their chosen alarm design. Chapter 7, “Rationalization,” is the heart of building the new alarm designs. It covers the technical procedures for how alarms are chosen, configured, documented, and folded back into the rest of the plant infrastructure. Chapter 8, “Enhanced Alarm Methods,” builds on the first-level alarm design to ensure that the alarm design accommodates to changes in plant situations.

Part III: Implementing Alarm Management

Chapter 9, “Implementation,” gets into the realities of taking a new alarm design and producing a new working alarm system ready to fully assist the operator. Chapter 10, “Life Cycle Management,” clears the way to understanding what is needed to keep a new alarm system working down the road so that it can deliver continuous operational benefit. Chapter 11, “Project Development,” provides alternative ways to produce a program for comprehensive alarm improvement, from start to finish, that matches the enterprise’s way of conducting work projects. Chapter 12, “Situation Awareness,” rounds out the entire work by providing the understanding and technology for improving the operator’s ability to manage a process without undue reliance on alarms.

BOOK DELIVERABLES

Upon completion, you will have a solid, clear foundational understanding of the purpose of alarms, the rationale behind a state-of-the-practice design, and sufficient how-to knowledge to competently perform in the technology. This book is designed to provide a basis for the following competencies:

- Understanding the proper use of process control alarm systems
- Knowing the underlying defining attributes and purpose of an alarm
- Appreciating the importance of effective alarm management
- Recognizing alarm system performance problems, including alarm flood
- Becoming knowledgeable in the best practices for alarm system design
- Learning the value of alarm data diagnostic tools
- Understanding the entire process for designing and executing an alarm improvement project
- Understanding the influence of good graphic interface design on plant operability and effective situation awareness
- Becoming a qualified participant in alarm improvement teams

IMPORTANT WORD

Please note that this book is not intended in any way to offer advice or recommendations as to the appropriateness or lack of appropriateness of including or excluding any specific alarm for any site. The choice of which aspects to alarm for the plant or process, the parameters of that alarm, the proper operator response to correct the alarm condition, and all other details of that alarm must be retained wholly by qualified, authorized members of the plant staff, who must act with full knowledge of their specific plant configuration, process conditions, equipment, and applicable statutory practices and requirements.

No single work is capable of conveying the entire collective experience and important nuances necessary for success. After you read this book, it is recommended that plants with intentions or plans for alarm improvement seek additional specific guidance and experience from knowledgeable experts.

NOTE

1. “The Use and Abuse of the Cept,” *Time*, March 26, 1965.

PART I

The Alarm Management Problem

Meet Alarm Management

If you need a new machine and don't buy it, you pay for it anyway but never get to use it.

—Henry Ford

An alarm is an announcement to the operator initiated by a process variable (or measurement) passing a defined limit as it approaches an undesirable or unsafe value. The announcement includes audible sounds, visual indications (e.g., flashing lights and text, background or text color changes, and other graphic or pictorial changes), and messages. The announced problem requires operator action. An alarm is a construction by which an aspect of manufacturing operation is identified and configured in a binary way to be either “in alarm” or “cleared” (i.e., not in alarm). The condition of *in alarm* is passed to an operator via intrusive sounds and notices placed on video display units or other devices to gain attention. The operator can manage these sounds and notices only via specific “silence the alarm” or “acknowledge the alarm” actions using the existing, planned infrastructure of the alarm platform. Usually, this alarm platform is an integral part of the process control system (PCS) infrastructure.

The PCS alarm system is a vital and productive tool for managing industrial process control plants. Through several unique cooperative endeavors, industry has identified a best practice for alarm system design. This design utilizes configuration changes, alarm reprioritization and balancing, alarm reductions, graphics modifications, online filtering, and decision support aids. Alarms perform the vital function of operational integrity monitoring. Properly designed alarms will notify the operator of abnormal situations with enough time to successfully manage them.

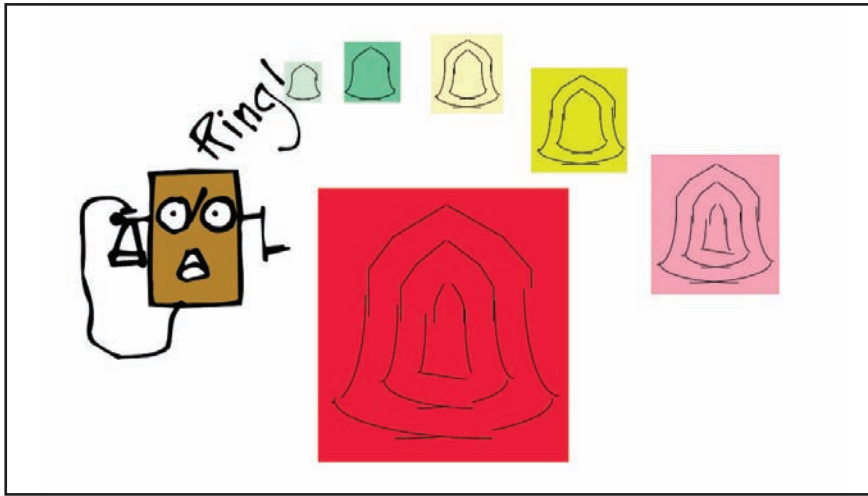


Figure I.0.1. Alarms are an intrusive notification to the operator

I.1 KEY CONCEPTS

Alarms are for the operator	The alarm system must be off-limits for all plant uses that do not directly require the operator to process actively the situation or information.
All of the objectives of alarm improvement are just good engineering	There is nothing that alarm improvement asks of plant operators that is over and above what constitutes effective plant design and operation. Somehow, bits and pieces are overlooked or shortcuts are taken. Poor or inadequate alarm performance is just the way we find out about these things. The technology of alarm improvement provides a focused, compact way of getting that job done.
Alarm redesign is based on important fundamental concepts	Alarm redesign is based on four powerful concepts: <i>only notify important conditions</i> , <i>notify in time</i> , <i>respond</i> , and <i>provide guidance</i> .
Initial alarm system performance matters little	Few, if any, unimproved alarm systems have been designed to meet the fundamental concepts; therefore, reducing alarm annoyance and activation rates only treats symptoms of a nonperforming design.
Improving alarms alone will not provide enough benefit	Good alarm systems only work when the entire plant infrastructure supports good operation.

I.2 ALARM PERFORMANCE PROBLEMS

Ask almost any operator if the alarm system is working for or against good process operation. The response you are likely to get is surprise—not because the question is unclear but because it took you so long to ask. Ask control engineers or process engineers that same question and they are more and more often going to say that the alarm system needs fixing. Ask experts in industrial accident investigation and they will tell you that the lack of adequate performance of the alarm system is contributory to a significant number of industrial accidents and major calamities. They will quickly suggest that you make plans to evaluate your PCS alarm system.

Symptoms

Right off the bat, there are clear indicators of alarm problems. If your site has *any* of these symptoms, there is cause for concern. If you can observe three or more of them, there is much serious work to be done.

- Alarm activations occur without need for operator action.
- There is no plantwide philosophy for the alarm system.
- There are no clear guidelines for when to add an alarm and how to do it.
- There are no controls for removing existing alarms.
- Operating procedures are not tied to alarm activations.
- When alarms activate, the operator is not always sure what to do about them.
- Seemingly routine operations produce a large number of alarm activations that serve no useful purpose.
- Minor operating upsets produce a significant number of alarm activations.
- Significant operating upsets produce an unmanageable number of alarm activations.
- Some alarms remain active for long periods of time.
- When nothing is wrong, there are active alarms.

Evidence

We look for evidence of alarm problems in four places. Two are quite objective; two are subtle.

- *Number of alarms configured in the PCS database.* How many tags are alarmed? How many alarms are configured for each alarmed tag? How close are the alarm limits to actual process limits? How closely is priority matched to actual operational risk?

- *Number of alarm activations.* What is the hour-by-hour average occurrence of alarms? How often do alarm floods occur? How many alarms occur during a flood? What is the distribution of alarm priorities during floods?
- *Operators' ability to gain insight and guidance from the alarm system prior, during, and after an upset.* If alarms are not active, how sure are the operators that the process is normal? When alarms activate, do they provide assistance for the operator to diagnose and remedy problems? Does the alarm system itself—by excessive activations, lack of proper activation, or existence of meaningless active alarms—interfere with or delay proper production management?
- *Operators' ability to determine how the process is actually performing from other tools and PCS capabilities.* What is in place that permits operators to view and understand how the process is actually performing? If there were no alarm system at all, how easily could the operator determine how the process was performing and how close it might be to an abnormal condition?

1.3 REASONS FOR ALARM IMPROVEMENT

No alarm system should be asked to overcome the intricacies and power of the uncontrolled effects of nature or the failed constructs of man. Pandora's box cannot be closed. Humpty Dumpty cannot be put back together. Yet the future is not grim. History is not written solely for the purpose of conveying the worst from our past. Alarm management is thus charged with aiding and abetting our best efforts for accommodating the worst and setting reasonable courses for recovery. Within these pages, you will find the concepts, ideas, and practical approaches to bring what is possible to you. You are encouraged to recognize that your best will neither prevent nor minimize all the effects of misdirection. You are empowered to believe that your best efforts will yield nourishing fruit. As Larry O'Brien and Dave Woll say in *Alarm Management Strategies*,

Alarm management is one of the most undervalued and underutilized aspects of process automation today. In most cases, alarm systems do not receive the attention and resources that are warranted. This is understandable, because alarming appears to be a deceptively simple activity. Many plants still use the alarm management philosophy developed by the engineering firm when the plant was built.

As alarm systems become less effective, they diminish the effectiveness of all automation.¹

How Alarms Fit into Process Operating Situation

Safety shutdown systems are designed to close down affected plant operations in the unfortunate situation where that operation is too close to an unsafe situation, an environmentally challenging condition, or a mode of operation that threatens the financial integrity of the plant. Once a shutdown occurs, the plant operation is significantly curtailed. This usually results in a loss of production, some equipment damage, and a

considerable degree of internal investigation. Prior to restart, there might be repairs, changes to equipment and procedures, and of course lots of administrative work.

Most plants would choose to avoid a shutdown if it could be done without risk. Abnormal situations rarely present themselves without some warning. But those warning messages and signs are not always picked up by the operator. They are often subtle. Sometimes they are downright abstract or confusing. Rarely are they front and center enough to be found in time and remedied. However, in a well-designed alarm system, one designed from the point of view of alarming abnormal situations rather than just abnormal variables, a significantly greater number of those early warning messages about abnormal plant operation can be seen. In this way, the alarm system might be considered to serve as a presafety shutdown system. Alarms are a way for the operator to see an important problem building and have an opportunity to keep it from leading to a more serious plant situation.

The process control system is set to the operating target (fig. 1.3.1). These controls are intended to keep production within the good operating region. Operation is still fine in the safe operating region, but the product is less valuable or more costly to produce. Few, if any, alarms should be designed to activate as the process approaches and appears likely to cross the boundary between good operation and safe operation. Alarming here is technically difficult and often results in many unnecessary alarm activations. The control system should be capable of responding to changes and disturbances that cause movement away from the operating target. Let it do its work. If tighter control is needed, either modify the controls or ask the operator to be more diligent and make more frequent adjustments to the controls (e.g., setpoint adjustments, supplemented with minor field adjustments).

Most alarms should be set to activate as soon as the process moves close to and appears likely to cross the boundary between safe operation and upset operation. At this point, there is a very high likelihood that the control system is unable to manage the situation properly. Manual operator intervention is required. The alarms are there

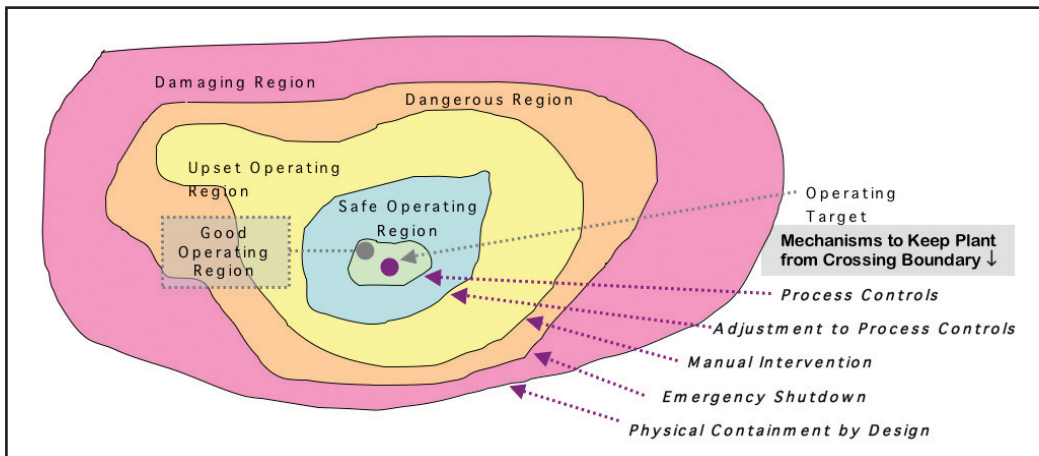


Figure 1.3.1. Operating region versus modality of remediation

to ensure that the operator does not miss these situations. If manual intervention by the operator is still not likely to ensure that the process remains within the upset region, alarms are used to mark the likely movement through the boundary from upset operation to dangerous operation. Any plant movement from dangerous operation into damaging operation should be managed by the emergency shutdown system. Alarms are too late here, so none are needed.

Alarm Management

Alarm management is all about the understanding, design, implementation, and operation of an effective alerting capability for production plant operators. These alerts are intended to notify operators of situations and events that require operator attention in an explicit way within an acceptable time frame. This book is written for users and designers of industrial process control systems. These systems are traditionally comprised of equipment to measure plant conditions, other equipment to transfer those measurements to devices that are capable of interpreting the measurements, still other devices that employ these interpretations and other information to manipulate yet other process conditions in order to realize an appropriate plant operation, and finally equipment that permits operators and others to view all measurements and intervene as needed.

Being more pragmatic, alarm management is therefore the determination of (a) all plant conditions that will be alarmed, (b) the parametric setting for the activation of each alarm event, (c) the classification of the importance of each alarm event, and (d) the collation and presentation of information that documents the best understanding of how to successfully manage the event.

Benefits

Alarm improvement works. It can deliver clear, auditable benefits. Let's cut to the chase, as they say. Plants that redesign their alarm systems using the best practices in cooperation with energetic and understanding personnel are seeing payouts in reduced maintenance costs and lower insurance rates. You were probably expecting things like better operation and higher quality and stuff like that. OK, that too. However, the real message, and the one that in a very noncircular way proves out the best practices, is that maintenance and insurance reflect the biggest operational integrity risks for enterprises.

Reduced Maintenance Costs

One of the biggest surprises in alarm management is the serious reduction in plant maintenance costs after improvement. Yes, it is easy after the fact to see how this might be true. With the operator able to catch errant operation earlier and do a better job of bringing things back in line, it is not too great a leap to see that the equipment is less stressed. Therefore, operators encounter fewer overpressure events, fewer high-temperature excursions, and less pump cavitation. Less-stressed equipment breaks down less often. The interesting

thing here is that in the past, operators did not expect to see these benefits. But now it has become obvious—alarm improvement works.

As you will discover later on in this book, improving plant maintenance is a vital requirement for gaining improved alarm system performance. It is a subversion of the alarm system to ask it to cover for all of the broken stuff, all of the missing but important stuff, and all of the other aspects that were designed into a plant but over time got lost. Maintenance is important. Going into alarm improvement, one might be concerned that maintenance costs would likely go up. Plants would need to fix everything that was broken. Repairs cost money; pay a little now. But what most do not realize is that the costs of fixing up return the favor in kind!

General results: within 6 months after alarm improvement work is commissioned and smoothly operating, plants see a 5% to 15% sustained reduction in unplanned maintenance costs.

Lower Insurance Costs

You might be new to alarm management. Your insurance company more than likely is not! Figures bouncing around in Europe reveal that the lack of an alarm management program increases premiums by substantial amounts. Figures for the United States are less, but U.S. experiences are limited. Insurance companies have followed the pacesetters in implementing alarm management. The 1999 publication of the Engineering Equipment Materials Users' Association (EEMUA) 191 guidelines² put out the word and showed everyone how to get started. As the numbers came in, they told the story. Again, this points to the fact that alarm improvement works.

General results: European manufacturers are seeing a 20% to 30% reduction in their risk operations insurance due to implementation of EEMUA-compliant alarm improvement.

Capture Workforce Knowledge

Manufacturing in many parts of the world is diminishing as industrial activity geographically redistributes in our mobile world. For a variety of reasons, the workforce in important segments of industry is aging. Fewer young workers are entering. At the same time, a disproportionate number of highly experienced workers will be leaving their positions through retirement, illness, or attractive cost-cutting management incentives. A great deal of unwritten knowledge will leave when they leave. According to *Power Engineering*³ (fig. 1.3.2), nearly 20% of the entire workforce will have reached normal retirement age by 2015 and nearly 40% by 2020.

Alarm redesign, by design, provides a comprehensive, structured way to capture important operating knowledge. The entire activity of identifying abnormal situations through alarms and what the operator is supposed to do to manage them properly is a key part of the rationalization activity. So, not only will the present operating team have the benefit of this information, but as each new member moves to the board, they too will be able to understand and use this valuable asset. For the reader who would like to have an advanced view of what this knowledge looks like, you may refer to the alarm response sheet in chapter 7.

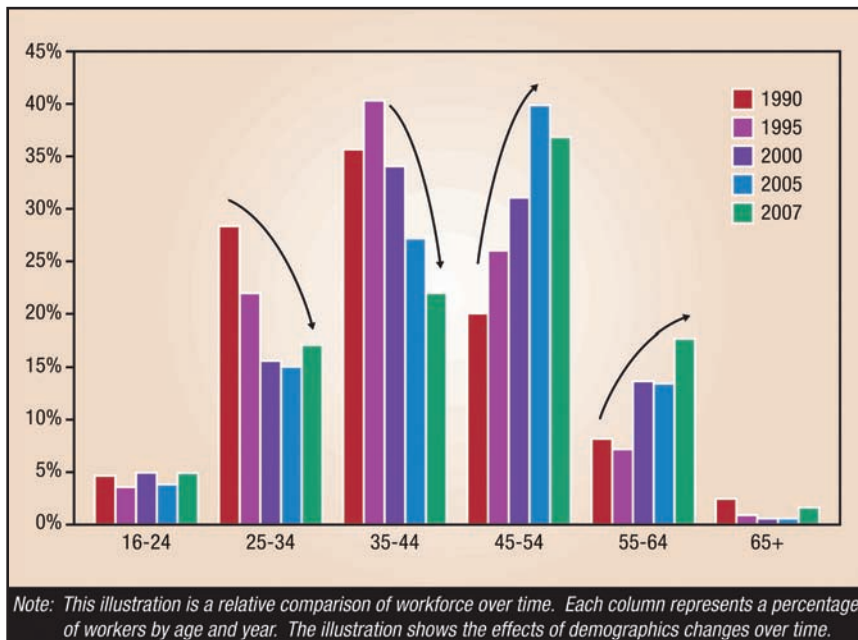


Figure I.3.2. Aging workforce in U.S. power industry

Shift Handover

If you are an operator, you know how important it is to receive a full briefing from the operator you are replacing. Even if you are coming on after a relatively quiet shift, a lot might have happened earlier that you would benefit from knowing about later. As it happens, the actual process of shift handover can be a very haphazard event. For some plants, the two operators barely have time to wave as they pass. Other plants have found the benefit of doing this well and arrange for an informal overlap of operators' time. Interestingly enough, operators have found it so useful that they do it without additional pay!

Plants have discovered that a well-designed alarm system will provide an important orientation edge to the handover. Operators discuss alarms that have activated during the shift. They discuss any alarms that might have been disabled, inhibited, or otherwise outside of their normal operating regime. The alarm information provides a checklist of items not to be missed. Moreover, those items are likely at the heart of the operability of the enterprise.

I.4 A BRIEF HISTORY OF ALARM MANAGEMENT

The year 1988 is the generally accepted earliest date for the first recognition of alarm system problems. Yes, there were those few early pioneers who faced operational difficulties and traced some or most of them to alarm system deficiencies. And these pioneers

certainly made improvements to their plants based on this understanding. However, their impact was limited to their parochial interests. Little alarm was raised to the body technical, as it were. This all changed in late 1988 and into 1989. A surprisingly large number of individuals from a broad range of industries who were working to better understand the way process upsets were being managed by operators came to realize that the alarm system itself might be a problem. By 1990, sites had worked out the basics of alarm improvement, and a few actually had begun to execute projects. But all this came to a surprising halt in early 1991. It was discovered that it was not possible to actually implement most alarm improvement plans within any currently used, conventional process control platform.

In 1991, they joined together in what is known as the Alarm Management Task Force (appendix 8). On a warm afternoon in mid-October that year in Phoenix, Arizona, the first of many meetings took place. It was represented by oil refining companies, chemical manufacturing companies, a controls equipment manufacturing company, and power companies from almost all segments of their respective industries. Over the next few years, they worked out the fundamentals of alarming, helped shape the requirements for alarm analysis tools and controls infrastructure, and plowed their way through the realization that prevention was the best alarm response possible. Along the way, the Abnormal Situation Management (ASM) Consortium was born and important paradigms were set for production management. By the mid-1990s, third-party software companies developed and refined important alarm capture and analysis tools.

In a parallel track, Brookhaven National Laboratory⁴ became fully involved in developing a better understanding of alarm systems following the Three Mile Island accident.

Using the collective knowledge from the Alarm Management Task Force, the ASM joined with leading technologists in Europe to support an EEMUA initiative. In 1999, EEMUA collated and published the first and most-recognized guide to alarm systems. It was revised in 2007. To date, Publication 191 functions as the de facto best practice. Unfortunately, the availability of good guidance does not necessarily lead to a widespread adoption. Thus, many industrial nations are now seeking to codify requirements that they believe will lead to improved safe operation of industrial plants.

1.5 THE “MANAGEMENT” IN ALARM MANAGEMENT

The management part of the phrase *alarm management* is a bit of a misnomer. Alarm management is a design and implementation process for the *entire redesign* of the portion of the process control system capability that is used to alert operators to conditions where an alarm is needed. The minute-by-minute managing of an alarm is but one small part of this much more encompassing technology. The full process includes the following:

1. Benchmark analysis of present alarm system performance, including its impact on production, safety, and environmental
2. Development of a philosophy governing the operation of the enterprise sufficient to specify a design basis for the required alarm system and supporting plant infrastructure
3. Selection of which variables to alarm

4. Setting of alarm limits
5. Setting of alarm priorities
6. Determination of recommended operator actions
7. Design of advanced techniques to facilitate improved alarm performance
8. Addition of plant condition monitors and decision support tools
9. Incorporation of new alarm system design back into the plant infrastructure
10. Continual audits, assessments, and modifications for improvement

Alarm management is a process. When we successfully do alarm management, we end up with a fully functioning alarm system suitable to meet production requirements to better realize enterprise goals.

1.6 ALARM DESIGN ROADMAP

Here is the basic roadmap we will use to structure the alarm system improvement work. It captures the key steps and order found to be most useful and best at leading to success. See Figure 1.6.1. The entry ticket into the alarm redesign game is to know your alarm problem and understand how large it appears to be. Assemble some data, analyze it, and reach preliminary conclusions. If there are sufficient grounds (and that is part of what this book is all about), you will take your story and go to management.

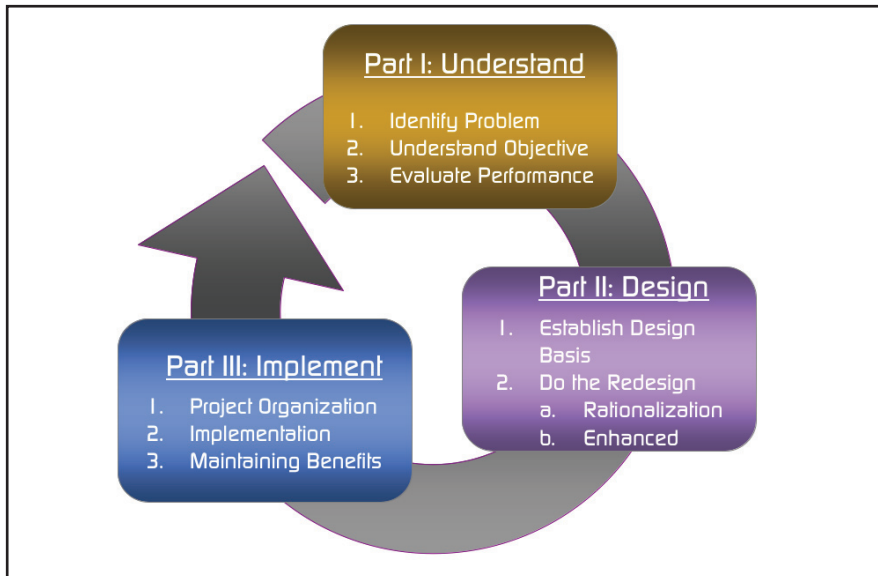


Figure 1.6.1. Alarm redesign roadmap

If your power of persuasion is strong enough and your case evident enough, management should offer up a commitment (let you propose a project and approve it) and help with the development of a site alarm improvement philosophy. Project in hand, you will continue (clockwise) and assemble a large amount of data sufficient to demonstrate most, if not all, of your site's alarm and related deficiencies. Next step is to analyze that data and reach conclusions that will assist you to focus your redesign project efforts where they are most needed.

The first actual changes to be made in your alarm management work appear in the next step—rationalization. This is a three-legged item. And the first leg is *housekeeping*, a vernacular word that means “fix everything that is broken.” It is simple. We should not ask the alarm system to act as a substitute for correctable defects. The next two legs involve the redesign of alarms to fit the new requirements and the addition of any specialized alarm processing needed to better handle unnecessary alarms and alarm floods. Except for housekeeping, everything we have done so far is on paper. We are ready to do it, but not yet. Implementation is when we take all of our new design and make it real. The last step is actually the one that we will use continuously: maintain benefits by monitoring, improving, and correcting.

1.7 AUDIENCE FOR THIS BOOK

This book is written for individuals with a general familiarity with modern distributed process control systems and how operators employ them to manage their plants. It is a comprehensive treatment of the current best practices. The work covers the entire alarm management process from how to recognize the current level of performance of existing systems through the methodology and procedures for redesigning (or designing new) state-of-the-practice alarm systems. Readers need not have any special or detailed experience in the configuration or specification of PCS equipment. The ability to appreciate technical issues is important, but there is no prerequisite for any specific technical, educational, or experiential background. If you are interested in alarm management, this is your book!

Anyone with a desire to better understand and improve PCS alarm systems will find the style and content useful and understandable. The majority of the material has been used for several years and presented to a wide audience in a variety of formats as industrial and professional short courses and workshops. Audiences have included plant operators, operations supervisors and managers, PCS technicians, instrument and control technicians and engineers, health and safety personnel, process engineers and engineering supervisors, all manner of support staff, and, notably, senior plant management. This material has been presented to international audiences with enthusiastic success.

1.8 IMPORTANCE OF ALARM MANAGEMENT

At the end of the day, when the alarm system has been redesigned and implemented, the plant will have a tool that significantly improves production performance. This

improvement will be seen both during normal operation (these periods will be longer and less eventful) and during upset periods (they should be less severe, less frequent, and better managed). We will see improved operator display screens that assist production personnel to ascertain plant operating conditions before most significant upsets occur. And, to return to the opening message, good alarm systems pay off in reduced maintenance and insurance costs.

When you think about it, a large percentage of currently installed PCSs provide only limited information regarding normal operation. It is up to the operator to search out those trends and critical variables and use intuition, experience, and insight to determine how normal things really are. As simple as it is to say, this is a difficult task to do. Not many of us can do it; even fewer can do it well enough to consistently manage even everyday problems. To make matters more difficult, plants are becoming more complicated, production requirements more demanding, and qualified personnel harder to justify and retain.

Still not convinced? Let us take a look at some of the statistics. It is not unusual for a medium-sized petrochemical company consisting of about six separate sites (refineries, chemical plants, etc.) to accumulate US\$50,000,000 to \$100,000,000 in yearly losses due to plant upsets and other production accidents. Alternatively, calculated another way, the generally recognized loss figure is 3% to 5% of throughput. On a U.S. national level, this number is pegged at around \$20,000,000,000 annually, year in and year out. If this is not significant enough to have an impact on your decision to be concerned, consider that many experts believe that these figures dramatically underestimate the real situation. Moreover, not included in these numbers are the rare tragic incidents like Bhopal and Valdez. Increasingly, the performance of the alarm system itself has been identified as a significant contributor.

Alarm improvement is a big deal. It involves careful planning, steady commitment, adequate resources, full cooperation of site players, ability to modify weak infrastructure supporting components, and an understanding that this is a lifestyle change, not just a once-through project. So now you ask, “What if there are only one or two things that I can do? I cannot support a full alarm redesign; in fact, I’m a few years away from that. Can you recommend a plan in the interim?”

The answer might surprise you. Before we get to that, let us understand that the bottom line here is not to get another alarm system designed. The prime objective is to significantly improve production integrity. Improved integrity is the mantra of a good alarm system, but the alarm system itself it is not necessarily the first step. Here is my list; stop at any place where you run out of money. But stop at the risk of enterprise operational integrity.

- Fix all broken equipment and keep it running well.
- Implement a policy of only operating when the plant is known to be operable (see chapter 5).
- Improve the operator’s ability be aware of the plant operational situation (see chapter 12).
- Redesign the alarm system (see this book).

1.9 FUNDAMENTALS OF ALARM MANAGEMENT

We design successful alarm systems by building our work from four fundamental precepts. I am sure that when you first became aware of alarm management, you might not have been certain that it had much to do with anything real, much less vitally useful, to you and the plant you support. Alarm improvement is a discipline with important technology that, when used, will significantly improve success.

As you do the job correctly, you will come to appreciate the importance of ensuring an effective operator support infrastructure. Operating procedures, training, safe operation, screen graphics and design, and maintenance will take on an entirely new level of importance. New concepts called “safe park” and “permission to operate” will become an integral part of your lexicon. You will come to believe that it not only will work, but its work will provide your plant with a level of operational integrity that is essential to a safe and profitable enterprise. You will wonder how it was possible that anyone would expect a plant to run well without this new approach.

Proper alarm design is a straightforward engineering process. Everything you know about engineering, about system design, and about project execution remains useful. Intuition is going to be useful. Moreover, while there are some who believe that alarm improvement is a complicated, delicate, and unforgiving process, it is certainly not. Yes, experience can be useful. If it is available, embrace it. At the end of the day, doing things well is easily within your personal reach.

Bottom Line of Alarm Management

This book is all about how to identify and configure vital alarms. Please, do not confuse “vital” with “emergency” or any other identifier that conveys extreme danger or loss. Vital simply announces to the world that this aspect of the plant, if not managed, will lead to operation that the enterprise has deemed to be unacceptable. Nothing more. If every alarm configured for a plant represented a vital aspect of plant operation and was engineered well, there would be no alarm management problems. No matter how many alarms there were, they all would be needed. If that many alarms would be too much for an operator to handle, then either the plant, the controls infrastructure, or the operations management would need modification.

Fundamentals

Right from the beginning, you are going to see every fundamental of importance for proper alarm management. This might be the first book you have ever read where the punch line—the essence of the story—is revealed in the very first chapter. There are four fundamentals—four precepts. Together they form the foundation of everything we need to know about the subject. They govern all successful alarm system designs. Knowing them should resolve almost every simple and usually every difficult decision you will face in understanding and designing new systems that work.

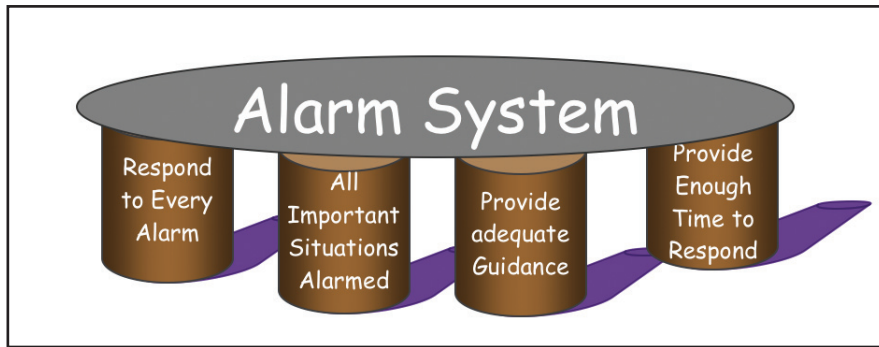


Figure I.9.1. Alarm design foundation fundamentals

- *Precept 1: Require action.* Every alarm requires timely operator action, and that action must be a necessary one.
- *Precept 2: Provide enough time for success.* Every alarm activation must occur in time to permit the operator to successfully remedy the situation, if that remedy is at all a reasonable outcome (given the realities of the situation).
- *Precept 3: Provide information.* Adequate information must be provided to the operator to work the alarm.
- *Precept 4: Alarm only important things.* Only alarm important conditions/situations.

Precept 1: Require Action

Precept 1 means that only when operator action is required should the potential alarm be configured as an alarm. This does not work both ways, however. The point will quickly be made that not every (and certainly not even most) operator action need be preceded by an alarm. Rather, the operator is primarily responsible for understanding the operation of his unit and maintaining good order in that unit. Alarms are not to be considered as any indicator of good or bad operation. Even perfect alarm selection and design are not meant to be surrogates for effective operator vigilance in maintaining awareness of the true operational situation of the plant.

Precept 2: Provide Enough Time for Success

Now that we know what constitutes an alarm, the second precept tells us how we must configure and support the alarm so that it will provide the requisite benefits. For this requirement to be met, every alarm must be configured to activate in time for the operator to understand and implement proper corrective action and give the process enough time to respond. This, in turn, tells the alarm designer when to activate the alarm and what information and other operator support are needed to ensure that the abnormal situation could be successfully managed.

Precept 3: Provide Information

An alarm activates, the operator is alerted, and the system is designed so there is enough time to manage the situation. At the same time, we need to provide all of the background information and current “what to do” information so that the operator can do the job.

Precept 4: Alarm Only Important Things

Only important abnormalities should be alarmed. Why? Well, without this restriction, we can be true to the preceding three precepts yet be free to alarm any event for which the operator has an action and for which we can provide a timely warning. There are so many nice things to warn the operator about that no one would have the slightest trouble providing a large number of alarms, and we did just that in the past. We provided wake-up alarms everywhere we could and we realarmed them if we thought the operator might have forgotten about them. Now, with precept 4, we place a value on each alarm. By appropriately understanding value, the alarm system is self-constrained in the number of alarms.

What should define a candidate alarm? A candidate alarm must represent any unwanted situation of importance that rises above a minimum threshold of impact and that can be announced by an alarm. Moreover, without an alarm, the operator is unlikely to observe this situation on his own.

Operator Action

Precept 1 requires all valid alarms to have an operator action. But to what operator actions does it refer? Suppose we always require operators to look at their watches and write down the difference between their watch time and the alarm time. That is an action, isn't it? A wave is an action. A look is an action. OK, you get the idea. We will need to nail down the meaning of operator action to get this right.

Operator actions can be broken down into two broad categories: primary and secondary. Operator action in response to an alarm must be a primary action. That is, in most instances, when an alarm activates, if the operator must usually respond with a primary operator action (see below), then the alarm is a proper alarm. Any alarm that is not a proper alarm should not have been configured as an alarm in the first place. But you already knew that! Let us formalize what actions are all about.

Primary Action

A primary operator action is one that directly modifies or changes something physical in the plant. Primary actions include starting something, stopping something, modifying something, and closely examining something with the intent of doing any of the earlier things on this list. Typical primary actions include putting a controller in manual, starting a pump, shutting a valve, reducing a controller setpoint, breaking a cascade loop, waiting longer to initiate a task or initiating a task earlier, or any number of the other things operators do to manage plants with problems.

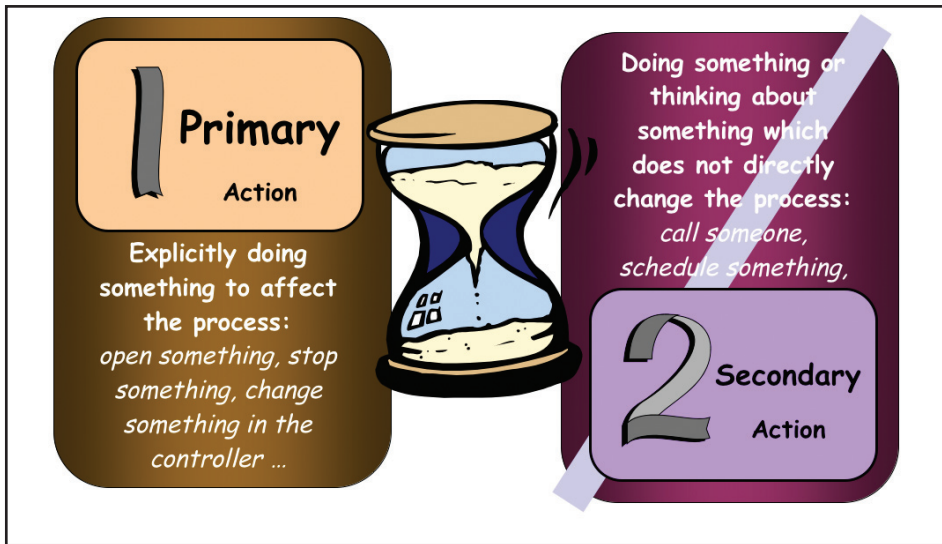


Figure I.9.2. Operator action types

Just to be sure we get this right, an operator can closely watch an abnormal process variable with the intent of jumping in and making adjustments should it range too far out of bounds but never actually make an adjustment. This counts because it is a situation that probably needs adjustments when it becomes abnormal. The operator retains control over when, how much, and even if an action is needed.

Secondary Action

A secondary operator action is any act that is not a primary action. Secondary actions include communicating with others, scheduling something contemporaneously, thinking about something, taking note of an event or condition or situation, and the like. Secondary actions may involve calling maintenance to come and do something routine, reminding an outside operator to blow down a sump, or any number of other things that occupy operators during the normal course of their shifts. We can split hairs on this, but let's move on.

A secondary operator action is not considered secondary when it is combined with a primary operator action—that is, if an operator performs a primary action along with a secondary one. Together, they are to be considered a primary action.

Importance of the Fundamentals

OK, that is it. These concepts reveal it all. Everything else in this book, and in alarm management in general, is commentary. At any time, when there is uncertainty about what to do or how to do it, refer to the precepts. Any decision of consequence can be derived from them. This is not to say that the rest of the book is now unimportant. This

book will show you how the fundamentals lead to the necessary understanding, tools, and insight to be successful. Contained within these chapters is a wealth of insight and practical methods. Using them will keep you honest to the precepts as well as save an enormous amount of time and effort in doing the important work of alarm design. This book brings to life what you will need to understand alarms and to design effective alarm systems. The precepts are about what to do. The rest of this book is about how to do it well.

1.10 DESIGN FOR HUMAN LIMITATIONS

A painter or writer can start with a blank sheet of paper, an empty screen, or a blank palate. An engineer or system designer can start with an approach that is limited only by what is believed to be in conformance with the rules of nature, economic viability, and good citizenship in a community. Of course, this situation is not as entirely unmanaged as these opening words would suggest. Good engineering practice is important. To follow what has been done successfully before is wise counsel, but that is not enough. The defining guidance will easily yield to discovery as soon as the designer insists that his creation be usable by the humans intended to use it. When all decisions have been made, the resulting design must fit the user's ability to successfully use it. Hence, you will find that all design goals and performance metrics for alarm management will be easily derived by considering whether or not a person can use them.

1.11 ALARM MANAGEMENT AND SIX SIGMA

One need not understand or apply any of the specific terminology and explicit practices of Six Sigma to do successful alarm management work. However, for sites with an active Six Sigma program, it is nice to know how the two relate. The Motorola Company developed Six Sigma as a business management strategy in 1986. They sought a more structured and updated methodology to focus the concepts and philosophy of the early quality giants: Deming, Crosby, Taguchi, Juran, and others.

With one important clarification, alarm management processes are an excellent fit with Six Sigma. That clarification is that alarm improvement (or design) is not driven by the actual performance data. Alarm improvement requires an explicit design methodology. The normal alarm events are usually considered to be data. However, any attempts to improve alarm performance cannot transcend a design that fails to comply with the fundamentals. Consider a civil engineering example. Improving highway bridges would be driven, not by bridge degradation and collapse data, but by the process of taking that information, uncovering root causes, and then modifying designs. Alarm improvement is this way as well. See Chris Wilson's article⁵ for a broader discussion on this topic.

The term Six Sigma is derived from the use of σ (the Greek alphabetic character sigma) in statistics. Very simply stated, if something is within a tolerance of one σ , it is 31% efficient (31% close to what is desired), which is not very close. Two σ would be better than 69%. Six σ is 99.9997%—extremely close! A process that is Six Sigma is

DMAIC		DMADV	
D	Define goals consistent with enterprise and business	D	Define goals consistent with enterprise and business
M	Measure key aspects of process from collected data	M	Measure (figure out how to) the future characteristics of process
A	Analyze the data and make appropriate inferences for results	A	Analyze and develop design alternatives to meet needs
I	Improve the process based on the data analysis results	D	Design the new design to meet requirements (may require some form of simulation)
C	Control the continuing process to ensure that continuous improvements are made	V	Verify that the design meets requirements and is ready for use

Table 1.11.1. Terminology for Six Sigma

Six Sigma	Alarm Management
Define/ Design	Construct and use a comprehensive alarm design philosophy
Measure	Alarm performance studies; configuration studies; incident studies
Analyze	Compare against best practices
Improve	Use proven alarm improvement technology to improve existing design
Verify	Compare new design to requirements and ensure they are met
Control	Use continuous improvement methodologies to evaluate and improve ongoing alarm system

Table 1.11.2. Six Sigma approach compared to alarm management

understood to have been designed to deliver 6σ benefits. Six Sigma utilizes two variants of a work process with acronyms DMAIC and DMADV. DMADV is used for processes that have not yet been developed; DMAIC is for processes that exist but need improvement.

Table 1.11.2 shows how alarm management and Six Sigma line up. Both alarm management and Six Sigma share the importance of top-down leadership, the necessity of

dedicated champions, and the requirement for proper training in and use of the technology. They are both designed for success.

1.12 CONTROLS PLATFORMS

Automatic process controls come in a wide variety of shapes and sizes. The variations start at the single loop contained in a stand-alone, separate box and progress up to tens of thousands of loops in a tightly integrated electronic and communications infrastructure. They include configurable built-in alarms and alerts. They might interface with an operator via a simple display of switches and lights. Or they might employ a sophisticated electronic display of panels, screens, sounds, and more. But they all have the same objective: keeping the plant properly operating. Since keeping something properly operating is not always easy, the equipment provides a way to inform the operator that things are not quite right. These we call alarms. Any way you look at it, it is not only possible but usual that the alarms part of things can become a problem.

Whenever alarms start to get in the way of effective operator activities, there is an alarm management problem. It matters little which controls platform or controls design is used. The concepts and technology advanced in this book are going to be useful and valid for the various controls designs and hardware/software platforms.

PLC versus DCS

The two workhorses of industrial controls are the programmable logic controller (PLC) and the distributed control system (DCS). At one time, PLCs were rarely used for heavy-duty continuous manufacturing operations and DCSs were seldom used for high-density sequencing and other intensive, stepwise production operations. The scale of PLCs was mostly on the small side. This meant that a lot of PLCs were required to manage an operation with a large number of items. The scale of DCSs was mostly on the very large side. This meant that they required too much cost and infrastructure for smaller operations. However, today, both structural platforms have been developed to be more scalable, and both have evolved to provide more of the other's features. Consequently, it should not be surprising to find that both alarm problems and alarm management solutions are not substantially different between them. This is not to say that there are not differences that bear discussion and special approaches. There are and they do.

The key differences derive from both inherent differences in the hardware platforms and associated equipment and the tendency to use PLCs for manufacturing facilities that have a large amount of equipment that is used for only parts of the manufacturing cycle or used for only specialized products that share the same controls infrastructure. The list includes the following:

- PLCs have either a dedicated hardware interface panel, no dedicated interface, or a more highly structured (and therefore less user configurable) electronic interface.
- PLCs have limited options for dealing with alarm matters.

- PLCs have limited ability to dynamically link information databases to operational displays.
- PLC-controlled older plants can have far fewer configured alarms.
- PLC-controlled plants have a significant number of pieces of equipment that are not used during portions of the manufacturing cycle.
- PLCs usually control operations that often produce different products at closely spaced but different times.

For a DCS, the first statistics that announce alarm performance problems are the large number of configured alarms, the high rate of alarm activations, and the dearth of useful information and guidance. It isn't uncommon to find several thousand alarms configured for each operator station.

For PLCs, the alarm performance problems are usually solved by ensuring that alarms are relevant to the current stage of manufacturing operations and that they provide useful operator support information and guidance. It is not at all unusual to find only a few hundred or less alarms configured for an operator area. Moreover, these processes very often involve portions of a plant that are used at different times (and so parts are shut down) or used in significantly different operating modes.

PLC Special Considerations

Most of the important benefits from enhanced alarm control will come from the ability to eliminate alarms from equipment that is not currently being used for production and spared equipment. Another benefit will come from the ability to tailor alarm configurations to the current production states. Thus, the key logic portions of interest will be *out-of-service plant* and *operating mode*.

In order to facilitate these logical judgments, it is very important that the alarm control/management engine be able to determine exactly where the plant is and exactly what equipment is part of the current campaign and which is not.

1.13 CONTINUOUS VERSUS DISCRETE AND BATCH

Alarm management came into the forefront because of the serious problems we saw in the continuous manufacturing industries. Many of the examples are taken from those applications. However, the methodology and technology is equally applicable to discrete manufacturing and batch production. The foundations are identical. The approaches are the same. Yet the practitioners in the discrete and batch industries are quick to say that their problems are different. Yes, the problems are different. But alarms are still used for the same reason. Operator overload is the same. The basic differences are illustrated in appendix 10. Please refer there for a detailed comparison between the manufacturing modalities.

Generally, the batch process industries will be spending more time defining the operating regimes and different situations under which the same or similar alarms are active and how the operator responses might differ for the same alarm due to the plant being in different operating situations. Also, there might be a different methodology for notifying operators of alarm activations, since they often are away from PCS operating screens during production runs.

1.14 APPLICATION EFFECT ON ALARM DESIGN

There is no form of manufacturing operation that cannot benefit from an effective alarm system. Chemical plants, petrochemical plants, breweries, bakeries, food processors, pulp and paper operations, power and distribution plants, pharmaceutical plants, metals and mining operations, upstream petroleum, and others too diverse to list here, all experience abnormal operation to the extent that the operator requires proper notification. Even to the inexperienced eye, most of these plants differ from others greatly. It is natural to ask how applicable all of this alarm management technology is to these broad classes of manufacturing. Do the different industrial segments have differences that affect how their alarm systems are designed? The answer is yes, but not strongly.

Current alarm design is sufficiently rich to be fully applicable to industry across the board. The fundamental concepts are valid. The process is viable. The end results are effective. But, the alarm systems are different. They are responsive to different needs. They utilize different hardware and software and they look different. Space and energy do not permit this book to approach a full discussion of the detailed differences between the many forms of application. Therefore, a decision was reached to target the general forms of petrochemical, power, and related manufacturing.

A brief discussion of how alarm system design would be responsive to differing manufacturing forms can be useful to illustrate how universal this technology can be. Consider how the alarm system might be designed to handle shutdown events. We examine a traditional chemical plant operation and contrast it with a remote offshore crude oil production platform.

Onshore plants are generally designed to take advantage of adequate space between dangerous parts of the plant and to provide multiple escape routes for personnel and multiple access routes for emergency preparedness and response activities to commence. Offshore platforms cannot be. Offshore, both the close proximity of equipment and personnel and the almost complete isolation from escape and rescue combine to require a more conservative design of conditions that prompt shutdown and a more stringent requirement for a proper shutdown. The operator has significantly different duty between onshore and offshore, and the alarm system design must be responsive to that need. Nonetheless, the alarm design principles and execution are quite similar for both.

	Chemical plant	Offshore platform
Normal operation	Alarms are designed and documented based on EEMUA and other best practices.	Alarms are designed and documented based on EEMUA and other best practices.
Before shutdown	Alarm system is designed to avoid shutdowns by enabling appropriate operator intervention when safe and possible. No shutdown confirmations are used as alarms.	Alarm system is designed to avoid shutdowns by enabling appropriate operator intervention when safe and possible. All shutdown confirmations are used as alarms.
After shutdown	Alarms are still active for all plant conditions that contain stored energy or dangerous materials or represent a risk to the integrity of the plant. Preshutdown alarms and (early-out) shutdown causative event(s) alarms are examined.	Alarms are still active for all plant conditions that contain stored energy or dangerous materials or represent a risk to the integrity of the plant. Postshutdown alarms are carefully examined to ensure that 1. the shutdown was complete and proper; 2. the shutdown contains no residual danger or risk; 3. the shutdown event raised no additional danger or risk. Preshutdown alarms and (first out?) shutdown causative event(s) alarms are examined.

Table I.14.1. Example of differing alarm design requirements for chemical plant versus offshore oil platform

I.15 TIME AND DYNAMICS

By now you are becoming familiar with the idea that alarm management is about production events where either something has gone wrong, the operator isn't really sure whether something has gone wrong, or things are OK. It turns out that both process dynamics and time are going to be very important to the fabric of successful alarm design. Let's take a look at the general time-dynamics situation. We will do this using a

fictional plant and a hypothetical form of view into the nature of that plant. The view is shown in Figure 1.15.1.

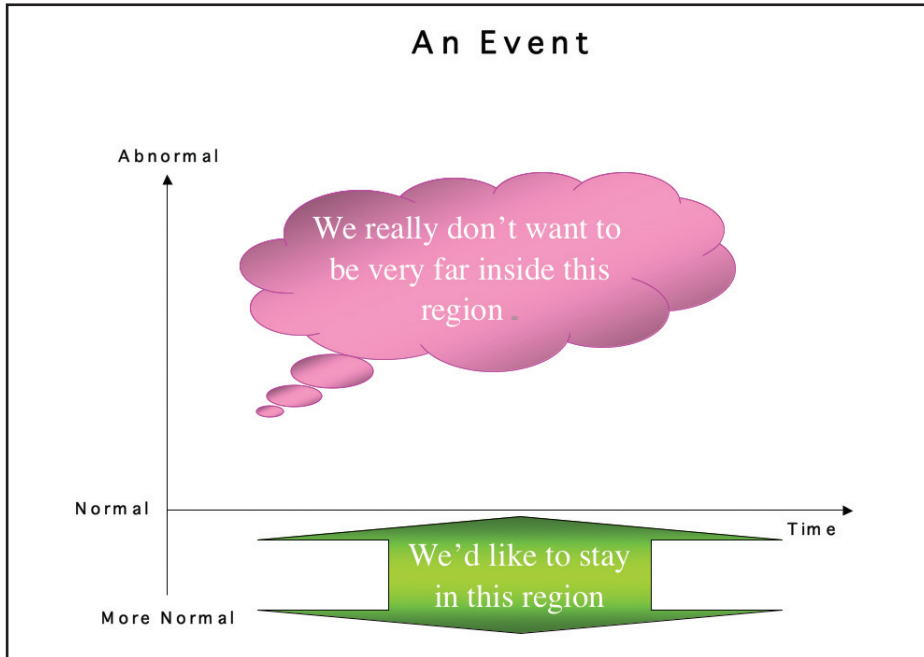


Figure 1.15.1. Magical viewer stage

In the figure we see a horizontal time line with the passage of time depicted as movement to the right. There is a label for “normal” at the left end of the time line. “More normal” which means that our magical viewer is telling us that the process is moving in a direction to be more normal, is below the time line. “Abnormal,” meaning our process is moving in the direction of becoming more abnormal, is above the time line. Let’s look into our “actual” fictional process timeline shown in Figure 1.15.2. There are eight segments in the response.

<i>Normal</i>	We start out with the process just a bit in the normal region (segment label NORMAL). For a while, the process moves into the abnormal region and then back into the normal region.
<i>Abnormal (no alarms)</i>	This segment (ABNORMAL—NO ALARMS) picks up from the NORMAL segment and moves deeper into the normal region before heading into the abnormal region. We are abnormal, but notice there are no alarms due to the process being in this state!
<i>Abnormal (alarms)</i>	Time progresses. This segment (ABNORMAL—ALARMS) sees alarms activate. At this point, the operator has received notice of a problem. The process continues to become more abnormal.

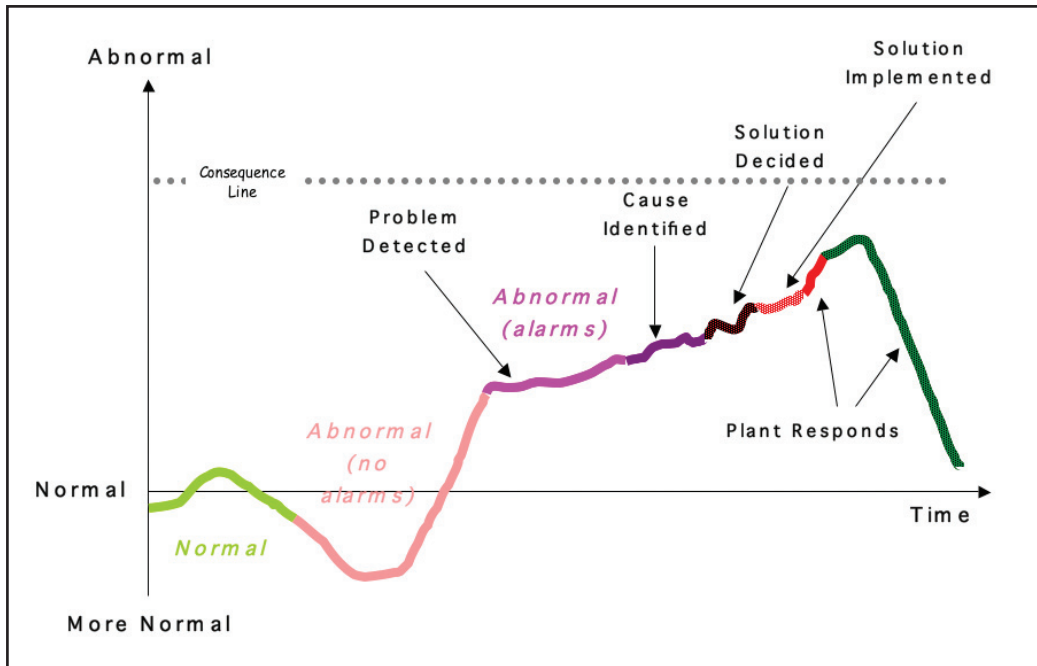


Figure I.15.2. Looking into our process

Cause identified

In this segment, the operator identifies the causes of the alarms. That is, the operator is now aware of what (is believed to be) the cause(s) of the abnormality. The process continues to move deeper into the abnormal region.

Solution decided

Time continues to progress while the operator decides what to do to remedy the problem(s). He decides here. But the process continues deeper into the abnormal region. Why? (A decision by the operator is not anything that can be “felt” by the process. The process must wait for the action.)

Solution implemented

Here the operator implements the remedial plan. Changes have been made, yet the process continues to deteriorate. Why? (An action is only a starting point. The process has dynamics or inertia. It will change in response to changes by the operator, but only in directions and with speeds that are inherent to its fundamental makeup and in some proportion to the magnitude of operator change.)

Plant responds

Next, finally, the plant responds—yet that response moves it deeper into the abnormal region before eventually and rapidly returning to nearly normal.

What does this little fictional account tell us? First of all, it illustrates that it is possible for plants to become abnormal without producing alarm activations. Next, everything takes time. It takes time to discover the problem, understand it, decide what to do to correct it, and implement it, as well as for the plant itself to respond. Therefore, alarm redesign must take into account that plants can only respond in a limited way and that response will take time. Both the ways it can respond and the time it will take are basic and inherent to each particular process.

1.16 HISTORICAL INCIDENTS

The inadequate performance of PCS alarm systems has become a significant cause of industrial incidents and serious accidents. Often either process plant operators are kept unaware of abnormal conditions due to the failure of appropriate alarms to activate or they did not activate with sufficient time to permit the operator to react effectively. We also see the “blinding” of operators by the tremendous avalanche of alarms during upsets. This effectively prevents the operator from identifying which alarms are important and which are not. In both cases, the very tool that was supposed to warn and guide the operator during an abnormal situation not only failed to do either but created a distraction and additional stress. Eventually, this interference leads to escalation of seriousness by causing what started out as a minor manageable upset to produce major accidents, some progressing to serious disasters.

Three Mile Island

At about 4 a.m. on Wednesday, March 28, 1979, a series of failures and operational missteps occurred that resulted in the release of a small but measurable amount of radioactive material into the air. While this incident did not lead to serious physical loss, the enormous political reaction would curtail all building of nuclear power reactors in the United States for the next four decades.

Interestingly, the specific alarm management issues relating to this incident presaged most of the modern approach to alarm management today.

- Alarms are not applied properly due to a misunderstanding of the purpose of alarms and a failure to appreciate the scale of using them without careful consideration.
- The use of alarms is not sufficiently well understood. One must measure relevant data, infer performance (metrics), know what to do in the event of alarm activation, and know how to build alarms.
- Alarm design reaches deep into the existing infrastructure: alarms must be coordinated with plant design and culture.
- Alarm systems can really work—they were ineffectual here, but a good design could have made a meaningful difference.

- Alarm redesign is not simply an add-on—appropriate lead time is needed to arrive at a new working alarm system.

Milford Haven

In the early hours of the morning of 24 July 1994, at a Texaco refinery in Milford Haven, England, lightning struck the unit causing problems with the vacuum unit, the alkylation unit, the Butamer, and the FCC. Immediately after the strike, a number of units shutdown due to lack of utility power. A production control valve closed (we think moved to its failure position) and a unit started to fill with liquid hydrocarbon. That control valve showed an erroneous state of being “open” on a process display graphic.

In response to the hydrocarbon build up, and as designed for safety protection of the vessel, the overpressure relief valve “popped” three times. The escaping liquid entered the relief system eventually ending up in the knockout drum. The knockout drum eventually overfilled (in part due to an earlier modification that had not been properly assessed at the design time, nor appreciated during the upset). The overfilled knockout drum then spilled liquid into a relief line that was not designed to contain such a flow. The resultant failure released about 20 metric tons of hydrocarbon into the operating plant. The vapor cloud produced by this release eventually ignited about 110 meters away from the rupture, causing a major explosion equivalent to 4 metric tons of high explosive. The explosion caused \$80 million damage and injured 26 people (thankfully, none seriously).⁶

There was an investigation. The Health and Safety Executive (HSE) identified a number of contributing factors to the refinery’s inability to recognize and contain the abnormal operation. They are summarized in Table 1.16.1.

Specifically, paragraph 69 of the HSE Report states, “Warnings of the developing problem were lost in the plethora of instrument alarms triggered in the control room, many of which were unnecessary and registering with increasing frequency, so operators were unable to appreciate what was actually happening.”

HSE’s specific recommendations directly point to the necessity to provide tools and technology so that the production operator is able to detect abnormal process conditions in a way that clearly extends beyond monitoring individual values of variables and their alarms. Moreover, we see here, perhaps many of us for the first time, the addition of another important element to the operating equation: the expectation that operators be able to manage the sometimes charged issue of continuing to operate versus initiating controlled shutdowns. The implied expectation of this particular item suggests that plants clearly visit, decide, plan for, and train for situations where operators will be expected to manage the explicit issue of continuing to operate or not. Additional HSE targeted items appear as numbered items below. The reference numbers refer to specific numbered items in the formal report.

Cause factor	Cause category
The “valve open” was a command signal, not an actual feedback indication.	Faulty indication to the operator of true status of important process equipment
There was no good overview display for the operator. Existing displays focused on unit details, not situations and imbalances.	Lack of effective situation indication to the operator of true status of the process
They tried to keep the process running, hoping to find and fix the problem.	Failure of management to set high-level operating rules and procedures, thus paving the way to unsafe operating situations
The original plant design would have coped with the knockout drum overfilling; the modification was intended to reduce “slops.”	Inadequate management of change (design and operation)
There were far too many alarms; some critical alarms were “lost” in the flood.	Inadequate alarm system design

Table 1.16.1. Contributing factor analysis of Milford Haven accident

- #3 Display systems should be configured to provide an overview of the condition of the process including, where appropriate, mass and volumetric balance summaries.
- #4 Operators should know how to carry out simple volumetric and mass balance checks whenever level or flow problems are experienced within a unit.
- #5 [Provide] clear guidance [to the operator] on when to initiate controlled or emergency shutdowns.
- #6 The use and configuration of alarms should be such that safety critical alarms, including those for flare systems, are distinguishable from other operational alarms; alarms are limited to a number that an operator can effectively monitor; and the ultimate plant safety should not rely on operator response to a control system alarm.

Texas City

At five minutes after three on the morning of 23 March, 2005 [at the BP refinery in Texas City, Texas], a high-level sensor alarm went off indicating rising levels of flammable hydrocarbons in a distillation tower, but a redundant alarm

never went off on the day of the accident, the investigator said. The [investigating] board estimated that liquid inside the tower ultimately reached a point of 120 feet or more. The tower normally operated with less than 10 feet of liquid at the bottom.⁷

The incident involved the raffinate splitter (a distillation column that separates gasoline-blending components) and the blowdown drum and stack (F-20), designed to handle pressure relief and vent streams. The investigation concluded that the explosions were most likely the result of ignition of hydrocarbon vapors released from the F-20. These hydrocarbons were discharged when the pressure in the splitter column increased rapidly and exceed the set pressure of the overhead line relief valves. The F-20 was unable to handle all of the fluids, vapors, and liquid discharged from the top of the stack. An unknown ignition source from the numerous potential ones present in the uncontrolled area (vehicles, trailers, etc.) ignited the resulting vapor cloud.⁸

The [incident] resulted in 15 deaths, about 170 injuries, and significant economic losses, and was one of the most serious U.S. workplace disasters of the past two decades. Key alarms and a level transmitter failed to operate properly and to warn operators of unsafe and abnormal conditions within the tower and the blowdown drum.⁹

Federal investigators say managers authorized the start-up of a unit in March despite knowing key alarms weren't working. That start-up killed 15 people.¹⁰

According to an Associated Press article, "The Occupational Safety and Health Administration agency also is considering whether to refer some violations to the Justice Department for possible criminal prosecution, said John Miles, Jr., regional administrator for OSHA."¹¹

Of a total of \$20,720,000 in fines levied against BP, the instrumentation and alarm system portion alone was \$2,170,000. We are led undeniably to value the importance of the instrumentation and control systems for safe process operations and the critical role played by the alarm system.

Why Now?

It must be clear to the reader at this point that the alarm system has two important functional requirements. First, it must detect and warn the operator of abnormal operating conditions that require attention. Second, it must not mislead, overload, or distract the operator while meeting the first requirement. As the above incidents tell and, unfortunately, similar ones reinforce, this situation seems to be getting worse. Why are we getting more alarms now than ever before? The answer points to an interesting illustration taken from nature: an iceberg (Figure 1.16.1). An iceberg floats with a bit less than 10% showing above water and the remaining 90-plus percentage hidden below. We see alarm

problems “above the waterline.” We do not see most of what really causes them “below the waterline.”

There are a number of suggestive industry trends that bear on the causes below the waterline. The affected industries have been mostly mature ones. Their products tend to be commodities. Over the past two decades, there have been serious economic pressures in these segments. The response of the enterprise managers was to cut costs, try to force operating responsiveness to more closely follow fast-changing market pressures, and adopt the expectation that new investments would rarely be forthcoming. This in turn led to the reduction of engineering and other support staff and the outsourcing of an increasing portion of what little technology applications remained. The causal

chain leads to plants having individuals with much less experience in both design and maintenance. The ultimate effects of all of this, eventually and proximately, wind up in decreased process reliability. Decreases in reliability show up as increases in abnormal operations. Abnormal operations are usually announced first by alarms. Hence, we see more and more challenges to the alarm system, just at a time that we have come to learn that the “tried and true” design is itself inadequate! We see (fig. 1.16.1) larger numbers of alarms (ice above the waterline). But those alarms are very often the result of underlying deficiencies (ice hidden below).

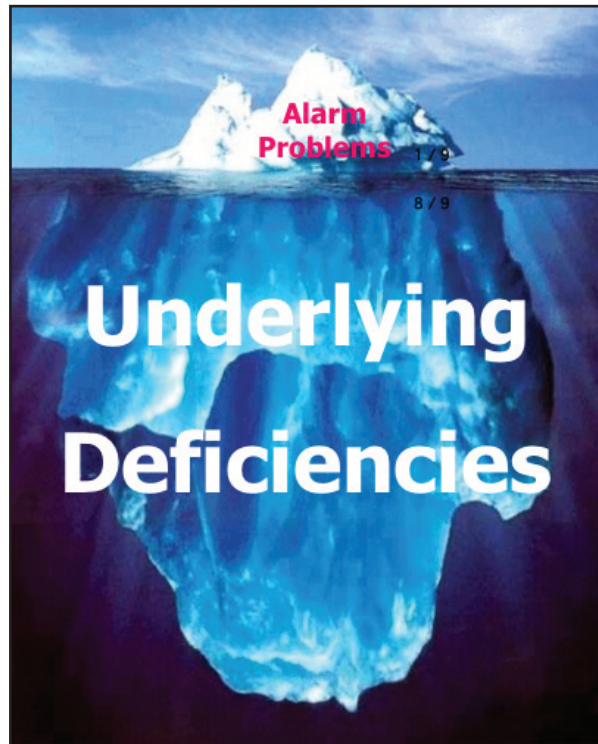


Figure 1.16.1. The iceberg of alarm management

1.17 THE NEW DESIGN

Not by Subtraction Alone

It will be very helpful for us to recognize that alarm management problems will not be, nor are most problems generally, solved by subtraction alone. That is, we should not expect to improve the alarm system simply by deciding which of the already configured

alarms must be removed. Many of those old alarms had been configured to assist the operator in some way. Unfortunately, those alarms did not deliver the expected aid. There are new alarms that need adding. Therefore, other, more effective means must be sought to fill in that void. Redesign is a package deal. It will change the look and feel of many of the operator's tools. It first requires the establishment of a philosophy with a set of clear alarm system design objectives and operating parameters. This philosophy includes specific guidelines and practices for the new alarm design. It also will visit what, if any, important tools will be added to provide operator assistance to manage situations that were, in error, assigned to the alarm system alone. Permission to operate and the situation awareness tools are examples.

Starting Alarm Improvement

Data gathering and analysis are used to provide a clearer understanding of existing deficiencies. Baseline performance metrics are calculated and used to specifically understand exactly what the current alarm system is doing. Later on, we will use these same measures to evaluate the new design behavior. Alarm conventions are established to determine the minimal required alarm configuration for the plant. Rules for priority and alarm activation points are established. Each alarm is fully documented, which, incidentally, results in a very good training and diagnostic tool for operators. Other advanced techniques are developed to help control alarm flooding as well as to ensure that extraneous alarms are reduced. Graphics are evaluated and improved to provide operators with the ability to understand the degree of normal of their plant operation.

Alarm Philosophy

All enterprises have goals for their operation and recognized limitations as to what they can accomplish. The alarm philosophy will recognize both and incorporate them into the alarm improvement process. In the alarm philosophy, alarms are defined, appropriate operator responses are identified, success criteria are established, and the roles that all other parts of the enterprise should provide to support the alarm system redesign and subsequent operation are explained. This is where the complete design is framed. Think of the philosophy as really meaning “fully expanded design specification” sufficient to provide the alarm improvement teams with the clear guidance necessary to produce the new alarm design.

Data Gathering and Analysis

No problem is understood until its true magnitude is known. Much of our information up until now is anecdotal and subjective. Hard data will be needed for the plant to understand the problems and generate the redesign activities to make the extensive modifications and improvements necessary to provide the proper operator support. Yet it

is the very nature of the problem that makes the capture and analysis of the data hard to do. The amount of data is extensive. For example, it is not unusual in any given 24-hour operating period for a typical plant (one board operator's area) to produce 1000 to 2000 entries in activity logs. These logs normally include alarm activations, alarm acknowledgments, alarm clearings, operator actions, and system status events. Three months of data are usually used. This normally means from 125,000 to 250,000 entries.

Let's look at some typical data. Figure 1.17.1 shows the frequency of occurrence of the top eleven alarm events over a period of 30 days. It has been sorted from highest to lowest. For example, the highest event, an off-normal alarm, occurred nearly 20,000 times. The eleventh highest event, also an off-normal alarm, occurred over 2000 times. Just considering the top eleven events, the operators of this area had to face an alarm about every 30 seconds, hour in and hour out. We will see in a later metrics portion of this book that this rate far exceeds any operator's ability to manage. And just as clearly, we conclude that either such frequent interruption will severely stress the operator or, what usually happens, alarm events will be relegated to background noise and largely ignored.

During upset conditions, alarms can activate so quickly that they actually appear to flood the system, hence the term *alarm flood*. Figure 1.17.2 depicts how a typical alarm flood might look. In our example, during a 5-minute period at the onset of flood, as many as 900 alarm events occur. Interestingly, alarm floods actually are defined to begin

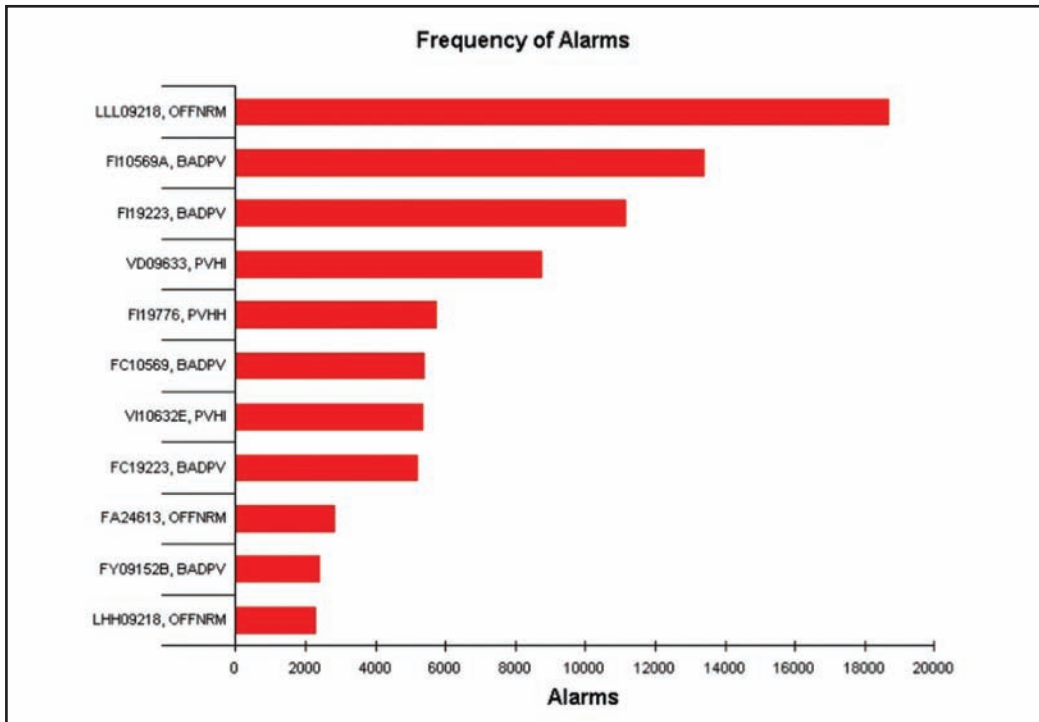


Figure 1.17.1. Number of alarm occurrences within last 30 days (by frequency)

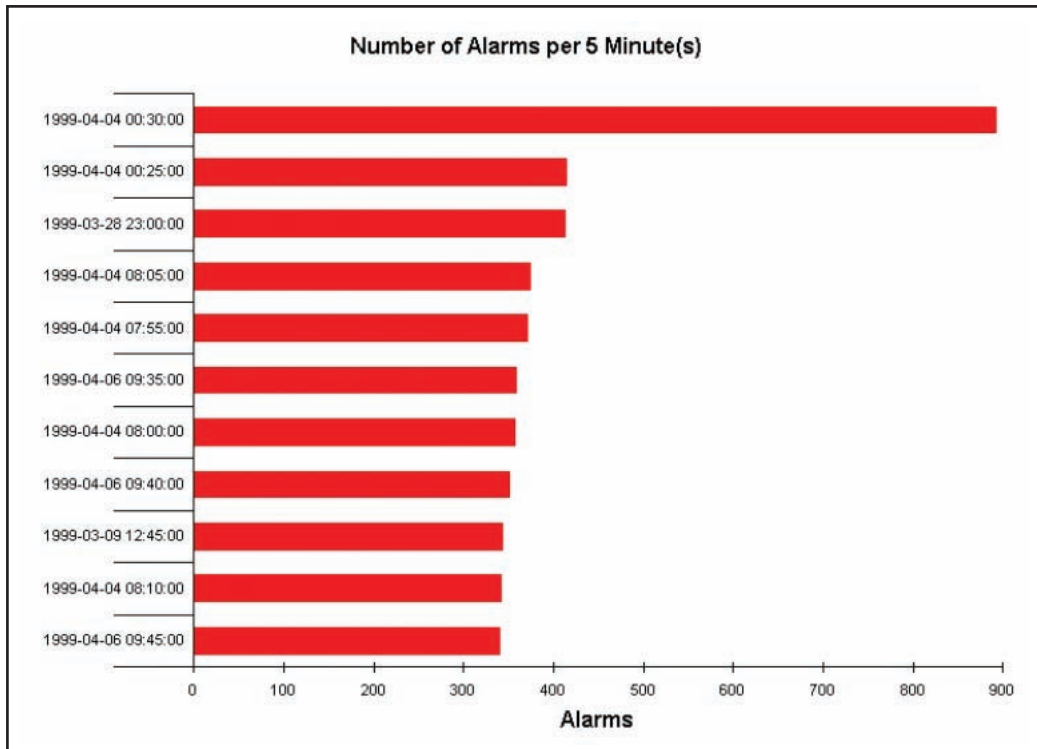


Figure 1.17.2. Example of an alarm flood

with ten or more alarms in a 10-minute time period. The figure shows typical alarm activation rates during an “alarm flood” situation to be 70 to 180 per minute (350 to 900 per 5-minute period). This calculates to be between one and three alarm activations per second. This is far beyond anyone’s ability to even read, much less understand and respond to.

Figure 1.17.3 illustrates the effects of the lack of uniform standards for setting of alarm priority. This figure differs from the earlier two in that it shows data from the PCS configuration. The bars do not represent activations, though it is likely that there will be some relationship. Note also that the ratio of low-priority to emergency-priority alarms is somewhat out of balance (it should be closer to ten or more to one, as opposed to two to one, as shown). However, the most startling discovery is the very large number of high-priority alarms in proportion to low-priority. We expect a ratio of four to five low-priority alarms to each high-priority alarm. In the case shown, the high priority is actually over two-and-a-half times more than the low priority.

Figure 1.17.4 demonstrates a clear lack of correlation between alarm activations and operator actions. Recall our fundamental definition of an alarm: $\text{ALARM ACTIVATION} = \text{OPERATOR ACTION}$. In this example, the alarm activations are a factor of 25% to 400% greater than operator actions. A good design has them about equal. It can be estimated

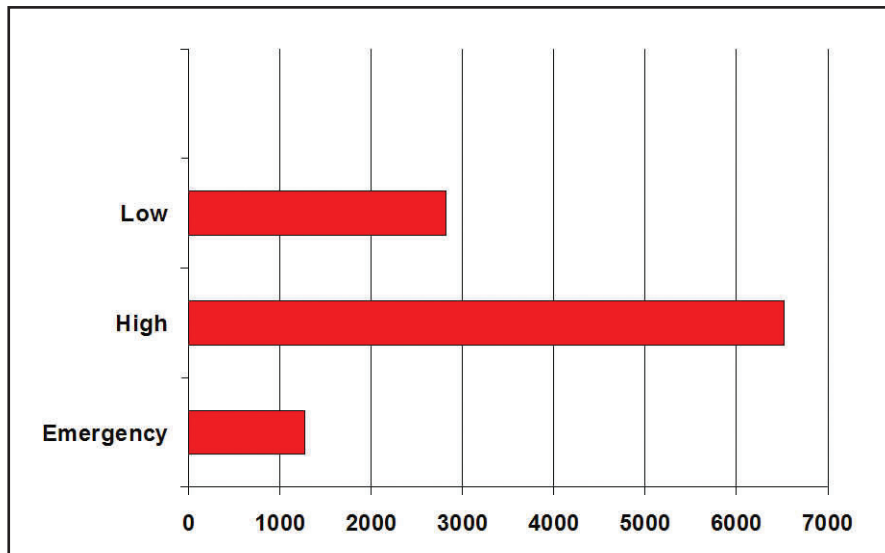


Figure I.17.3. Typical alarm priority spread

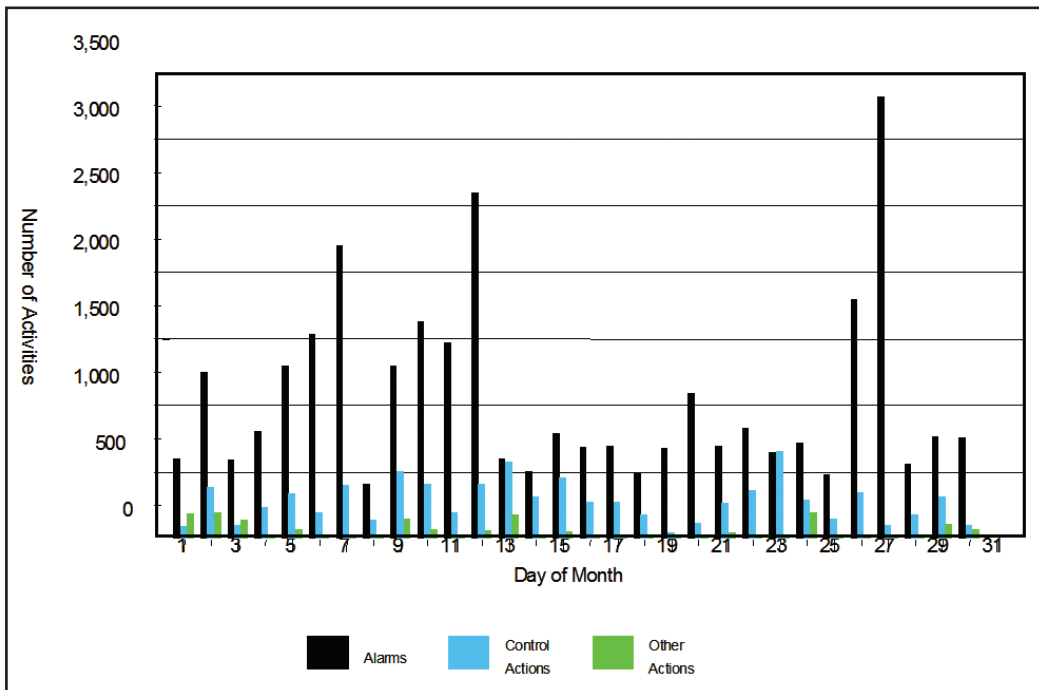


Figure I.17.4. Link between alarms and actions (3 months)

that actions occurred for only about 30% of the alarms. A conservative estimate would conclude that the alarms could be pared down to less than one third. The alarm system should not substitute for operator vigilance. Alarms are not “wake-up” calls. Useless alarms serve no purpose.

- Any alarm activation that occurs for which the operator has no understanding of what action is called for is a useless alarm.
- Any alarm activation that occurs for which the operator knows the action but cannot implement it is again a useless alarm.
- Any alarm activation that occurs for which the operator knows the action and implements it but cannot determine whether the action has been effective is a useless alarm.
- Alarm activations that occur too quickly for all to be either acted on or understood are useless. (The alarm system itself has been identified as a prime cause of an operational upset for many of these cases.)

Now that we have had a chance to look at typical data, we are in a better position to understand the importance of the basics of effective alarm management. A key benefit derived from the alarm performance data is the identification of “bad actors.” Quite often, a relatively small percentage of configured alarms will be responsible for a large percentage of the actual alarm activations. Refer again to Figure 1.17.1. Looking at the first tag (the one at the top in the rank-ordered list), activations occur about ten times the activation rates of the last two tags in the list. To place these first eleven in perspective, the median number of all activations for the month is approximately 1/10,000th of the highest one. This exponential form of falloff is typical. To eliminate bad actors, focus on the underlying issues that led to the alarms: wrong point to alarm, incorrect alarm limit, unresolved process or instrumentation problem, inconsistent alarm activation parameters (lookup, etc.), and more. But, as troublesome as they are, bad actors are only part of our problem. Simply fixing them all will not resolve your basic alarm management limitations. Redesign is in order.

Your data can be instrumental in assisting the improvement teams to develop a proper and useful alarm philosophy. A good philosophy is the blueprint for a good design. Once the nature of the problem is better understood, it aids the process of focusing on the major contributing aspects to the problem. Understanding the data requires tools. Chapter 4 discusses the major providers and their products.

Alarm Conventions and Redesign Guidelines

A useful measure you will use to evaluate the design of your alarm system will be to compare your site’s data against established norms for the industry. There are two categories of data: static and dynamic. *Static data* are the data contained in the PCS configuration that specifies what is alarmed and how. This type of data is also referred to as *configured alarm data*. *Dynamic data* are the data contained in alarm activation logs. Each time an alarm occurs, it is called an alarm activation. A single configured alarm can activate

many times (it will generally do so every time the process variable crosses over the alarm limit). Many configured alarms never activate. Clearly, there is a link between configured alarms and alarm activations. However, the link is rather indirect, though the more that are configured, the more will likely activate. As we have seen, this is especially true during upset situations.

The list of static alarm metrics includes the following:

- Number of alarms configured; the priority spread of configured alarms
- Number of alarms configured per control loop
- Number of alarms configured per analog measurement (not part of a control loop)
- Number of alarms configured per digital measurement

The list of dynamic alarm metrics includes the following:

- Short-term rates of activations
- Long-term rate of activations
- Priority spread of activations
- Time for the operator to acknowledge alarms
- Time for the alarm to return to normal
- Rate of activations during alarm floods; number of stale (or standing) alarms
- Ratio of alarm activations to operator actions

The alarm system is redesigned to bring the plant's data closer to industry standards for the related applications. Alarm system redesign involves a complete review of all alarms. It uses the alarm philosophy to enable system designers to set standards and implementation criteria to design a properly functioning system. Most major aspects of the enterprise will be examined. They include operating procedures and practices, control graphics, training, and maintenance. The process of redesign (alarm rationalization) relies on a hierarchy of specialized procedures. In the final analysis, it is really quite straightforward:

1. Eliminate all redundant alarm points or start from no configured alarms and configure only the minimum needed alarms.
2. Determine the alarm activation point(s).
3. Determine the correct priority for each alarm.
4. Develop a plan to handle each alarm—what it means, how to recognize its symptoms, and what to do to remedy the problem announced by the alarm activation.
5. Design the strategy to handle alarm flood.
6. Design an enhanced ability of the operator to detect early malfunctions of the plant.

7. Design the implementation plan.
8. Document all changes (manuals, graphics, management of change, training, etc.).
9. Work out the process for keeping the design effective down the road.

Using the above process, you will find either the number of points in the new alarm system is modestly less than it was originally or they are substantially less. It all depends on how carefully the alarm philosophy was developed and how dedicated its application was to the alarm improvement process. If the results achieved do not appear to be sufficient, the process is repeated, with more attention to truly understanding the essential need for each alarm.

1.18 EXAMPLE ALARM REDESIGN (RATIONALIZATION) RESULTS

One of the more surprising realizations to relative newcomers to alarm management is how many alarms are eliminated or modified by a proper rationalization. In the beginning, they are prepared to find from a quarter to a half of the original alarms eliminated. In fact, the expected reduction is more like 75% or 80%. At this point, the reader must be coming face-to-face with the realization that there is more to alarm improvement than a bit of handy engineering.

As an example, and to illustrate the process and results to themselves, a chemical plant developed a test site case for alarm improvement. This particular test was a small part of a single-operator area. They start out with a total of 154 configured alarms. What follows is a line-by-line explanation of where the alarm system was modified. Please take care to note that while each line item is correct, many of the categories overlap. Therefore, simple mathematically sums will be misleading.

Start with 154 configured alarms.

- 62 (of the 154) were deleted outright. They were unnecessary.
- 59 (of the remaining 92) had documentation errors that were corrected.
- 52 (45 from the 92 remaining; 7 from the 62 deleted) changed to alerts (an alert is a message to the operator that does not use the alarm system to deliver; see chapter 12).
- 50 (of the 47 remaining, some more than one each) had configuration corrections (some aspect of the point needed to be changed to conform to the original engineering design requirements; changes included priority and alarm setting below).
- 26 (of the 47 remaining) had their priority changed.
- 19 (of the 47 remaining) were reduced to 7 alarms.
- 7 (of the 35 remaining) were reduced to a single alert.
- 3 (of the 28 remaining) had the alarm settings changed.
- 2 new alarms were added (making a total of 30 alarms).

- 1 new alert was added.
- 14 (of the 30 alarms) were “toggled” on or off based on plant state.

RESULTS:

- 30 configured alarms
- 53 alerts (52 initially, which counts the ones reduced to an alert, plus the added alert)

This is an 80% reduction in alarms. They were able to gain this impressive improvement only by going back to basics. Tinkering just prolongs the process. Success is attained by understanding the real purpose of alarms and seeking fundamentals by which to approach a redesign. Applying the new knowledge and using good engineering practices can attain truly impressive results.

1.19 COMPLETING THE DESIGN

It has often been recognized that good alarming practices can be achieved only after the production plant process itself is better understood. As a result, not only is the plant on the way to an improved operational tool (the alarm system), but the operators better understand what they are doing and how best to do it. It is a nice synergy.

There is more to be gained if you are to realize the full potential of your redesigned alarm system. The remaining topics provide the ingredients for task completion.

Advanced Techniques

Up until this point, all of our focus and discussion about alarms has been about alarm points individually. We decide whether or not to alarm the point. If we alarm it, we assign activation points and priority. Then we decide what to do about the alarm. But the alarm points individually are only part of the story. Just as the plant is interrelated and interconnected, so are the alarm points for the plant. We now take into understanding these interrelationships. Using advanced techniques (discussed later), you will eliminate alarms for equipment that is not operating at the time. You will also manage alarms that can occur individually but often occur together. There are various means to do this. Most employ some logic to detect operating states of equipment or alarm status of other alarm points.

Situation Awareness

About now careful readers are about to reach a conclusion:

Now that I've carefully done all that was needed to redesign my alarm system, I feel that I have ended up with many fewer alarms than I thought I needed to run

my plant. How am I supposed to find out what is really happening deep inside it? How will I know that something might be wrong? What do I need to know to tell the operator when anything does go wrong?

If alarm system design were as far as it goes, the answer would have to be, “You’d just have to take your chances with fate.” Fortunately, this isn’t as far as things go. Our next step will be to improve the operators’ ability to watch the process and understand how it is actually performing, which is, after all, one of the key reasons why the alarm system is there and why it somehow grew into that awful monster that caused most of the alarm management problems we needed to fix. This ability to understand the operating condition of the plant is called *situation awareness*. To acquire situation awareness we provide the operator with tools for early detection of operational problems. Such tools include sensor validation, valve monitoring, control loop integrity monitoring, and process condition monitoring (tower flood, reaction runaway, compressor surge, etc.). These tools provide a significant benefit over the old way of hoping that either the operator can spot the problem or, if he does not, the alarm system will detect it for him in enough time for disaster to be avoided. There are a growing number of techniques and commercial tools now in the marketplace to assist situation awareness and thus improve production.

Operator Screen Design

Key to better plant performance is the operator’s ability to see what’s going on in the process. Graphic control screens are the primary means to do that seeing. When the screens do not guide the operator, when the information is too hard to find, when the information is confusing, or when the information is not there, the operator will not be able to manage as well as required. The current best practices in operator graphics involve a hierarchical structure of displays, clear navigation between displays, and a straightforward causal organization of information on each display (limits on use of color, control of flashing items, and exploitation of icons over text and figures, to name a few). Chapter 12 contains complete coverage of this material.

Operational Integrity Improvement

Anyone who spends time looking over the shoulder of a production plant operator will quickly realize what an enormous task it is to watch the many hundreds of variables, keep track of how they interact, and detect developing problems. Most try. Very, very few are able to do it well. The new approach relies on some very solid, traditional engineering:

1. Design and build the physical plant for operability
2. Develop and implement comprehensive procedures for operation and maintenance
3. Train extensively
4. Keep things maintained

5. Monitor performance
6. Feed results back and make improvements

Condition Monitoring

As important as they are, the items above are not sufficient to do the job. Consequently, there are a number of specialized tools to assist the operator. They range all the way from sophisticated mathematical techniques to pragmatic algorithms. An abbreviated list includes the following:

1. Controller tuning monitors
2. Controller mode tracking and utilization monitors
3. Extensive mass and energy balances
4. Sensor validation
5. Unit operation integrity monitors
6. Multivariate statistical analysis (multivariable state estimation)
7. Advanced controls
8. Adaptive controls

1.20 ALARM IMPROVEMENT PROJECTS

We have recognized the need and have the desire to improve our alarm system. Here are the key steps in the process.

Phase I: Problem Awareness and Solution Framework

- *Assess the current alarm situation.* Assemble the data-gathering tool kit, gather alarm performance statistics, identify upset histories, and assess equipment maintenance relationships with operational integrity and alarm performance.
- *Develop an alarm management philosophy.* Make the effort plantwide, include relevant enterprise goals, and provide guidance and specifications for alarm redesign.

Phase II: Alarm Redesign

- *Do housekeeping.* Fix all of the other problems in the facility that have been engineered and installed and should be working but are not.
- *Perform alarm rationalization.* Conduct actual redesign of alarm system including configuration and graphics.
- *Incorporate enhanced alarming techniques.* Design any enhanced alarm capabilities needed for managing alarm flood and so on.

Phase III: Implementation

- *Reconfigure PCS for new alarm system design.* Install new configuration changes (including parameters and priority modifications) and graphics.
- *Modify operating procedures to align with new alarm design.*
- *Modify training to align with new alarm design.*
- *Complete a management of change.*

Phase IV: Continuous Benefit

- *Perform periodic follow-up alarm performance studies.*
- *Investigate alarm floods and process upsets.*

1.2I LESSONS FOR SUCCESSFUL ALARM MANAGEMENT

As you have come to expect, this book is going to reach straight for the problem of what's wrong and then march directly onto the path of a successful resolution to get it right. To do this well, you will need the eyes of a military lookout to see the real problems, the wisdom of a seer to get to the heart of the matter, the strategy and planning of a general to get it done, and the heart of a healer to keep the heady success vision from overcoming the needed reality to get it done with style and respect.

Lesson 1—THEORY

- *Beautiful theories are often destroyed by ugly facts.* Improving the alarm system alone will not improve the control room.

Lesson 2—PROGRESS

- *Real progress often requires a change in direction.* It is time to end the “blame the operator” approach to control room problems.

Lesson 3—HISTORY

- *Do not forget about history.* Incidents and accidents are powerful teachers but not the only ones.

Lesson 4—HUMILITY

- *It is always wise to maintain some humility.* Almost everything we think we know about alarms will change.

Lesson 5—TRUTH

- *Technologists must always have a single agenda—the truth.* Get good data, perform adequate analyses, and believe the results.

Lesson 6—EVIDENCE

- *Incredible results require incredible evidence.* Plants without a lot of alarms actually work better.

Lesson 7—FUNDING

- *A good idea does not always attract funding.* EEMUA, OSHA, ISA 18, and NAMUR all need a business case as well.

Lesson 8—PREPARE

- *Be prepared to be unpopular and uncomfortable.* Every activity in the plant will be touched by alarm improvement work.

1.22 IMPORTANT DESIGN AND SAFETY NOTICE

In addition to the broad and comprehensive approach to developing a working solution to the alarm management problem, an important strength of this book is the wealth of examples, alternatives, and suggestions for your consideration. All control schemes, design suggestions, displays, diagrams, tables, figures, trend charts, and the like described and illustrated in this book refer to materials that have been designed to amplify and explain concepts and practices used for alarm management understanding. They are provided for training and understanding purposes only and are not intended for implementation. The choice of which aspects to alarm for the plant or process, the parameters of that alarm, the proper operator response to correct the alarm condition, and all other details of that alarm must be retained wholly by qualified, authorized members of the plant staff, who must act with full knowledge of their specific plant configuration, process conditions, equipment, and applicable statutory practices and requirements.

No single work is capable of conveying the entire collective experience and important nuances necessary for success. After reading this book, it is recommended that plants with intentions or plans for alarm improvement seek additional specific guidance and experience from knowledgeable experts.

1.23 CONCLUSION

Alarm management problems announce themselves. There are always alarms on the screen. Alarms occur too often or too quickly when things go wrong. When lots of alarms do activate, it is rarely clear what to do about them. Sometimes, the very alarm system itself contributes to poor upset response.

Successful alarm management works because it points the way to significant plant improvements. Not only are the alarm activations less frequent but they are more meaningful when they do occur. And quite apart from individual alarms, the redesign process points out the need for operator support tools to identify early process problems and to better convey the plant information through the graphics. Alarm management is truly a synergistic activity!

I.24 NOTES AND ADDITIONAL READING

Notes

1. Larry O'Brien and Dave Woll, *Alarm Management Strategies*, ARC Strategies (Boston: ARC Advisory Group, 2004).
2. Engineering Equipment Materials Users' Association, *Alarm Systems—A Guide to Design, Management and Procurement*, EEMUA Publication No. 191 (London: EEMUA, 2007), 91. <http://www.eemua.co.uk>.
3. Kevin McCarthy, "Facing a Long-Term Memory Loss," *Power Engineering*, October 2008, 112, 100.
4. John M. O'Hara and William S. Brown, "Human Factors Engineering Guidelines for the Review of Advanced Alarm Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, NUREG/CR-6105 BNL-NUREG-52391 (Washington, DC: U.S. Nuclear Regulatory Commission, 1991).
5. Chris Wilson, *Applying Six Sigma to Alarm Management*, TiPS TechDoc White Paper (Georgetown, TX: TiPS, Inc., 2008).
6. Health and Safety Executive, *The Explosion and Fires at the Texaco Refinery, Milford Haven, 24 July 1994* (Sudbury, Suffolk, UK: 1994).
7. *Fatal Accident Investigation Report—Isomerization Unit Explosion Interim Report, Texas City, Texas USA* (London: BP, 2005).
8. Ibid.
9. U.S. Chemical Safety and Hazard Investigation Board, "Urgent Recommendation [BP Texas City Explosion and Fire, March 2004]," news release, August 17, 2005.
10. InTech, Instrumentation, Systems, and Automation Society (now the International Society of Automation) (Research Triangle Park, NC: 2005).
11. U.S. Chemical Safety and Hazard Investigation Board, Investigation Report, Washington, DC, Refinery Explosion and Fire, BP Texas City, Texas, Report No. 2005-04-I-TX, March 2007.

Recommended Additional Reading

- Brabazon, Philip, and Helen Conlin. *Assessing the Safety of Staffing Arrangements for Process Operations in the Chemical and Allied Industries*. HSE Contract Research Report 348. London: HSE, 2001.
- Bransby, M., and J. Jenkinson. *The Management of Alarm Systems*. HSE Contract Research Report 166. London: HSE, 1998.
- Nimmo, Ian. *The Safety Issues of Batch (and Other) Controls*. Phoenix: User Centered Design Services, 2005. <http://www.mycontrolroom.com>.
- Shook, D. *Alarm Management—What, Why, Who and How?* Matrikon White Paper. Edmonton, Alberta: Matrikon, Inc., 2007.

- Smith, W. H., C. R. Howard, and A. G. Foord. *Alarms Management—Priority, Floods, Tears or Gain?* London: 4-Sight Consulting, 2003.
- Thomas, Brent J. “Six Sigma Alarm Management.” *ControlGlobal*. 2008. <http://www.control-global.com>.
- Wilson, Chris. *The Operations Excellence Puzzle—The Alarm Management Piece*. TiPS TechDoc White Paper. Georgetown, TX: TiPS, Inc., 2005.