ISA™

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

eBook available!

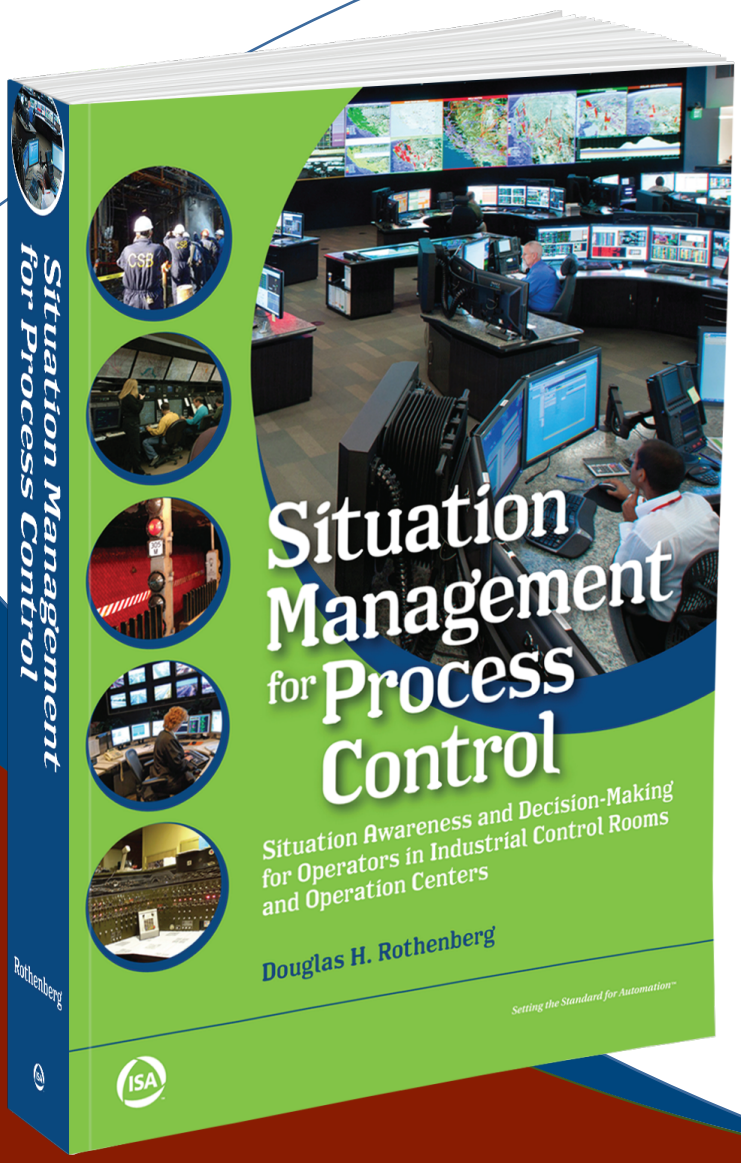

Table of Contents

View Excerpt

Buy the Book

Setting the Standard for Automation™

Situation Management for Process Control

Situation Awareness and Decision-Making for Operators in Industrial Control Rooms and Operation Centers

Douglas H. Rothenberg

Notice

The information presented in this publication is for the general education of the reader. Because neither the author nor the publisher has any control over the use of the information by the reader, both the author and the publisher disclaim any and all liability of any kind arising out of such use. The reader is expected to exercise sound professional judgment in using any of the information presented in a particular application.

Additionally, neither the author nor the publisher has investigated or considered the effect of any patents on the ability of the reader to use any of the information in a particular application. The reader is responsible for reviewing any possible patents that may affect any particular use of the information presented.

Any references to commercial products in the work are cited as examples only. Neither the author nor the publisher endorses any referenced commercial product. Any trademarks or tradenames referenced belong to the respective owner of the mark or name. Neither the author nor the publisher makes any representation regarding the availability of any referenced commercial product at any time. The manufacturer's instructions on the use of any commercial product must be followed at all times, even if in conflict with the information in this publication.

Printed in the United States of America.
Version 1.0

ISBN-13: 978-1-945541-65-0 (Hardback)
ISBN-13: 978-1-945541-99-5 (EPUB)
ISBN-13: 978-1-945541-98-8 (MOBI)

ISA
67 T. W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

Library of Congress Cataloging-in-Publication Data in process

Copyrighted Material

Contents

List of Figures xxv

List of Tables xliii

Foreword xlv

About the Author xlvii

Acknowledgments xlix

Part I Operational Integrity 1

Chapter 1 Getting Started 3

1.1 Key Concepts 4

1.2 Introduction 5

1.3 Cautions and Ground Rules 8

Design and Safety Notice 8

Conflicts with Established Protocols or Statutory Requirements 9

Exclusion of Special Systems and Responsibilities 9

How to Read This Book 9

1.4 Audience 10

Operators, Engineers, Technicians, and Support 10

1.5 Contribution and Importance 11

1.6 Situation Management 11

Situation Management Is Straightforward 13
Situation Management Fits Like a Glove 16
1.7 Structure of Situation Management 18
Structure of Situation Management 19
Essential Components of Control Room Management 20
Essential Components of Situation Management 22
Success Is Not a Trade-Off 23
1.8 Fundamental Tools for Situation Management 24
Reminder about Management's Role 26
Getting to Good Situation Management Can Be a Big Step . . . 27
TransAsia Crash 28
1.9 The Power of Time 30
See-Understand-Decide-Act and Process Safety Time 30
1.10 Defensive Operating 32
Five Principles 33
Supplementary Guidance 34
1.11 Situation Management Changes the Game 35
Situation Management 37
1.12 The Overall Operational Setting 39
Alarms (Something Is Wrong for Sure) 40
Strong Signals (Something Is Wrong but Not Sure What) 41
Weak Signals (Clues Something Might Be Wrong, Find Out) 41
1.13 Standards, Guidelines, and Practices 42
Standard 43
Recommended Practice 44
Best Practice 44
Guideline 44
Recognized and Generally Accepted Good Engineering Practice 45
OSHA 29 CFR 1910.119 45
Best Available Technology Not Entailing Excessive Cost 46
Duty of Care 47
Discussion 47
1.14 Management's Role 47
1.15 The Human Operator 48
1.16 Frontline Supervisor's Role 49
Administrative Supervision 50
Development Supervision 50
Operational Supervision 50
Takeaway Message 50
1.17 How Situation Management Really Works 50
1.18 How Real Is All of This? 53
ABB 53
Emerson 54
Honeywell 54

Rockwell Automation 54
Schneider Electric (Foxboro, Invensys) 55
Yokogawa 55
1.19 Contribution and Importance 56
Audience 56
Suggestions for Reading 56
1.20 Things to Keep in Mind 57
To the Reader 58
To Operators 58
To Engineers and Technologists 59
To Supervisors 59
To Senior Management 59
To Regulators and Inspectors 62
Dual Responsibilities 62
1.21 Review of Book 62
Part I: Operational Integrity 63
Part II: Situation Awareness and Assessment 64
Part III: Situation Management 64
Putting It All Together 65
1.22 Suggestions for Using This Material 65
Good Engineering Practice 65
Evaluate and Improve Everything 69
1.23 Actually Getting Started 69
Suits and Coveralls 70
Key Ingredients for Operational Success 70
Some Causes of Poor Operation 71
Knowing What Is Right 73
1.24 Limitations of Situation Management 75
1.25 Close 75
1.26 Further Reading 76

Chapter 2 The Enterprise 77
2.1 Key Concepts 78
2.2 Introduction 78
The Enterprise 79
It is All About Culture 79
Walk the Walk 80
Understanding the Plant or Enterprise 81
The Mindful Organization 81
2.3 Silos 82
Information Silos 84
Functional Silos 84
Communications between Silos 85
2.4 Enterprise Capabilities 86
International Association of Oil and Gas Producers on Process Safety 86

Institutional Failure: PG&E San Bruno Pipeline 87
Process Safety Begins in the Boardroom 87
High-Reliability Organizations 88
2.5 Short-Term versus Long-Term 89
Story of Two Enterprises 89
Valuable Message 92
2.6 Delegation of Responsibility 92
2.7 Operational Integrity 93
Operational Integrity Levels 95
Plant Operability Components 95
OiL as a Measurement Evaluation 97
2.8 Safety 99
Characteristics of Safety 100
Components of Safety 101
Delivering Safety 103
2.9 Responsible Engineering Authority (REA) 103
2.10 The Magic of a Control Loop 105
Temperature Control Example 105
Flow Control Example 106
Useful Message about Moving Disturbances 107
2.11 Selective Automation 107
Advanced Basic Control 108
Advanced Control 108
Procedural Automation 110
2.12 The Automated Plant 112
Selective Automation 113
Operate Periodically with Automation Off 113
Cease Operations during Significant Upsets 114
Summarizing 114
2.13 Plant (or Enterprise) Area Model 115
2.14 Decomposition 117
Decomposition Basics 118
Subsystem Boundary Attributes 118
Subsystem Internal Attributes 119
2.15 Decomposition Underlying Situation Management 120
Structure of Decomposition 120
Looking for Abnormal Situations in Key Repeated Elements 123
Looking for Abnormal Situations in Key Repeated Subsystems 125
Summarizing 127
2.16 Transformational Analysis 127
How It Works 127
Using Transformational Analysis for Risk Assessment 129
Using Transformational Analysis for Decomposition 130
Use for Operational Area Division of Responsibility 131

Identification of Structural Operational Issues 131
2.17 Near Misses, Incidents, Accidents, and Disasters 132
Pay Retail or Pay Wholesale 133
Hazard 134
Abnormal Situation 134
Near Miss 135
Accident 136
2.18 Critical Failures 137
Chains 138
Disasters in Review 140
2.19 Process Hazard Management 146
2.20 Root and Other Causes 148
Definition of Root Cause 148
Explanatory Case for Root Cause 148
Proximate Cause 149
2.21 Layers of Protection 150
Layer of Protection 150
Independent Protection Layer 150
Layers of Protection and Situation Management 150
2.22 Close 151
2.23 Further Reading 151

Chapter 3 Operators 153
3.1 Key Concepts 154
3.2 Operators' Creed 155
3.3 Operators and Operations 155
Definition of an Operator 155
Peopleware 156
Plants and Operations 156
3.4 Boundaries and Responsibilities 157
Responsibility 158
Control 158
Crossovers 159
Crossover Management 159
Control Room Coordination with Its Operational Area Field 161
Maintaining Responsibility 162
3.5 Operator Readiness 164
Understanding Fatigue 164
Managing Fatigue 168
Understanding Impairment 168
Managing Impairment 169
Understanding Overload 170
Managing Operator Load 171
Operator Alertness 172
Improving Operator Performance 173

3.6 Operator Training 173
Training and Skills 174
Skills Training 176
Competency Training 176
"Personal" Tools 177
Process Understanding 178
3.7 Qualified Operator 178
Brief Glossary 179
Message of Operator Qualification 181
3.8 Operator Tools 181
Checklists 182
Protocols 183
Procedures 183
Simulators 184
Reports 185
3.9 Shift Handover 185
Reasons for Shift Changes 186
Beginning of the Operator's Shift Role 189
Ending of the Operator's Shift Role 190
Functional Components 191
Noncontiguous Shifts 196
Logs and Reports 196
Handover 198
Field Operators' Handover 202
Shift Handover for Supervisors 204
Special Case for Maintenance 206
3.10 Information Content of Shift Handover 208
3.11 The Mobile Operator 210
Control Room Mobility 210
Plant Area Mobility 211
Large Geographical Mobility 211
Requirements for Mobility Support 212
3.12 "Long Arm" of the Operator 213
3.13 Goals, Roles, and Culture 214
Basics of Motivation 215
Tenets of Operation 217
Operator Objectives 218
Message 222
3.14 Close 222
3.15 Further Reading 222

Chapter 4 High-Performance Control Rooms and Operation Centers 223
4.1 Key Concepts 224
4.2 Introduction 226
4.3 A Note about Scope 228

4.4 Control Room and Operation Center Requirements 229
Physical Protection and Security 229
Environmental Controls 229
Information Support Tools and Technology 230
Sufficient Process and Operational Controls 230
Operational Support 231
Control Room Access Management 231
Special Operating Situations 232
Permits, Personnel, and Visitors 232
Scope Note 233
4.5 The Control Room 233
A Control Room Is Remote (but Not Necessarily Distant) . . . 234
Design Evolution 234
Architectural Aspects 235
4.6 Operation Centers 236
4.7 Collaboration Centers 237
Requirements 237
Configurations 238
Importance 238
4.8 Advanced Technology Control Centers 239
4.9 Design of Effective Work Spaces 241
The Concept of Space 241
A Few Thoughts 244
4.10 User-Centered Design 244
Human Factors Details 245
Environment 245
Scaling 246
Compensation 247
Understandability 247
Implementability 248
Unified Feel 248
Example of Mixed Technology 248
4.11 Control Room Design 249
Location 250
Security 251
Building Style 251
Layout 251
Design Considerations 252
Principles and Ergonomics 252
Console Design 252
Life Cycle 253
4.12 The Mobile Control Room 253
4.13 The Role of the Control Room 254
4.14 Looking to the Future 255
4.15 An Architect Weighs In 256
4.16 Close 257

Chapter 5 The Human-Machine Interface 259
Not a One-Stop Shop 260
Chapter Coverage 260
5.1 Key Concepts 261
5.2 Introduction 262
Physical Differences and Preferences 262
5.3 Nomenclature for Display Screens and Components. 263
5.4 Four Underlying Requirements for Operator Screens 265
Requirement 1: Purpose 266
Requirement 2: Understanding 266
Requirement 3: Use 266
Requirement 4: Complete 266
5.5 Principles of Display Screen Design 267
Wickens's 13 Principles 267
Engineering Equipment and Materials User Association's 10 Principles 269
Five Design Principles 270
ISO 9241 Seven Design Principles and Five User Guidance Principles. 271
5.6 Seven Principles of Workspace Design 272
5.7 The Human-Machine Interface 274
A Wartime Story Sets a Stage. 275
Components of an HMI 277
HMI Design Philosophy 278
Style Guide 279
Graphics Library 280
5.8 Display Screen Design 281
Overview of Display Screen Design 281
Display Screen Structure 282
Flash. 291
Display Screen Design 292
Dynamic Page Assembly 295
Display Complexity and Minimum View Time 297
Color Blindness 297
5.9 Navigation. 298
Purpose of Navigating 298
The Navigating Cycle 299
Navigation Tools 302
The "Product" of Navigation 303
5.10 Glyphs, Icons, Dials, Gauges, and Dashboards 305
Relationship to Style Guides 305
Glyphs 305
Icons. 308
Dials and Gauges 311

Dashboards . . . 318
5.11 Design Fundamentals for Icons and Dashboards . . . 325
Foundations . . . 326
Design Types of Dashboards (and Dials and Gauges) . . . 327
Salience Requirements . . . 328
5.12 Trend Plots . . . 329
Build-on-Demand Trends . . . 330
Continuous Trends . . . 330
Pop-up Trends . . . 330
Complex Trends . . . 331
Trend Components . . . 332
Special Types of Trend Charts . . . 332
5.13 Example Display Screens . . . 334
Overview Page . . . 335
Secondary Page . . . 339
Tertiary Page . . . 343
Pop-ups . . . 345
5.14 Mass Data Displays . . . 345
Departure from Steady-State Value Mode . . . 347
Departure from Normal/Expected Value Mode . . . 347
Things to Keep in Mind . . . 347
Extending Mass Data for an Overview . . . 349
5.15 Multivariate Process Analysis . . . 349
What Is Multivariate Process Analysis? . . . 349
Bender Treater Example . . . 351
Important Note . . . 353
5.16 Displays Large and Small . . . 353
Workstation Displays . . . 354
Off-Workstation Large Displays . . . 356
Requirements for Large Off-Workstation (OWS) Displays . . . 358
Illustrations of OWS Large Displays . . . 360
Off-Workstation Small Displays . . . 361
Head-Up Displays . . . 363
5.17 Video Walls . . . 365
Conventional Video Walls . . . 365
Video Walls for Control Rooms . . . 366
5.18 Paper versus Electronic Screens . . . 370
Pros and Cons . . . 372
Naturalness . . . 373
Readability . . . 373
Following the Thread . . . 374
Personalization and Annotation . . . 376
Comparisons to Think About . . . 376
5.19 Fire, Gas, Safety Instrumented Systems, and Security Systems . . . 377

5.20 Sound, Audio, and Video 377
Sound 377
Cues 378
Announcements 379
Video 380
5.21 Evaluating Effectiveness 380
5.22 Loss of View and Key Variables 383
5.23 Building Effective Screens 385
5.24 Further Reading 386

Part II Situation Awareness and Assessment 389

Chapter 6 Situation Awareness and Assessment 391
6.1 Key Concepts 392
6.2 Introductory Remarks 392
6.3 The Situation Management "Situation" 393
The Operational Setting 394
6.4 Situations to Be Aware Of 395
Problematic Situations 395
Operational Situations 396
6.5 Strong Signals 396
Indirect Strong Signals 397
Direct Strong Signals 398
6.6 Situation Management Roadmap 399
The Process of Situation Awareness 400
Active versus Passive Monitoring 401
6.7 Situation Awareness Tools 401
6.8 The Psychology of Situation Awareness 402
Ownership 403
"Relative" Prime Responsibility 403
Accepting Reality 404
Leadership and Cooperation 404
The Triple Package 405
Intuition and "Raw" Information 406
6.9 Situation Assessment 406
Situation Assessment Question 406
6.10 Surrogate Models 407
Sources for Surrogates 408
6.11 The Four-Corners Tool 409
Acting, Outcome Questions 410
Not Acting, Outcome Questions 410
Discussion 410
6.12 Close 411

6.13 Further Reading 411

Chapter 7 Awareness and Assessment Pitfalls 413
7.1 Key Concepts 415
7.2 Introduction 416
7.3 Readers' Advisory 416
7.4 Why We Make Mistakes 416
Looking without Seeing 418
7.5 Dangers from Automation 418
The Substitution Myth 419
Automation Complacency 420
Automation Bias 421
The Generation Effect 422
7.6 Mental Models 422
Expected Roles 423
Failure Avoidance 425
Logic-Tight Compartments 427
Surrogate Models 429
The Surrogate Model Test 430
The Deception of Two Reasons 430
Remembering 431
Good Is Not Really Good Enough 431
7.7 Doubt 432
Possible Doubt 433
Probable Doubt 433
Reasonable Doubt 433
Shadow of a Doubt 434
Dealing with Uncertainty 434
Lingering Doubt 435
Managing "Truths" 435
7.8 How We Decide 436
Short-Term versus Long-Term 436
Loss Aversion 438
Sixth Sense 440
7.9 Biases 441
Confirmation Bias 442
Continuation Bias 445
Anchoring Bias 445
Halo Effect 446
Bandwagon Effect 446
Diffusion of Responsibility 446
Post Hoc Ergo Propter Hoc 447
The "What Then" Question 448
7.10 Inattention Blindness 448
7.11 Partial Information 450

7.12 Myth of Multitasking 452
Setting the Stage 452
Multitasking 452
7.13 Personalities 454
Accident-Prone Behavior 455
The Quiet Ones 455
Situation Management Points 456
7.14 Geography of Thought 456
Norms and Conventions 457
Logic and Reason 460
Individuality 463
Handling and Reporting Problems 463
Three Postal Codes 464
7.15 Institutional Culture versus Individual Responsibility 464
Polarity 464
Alignment Failure 465
Historical Incidents 465
7.16 Close 469
7.17 Further Reading 470

Chapter 8 Awareness and Assessment Tools 471
8.1 Key Concepts 472
8.2 Introduction 472
Knowledge Fork 473
Awareness and Assessment Situation 473
8.3 Alarm System 477
Alarm Fundamentals 477
Anatomy of an Alarm 478
Alarm Philosophy 479
Alarms 480
Alarm Management 480
Alarm Rationalization 482
Alarm Response Sheet 485
Process Trouble Point 489
Alarm Activation Point 491
Alarm Priority 494
Alarm Rationalization Step-by-Step 497
Alarm Metrics 499
Operator Alarm Loading 501
Contribution of Alarms to Situation Management 503
8.4 Operator Ownership Transfer at Shift Change 503
Transferring Information 504
Receiving Information 505
Verifying Information and Taking Ownership 505
In-Shift Handover Emulation 506
8.5 Alerts, Messages, and Notifications 506

Notifications as Weak Signals 506
Properties of Notifications 508
General Design and Implementation Guidelines 509
Notifications and Logs 511
8.6 Putting It All Together 511
8.7 Making Situation Awareness Happen 512
Capable of Doing the Job 513
Design and Implementation 513
Usability 513
Selling Management 513
Auditing 514
8.8 Close 515
8.9 Further Reading 515

Chapter 9 Weak Signals 517
9.1 Key Concepts 521
9.2 Introduction 522
A Word to the Reader 522
9.3 Weak Signals 524
Weak Signals Announce 526
Finding Weak Signals 528
Weak Signals for Situation Management 529
Categories of Weak Signals 532
Weak Signal Concepts 533
What Weak Signals Look Like 534
Examples of Weak Signals 537
Hunches and Intuition Might Be Weak Signals 540
Expectations Will Interfere with Weak Signals 540
9.4 Building and Displaying Weak Signals 541
Characteristics of Weak Signals 541
Weak Signals from Direct Measurements and Observations 542
Weak Signals from Indirect Measurements or Observations 545
Weak Signals from Trend Plots 562
The Role of Icons, Dials, Gauges, and Dashboards 564
Intuition and "Raw" Information 565
9.5 Models for Weak Signal Analysis 566
9.6 Weak Signal Management 566
The Work Process 567
Step 1: Identification 569
Step 2: Forward-Extrapolation 570
Step 3: Backward-Projection 573
Step 4: Evidence for Confirmation 575
Step 5: Resolution 581
Never Assume the Problem 582

Recapping the Steps. 582
Classifying Weak Signals—A Review 585
Summary of Extrapolation and Projection. 586
Weak Signal Management: Before and After. 586
9.7 Digging into Weak Signals. 587
Trouble Indicators Come in Sizes 588
Actively Looking for Weak Signals. 591
Special Case of a Weak Signal Mapped to a Specific Problem. 593
Prove True or Prove False. 594
Weak Signals Observed by Experts. 595
Collaboration and Consensus 595
Weak Signals Do Not Escalate. 596
Weak Signals as Flags. 598
Two-Cycle Weak Signal Analysis 600
Accentuate the Negative, Eliminate the Positive. 602
Weak Signals and Checklists. 602
Persistent Weak Signals 603
Weak Signals That (Seem to) Lead Nowhere. 603
Weak Signals among Strong Signals. 605
Actively Looking for Weak Signals. 606
9.8 Weak Signals Might Not Persist Very Long. 607
Weak Signal Life Cycle 608
9.9 Other Weak-Signal-Type Extrapolations. 609
Near Hits (Near Miss). 609
What-If and HAZOP 610
Root Cause Analysis 610
Alarm Rationalization. 611
9.10 Weak Signal Templates? 611
9.11 Retrospective Weak Signals Case Study. 612
Texas City 612
9.12 Relationship between Weak Signals and Alarms. 615
Situation Awareness Depends on Both Alarms and Weak Signals 617
Few Weak Signals Lead to Alarms 618
Precedence of Operator Activity 618
Weak Signals from Alarm Activations. 618
9.13 Relationship between Weak Signals and Critical Variables 619
9.14 Operator Weak Signals Are Tactical (Short-Term). 619
Tactical versus Strategic 620
Tactical Weak Signals 620
Strategic Weak Signals 621
9.15 The Dependence of Weak Signal Analysis on Model Quality. . . 622
Model Fidelity 622
Identifying Model Inadequacies 622
Weak Signal Work Process. 623

9.16 Getting Weak Signals Working 623
Proper Foundation 624
No Shortcuts for Weak Signal Management 625
Weak Signal Overload 626
Selling Management 628
9.17 Troubleshooting Guide 628
Finding Too Few Weak Signals 628
Finding Too Many Weak Signals 628
Cannot Forward-Extrapolate a Weak Signal 629
Finding Too Many Problems When Forward-Extrapolating 629
Many Weak Signals Forward-Extrapolate to the Same Problem 629
Cannot Backward-Project a Potential Problem 629
Many Potential Problems Backward-Project to the Same Evidence 629
Confusing Evidence Obtained from Backward-Projections . . . 629
No Evidence Found from Backward-Projections 629
The Weak Signals Procedure Does Not Seem to Work at All 630
The Weak Signals Procedure Does Not Work All the Time 630
The Weak Signals Procedure Is Too Hard to Use 630
Finding Evidence of Potential Problems Actually Present . . . 631
9.18 Additional Thoughts about Weak Signals 631
Artificial Intelligence for Weak Signal Analysis 631
Identifying Gaps in Training and Procedures 632
Weak Signals and Incident Investigations 633
Weak Signals Are Not the Only Way 634
Skipping over Weak Signal Processing 634
Wrapping It Up 636
9.19 Close 637
9.20 Further Reading 637

Part III Situation Management 639

Chapter 10 Situation Management 641
10.1 Key Concepts 642
10.2 Introduction 643
The Situation Management Activity 644
Step-by-Step Working Process 645
10.3 Lessons from Air France Flight 447 647
Background 647
History of Failures 648

Lessons 648
10.4 Operations Safety Nets 649
10.5 Using Experts and Benefiting from Experience 651
Experience 652
Expertise 652
10.6 Safe Conversations 652
First, a Word about Safety 653
Safe Communication 653
Mindful Conversations 655
Mirroring, Acknowledging, and Tracking 656
10.7 Operational Drift 658
Tenets of Operation 660
10.8 The Restricted Control Room 661
Control Rooms in Normal Operations 661
The Control Room in Abnormal Operating Conditions 662
Restricted Control Room Conditions 663
Initiators of a Restricted Control Room Condition 663
Termination of a Restricted Control Room Condition 663
10.9 The Sterile Control Room 664
Sterile Conditions 664
Initiators of a Sterile Control Room Condition 665
Termination of a Sterile Control Room Condition 665
10.10 Lessons of Defensive Operating 665
10.11 Managing Everyday Situations 666
Fictional Illustration 666
Operator Intervention Caution 667
Operators Must Not Be Innovators 668
Operator Duties 669
Following the Rules 669
Flow of Operator Activities 670
General Flow of Operator Activities for Situation Management 670
10.12 Doubts and Concerns 673
10.13 Delegation 674
10.14 Collaboration 675
Use the Knowledge Fork 675
Caution 676
Air Florida Flight 90 Crash 676
Crew Resource Management 678
Worst Case First 680
10th Man Doctrine 680
Triangulation 681
Red Teams 684
10.15 Permission to Operate 684
Management's Role 686

Operating Situations 686
Operational Modes 688
How Permission to Operate Came to Be 689
How Permission to Operate Works 690
Permission to Operate 691
Withdrawn Permission to Operate 692
Alternate Methods for Having Permission 692
Safe Operating Limits 694
Managing the Operator's Permission 694
10.16 Escalation 696
Communication and Collaboration 698
Escalation 700
Escalation Resources 702
Direction of Escalation 703
First Duty of Escalation 703
The Process of Escalation 704
When to Escalate 704
Escalation Design 706
Escalation in Perspective 706
10.17 Escalation Teams 706
Escalation Team Composition 708
The Escalation Activity 709
Frontline Coaching and Mentoring 709
Readiness Evaluation Role 710
Training 711
Abnormal Situation Management Process Model 711
Weak Signals for Abnormal Situation Management 712
10.18 Command and Control 713
Supervisor Not Fully Qualified to Be an Operator 713
Supervisor Is Fully Qualified to Be an Operator 714
10.19 Alternate Safe Operating Modes 715
Operator-Initiated Shutdown 715
Automated Shutdown 716
Alternatives to Shutdowns 716
Safe Park 718
Keeping Perspective 719
10.20 Managing Major Situations 719
Major Situations 720
Operator Redeployment 720
10.21 Control Room Situation Codes 725
Code Gray 727
Code Orange 728
Ending Codes 728
10.22 Operability Integrity Level for Online Risk Management 728
10.23 Managing Biases, Overcoming Pitfalls 730

10.24 Safety and Protective Systems 731
10.25 Key Performance Indicators 731
10.26 Miracle on the Hudson 732
10.27 Achieving Situation Management 735
Control Room Management Choices 737
The Process Engineer 738
The Controls Engineer 738
The Operations Engineer 739
10.28 Training, Practicing, Evaluating, and Mastering 739
Weak Signals 740
Collaboration 740
Escalation 740
Permission to Operate 740
Other Tools and Support 740
10.29 Closing Thoughts on Situation Management 741
10.30 Further Reading 741

Appendix: Definitions of Terms, Abbreviations, and Acronyms 743

Credits 761

Index 763

Foreword

Accurate situation awareness is critical to effective control room operations. Control room operators must monitor and understand a wide variety of information that can change rapidly, often across distributed complex systems. This can tax the ability of even experienced control room operators to stay on top of what is happening, and not just react, but project future trends so as to make proactive decisions that maintain the safety and efficiency of operations.

In *Situation Management for Process Control*, Doug Rothenberg addresses this need for situation awareness and provides tools for operators and managers of control rooms to actively manage the situation. This includes a consideration of both normal and emergency operations along with many real-world examples. Operator readiness, training and support tools are covered, along with key components of effective shift handovers. Rothenberg also covers the importance of effective control room design, with an emphasis on systems that are both user-centered and that conform to human-machine interface design standards. Overreliance on automation and alarm systems are shown to be particular hazards that Rothenberg focuses on.

This book is written for operators, engineers, and line managers of process control rooms who want to improve the safety and effectiveness of their operations. Rothenberg's focus on situation management emphasizes the need for the highest level of situation awareness—projection. It requires that operators be provided with early warning for proactive management of abnormal situations, plans for various contingencies, and the needed resources and authorities to resolve operational problems quickly and efficiently when they arise. The key tools for success can be found

in not just relying on operator training, but on equipping operators with systems that support their real needs for situation awareness, coupled with organizational tools to support rapid decision-making and action when needed.

Mica R. Endsley, PhD
President, and CEO of SA Technologies

About the Author

Douglas H. Rothenberg is the president and principal consultant of D-RoTH, Inc., a technology consulting company that provides innovative technology and services for industry. D-RoTH, Inc. currently specializes in alarm management, control room management, fit-for-purpose product design, and innovation development for new products and services. Rothenberg is a leading authority in the field and provides professional consulting and services worldwide. He is the author of *Alarm Management for Process Control*, a defining reference book in the field.

Rothenberg was a faculty member in the Systems Engineering Department of Case Western Reserve University and spent over 20 years with Standard Oil, BP Oil, and BP Amoco where he was responsible for new state-of-the-art technology to support advanced manufacturing solutions.

Rothenberg has a PhD in philosophy, systems, and control engineering from Case Western Reserve University, an MS in electrical engineering from Case Institute of Technology, and a BS in electrical engineering from Virginia Polytechnic Institute. He has several patents in instrumentation and controls and alarm management. He is active in the International Society of Automation (ISA) and is a member of Sigma Xi. He is the recipient of the 2005 Educator-of-the-Year Award from the Cleveland Technical Societies Council in Cleveland, Ohio.

Note from the Author: Gender Neutrality

The book is intended to be gender neutral. The words *he*, *his*, and *him* are meant to be placeholders for individuals of all genders.

Doug H. Rothenberg

Part I

Operational Integrity

1
Getting Started

If you think safety is expensive, try an accident. Accidents cost a lot of money. And, not only in damage to plant and in claims for injury, but also in the loss of the company's reputation.

Trevor Kletz (Process Safety Expert)

When we think about the future of the world, we always have in mind its being where it would be if it continued to move as we see it moving now. We do not realize that it moves not in a straight line … and that its direction changes constantly.

Ludwig Wittgenstein (Philosopher)

Control room operators and operation center controllers (hereafter we will use the term *operator* for both) manage the real-time performance of a capital enterprise easily worth many hundreds of millions of dollars. We ask them to shoulder the burden of everything that goes wrong during their watch, all without any recognition when nothing does, and precious little (if not actual blame) when something goes wrong and they are just barely able to manage things. Within their area of responsibility and authority they must be able to view every control loop, most sensors, all the equipment, and much of the supporting utilities, and then adjust as appropriate. This is not an easy job. When something actually does go very wrong, the inability to maintain situational awareness is a major loss. Its loss directly contributes to almost every disaster event that was not the result of spontaneous complete surprise. No one wants

an incident. But incidents and disasters happen. We now know to a high degree of certainty that they happen because those in charge of ensuring that they do not happen are not aware that they are. They fail to know the situation. They are unaware of what is really going on, what is likely to happen, or what is not happening that they think is.

There is a lot of material here. But it is not intended to be exhaustive. Rather, it is a very good overview. It has been written in a relaxed style. Most of all, it should make sense and give you a very good start at putting your arms around control room operational safety. This book is about how to design for, attain, and sustain a responsible level of operational safety. We will get more into safety in the next chapter. For now, let us get started. Each chapter begins with a framework of important points. These key concepts should be helpful to identify important thoughts about the material.

1.1 Key Concepts

Top Line	The only pathway to commercial success is to operate safely and responsibly. Safety and responsibility go hand in hand. All enterprises are capable of doing it that way. And the tools and skills are readily available and effective to use.
Enough Time	Having enough time is the single most essential ingredient for successful situation management. Notwithstanding everything else, if one has enough time, everything is possible. Without it, almost nothing is.
Manager's Role	It is management's duty to ensure that the enterprise is appropriate to task, the operations team is effective, and the operational requirements are set for safe, responsible, and effective operations.
Operator's Role	The operator is an essential part of the manufacturing team. Operator success will be limited by the extent that the enterprise is effectively designed, appropriately constructed, properly maintained, and responsibly managed (financially and administratively).
Situation Management	Situation management is a technology mature enough to provide a framework and methodology for an enterprise to significantly improve operators' abilities to effectively and successfully manage.
Cornerstones of Situation Management	The enterprise must provide: 1. Early enough warning to provide sufficient time for proactive and successful remediation to abnormal situations 2. Effective plans with appropriate contingencies 3. Sufficient resources at hand to be successful at managing, if success is possible 4. Conditional authority for all parties to act or continue to act to resolve operational problems so long as such action is appropriate

Accidents and Incidents	Accidents and incidents are not only growing in frequency, the extent of damage they cause is alarmingly increasing. If we are able to learn from the experiences of others, we might avoid many of the devastating impacts of firsthand knowledge. A failure-to-operate of any safety-related protection device, even if a second such device provided eventual full protection, is an incident and not a near miss.
Last Opportunity	Situation management provides the wherewithal and technology for the operator to attempt to successfully manage abnormal situations before existing infrastructure safe-operational safeguards are challenged.
Managers' Bottom Line	No reasonable amount of personnel selection, training, requirements enforcement, or anything else can surmount the reasonable ability of any individual person to perform. It is not responsible practice to place the majority of the burden on the hands-on operator beyond his appropriate capabilities. It is therefore a requirement for responsible enterprise operation that management provide appropriate tools, supervision, and assistance.
Operators' Bottom Line	It is the sum total of the decisions and actions the operator makes, within the capabilities of the enterprise, that determines whether or not the enterprise in his care operates safely and productively.

1.2 Introduction

This book is intended to give you options, not tell you what to do. But, it is not meant to be a "choose one from column 1 and one from column 2" and so on. Rather, the coverage is intentionally broad. It is designed to reinforce your background if you are already working on control room technology and operator support. The materials here are not the only ways to achieve the goal of effective situation management. On the other hand, if you are new to all of this, this book provides a supportive background and comprehensive introduction. Certainly, there are additional resources that go considerably deeper into the ergonomics of operator station design, control room architecture, detailed construction of human-machine interface (HMI) screens and controls, and more. The references at each chapter end provide a few selected resources. Consider those once you have a good framework of what to ask and how to approach things.

This book is intended to give you options, not tell you what to do.

Take the time to understand what is going on and what is needed to do the job well. *Situation Management for Process Control* unifies the understanding of how to deliver real value to control room operations. Properly understood and executed, it

is a game changer for safe and effective real-time management of industrial plants and operations. It delivers a firm technical framework that ties together all the traditional individual aspects (procedures, HMI, control room design, alarm systems, etc.) into a technology to understand and design effective control room management operations for enterprises. This is a unified approach with explicit tools to deliver situation management to control room operators. An important new contribution is the concepts and technology of weak signals and their use to supplement the alarm system to cover the rest of the situations that alarms are not intended or able to manage.

Operators monitor, understand, and manage situations and events that need intervention. We use people because of the expense of fully automating proper management without them; the complexity of automatically managing that makes it very difficult to design appropriate technology; the inability to predict events or manage those events that might be predictable but are too "soft" to prearrange for their management; or, most often, a combination of these reasons. With the support of the operations team, operators ensure proper operation. The job to ensure proper operation must be accompanied with the ability to be successful. Doing this right provides the world's population with goods and services to make their lives more comfortable and enjoyable. From food and pharmaceuticals to the expansive host of consumer products, to the iron, steel, and engineered materials to make them, the process industry depends on operators to competently manage. They are on duty second-by-second, minute-by-minute, and hour-by-hour, day in and day out, attending to the making and delivering. To meet this responsibility they must be qualified, motivated, unimpaired, undistracted, and trained; and they must have all necessary tools.

Operators must actually be able to monitor what is in their charge, understand what that monitoring is showing them, and plan and actualize any needed changes. This begins with situation awareness. *Situation awareness* means knowing what is happening in the plant or operation and understanding what it means. The unfortunate reality is that there are few ready convenient indicators available to measure whether or not operators achieve good situation awareness, nor whether they even have the chance to achieve that awareness as a consequence of the design of their operator interface equipment. Missing situation awareness has been implicated in most of the incidents that have led to significant loss of life or plant damage and consequential environmental exposure. However, it is the combination of situation awareness, situation assessment, and the ability to successfully manage abnormal situations that we need—in other words, *situation management*. Proper situation management changes the game.

The undeniable and unavoidable facts that govern successful control room operator performance center directly on what is expected. *What is expected* is simple and profound: watching to make sure that the operations are properly progressing or not. When they are not, operators must understand what is going wrong and take corrective action to make it right. This requires two skills: the cognitive skill of seeing and understanding whether or not something is going wrong, and the skill for performing the direct intervention to make proper changes that work. The main thrust of situation management includes those cognitive skills as well as the resources for guiding intervention. The specifics of what intervention should be effected is left to experts in the process or enterprise as documented in the totality of operating procedures and protocols. This book knits those aspects together into an effective whole, supplementing missing structure and tools wherever possible.

According to a recent survey of process automation professionals conducted by *Control* magazine,

> Survey respondents acknowledged the potential for operators to significantly influence plant performance, as well as ongoing need to improve measures that would make them more effective in their jobs.
>
> When asked to what extent better prepared operator could positively influence key performance metrics, respondents placed significant accountability in the hands of the operators. Operators not only have a big impact on availability, equipment damage and personnel safety, but can play a big role in quality, environmental and economic performance as well….
>
> But an overwhelming majority of survey respondents also confirmed the increasing scope of board operator responsibilities, with more than three-fourths indicating a growing workload….[1]

Operational success rests squarely on operators' shoulders. Providing the tools, processes, and technology for them to be dependably successful has been a challenging task. There are many options for almost every situation. Most plants and operations have settled into similar tool kits and operation protocols. Yet production and operations continue to be fraught with an unacceptable level of incidents, accidents, and disasters. Personnel are deliberately hired and trained; operating schedules purposefully set and closely maintained; operating goals and requirements carefully laid out; most operating procedures designed, trained against, and largely enforced; and all manner of reporting and daily communications performed. But, when we strip everything extraneous away, operating was largely done by practicing what was

1 Keith Larson, ed., "Operator Interface—State of the Technology Report," *Control*, April 2015.

taught through on-the-job training, occasional qualifications testing, and other loosely structured ways. This is not to say that anything was careless or thoughtless. Just the opposite—a purposeful action plan was usually followed. Unfortunately, most of the action plans are weak in actual effective operational technology. The operator has a great deal of responsibility but few really good tools to meet it.

What we did not fully appreciate was that the control-room operating environment must provide all the necessary tools to allow the operator to meet that responsibility. Operating displays, instead of simply housing data, information, and control handles, must organize and convey the information in ways that operators readily, almost instinctively, use. This means information must be predesigned and appropriately located to be available so the operator does not have to graze and hunt for clues and causes. The alarm system must be designed to find all abnormal situations engineering and good operating experiences can identify that require intervention. Color is used only for information. Nested levels of display structure should be designed so that important problems and concerns are readily discernable and subtle problems and issues are easily noted. Icons, gauges, and dashboards are used to clearly expose early operational unusuals. Their design must explicitly ensure that operators understand the limits of their effectiveness. And we must provide powerful assistance to coordinate with additional personnel during serious events.

1.3 Cautions and Ground Rules

Design and Safety Notice

In addition to the broad and comprehensive approach to developing a working solution to the situation management problem, an important strength of this book is the wealth of examples, alternatives, and suggestions for your understanding and consideration. All control schemes, design suggestions, displays, diagrams, tables, figures, trend charts, lists, and the like described and illustrated in this book refer to materials that have been designed to amplify and explain concepts and practices intended to help get this material across to you. They are provided for training and understanding purposes only and are not intended as models for design or for implementation. The choice of what to design, which aspects to implement, and how that will be done must be retained wholly by qualified, authorized members of the enterprise 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, if you have plans for

implementing the suggestions presented, please seek additional specific guidance and experience from knowledgeable experts.

Conflicts with Established Protocols or Statutory Requirements

The express purpose of this book is to place a wealth of best practice information into the hands of the industrial and enterprise community for their understanding and consideration. It is the sole responsibility of the user community to decide their specific operational policies. No material contained herein is intended to circumvent that responsibility.

No claim in this book is meant to imply or otherwise suggest that any item, example, technology, tool, or illustration is or would be a sufficient solution for responsible operation. No included material is meant to suggest compliance with any policy, standard, or legal or other statutory requirement.

Exclusion of Special Systems and Responsibilities

This discussion mentions important aspects regarding the safety of personnel, the physical security of plants and enterprises, and related aspects that may in some way apply or relate to operators, control rooms, and operation centers. All of these topics require special knowledge and additional practices that are well beyond the scope and intention of this reference. No aspect of this coverage is intended to guide or inform as to their proper design or use, with the possible exception of alarm compatibility and control room human factors considerations. Even those must be carefully designed and implemented by appropriately qualified personnel.

How to Read This Book

You have opened a substantial reference book. Lots of pages. Lots of material. Lots of ideas and concepts; some you may already know, others are very new. The organization of the material has been carefully selected for a reader beginning at the start and carefully reading to the end. This helps orient you to relate what you read to what you already know. It allows each topic to progress within a framework and foundation so you can add each part as you come to it and choose to use it. And it provides a good way to tie it all together, rather than have you end up with many distinct ideas and tools. Sure, individually they are sharp and useful. But you already know that is not enough. For it all to make a difference for you, your operators, and your enterprise, it must fold back into your culture in a way that reinforces everything that is already there. That is what you will be doing. I provide the concepts, tools, and motivation.

2
The Enterprise

The fact is that management can not learn by experience alone what they must do to improve.

The job of management is inseparable from the welfare of the company.

W. Edwards Deming (Quality Expert)

Don't be tempted to equate transient dominance with either intrinsic superiority or prospects for extended survival.

Stephen Jay Gould (Evolutionary Biologist)

The enterprise or plant working as needed is the entire reason for its being. So it is important to know what is useful to be there so that everything that is needed is there and works to deliver. This way, the operator will be able to do his part. Safe and responsible operation is the only way to stay in business. You cannot set a safe level of unsafe that agrees with a budget or allows you to manufacture your products at a selling price that returns a decent profit and expect that any safety level will be okay. So how does management decide what to require and what to "take chances with"? The answer will determine whether or not the plant or enterprise will be sustainable. Safe operation is a threshold. This is the minimum. Everything below it will not work. Above that level is not guaranteed to be safe, but it should meet the generally accepted criteria for due diligence. The need is to achieve "best practices." If they do not seem needed, appear too complicated for your culture, or cost more than you are prepared to spend, perhaps

you might want to place your time and treasure into another investment—this one is going to let you down when you can least afford it.

The *situation management* premise, and core message of this book, is that for an enterprise to expect an operator to properly manage, the enterprise and operator must possess a complete and proper infrastructure: equipment, maintenance, processes and procedures, training, and pride of participation from all. Collectively, these constitute best practices. A few items may be entirely new to you. Others you may know. You can find them in many industrial management resources. We cannot completely cover the topics here. Rather, the intent is to introduce them into a larger frame of situation management. When you are ready for more, there is a wealth of available information out there. Situation management provides the integration pathway that puts it together in ways that both make sense and work. It is the reason why and the glue for getting the job done. Without a strong infrastructure in place and fully operational, no amount of attention and care during operations can be strong enough to overcome missing parts.

2.1 Key Concepts

The Importance of Safety	If you intend to stay in business, safe and responsible operation are not parametric. Safety is not anything until it is everything.
Quality of Operation	Management culture and style is the most important determinator of long-term operational success and operator effectiveness.
Short-Term versus Long-Term	Any responsible long-term objective when compared to a similar short-term one will *always be worse in the short term*. Therefore, all attempts to compare them in the short term are a deliberate effort to be unfair. All plans and work must be long term.
Enterprise Design	Enterprise design determines the upper limit of operational ability. No amount of operator attention and proper operational decisions can overcome the inherent weaknesses in equipment design and maintenance, ineffective procedures and protocols, and lack of proper training and supervision.
Perfect Process Understanding	A perfect understanding of an entire plant or enterprise is not essential for good and proper operation. However, every piece used must be reasonably well understood and specifically accounted for in the operation procedures, protocols, and training.
Essential Decomposition	The ability to decompose a plant or enterprise into well-defined, understandable pieces is essential to being able to understand and manage it.
Perishable Skills	All skills tend to degrade if not refreshed and then properly evaluated and reinforced.

2.2 Introduction

This chapter begins with the basics of enterprises and the inherent responsibilities of their senior management. The culture and constitution of an enterprise are the

most reliable predictors for long-term operational success. The chapter concludes with important technology for carving out small enough parts of the enterprise to have a good understanding of how it works and where it can benefit from your attention. The ability to decompose a plant or enterprise into well-defined, understandable pieces is essential to being able to manage it.

The Enterprise

An enterprise (plant or operation) is often an extensive organization with many moving parts and complexity. It is the organized action of making of goods and services for sale; enterprises can be any type of organization, including businesses, nonprofits, and government agencies.[1] The term *commercial enterprise* combines the meanings of the words *commerce* and *enterprise*. Therefore, a commercial enterprise is a business that engages in buying, producing, and selling activities for the purposes of making a profit.[2]

Enterprise is one of the broadest terms used to describe an organization. In general, an enterprise is an organized collection of people and systems working toward shared goals. A more specific interpretation of enterprise expects that all departments and employees within the organization have synergistic responsibilities to achieve goals.[3]

It is All About Culture

A poignant experience with the then-manager of BP's Toledo Refinery (Toledo, Ohio, United States) reveals the mark of a leader. This story goes back a few years.

> Soon after taking over the leadership, he noticed that the equipment painting in the refinery was in dire need of refreshing. He tasked the maintenance manager to review the situation and produce an estimate for doing the work. The estimate was done and duly delivered. After carefully looking it over, the refinery manager asked whether in fact the entire refinery could be properly repainted for the estimated amount. There was a rather long and silent pause. At the end, the maintenance manager admitted that it could not. When asked, he replied that he did not think the actual estimate would be accepted since it was a considerable expense. Whereupon the refinery manager said that it was the maintenance manager's responsibility to produce appropriate, truthful, and accurate reports. It was the refinery manager's responsibility to decide the appropriate action. In this case he noted that if the estimate were too much for one year's budget, he'd stretch it over to two. The maintenance manager got the message. The refinery got properly repainted.[4]

---

1 "Enterprise," Wikipedia, last modified May 17, 2018, http://en.wikipedia.org/wiki/Enterprise.
2 Neil Kokemuller, "What is a commercial enterprise?" Bizfluent, last modified September 26, 2017, http://www.ehow.com/facts_7207187_commercial-enterprise_.html.
3 Kokemuller, "What is a commercial enterprise?"
4 Jim Shaeffer, personal communication with the author, ca. 1993.

Unless your plant or other enterprise has its "ducks in a row," it is unlikely that it can perform. It does not happen without purposeful design that includes the physical equipment (including maintenance), operational procedures and protocols, a willing and able professional staff, and a rich culture that melds it all together into a reliable and safe entity. Let us visit some important parts.

Walk the Walk

Leadership requires capable leaders (knowledgeable, honest, and communicative) with a message that captures the hearts and hands of followers, and methods that are fair and effective. Responsible leadership requires that the desired goals be reachable and sustainable. Effective leadership requires that the leaders share the workload and the prizes. Sure, different hands do different work. But work is done. Managers must do the hard work and share equitably the spoils of success.

Some of this hard work is actual work. For example, three important uses of emergency and crisis management teams (Chapter 10, "Situation Management") are to conduct readiness assessments, provide coaching, and perform training evaluations. While most of the detailed design and implementation of an enterprise is done by subject matter experts, senior personnel should do the evaluations of performance. Delegation must not get in the way of responsibility and control.

Walking the Walk

Leaders walk the walk. This is a not-so-subtle expression that it captures all—leaders must "get down into the trenches" and see what their followers see; feel what their followers feel; and give to the enterprise what they ask their followers to contribute. Sure, the workforce (middle managers, supervisors, engineers, technicians and journeymen, operators and attendants, and all manner of other support personnel) does not expect that managers wear the same shoes as they wear. But they do expect those fancy shoes to get dirty when they should. But dirty shoes cannot be the only ticket to leadership. Workers expect to see hard decisions made carefully—just as leaders expect careful attention by all their personnel to their duties and responsibilities. Leaders are expected to lead in integrity, responsibility, honesty, and success. Here are examples:

> When Hewlett-Packard (HPQ) faced a recession in 1970, co-founder Bill Hewlett took the same 10% pay cut as the rest of his employees.
>
> During the early years at Charles Schwab (SCHW), whenever the customer-service phone lines got really busy, founder "Chuck" Schwab dropped everything and answered calls along with everyone else at the company who had a stock broker's license.
>
> Whenever Wal-Mart founder (WMT) Sam Walton traveled on business, he rented the same compact economy cars and stayed in the same inexpensive hotels as his employees.

> For the first nine years that his Union Square Café was in business, owner Danny Meyer was there in person every day—clearing tables and mopping spills along with his staffers—as together they made it a top-ranked restaurant in New York City.
>
> Ray Kroc picked up the wastepaper in the parking lot whenever he visited a McDonald's (MCD) to show cleanliness was a continual job for everyone—even the CEO.[5]

These brief illustrations get to the heart of the message. Please walk that walk.

Talking the Talk

Communication is a great tool. Leaders need to use it effectively, consistently, and often enough. Well, that is the easy part. Easy because leaders talk "top down." Their talk is broadcast using the very fabric of the enterprise infrastructure: newsletters, memoranda, town hall meetings, and the like. But "talk" is not communication. Effective communication begins with listening. Responsible organizations develop powerful mechanisms for all stakeholders to communicate—to talk and to listen.

Understanding the Plant or Enterprise

A perfect understanding of an entire plant or enterprise is not essential for good and proper operation. However, every piece used must be reasonably well understood and specifically accounted for in the operation procedures and training. This goes way beyond familiarity. We are talking about a level of expertise that permits those in control of operations to recognize proper operation, understand the nuisances of operation going astray, and professionally manage situations that require intervention. This understanding must be embedded into the fabric of the enterprise to ensure continuous improvement and continuity between stewards.

The Mindful Organization

A *mindful organization*[6] may seem like something made up to sound important and provide good filler for a politically correct chapter in a book. This is not the case here. A mindful organization or, as you may be more familiar with it, a *high-reliability organization* is one that has achieved a sustained level of successful operation.[7] Much of the success is attributable to the inherent fabric of its design. It is so important that no organization can aspire to achieve such success without it. To the point of this book,

---

5 Alan Deutschman, "How authentic leaders 'Walk the Walk,'" *Bloomberg Business Week*, September 18, 2009, https://www.bloomberg.com/news/articles/2009-09-18/how-authentic-leaders-walk-the-walk.

6 Karl E. Weick and Kathleen M. Sutcliffe, *Managing the Unexpected: Resilient Performance in an Age of Uncertainty* (San Francisco: Jossey-Bass, 2007).

7 Todd La Porte and Paula Consolini, "Theoretical and operational challenges of 'high reliability organisations': Air traffic control and aircraft carriers," *International Journal of Public Administration* 21 (6–8): 847–852.

yes, there are going to be a large number of useful tools and ideas presented. At the end of the day, they are going to be largely a waste of time unless your organization itself is healthy and fit—highly reliable. There is more later in the chapter.

2.3 Silos

This topic is important for an effective enterprise. Probably everything you have heard about silos in organizations was negative: make sure you do not have any silos; if you have them, get rid of them. That is because of the "silo mentality." Silos here are a very different story. Most silos are really beneficial. Having them well developed and competently used is going to be an enterprise best practice. First we split silos into two discussions. There are information silos; those are the bad guys. And there are functional silos; the ones that produce expertise and competence for well-functioning component parts to an organization. Let us begin with what a silo is and go from there.

A *silo* is usually thought of as a tower used to store bulk material like grains. Most silos are in the form of a cylinder and bring to mind an idea of something large with a lot of internal content but not much connected to anything else. On a farm they would look as shown in Figure 2-1.

Our silo is a conceptual term used to describe a collection of stuff (people, equipment, documents, collective memory, etc.). Most of what is inside goes together. That going together can be a nice organized fit or just a mishmash. Our silos are mostly organized around the organization and function of plants and industrial enterprises. Figure 2-2 depicts one representing "mechanical" from the set of engineering silos. Inside is a trained group of mechanical and related engineers. They have an appropriate range of experience. They are required to maintain a certain acceptable level of

Figure 2-1. Agricultural silos illustrating their individual significant size but showing no visible connection between them.

Figure 2-2. Pictorial depiction of a mechanical engineering silo.

competence. This may include certification and possibly registration. They are encouraged to participate in professional enrichment programs. They have access to technical resource materials in their discipline. There is a well-established protocol for consulting outside resources for guidance, assistance, or handoff. Summarizing, within the mechanical silo are all the necessary resources for it to be relied on by the enterprise for mechanical engineering services.

Figure 2-3 depicts a larger organization composed of silos for engineering operations, maintenance, and sales and marketing. Management and support, legal, and environmental silos are also needed but are not shown in this figure. Notice there are silos within silos. The silos within silos depict the way individual centers or functions

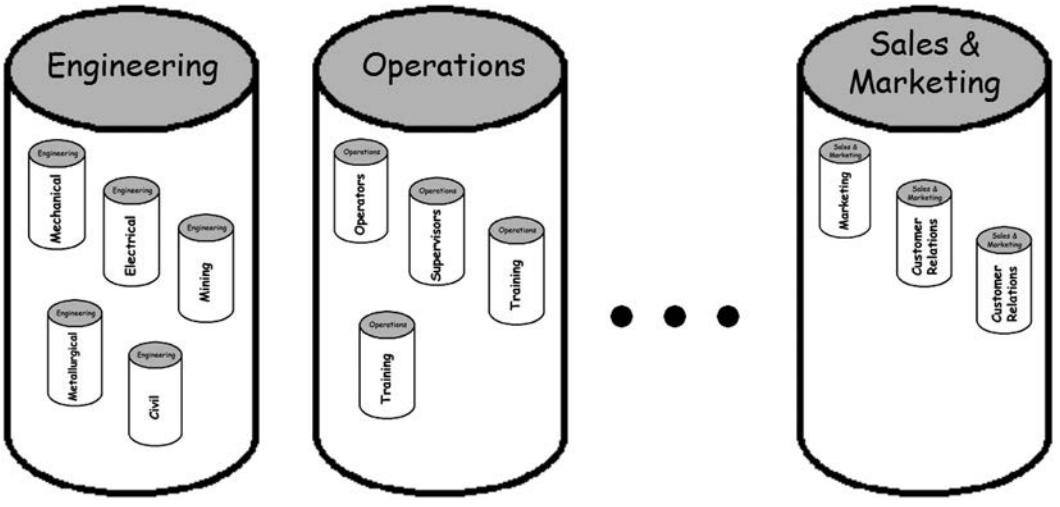

Figure 2-3. Depiction of an enterprise with component organizational parts shown as silos. Three are illustrated. Of course, there are more. Within each is a complete set of organized components (let us also refer to them as subsilos, but each is a silo as well) that together make up a well-functioning component. Each silo and each subsilo has the essential properties within itself to properly function.

3 Operators

Everyone doing his best is not the answer. It is first necessary that people know what to do.

W. Edwards Deming (Quality Expert)

It should not be necessary for each generation to rediscover principles of process safety which the generation before discovered. We must learn from the experience of others rather than learn the hard way. We must pass on to the next generation a record of what we have learned

Jesse C. Ducommun[1]

Recalling from Chapter 1, *Operators* form the front lines of safe and effective manufacturing, transportation, and distribution. Operators are a backbone for responsible activities to provide the world's population with the goods and services to make their lives more comfortable and enjoyable. From food and pharmaceuticals to the expansive host of consumer products, to the iron, steel, and engineered materials to make them, the process industry depends on operators to competently manage. They are on duty second-by-second, minute-by-minute, and hour-by-hour, day in and day out, attending to the making and delivering. To do this right requires proper tools and competencies. *Situation management* is about providing sufficiently capable, properly tooled, and available human operation to a control room or operation center.

1 BP US Refineries Independent Safety Review Panel, "The Report of The BP US Refineries Independent Safety Review Panel" (Washington, DC, January 2007).

The hard work of operating is the operator's (or controller's) responsibility. The mastering of sufficient skills and capabilities is his responsibility. The arrival for duty and continuation of attention during the full course of duty is his responsibility. Skillfully performing the needed activities is his responsibility. But all the rest is the enterprise's responsibility. The enterprise must establish proper personnel requirements and exercise appropriate measures to ensure they are fully met. The enterprise must establish necessary skill and capability requirements and exercise appropriate measures to ensure that they are mastered and kept up to date. The enterprise must set forth appropriate interpersonal cooperation and respect expectations, and take all necessary steps to ensure that they exist and are effective. The full list is longer, but you get the idea. Unless the enterprise delivers on its part, no amount of rulemaking or strong enforcement will make the operator effective enough. Here is what the enterprise will need to consider for the operator to have a responsible chance to do his job well.

3.1 Key Concepts

Operators As Professionals	Develop and support the full professional expectation and policy for all operators.
Basic Needs	In order to be appropriately functional, all operators need to (1) be in a comfortable environment free of unnecessary distractions and encumbrances, (2) feel physically and emotionally safe, and (3) feel accepted.
Impairment	There is no such thing as an okay impairment. All functional and/or performance limitations must be explicitly and effectively managed for everyone, all the time.
Readiness Responsibility	It is the responsibility of operations management to ensure that all operators on duty are ready (free of impairment including overload). Ready access to appropriate management support is an integral part of operator readiness.
Training Responsibility	If training is needed to prepare any individual for his assigned job, it is the responsibility of senior management to ensure it is done, adequate, and effective.
Training Objectives	Competency training followed by critical skill development is the only effective protocol.
Conducting the Training	Training should only be done by the most experienced and expert personnel. Training for task and on-the-job training are to be avoided.
Shift Handover	Any time a shift ends or begins, even if the same operator resumes work after a gap (overnight or over weekend), an adequate shift handover is required.
Maintenance	Maintenance personnel must be granted temporary ownership of equipment, and the operator must formally take back ownership at the end.
"Long-Arm" Operations	Where remote site personnel are assisting the operator at distant equipment locations, the operator retains full equipment ownership at all times.

3.2 Operators' Creed

The production *operator* of an industrial plant or other operator-managed enterprise activity is the responsible individual entrusted with the second-by-second, minute-by-minute, hour-by-hour, day-in and day-out successful operational outcomes. From the moment he assumes operational control until the moment it is either ended or passed on to another, we expect him to do all in his power to ensure safe, effective, reliable, and responsible operation. He is an essential member of the enterprise team. He is a professional.[2]

A creed in these modern times is understood to be a deeply held expression of dedication to a belief. It is taken to be an expression of professionalism. Among the better-known technical creeds are the Engineers' Creed (United States) and the Obligation (Canada). In recognition of the responsibility society places on the shoulders of operators and as an expression of and respect for this level of professionalism, a draft Operator's Creed is offered here for the consideration of professional operators. This is new.

Operator's Creed

I accept responsibility for the safe, reliable, effective, and responsible operation of the facility under my control. I arrive fit for duty. I take responsible charge. I properly utilize the resources and tools at my disposal. I place safe and responsible operation above all else. When duty is done, I effectively close operations or pass on responsibility to my relief. I leave duty in a responsible manner.

This expression of responsibility is offered for operators to consider as an expression of their professionalism and acceptance of responsibility, as they may find useful.

3.3 Operators and Operations

Definition of an Operator

1. "The person who operates equipment for its intended purpose. Note: The operator should have received training appropriate for this purpose."[3]
2. "The person who initiates and monitors the operation of a process."[4]

---

2 "Professionalization," Wikipedia, last modified April 1, 2018, http://en.wikipedia.org/wiki/Professionalization.

3 International Society of Automation (ISA), *The Automation, Systems, and Instrumentation Dictionary*, 4th ed. (Research Triangle Park, NC: ISA, 2003).

4 ISA 82.02.01-1999, *Safety Standard for Electrical and Electronic Test, Measuring, Controlling, and Related Equipment—General Requirements* (Research Triangle Park, NC: ISA [International Society of Automation]).

Peopleware

Peopleware is an invented word. You will find it useful to separate it from the hardware and software operators use. The word is intended to be a collective term for the tools and identifiable resources operators use to get the job done. Peopleware includes the "soft stuff," meaning things such as skills, training, and performance protocols (e.g., call out and escalate before working on hard problems). It is the appropriate combination of peopleware, hardware, and software that leads to control operating room success. Peopleware includes an important designer component: the plant or operation designer is obligated to pay sufficient attention to the operability of his creation. This is over and above the attention devoted to the plant's actual concept, design, and implementation. Those are important dual requirements. We are now ready to ask the question: what does it take to properly equip an individual operator to do his job in the control room effectively with neither inappropriate nor excessive demands? And having identified those needs, we must immediately provide for them.

Each plant or operation is complex and unique. As you might imagine, it is well beyond the scope of this chapter to be able to fully identify those needs for you; rather, it suggests that they are necessary.

Plants and Operations

Throughout this book you will find the dual term of *plants* and *operations*. Operators operate both. A *plant* is the collection of physical equipment, energy, and resources usually used to manufacture or produce something. Things like petroleum refineries, chemical plants, electrical power generation, pipelines, electric transmission lines, food processing, and raw materials processing, come to mind. In general, they could not operate without supervision. An *operation* is more often an existing entity that is placed under an operator's management because of its complexity or requirements of public safety or critical public resources. Things like highway transportation networks, electronic data networks, and air traffic and security monitoring systems come to mind. In general, they might operate without supervision, but supervision brings an important level of performance not attainable without it.

The scale of plants and operations is of little concern unless they are very small or very large. The very small ones are for special purposes; those purposes generally require special operational management. The very large can be so impactful to a community or a locale that special operations practices and regulations govern.

It is because of the benefits of including human operators into this setting that both very small and very large plants are covered in this book. Real things are going

on that require personal monitoring and responses as opposed to just mechanical (or computer managed) watchfulness and control. Notwithstanding the frequency of operator intervention, an operator's role is not "babysitting." Operators are expected to fully understand the plant or operation. They must keep fully abreast of what is going on through active monitoring and testing. They are asked to initiate and follow through with any and all corrective actions required to keep things properly operating. And they are required to seek outside assistance for all situations that challenge their resources to properly manage.

3.4 Boundaries and Responsibilities

Operator-responsible operational boundaries and responsibilities and how they are adversely challenged is an important aspect of control room management. We take for granted that the operator is charged with ensuring effective operations. After all, that is why we use operators. If everything could be fully and completely instrumented and automated to manage things as good as or better than manned operations, and it were cost-effective, no plant or operation would need operators. Alas, such a plan is presently too expensive to consider. Eventually, that may not continue to be the case. When we arrive at that place, everyone can revisit. For now, let us agree to take the presence of an operator for necessity.

An enterprise (or modest to large plant) will usually have several operating areas. An operational area is the physical extent of equipment that a single operator is responsible for. Figure 3-1 schematically depicts this situation. There is a small interior portion

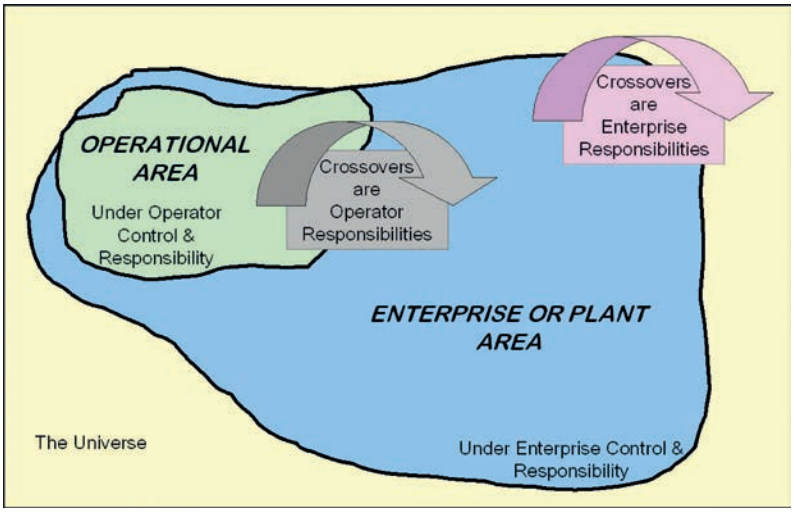

Figure 3-1. Boundaries and responsibilities that identify who is responsible for trying to prevent operational excursions, from what region of operation, and who is in charge once an excursion has occurred.

noted as the operational area. The *operational area* is contained within an *enterprise or plant area*. The enterprise area is contained within the *universe*, which is shorthand for everything else outside of the *enterprise* (e.g., the community).

The operational area is expected to be fully under the control of the operator who has the responsibility for it. There may be other operational areas, each with their own operator (not shown in the figure). Generally, all the operating portions of the enterprise will be within one or another *operating area*. When things go wrong inside an operational area, we expect the relevant operator to manage them. So long as the effects or issues about that operational area remain within it, that plan will work. Once the issue or abnormal situation threatens to cross a boundary into another operational area, into the enterprise in general, or outside the enterprise, enterprise resources must be brought to bear. Now the issue or abnormal situation transfers to the enterprise personnel (perhaps shared with a relevant operational area whose boundary has been crossed). Any operational details of this transfer process will be addressed in escalation protocols.

The following discussion is extremely important. At first glance, it may appear to be more about definitions and categorization. It is far from this. As we will see, when we understand how responsibility and control works, everyone must understand how abnormal situations that get beyond local hands to manage are handled. First, let us set the proper stage. The operator is expected to properly understand and manage any area where he has both *control* and *responsibility*. Now consider situations where both are not necessarily concurrently present.

Responsibility

Consider responsibility first. The term *responsibility* is used to clearly identify who must bear the operational burden—whose hands are on the controls. Within his operational area the operator must take charge of the outcomes. If he also has control (see next discussion) then he is expected to actively, with his own actions, make the necessary adjustments and such to manage. If he does not have control yet retains responsibility, then he must alert those who do have control and have responsibility for the situation. Once he has done the notification, he returns to the job at hand of managing his own operational area. If he is needed for operational changes to assist with the alerted activity, and that can be done without undue risk to his operations, he would do so.

Control

Having control means that the responsible individual, the operator for us, has at his disposal and use all the existing "handles" for changing and modifying operations.

He can start up conveyors, change the speed limit on the eastbound bridge lanes, and reduce the distillate product flow from a separator. If he also has responsibility, he makes these changes at his own discretion. If he does not have responsibility, he will make changes and modifications only at the direction of others with responsibility.

Enterprises must carefully clarify the delegations for control and for responsibility.

Crossovers

A *crossover* is when the impacts of operation cross the boundary between responsibility from one operator to another, from an operator to the enterprise, or from the enterprise to the rest of the world (the universe). It is in these situations that the usual operating procedures and protocols are at the most risk of failure. This is because of the sheer complexity of alternate scenarios of failure and the inherent difficulty in providing comprehensive plans for all. It is compounded by the fact that different individuals are involved—with different responsibilities, possibly different cultures, and often different managers. The approach is to recognize when a crossover is either likely, occurring, or has occurred, and adjust operational activity to take it into proper account.

Crossover Management

Basic Procedure Framework

Operating procedures and training should be explicitly designed to handle crossover situations. This includes the following:

- What defines a crossover (beginning and ending)
- What must be coordinated
- Who will do the coordinating
- Who will be lead
- How the coordination is to be carried out (protocols, procedures, decisions of how to deal with the conflicting aspects)
- What, if any, additional within-area operational changes are needed

Crossing from One Operational Area to Another Operational Area

Abnormal situations (really, the effects from one) that cross from one operational area to another are the most common crossover. Most crossovers are directional. That is, the problem from one affects the other, but not necessarily the other way around. What has

4

High-Performance Control Rooms and Operation Centers

We shape our buildings; thereafter they shape us.

Winston Churchill (British Statesman)

We require from buildings two kinds of goodness: first, the doing of their practical duty well: then that they be graceful and pleasing in doing it.

John Ruskin (Art and Architecture Critic)

Architecture begins where engineering ends.

Walter Gropius (Architect)

When your operator enters his control room, you expect him to be in charge and successful. The more the control room form and design matches his needs and expectations, the closer he will be to getting into the roles and working out his tasks. That is no different from what your and my reactions would be to entering an amazing building and feeling its awe and inspiration. Sure, control rooms are not building lobbies, or museum exhibits. But that is not the point. The message here is that the care of design, the thoughtfulness of purpose, and the completeness of execution will make a positive difference. Let us do it right. Remember that this book is not the be-all and end-all of control room design. It is intended cover enough so you can get a good start on your own work.

So, what are control rooms and operation centers? What characterizes them as different, important, and necessary? What are their differences? Why are they needed?

And how will knowing the answers be helpful? It is all about what the room is for. It is guided by who is inside. The room is where the operator, your operator or perhaps you, work. It is where operators do the job of keeping things right. Industrial control rooms are used for operating petrochemical plants, electrical power generation stations, food processing plants, pharmaceutical manufacturing sites, and the like. They also include operation centers, for example, electrical power dispatch centers, mass transit monitoring and control centers, telephone monitoring and routing stations, security monitoring and dispatch centers, military command and control centers, and many more.

A control room is the setting for successful cooperation between the human operator(s) and the interface equipment provided to help do that job. This includes the spatial arrangements of equipment; the environmental management of the work space, who goes in and why; and the designs of the equipment and other related tools. Proper design will enhance operators' working experience and provide the necessary confidence that their tools are going to be helpful and trustworthy. When we understand and follow best design practices, operator work spaces are built that greatly enhance operators' success.

Control room discussion is offered because an effective control room or operation center is a basic requirement for enabling situation management to work. Without a comfortable and efficient control room, it would be difficult to adequately support operators for situation management. Careful control room design is essential to promote effective work practice. The design of the control room must not get in the way. We do not fully cover the topic to the extent that you can extract material from this chapter, give it directly to an architect, and ask for a specific control room in return. But, and it is an important *but*, almost everything in this chapter should provide background and alert you to issues to bring up with your control room designer so together you can figure out how to include the capabilities you require in your design. It is here to inform and empower your efforts to improve your operators' work spaces. Here is a brief look.

4.1 Key Concepts

Chapter Purpose	This chapter outlines what to think about and care about to provide the physical tools and space that we call a *control room* or an *operation center.* The chapter is designed to set the stage for operator success

Control Room; Operation Center	A dedicated separate space for the sole purpose of providing the operator of a plant or operation with the sufficient operational state information, adequate operational objective information, and appropriate operational tools to effect necessary operational adjustments in order to meet all operational objectives and requirements. It is distinguished from other control spaces by the fact that the operational state information is conveyed by electronic or other remote surrogates about the actual operation, and the operational adjustment ability is effected by electronic or other remote operational surrogates to implement actions ordered. The space is for operators and only operators for the purpose of operating and closely related activities. This precludes the space from being used as a convenient rest stop, toilet access, or temporary gathering center for others.
Design	The "gut" feeling felt when the control room space is entered can make or break the operator's connection to and respect for the control room. In many ways it will affect his dominant behavior while inside. When many individuals share a control room, how each control room design contributes to the essential needs of collaboration, individuality, and inclusion is vital. Illustrative attributes include line-of-sight visibility versus back-to-back sitting, visual access by standing over partitions versus access by walking around partitions, sound isolation between operators versus sound cues that are not distracting, and control space replications for shared work areas as needed (e.g., situational advice, crisis management, and special task coordination not able to be done individually). The equipment location and how it is used must be carefully designed and managed. The seemingly simple height of the operator desk can assist work or produce unnecessary fatigue. Nowhere is the concept "a place for everything (needed) and everything in its place" more important or impactful.
Control Room Environmental Parameters	The following environmental parameters are vital. **Lighting**: All illumination in control rooms should support the operations tasks and the duration an individual works in the control room. **Sound**: The room design should support the auditory requirements of the user of the control room, allowing clear and unobstructed communications, absence of distraction, and evocation of serenity and stability. **Vibration**: The sensing and/or feeling of external vibration is a clear stressor and must be eliminated. Subliminal effects can be alarmingly uncomfortable for individuals. **Comfort controls**: Provide a uniform, stable, and comfortable temperature and humidity control without drafts.
Physical or Virtual Control Room	As technology evolves and our understanding of how operators are best utilized to manage operations, it might be that the best control room may just be no control room at all. Or even a virtual reality control room. But that lies a bit ahead of this story and will have to wait.

4.2 Introduction

This chapter discusses the considerations for providing the physical tools and space that we call a control room or an operation center to set the stage for operator success.

No matter what the size of your plant might be, what the finished products being manufactured are, or what the provided services might be, all control rooms have similar issues and related requirements. They must adequately support human users of automation systems. Early control rooms were designed to display and store instrumentation equipment with an afterthought to providing work space for people to interact with that equipment. That has all changed.

Figure 4-1 illustrates the visual and mechanical complexity of an early central control room. The individual dials, alarm panel, switches, lights, electrical indicators, and other elements are all mounted on metal wall panels. The arrangement is designed to facilitate one's ability to grasp an overview of the entire production operation. Each indicator represents an important aspect of knowledge or control for situation awareness.

Figure 4-1. Early control room, circa 1950 design. Note the presence of important indicators yet few controller stations. The operator was expected to be able to gain a good overview of the entire process by "eyeing the board."

Today's effective control room design is all about making it a purpose-built tool to house the individuals and equipment in a way that supports effective operations managed by people. Control rooms need to be much more than spaces we fill with people and their stuff. They must be fit-for-purpose designed and built. Successfully addressing these issues requires insight into human factors engineering and the best practices around ergonomics. A great deal of this forms the backbone of affecting the operator's ability to do his intended job. Part of the backbone includes management systems, such as procedures and checklists as well as the design of the control room itself.

Figure 4-2 illustrates a popular design of individual work areas for operators arranged around a shared segmented partial video wall. Later, we will see why this design is not recommended. Rather than being a bigger personal view, video walls are used more for overview and collaboration functions. The figure shows what it might look like spatially.

Figure 4-3 shows an extensive meteorological control room with many displays for relatively few operators. It suggests how a control room design fits the operational purpose.

Figure 4-2. Contemporary control room circa 2014 illustrating the human-machine interface (HMI) configurations for each individual operator as well as the large shared displays for coordination and overview.

Source: Reproduced with permission from California Independent System Operator corporation (CAISO).

Figure 4-3. Meteorological control room for the European Organisation for the Exploitation of Meteorological Satellites with many displays arranged in a wide sweeping arc. Note that there are few operators.

Source: Reproduced with permission from EUMETSAT.

4.3 A Note about Scope

By plan, this book does not include a discussion about the physical safety aspects of control room design or location. There is no extensive discussion of angles of view and other useful and important ergonomics that all control room design requires. Those considerations are extremely important and impactful. To design a control room properly requires expertise well beyond the intent of this book. You are advised to seek expert guidance in this area. Useful resources include the Engineering Equipment and Materials User Association (EEMUA),[1] International Standards Organization (ISO) 11064,[2] Edmonds,[3] Hollifield et al.,[4] and the Abnormal Situation Management (ASM) Consortium.[5]

---

1 Engineering Equipment and Materials User Association (EEMUA), *Process Plant Control Desks Utilising Human Computer Interfaces – A Guide to Computer Interface Issues*, Publication Number 201, 2nd ed. (London: EEMUA, 2010).
2 ISO 11064 Parts 1–7, *Ergonomic Design of Control Centers* (Geneva, Switzerland: ISO).
3 E.J. Skilling, C. Munro, and K. Smith, "Building and Control Room Design." in *Human Factors in the Chemical and Process Industries*, ed. Janette Edmonds (Oxford, UK: Elsevier, 2016), 187–202.
4 Bill Hollifield, Dana Oliver, Ian Nimmo, and Eddie Habibi, *The High Performance HMI Handbook – A Comprehensive Guide to Designing, Implementing and Maintaining Effective HMIs for Industrial Plant Operations* (Houston: Plant Automation Services, 2008).
5 Abnormal Situation Management (ASM) Consortium, "ASM Consortium Guidelines – Effective Operator Display Design" (ASM Joint R&D Consortium, Phoenix, 2008).

4.4 Control Room and Operation Center Requirements

By now you can appreciate that a good control room or operation center is an important enabler of effective situation management. But that benefit only comes from understanding what these rooms or centers must provide to the operator. We begin this important discussion with the essential (or proscriptive) requirements. These requirements lay down the needs. At this point, we do not discuss how to deliver those needs—that is part of the rest of this book. First, let us understand and agree on requirements. Later, you will be able to pick ways to meet them that respect your operating culture and personnel. Here are the requirements.

Physical Protection and Security

The enterprise must provide the operator with all the design, construction, and operational infrastructure to ensure the following:

- Appropriate and effective physical protection from danger and harm resulting from the production or operations gone wrong
- Appropriate and effective physical protection from the errant effects of nature, both for direct protection and well-being of the personnel as well as the ability to maintain critical operations
- Appropriate and effective physical protection from violence, intimidation, and related nefarious activity
- Appropriate and effective cybersecurity to ensure that unauthorized personnel are prevented from operating, modifying, or otherwise affecting the operation of the enterprise or the underlying support activities

Environmental Controls

The enterprise must provide the necessary infrastructure to ensure appropriate health, comfort, and absence of distraction for the operator. This includes the following:

- Appropriate and properly managed facility temperature, humidity, and clean, fresh air
- Appropriate and proper management of noise and vibration
- Appropriate and effective design and operation to ensure effective visual, voice, and other means of communication for person-to-person, person-to-equipment, and equipment-to-person interactions

5
The Human-Machine Interface

The designer of a CRT display must study and work … .
Know the user of the display; design the display for that user.

Richard S. Shirley (Foxboro Co.)

Operators cannot manage what they cannot see. The HMI delivers most of what they need to see. A control room must be fitted with enough ways to see where things are, what the current situations might be, what might be going wrong, how wrong it may be, and where and how to intervene to make things better. Operators can then manage what they can see and understand using expertise and appropriate tools. The modern video display provides the platform for this to happen. This chapter provides a solid foundation for the design and implementation of the best practices for video displays, the HMI. These *displays* are the primary way to provide operators with enterprise information and situation awareness inferences. They are also the vehicle for providing operational documentation and task guidance. Screen design has evolved from the early versions that stressed the colorful, dense, and flashy, into a technology that is capable of providing appropriate information in a manner that facilitates user appreciation, understanding, and task-supporting interaction.

At first, video displays seemed to represent a significant step forward when they replaced panel boards. It was a step forward in technology but a significant step backward in operator support. This was an unintended result of the evolution of screen design, not the result of intrinsic faults or limitations of displays, that led us down the wrong early paths. Once the faceplate barrier was broken, so to speak, the world of

graphic design seemed to open up. When color made the scene, all the process control system (PCS) manufacturers started a race to see who could use the most appealing and flashy colors to preen in front of prospective buyers. Three-dimensional looks and animation made the situation seem even more appealing but cut into usefulness in a big way. What was missing from all this new technology was meeting the objective of what the video display should do and how best to do it.

Not a One-Stop Shop

You will not find a one-stop shop for HMI design here! Sure, there is a lot here. This wealth of information gives you a good framework to understand what the HMI is all about. This material is intended to supplement the designer's extensive knowledge of enterprise, culture, and locale. What you see here is intended to add to what you already know. Or, if you do not know something, to properly introduce it. There are topics and aspects that are not covered here. Everything has a finite and reasonable limit. This chapter has limits. Readers who are deeply familiar with HMI design will find many items that they may not have considered before, may disagree with now, would explain differently, want to use, or would never use. More breadth and a greater depth of the detail, hardware, and technological implementation are well covered by others.[1] They provide extremely useful interpretations, guidelines, and tools. This chapter is designed to establish a richer understanding of what the whole HMI is about. It positions you to read and understand most other material. Here you will find broad, clear basic design principles functionally linked to *situation management*. You will also find discussions of useful and interesting concepts to assist you in appreciating the various tools, what their capabilities might be, and what to look for as you build or design your own equipment. Knowing what to do with the objectives and processes for good situation management will enable you to identify your HMI needs and work out practices that effectively support them. Each section in the chapter has been written with that objective in mind. Those of you who are familiar with HMI design will easily conclude that rather than this being material in conflict with traditional design, it firmly assists in shaping that design to better fit for purpose.

Chapter Coverage

Covered topics include display screen configurations for operator stations; display screen layout and construction; navigation and operator interactions; styles and style guides; trends; icons, dials, gauges, and dashboards; very large and very small displays; use of sound and video; and methodology for evaluating effectiveness. Again, as a reminder, the specific technology for detailed designs is well outside the scope of

1 See the Further Reading section for more information.

the coverage here. This chapter is rich with a discussion of specialized display screens and their associated *pages*, *windows*, *formats*, and *elements* (special HMI nomenclature is explained in Section 5.3). The goal is to provide overviews and insights, not background tutorials. They are here rather than in the next chapter on situation awareness and assessment, though they are directly intended for awareness, assessment, and management. This was done to provide a natural flow through the fullness of HMI design. As you discover information and situations that operators need to understand and manage, you will have a good idea of effective ways for delivering it to your control room or operation center, or to your clients engaged in those activities.

5.1 Key Concepts

Fundamental Guide	Put no information in front of the operator unless the designer knows (a) what it is for, (b) how it must to be understood, (c) how it is to be used, and (d) is complete enough for that purpose.
Concept Design	Understanding and employing the critical design concepts for the HMI provides the power to see and understand developing abnormal situations as well as manage each situation effectively.
Evaluation	Users are effective at evaluating their HMI design for local style adaptations and usability after design and/or implementation. However, they are unequipped with the tools and design concepts to perform that design themselves.
Data vs. Information	Presenting only data means that the importance and significance of those data values are blatant, obvious, or trivial. Otherwise, it is the designer's responsibility to recast the presentation to show information relevant to the task and situation.
Concurrent Visibility and Accessibility	Operators should not need to write down or remember information and controls needed to coordinate operations and manage situations.
Color	Color is used *exclusively* to convey information. There is no other acceptable use; when used it must be globally consistent (same conventions everywhere).
Truth	All information provided to the operator must be accurate, appropriate, and framed. This means that measurement noise is sufficiently rejected, significant digits of display are the least necessary, the right signal is used to convey needed information, and the appropriate maximum/minimum or historical variations are provided to understand the current value(s).
Workload	Builders of displays need to assess the time to understand and interact with each display to factor in the overall operating load on operators.
Intuition	Any design for the HMI based largely on intuition and appearances will not work. The irony is that it may seem to work for a while and be reasonably comfortable, but it will fail due to excessive user effort needed for routine tasks and will be ineffective for abnormal situation management.
Video and Animation	All movement of information or other display screen content distracts. Animation and video should not be used *unless* it is under the direct control of the operator and is used to sequentially reveal information that is necessary to understand or manage.

5.2 Introduction

The first thing you will notice as you dive into this chapter is that you will not be asked to use much in the way of intuition. Everything, well almost everything, you might have been using before may need to be put aside, at least for a while. This does not mean that your earlier work was done wrong. Rather, we are going to take a second look. And by looking again, we will develop a better understanding of inherent purpose and usability. In all likelihood, previous designs were done with best intentions and honest effort. Much did appear to work, to give credit where credit is due. The operators either liked it or did not complain much. Hopefully, they did provide timely feedback to smooth over any rough spots and make things more convenient. Yet there were real problems:

- Operators had to work at looking around to ensure that they really understood how the actual operation was getting along.
- Operators found that doing routine tasks appeared to take more effort than they thought necessary.
- Operators found that during attempts to manage operational upsets, they were too much "in the dark" with respect to needed tools and information.
- Managers noticed that new operator training seemed to take much more "remembering" and "false starts" than "observing" and then "figuring things out."
- Incident investigations often pointed out that the operator response was delayed, had ineffective results, or even had downright errors.

All of this points to problems. This book is about helping to turn these problems into opportunities that can then assist delivering HMIs that work better. It is about the real needs of the operator and how to meet them in ways that work. Let us define the most-used terms for HMIs as we start things off. Take care here as few are used consistently in the field.

Physical Differences and Preferences

No physical design guidelines or recommendations for the size and location of control room equipment are included in this chapter. However, the importance of ensuring equipment is compatible with a wide variation of operator stature, reach, and other aspects of hands-on interaction must not be underestimated nor inadequately accounted for. This variation includes a person's physical size and weight,

handedness, preferred positions (standing, sitting, varying, etc.), and other limitations and preferences due to physical condition, illness (temporary or long-lasting), gender, age, and more.

5.3 Nomenclature for Display Screens and Components

We use British Standards Institution (BSI) Standard ISO 11064 for nomenclature in this book.[2] Figure 1 from the Standard is reproduced as Figure 5-1 on the next page. For example, the physical hardware device that would be used to show all the content is termed *display*. All of that content would be conveyed to the viewer on *display screens*. The content builder would be free to design and provide at will so long as it was within the capabilities and limitations of the display hardware and the display screen software. Any individual display screen (or as many as you need) would show content utilizing these aspects:

- **Display** – The physical hardware (on which content display screens are shown).
- **Display screen (or screens)** – The actual content (information, real-time data, text, etc.) that is available for operator selection and showing on the physical display.
- **Page** – The totality of viewable content, of the moment, that the display screen contains.
- **Window** – Any of several (usually) individually managed visual subsets of content on a page. A page may contain a single window (occupying either the entire viewable area or a part of the viewable area with the rest without any content) or many separate windows (with due regard to visibility).
- **Format** – Any of several content clumps (we will leave that undefined for a while, but think charts, pumps, diagrams, status text, etc.) that occupy any given window.
- **Element** – Any needed basic content items used to build a format.

Later in this chapter we will need to have a group label for all the places where content (stuff) is placed for the operator to see on the HMI. Let us call them *display screen components*. Everything must be on a display screen. If there is no structure to a given screen, then the entire display screen is built as one piece. Information and

2 BSI, *Ergonomic Design of Control Centers.*

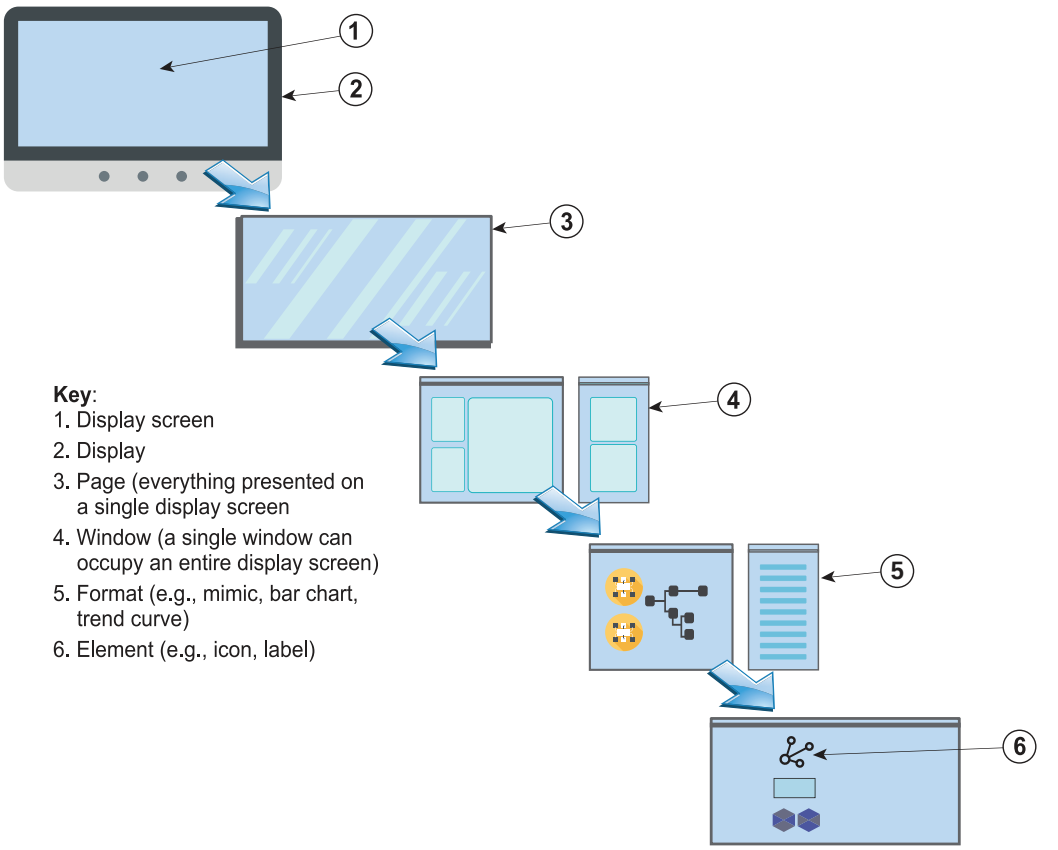

Figure 5-1. ISO 11064-5 nomenclature diagram for graphical displays. This level of detail permits specific reference and discussion. Starting from the upper left, each successive component will be found as continuing a part of the component above.

graphics and all the rest of the stuff we want to show the operator will be placed on display screen components: pages, windows, formats, or elements. A page may have windows by themselves, formats by themselves, elements by themselves, or a mix of any and all. In similar fashion, each window may have none or as much as needed of the HMI parts that are below it in the construction hierarchy. And the same goes for each component going down the hierarchy.

Let us be sure we understand how this works. Using this terminology, no content whatsoever (visible or not) can be on a display screen unless it is on a page. Nothing can be on a page that is not contained in (one or more) windows that occupy any of the various pages available for view. Nothing can be contained within any window that is not part of any format. All formats (there are many) are built from as many elements as needed. Any or all of the various pieces can be reused as needed; that is,

no element is restricted to a given format (unless the designer has special purposes in mind); no format is restricted to a given window, and so on. Moreover, any given piece (element, format, window, etc.) can be derived from any other similar one and modified as desired.

So why devote this attention to something that may seem to be overly complicated and not easy to use? The reason is to allow you to establish a vocabulary and construction methodology that will work. You have here the proverbial "double-edged sword." Swinging one way, the display screen can be configured to provide an almost limitless design and array of content. It would be enhanced by the designer's ability to visualize graphical elements and formats (from Figure 5-1). It would be as powerful as the designer's ability and knowledge of the information and data content required. Swinging the other way, depending on what was selected to show and how it was designed to be shown, the viewer could be well enabled to find, visualize, and understand the content, or be completely frustrated, or worse, dangerously misled. You are well aware of this dichotomy. Our discussion is to inform you about what is recommended and the power of why it is beneficial.

The next several sections will provide useful "cornerstone" guidance about what to consider as you evaluate and design useful and functional operator screens. Section 5.4 will lay out the overall requirements. These are basic and should be in the front of your mind as you do the work. While you may consider various styles, your choice will need to deliver on all these requirements. You do not need to remind me that you know better than I that these requirements, as important and useful as they are, do not give much in the way of specifics. Section 5.5 provides an introduction into the specifics by providing two important lists of "do's" and "don'ts" to follow as you begin to work out your display designs. Section 5.6 moves the general recommendations up a level. It respects the reality that operator screens do not exist in thin air. They are integral to the operator workspace. The section provides useful ways for you to integrate your display design into your workspace design.

5.4 Four Underlying Requirements for Operator Screens

There is an extraordinary power given to the designer of operator screens. Let us be blunt here: everything the enterprise will need the operator to know or find out about the equipment under management must be either available for view on the HMI or obtainable some other way (external documentation, checking with someone else, etc.). Here we deal with what is put on the HMI.

Part II

Situation Awareness and Assessment

6

Situation Awareness and Assessment

Because you can predict does not mean you understand.
The ability to observe does not mean you will get it right.

Unknown

We learn so little from experience
because we often blame the wrong cause.

Joseph T. Hallinan (Author)

Prior to any major accident there are always warning signs which,
had they been responded to, would have averted the incident. But they weren't.
They were ignored. Very often there is a whole culture of
denial operating to suppress these warning signs.

Andrew Hopkins (Australian National University)

This chapter introduces the reader to the dual importance of *situation awareness* and *situation assessment*. Together they play a vital role in the job of operating successfully. The overwhelming preponderance of experience and written work on these topics is from aircraft operations. A great deal of high-quality literature covers both topics. Therefore, this chapter is brief. This book is more about the processes, tools, and technology to successfully bring these concepts into the control room. The chapter lays out a foundation for situation awareness and assessment, discusses how individuals perceive the same events and aspects differently, and provides some acceptable ways

to influence both the individuals and their process of awareness in the directions of success. Later chapters will build your knowledge and confidence.

6.1 Key Concepts

Situation Awareness Question	How can the operator become aware of all the things needing attention that are going wrong or about to go wrong in a way that is understandable and manageable?
Situation Assessment Question	How does the operator determine all the reasonable and plausible explanations for the "data" observed from situation awareness, and from that list, select the one(s) he will "hang his hat on"?
Roles and Results	An effective functional balance between individuality and collectivity is vital for collaborative success. There is no success in the control room without collaboration.

6.2 Introductory Remarks

Start with everything normal. Good operation relies on situation awareness to expose any attention requirements by operators. Awareness is the state or ability to perceive, to feel, or to be conscious of events, objects, or sensory patterns. At this level of consciousness, an observer can see or sense without necessarily implying understanding. *Awareness* is defined as perception and cognitive reaction to a condition or event.[1] This awareness can be the process of observing or actively seeking, or just a feel, often referred to as our *sixth sense*.

Awareness provides the "data" for our operator to question. Situation assessment's responsibility is to produce judgments about those questions regarding operational conditions of production or operation. Situation assessment is what operators do with the "data" of situation awareness. To begin, you will want to get a sense of what goes on in the control room or operation center globally. Once you are aware of the effects of culture and expectation and how they pervasively influence behavior, you can be in a position to consider what you might do to make improvements. Without taking a hard look, it is too easy to gloss over a situation and decide there is not much to it. Another improvement opportunity that might be lost.

A principal purpose of this book is to provide a comprehensive perspective that helps you reach a good basic understanding. The book is designed to provide a useful

1 "Situation Awareness," Wikipedia, last modified May 20, 2018, http://en.wikipedia.org/wiki/Situation_awareness.

framework rather than list after list of things to keep in mind. This framework gives you the right amount of detail to wrap your arms around the concepts so you can feel comfortable with understanding, designing, and implementing your solutions. Then, as you need them, you can pick up the specific technology and tools for the task. These are here as well, of course.

6.3 The Situation Management "Situation"

Ask the questions that are on your mind. What does *situation management* bring to the table that is not already there, or if not there, not truly necessary? Why is it so important to read this book? You might think that your plant is doing well. You might wonder what you will gain by getting upset about gaps and about all the work this book is probably going to suggest that you must do and cannot operate without. These are valid questions. The answers are the reason for this book. If you take successful plant operations seriously, this material can better the odds for your operator.

I am not sure exactly what it takes for your operators to show up in the control room for every shift knowing full well that "today might be the day." What level of internal fortitude must they have that keeps them from stressing out or chilling out to the point that they more or less ignore the dangers and exposure? Yet they do not. For the most part, they do well. But the risks of not performing their jobs well persist. We are working to change the balance to the success side of things.

Let us clarify what operators do in the control room. They enter duty, work a shift on duty, and exit duty. Figure 6-1 depicts this. Every activity and responsibility must be supported by a full understanding of the activity and the degree of responsibility for success. Every duty must be backed up with appropriate operating procedures, effective training and evaluation, and proper tools to do the work right.

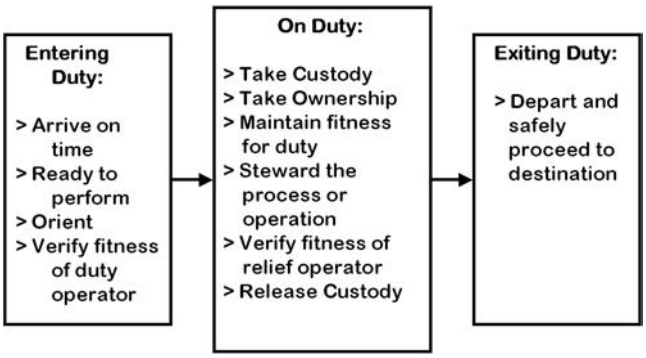

Figure 6-1. Operator roles and responsibilities and how they differ depending on where he is during the shift.

Operators are in charge. They are responsible. They are directly in the line of blame for most incidents, accidents, and disasters—and they know it. Let us change their odds to improve success.

The Operational Setting

We return to the operating setting by revisiting the operating regions introduced in Chapter 1, "Getting Started." Good operation is about "driving" production around the potholes, barriers, and missing guardrails so that it keeps working properly. Situation management is a big part of that. Figure 6-2 (from Chapter 1) again shows us the entire operator arena, but this time we see specifically where the control system is expected to do its job and where the operator must intervene to put things back to right. The illustration is a bit simplistic, but you can see how the operating arena works.

Let us start with things going almost perfectly: operation is inside the magenta dot at the center. No one asks for perfection. Staying "very good" is hard and expensive, so it does not stay there. All the normal variations in operation get to have a say in what is going on. Temperatures, pressures, and flows change a bit. Raw materials change a bit. Production rates or demands change a bit. So, things move out of the "sweet spot" to where they are still good. Nothing must be done here. The process control system is designed for just this goal. It will do that job until it cannot. Sometimes controls adjustments are needed. But if things go too far, direct manual intervention is a must. Alarms are the operator's normal notification of something going wrong. Good situation awareness must cover the rest.

If operation continues to degrade outside the safe operating region, we expect all the protection mechanisms (e.g., interlocks, relief valves, and emergency shutdown

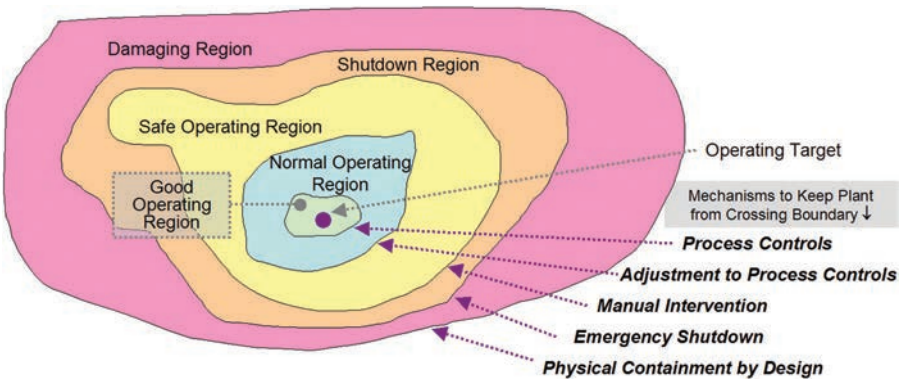

Figure 6-2. This illustration identifies the different operating regions and their "nested" nature as operation deteriorates from being on target through upset and potentially damage. Also shown at the right side are the parts of the infrastructure that are intended to manage upsets or, if they happen, to protect against the worst.

activations) will protect. We expect that level of good enterprise design and maintenance to be there. Our focus here is operations and operators.

6.4 Situations to Be Aware Of

"Situations to be aware of" may sound like a lot of carts coming before a single horse. Of course, you want your operator to know how the plant or enterprise entrusted to his care is really doing. Is it performing as expected? If it is not, how far astray is it, and where is this abnormal operation happening? Clearly, knowing where things are okay is important. However, one must also realize that situations can change in ways that might be subtle and hard to see. This chapter is designed to convince you of the importance of operators being fully aware of the operational status. Fortunately, there are powerful tools to handle these situations. The next chapter will lay them all out. Let us get our arms around the situations first.

Problematic Situations

Trouble does not usually come from nowhere. For all but the most unexpected events, there are always clues, innuendos, and other subtle suggestions and information that signal a problem. The operator's task is to find them and make sense of what is found. Some situations are more likely to result in problems than others. In such situations, the operator should be forewarned to actively look for trouble brewing. The following situations might appear on an operator's radar screen to point him to potential problems:

- Broken equipment or equipment whose operational range is restricted by not being in full working condition
- Maintenance operations ongoing, just completed, or soon to be started
- Procedures that are not working exactly as expected or not working the same way they did when they were last used
- Plant documentation with errors, omissions, or aspects that cannot be verified as either correct or incorrect but are of concern
- Data missing or having suspect values or behavior (laboratory data, HMI screen information, data forms or permits, etc.)
- Deliveries of anything, including routine and nonroutine, that have started or are soon to start in the plant or operation area
- Presence of unexpected or unauthorized personnel in the plant or operation area

- Substitute operational, maintenance, or support personnel presently working
- Any multi-step operation without a specific procedure or annotated checklist to follow
- Any individual whose workplace location is at the site but whose present whereabouts is unclear or unknown
- Any personnel injury

Our job to provide the information. This list is a partial one. Please use it as a starting point for your list to help understand the need to exercise more than ordinary care when these situations exist. You can add to this list from your own operational experiences.

Operational Situations

Trouble can also come when operation is somewhat near the outside boundaries of normal or usual. There is a built-in temptation to assume that things are okay and that nothing unusual is going on. Much of the time that is true, but not always. It is the "not always" part that operators need to be aware of and attentive to. Operational situations that might result in problems include the following:

- More than just minor changes in operation (10% or higher rate of production change, product changes, online equipment changes, etc.)
- Any alarm activation
- Any challenge to an interlock or permissive that did not result in a direct shutdown
- Any spill or loss of integrity even if it is water or some other seemingly harmless material (unless a part of and expected during routine operations)

This list is a partial one. Please use it as a starting point for your list to help understand the need for the operator to exercise more than ordinary care when such situations occur.

6.5 Strong Signals

Strong signals appear as either direct or indirect clear indications of operational problems to be resolved in a timely manner. The "strong" part is that there is nothing ambiguous or subtle about the fact that there is a signal. Operators must always verify that the problem they think is indicated by the strong signal is actually that problem. Properly

resolving these problems requires deep understanding of the process and proper operating procedures. "Weak Signal Management" in Chapter 9, "Weak Signals," provides a more detailed discussion of this topic. For now, we will make the point that enterprises need to be carefully designed, maintained, and managed. Otherwise, the constant challenges to good operation will demand too much resource and dilute the ability to manage effectively. This need for whole enterprise responsibility is a critical recurring theme for sustainability and the essential enabler of the useful tools for ensuring it. Operators (and supervisors) need expertise and experience to keep things right.

Indirect Strong Signals

Unlike alarms that directly point to specific abnormalities with predesigned protocols for handling them, *indirect strong signals* announce that something is clearly wrong, but not what is wrong, why it is wrong, or how to fix it. Here is a brief listing of how indirect strong signals might appear:

- Missing procedure for a (nontrivial) task the operator must perform
- Malfunctioning equipment, sensor, or controls
- Important process conditions that are either unavailable or hard to know
- Procedure that is being followed but is not working as expected
- Required or recommended personnel not present when expected or needed
- Tasks that are falling behind or not completed because of operator workload or distraction
- Too many alarms activating
- Production quality or quantity that is not what it should be or is becoming problematic
- Outside conditions (weather, security, utilities, etc.) that are either not taken into consideration or beginning to require significant operator resources

So, what do operators do with indirect strong signals? For any situations that are covered by existing procedures and practices, operators should follow them. For the rest, they should begin by noting that each item is really a symptom of a likely much larger problem. Identifying them as symptoms is important. Proper problem remediation requires approaching the underlying root cause and resolving it. Sure, treating symptoms can be a stopgap. At times, both treating symptoms and identifying the root cause is advisable but not as policy. We still need to know what is wrong. An excellent process for root cause discovery would be *weak signals*; this topic is covered in Chapter 9, "Weak Signals."

7

Awareness and Assessment Pitfalls

"People look without seeing, hear without listening,
eat without awareness of taste, touch without feeling,
and talk without thinking."

Leonardo Da Vinci (Renaissance Man; Italy 1452–1519)

This chapter provides insights rooted in anthropology, psychology, and sociology. Please do not think that because these insights are not rooted in engineering, they are not powerful and important. As you read about mental models, doubt, "how we think," and biases, you may wonder if such material belongs in a practical technology reference book about control room management. It does. These insights can be just as important as traditional design and engineering guidelines. In fact, social scientists have long been involved in investigating the many psychosocial contributors to disasters. They devote time, money, and reputation to this work. From their investigation, we gain important insights into understanding and managing such disasters. Drawing on their analyses and applying their lessons can help us avoid embarrassment, increase job satisfaction, and dodge or reduce the frequency of disasters. All are worthy goals. Each one gives us a heads up about what often gets in the way of successful *situation management*.

The material in this chapter speaks to the heart of situation management. And it respects the very nature of human nature. Operators are individuals with distinct personalities, histories, aspirations, preferences, dislikes, worldviews, and a host of other traits and opinions including having no opinion whatsoever. They perceive

the world and who they are in their own personal ways. But their individual parts are not the only things they bring to the table. They also bring along deep-seated effects of our rich human nature past. Over the millennia humans have evolved important traits that have protected us and allowed humanity to evolve to where it is today. One of these traits is that when faced with a situation, we instinctually handle it based on our expectations and experiences to work out how the present situation matches what we expect and have experience with understanding and handling. This is why we immediately move out of the way of a falling object. No time is lost by considering exactly how far away it may be or how heavy or dangerous it might be. We just get out of there fast. But, just because it is in our survival nature to always compare what we see and feel to that vast yet mostly hidden instinctual "database" does not mean it works everywhere. One place where it does not work is in the control room.

Even though the control room has been designed to be an optimized workspace; the plant or operation has been designed, built, and maintained to high standards; the procedures and documentation are effective and accessible; the task and competency training of the operator is top-notch; and the personnel practices are effective to ensure readiness and fitness for duty, unless the individual operator (or supervisor) properly uses this infrastructure, good outcomes will not predictably result. As you will see in Chapter 8, "Awareness and Assessment Tools," control room management works very hard to provide appropriate warning and enough time to manage situations where operator management is reasonable, and it designs the rest to fail to safe. Proper use depends on two critical expectations:

1. Appropriate peopleware and technical infrastructure that are carefully put in place to accommodate the honest differences and likely foibles of our human nature.

2. The designer, operator, and supervisor who are carefully trained to be aware of how thought processes and natural biases will get in the way of careful judgment and deliberate actions, and then to work diligently to minimize these disruptive effects.

Our individual differences in thought and logic are important cultural distinctions that profoundly shape our well-being and life. These differences should not be perceived or judged as being better or worse than any other. Logic and truth are not universal, nor universally sought or praised. Behavior in the control room must accommodate the culture and norms of the community without sacrificing proper enterprise-responsible operation. Seeking the goal of safe and respectful operation is

the best path toward universally understood good. In this chapter you will explore individuals' differences, foibles, and seductive natural biases. You will be able to better understand them and work to manage their untoward interference in the control room. It is that important. Let us take a look.

7.1 Key Concepts

Design	Procedures and policies must specifically take into account all the naturally occurring intuitive foibles and limitations of the human operator.
Doubt	No matter how thorough the training, no matter how important the job, and no matter what the reason, if an individual does not believe something, and proper action based on that belief is required, it will not happen.
Multitasking Is a Myth	There is no such thing as multitasking. Any time the thinking part of us must be engaged, it can only focus on one item at a time. Even if that other focus is devoid of emotion or lightly engaged, focus will not split. Multitasking should not be a permitted behavior in the control room.
It Is Judgment	Differences in thought, logic, and life are important cultural distinctions that profoundly shape well-being and lives. These differences should not reflexively be perceived as being better or superior to any other.
Which Time Zone	Logic and truth are not universal, nor universally sought or praised. All expected behavior in the control room must be gained in a way that accommodates the culture and norms of the individual and community *without sacrificing proper enterprise responsible operation*. For example, not all cultures accept a scientific basis for reason.
Danger of Fear of Failure	When fear of failure is perceived to be more important than the actual consequences of failure, operational failures will almost always result.
There Is Only One Logic in the Control Room	In the control room, it is essential that shared successful operating principles and beliefs be developed in a way that is fully competent, understood, accepted, and practiced by operators, supervisors, and managers.
We Look without Seeing	We filter everything our eyes take in through our mood, our culture, and other distractions in view. This has the powerful negative effect of blinding us to almost everything else.
The Reality of Complexity	As soon as we suspect something is complex, we most often balk at "going on to find out really what it is all about," and instead fall headlong into our biases and preconceived notions.
Managing Cross-Purposes	If two institutional goals compete with one another, such as productivity and safety, the higher goal must be clearly expressed. Otherwise, you risk control room chaos. Or, if an individual feels threatened by a loss of security, earning potential, or prestige by divulging rare or hard-won knowledge, key information might not be shared with newcomers.
Our Foibles Are Always Present	No matter how well the equipment is designed, how effective the procedures and operating instructions are, how well trained operations personnel are, or how fastidiously equipment is maintained, unless all of this is properly utilized by operators, successful outcomes are at risk.

7.2 Introduction

Your operator is on shift in the control room. Good operation relies on good situation awareness to expose operational irregularities. Awareness is the state or ability to perceive and feel so that we are conscious of events, objects, or sensory patterns. In this level of consciousness, an observer can confirm data without necessarily implying understanding. Understanding comes later. Patience. *Awareness* is defined as perception and cognitive reaction to a condition or event. This awareness can be the process of observing; actively seeking; or just a feel, often referred to as our *sixth sense*. Awareness provides the "data" for our operator to use. Situation assessment's responsibility is to produce judgments about the operational condition of the production in his care. Situation assessment is what operators do with the "data" of situation awareness.

We now look into what might get in the way of situation assessment going well. The issues and concerns are as real as incidents and accidents. Few major incidents occur without one or more of these impediments and limitations being the root cause of mismanagement into disaster.

7.3 Readers' Advisory

This chapter contains material that goes to the heart of how individuals are profoundly influenced and guided by their beliefs. These beliefs often come from cultural heritage, geographic locale, and other respectful influences. As you read, please understand there is no intent to judge any belief or personality. As members of the community of the world, we are all important and worthy.

A reader may be tempted to find an aspect of culture or personality that may get in the way of successful situation management. It would be most unfortunate if consideration of fitness for operators were based on any material here. This is not the intent, nor is it in any reasonable way necessary or responsible. The express purpose of this discussion is to advance understanding and practices of effective ways to manage important (operator) situations. In doing so, this book attempts to provide honest, respectful, and potentially valuable insight into ways of guiding the professional behavior of operators.

7.4 Why We Make Mistakes

A big mistake is to think that we do not make many mistakes. An even bigger mistake is to avoid understanding why we make mistakes. A way to introduce this concept and make it personal is through what I call "traveler's immunity." It is no accident that

when people are out of their element, such as on a trip away from home, they often do more daring things. Why is that? Sure, there is a certain freedom that comes from getting out of regular habits and away from the daily grind. And that is a part. But dig a little deeper and something important comes up. Being away from the familiar seems to grant us special powers over physics. The ground there cannot be as hard as at home, the water cannot be as treacherous as the water at the local beach, the roads are not as dangerous as back home. It is as if being away can convey a special immunity from the ordinary dangers at home. Sure, the "back home" dangers are really back home. But physics is the same everywhere.

Let us examine the "physics" of why we make mistakes. The best list I can think of comes from Joseph Hallinan:

- We look but do not always see.
- We all search for meaning (before understanding).
- We connect the dots (even when they are not connected).
- We wear rose-colored glasses.
- We can walk and chew gum—but not much else.
- We are in the wrong frame of mind.
- We skim.
- We like things tidy.
- Men shoot first.
- We all think we are above average.
- We would rather wing it.
- We do not constrain ourselves.
- The grass *does* look greener.[1]

This chapter is all about understanding and building in ways to keep the items in this list from getting too much in the operator's way.

---

1 List adapted from the table of contents from Joseph T. Hallinan, *Why We Make Mistakes* (New York: Broadway Books, 2009).

Looking without Seeing

The bottom line is that operators use seeing as the overwhelming source of information for keeping track of things. Yes, there is an alarm system intended to interrupt business as usual and focus on an abnormal situation requiring immediate attention. But if the operator were able to see things going awry early enough, most alarmed abnormal situations could be worked on before the alarm activates. And for all the rest, we depend on the operator seeing it on the HMI screen or on laboratory reports and the like. The "uh oh" part of this is that it is really hard to look and see what needs seeing. Our eyes and brain are not set up well for this seeing part. So seeing can be really problematic. If nothing else in this book seems useful to you, this should be. Understanding and managing how the operator sees (because we cannot actually fix it) is why we spent time on HMI design in Chapter 5, "The Human-Machine Interface," and everything that goes into carefully building HMIs.

Let us review a few of the important design aspects:

- Information displayed for the operator must be for purpose—everything must be needed; observe it all.
- Displayed information must be placed in context—to facilitate needed associations.
- Information must be in a form that is usable—jobs that need doing are supported by where the job is located and how the information is shown.

Before leaving this section and the importance of "looking and seeing," let us prepare for the important ways for the "looking" part to work better. Operators are expected to be able to find situations before they become problems. Yet human nature gets in the way. So, we will need to find ways to look that can make the seeing work. What does not work well is the old-fashioned method of "looking around." "Keep an eye out" is not a good work plan. Using current best operator practices should help turn this around. Chapter 8, "Awareness and Assessment Tools," Chapter 9, "Weak Signals," and Chapter 10, "Situation Management," will show you the tools and how to use them.

7.5 Dangers from Automation

Automation is a powerful technology that enables operations to be done more safely, more reliably, and more efficiently. That's all well and good. On the other hand, where automation is hand-in-hand with human operations, certain dangers are exposed that must be recognized and managed. These activities mean that the design of the automation requires care to ensure that operators remain fully engaged, and specific

procedural requirements must be established to improve and maintain operator engagement. Otherwise, the unintended consequence will be an operator who is more of an observer than a participant. This topic is not intended to be lip service or boilerplate. We are talking about real concerns with real needs.

Nicholas Carr has exposed these unintended dangers nicely.[2] The following topics raise real concerns that you should understand and provide meaningful ways to avoid. The discussion that follows uses Carr's terminology and includes a few of his examples.

The Substitution Myth

What if we wanted to change one small thing? If we could change it a little bit, making the change would not cause any undue effects anywhere else, would it? So, changing might be a way to go. In the front of our mind (as opposed to something in the "back of our mind") is the expectation that this change will not get overblown. Why should it? After all, it is just a small part. Substitution is the act of replacing one thing with another with the expectation that both are equivalent. The myth is: Whenever you automate any part of an activity, you are not just making a change; the act of automation fundamentally changes the broader activity. Small changes can have profound effects. These changes must be understood and accepted before being implemented.

Following that line of thinking, we might think about "bending a rule" here or there; for example, forgetting to report a bit of income on a tax form or overlooking someone shoplifting. We can and sometimes do. Let us leave the moral and legal issues behind; they are not where this topic needs to go. Where this wants to go is three other places:

1. How large is the sensitivity to the change or degree of importance of the effect of the change? Often, perhaps more often than not, small things have small importance, but not always—not always enough to ever be counted on. According to Carr in *The Glass Cage: Automation and Us*, more often than we can foresee, small changes introduce important, sometimes fundamental, effects.[3] Although each change in the following list may seem small, its effect can be significant, but not all the time:

    a. Not fully reading a procedure

    b. Skipping a step in the procedure

2 Nicholas Carr, *The Glass Cage: Automation and Us* (New York: W. W. Norton & Company, 2014); Nicholas Carr, "The Glass Cage: Automation and Us," YouTube video, 55:54, from a lecture to Google employees on October 8, 2014, posted by "Talks at Google," October 14, 2014, https://www.youtube.com/watch?v=Mt8ooCms4sE&feature=youtube_gdata_player.

3 Carr, *The Glass Cage.*

8

Awareness and Assessment Tools

Intuition will tell the thinking mind where to look next.

Dr. Jonas Salk (Physician; Discoverer of the Polio Vaccine)

When you find yourself on the side of the majority, you should pause and reflect.

Mark Twain (Author; Samuel Langhorne Clemens)

Operators must ever look for problems, issues, irregularities, and anything else that might be useful to point out operational concerns that need knowing. This task is an enormous responsibility. Think about it. Your operator is the next to last line for the enterprise's ability to manage serious operational challenges. Anything missed or handled ineffectively leaves the enterprise's sole means of protection entirely up to robust and safe design, the safety shutdown systems, and physical protections and containment. When carefully and responsibly designed and maintained, they generally do the job. But it is at a cost. Emergency shutdowns, automatic shutdowns, and containments are not pretty. They do not do their job gently. And they will not necessarily position the enterprise for a comfortable restart, if restart is even in the cards.

Operators are therefore tasked to use their competency to observe and collect clues of impending problems and concerns while they could be manageable short of other harsh, protective systems. The operator's job is to recognize the obvious and also search out and bring to the surface the hidden, obscured, or subtle goings on of their operation as early as reasonable. To be useful, *situation awareness* requires the suspension of

any preconceived assumptions about problems and outcomes. That is the job of *situation assessment*. That comes later on, not here, not now. We want operators to see what is lurking about first, *without any attempt to assign any meaning to what they find*. Just look. Collect the clues. Then in situation assessment we will work out what it means.

8.1 Key Concepts

Operators Are Not Born with Situation Awareness Genes	The capability to find out or figure out what is going on inside the process or operation must be provided for by the enterprise. There is no reasonable way that any individual can be expected to keep on top of subtle operational threats without competency training and purpose-built tools.
Knowledge Fork	All information, data, procedures, and operating requirements fit on one of the three tines of the fork: known, unclear, or assumed. Nothing but knowns can be used. Throw away the rest unless it can be fully verified as known.
Role of the Alarm System	Each alarm activation is a situation in need of management. Alarms are designed to provide the last clear opportunity for operator intervention to resolve an abnormal situation before it challenges design limits or safety systems, if present.
Abnormal Situations	All abnormal situations that need operator attention must be either alarmed or identifiable by the operator using other tools in the operator tool kit (not left up to chance).
Role of Messages	Alerts, notifications, and messages provide predetermined notice (unprejudiced—not necessarily good or bad, just information) of states of operation, risks and irregularities, and specific tasks to consider doing.
Shift Assessments	The shift-handover process can provide a powerful protocol and tool for in-shift assessments of operational status.

8.2 Introduction

Situation awareness does not happen just because our operators need it. Carefully crafted tools, protocols, and competencies must aid it. It is a vitally important skill for operators to have. The better they are at understanding and managing data and information, the better the job is done. Most of their capability is usually built around experience, availability of useful procedures, intuition, and no small measure of luck. Luck, in that bad things that happened during the shift were manageable. Luck, in that unmanageable situations did not occur on the shift. This chapter takes the operator's responsibility for knowing what is going on away from luck, ad hoc, and "just keep an ever watchful eye" to the level of a supportive technology. This is a competency that we now know much more about how to provide. The technology addresses *what* to provide and *how* to provide it for a properly effective capability. The tools for that job

are in this chapter. In Chapter 6, "Situation Awareness and Assessment," we went over how operators develop the ability to understand and work with situation awareness. Now you will see the working power of the tools. By understanding and being able to design and implement them, you can provide an important measure of capability to the operator for *situation management*.

Knowledge Fork

We want to be able to bring information, opinions, and observations into play. Let us work on making sure all are clear, accurate, and verified. The *knowledge fork* helps ensure that each bit and piece brought to the table is dependable (see Figure 8-1). Every observation, every bit of data, and every other item that is put on the table must be clear. As each bit of information (including observations as well as procedures that appear to be relevant) comes in, use the tines of the fork and classify it as known, unclear, or assumed. Make sure that everything is classified. Use written notes, annotation, and sticky notes on documents or screenshots to track it. This can be done as each bit comes in or after a few are in. Remember that the later it is done, the easier it is for assumptions and unclear parts to lose their proper category and just fall into the basket of knowns. Only known information can be relied on. The rest must be ignored until properly verified.

The knowledge fork categorization must be used to clarify all information used by operators. It needs a prominent place in the tool kit! Operators will use it to pick up everything.

Awareness and Assessment Situation

The job of your operator is to successfully operate the plant or operation. Success means that operations are in conformance with the requirements. During the assigned shift or operations window, operators will utilize skills, employ available tools, and rely on established protocols and equipment. Operators must be aware of anything

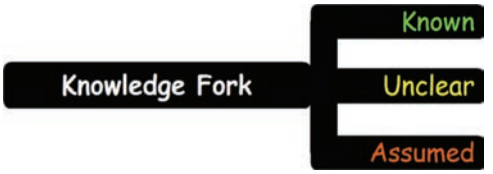

Figure 8-1. Knowledge fork with the three "tines" describing how to qualify every bit of information available and intended to be used for problem identification and remediation (if needed). These classifications ensure that decisions are made from only known information. Anything unclear or assumed must be verified to the level of "known" to be used.

going on that represents a threat or potential threat. They need to take appropriate remedial actions against those threats. Without awareness, no operator would know that anything might need assessment and management. So, what does awareness need to look for?

> Only a few incidents started with the sudden failure of a major component. Most started with a flaw in a minor component, an instrument that was out of order or not believed, a poor procedure, or a failure to follow procedures or good engineering practice.[1]

A cornerstone of situation awareness is the alarm system. A proper alarm system aids awareness. Alarms are used to identify all problems requiring operator intervention that result from all abnormal situations that enterprise designers and operations experts identify. This critical understanding for alarm system design leads to a high level of alarm system effectiveness. Figure 8-2 depicts the general situation. The desired state for the plant to be is *process normal*. When things go wrong enough, some part of the process

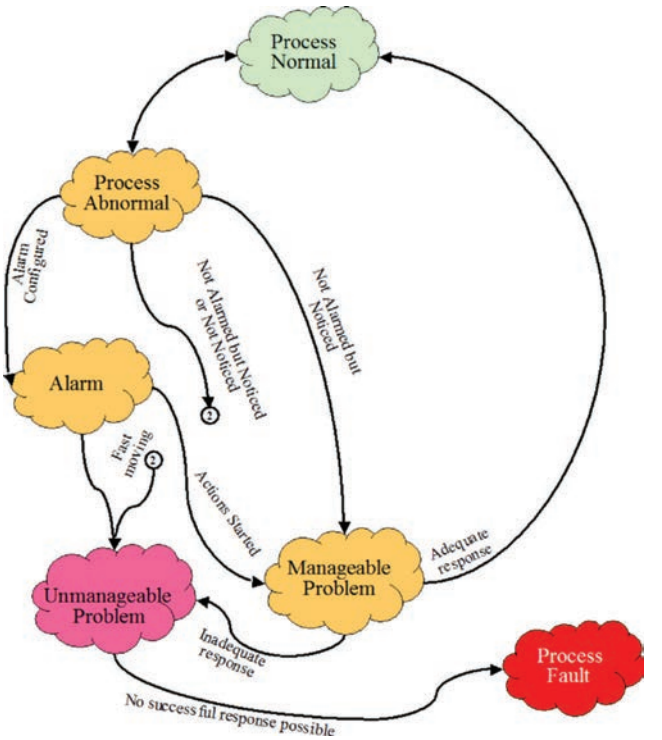

Figure 8-2. Operational conditions from normal showing the current primary structure in the control room. Most conventional operator monitoring relies on either alarms or serendipitously coming across the other problems before alarms. This chapter adds other tools to this.

1 Trevor Kletz, *What Went Wrong? Case Histories of Process Plant Disasters*, 3rd ed. (Houston, TX: Gulf Publishing Company, 1994).

becomes *process abnormal*. If alarms are configured for these abnormal conditions, an alarm will activate. If the problem is manageable and the operator works the situation successfully, the situation will return to process normal. On the other hand, if the situation is an *unmanageable problem*, the operator will not be able to prevent a *process fault*.

If alarms are not configured for the process abnormal condition, but the operator notices that there is a situation that needs attention, one of several outcomes could occur. If it is a *manageable problem* and it is done correctly, the process normal will be restored. If it is done incorrectly, or if the process abnormal situation is entirely missed by the operator, the situation will be an unmanageable problem and a process fault will result.

How will the operator find all of the ways that threats might impact a plant or operation? What can operators use to find them? Besides waiting for alarms to notify of threats, operators have little else in the way of specific tools and other defined resources. In an attempt to fill this gap, many planned ways have evolved. A partial listing includes the following:

- Carefully designed HMI that is closely monitored
- Clear and complete operating procedures and protocols
- Routine scheduled monitoring of important operating parameters and conditions
- Periodic monitoring of operations looking for problems or concerns
- Using materials and energy balances
- Preparing for and conducting shift handovers
- Conducting training in looking for problems, issues, and potential concerns

All of these are rather general. With the possible exception of the balances, they do not much relate to any specific minute-by-minute ways an operator would be able to identify potential problems. This means that for most operating situations not covered by alarms, the operator might not have enough help.

Figure 8-3 collects all these situations within the "cloud" labeled "process is not normal but not yet abnormal." For the moment, focus on the top four clouds: *process normal*, *process abnormal*, *alarm*, and *process is not normal but not yet abnormal*. We have already gone over the pathway from process normal to process abnormal to alarm. The

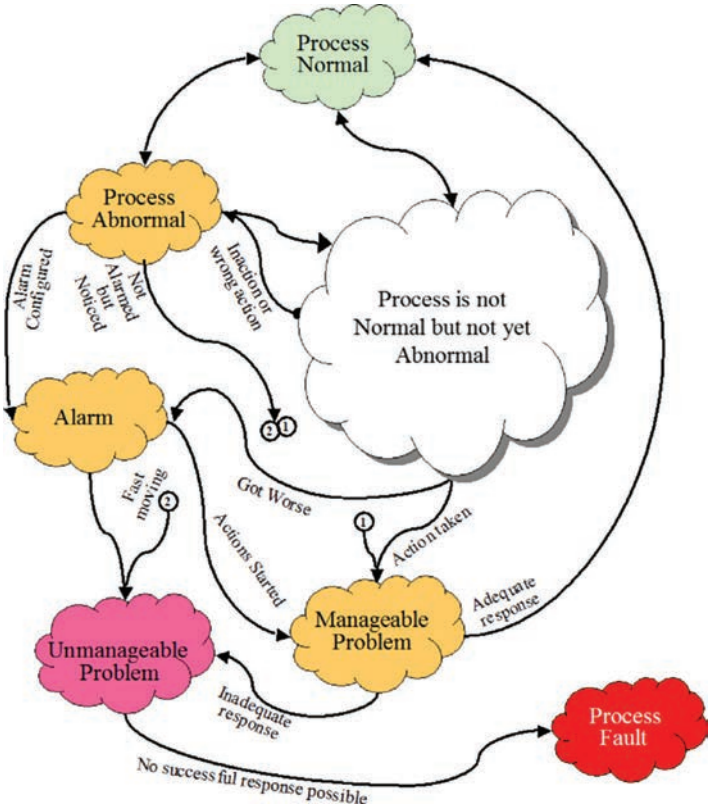

Figure 8-3. Operational conditions from normal showing an extended awareness structure in the control room. In addition to alarms, the process of identifying and evaluating off-normal situations is added to the kit.

rest of the problems the operator must deal with are contained in the cloud *process is not normal but not yet abnormal*. There are four states that the plant can move to:

1. Return to process normal.
2. Move to process abnormal.
3. Go directly into alarm.
4. Be judged a manageable problem (for the operator to begin to manage).

The first three states constitute the usual operator situation. They will have adequate procedures, and the operator is trained to handle them. We will now work on extending the operator's skills by introducing situation awareness for the operational state where their plant or operation is not normal but not yet abnormal. This chapter provides many clear and useful tools in those four situations. We will start with the alarm system.

8.3 Alarm System

A proper alarm system is a cornerstone for responsible operation of industrial plants. It enables operators to be notified of a subset of abnormal situations in time to make the difference. Providing alarms for all abnormal situations needing operator intervention is part of the process design and operation requirements. These abnormal situations should be specifically identified during the process design, implementation, and operational design activities. Figure 8-4 shows how alarms fit in. Note that operators also need a way to identify those other abnormal situations not covered by alarms. This chapter and the next are designed to find those. Finding and managing them is a core requirement for proper situation management.

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.

Alarm Fundamentals

Successful alarm systems are built on four fundamentals (Figure 8-5). Proper alarm design is a straightforward engineering process. Everything you know about

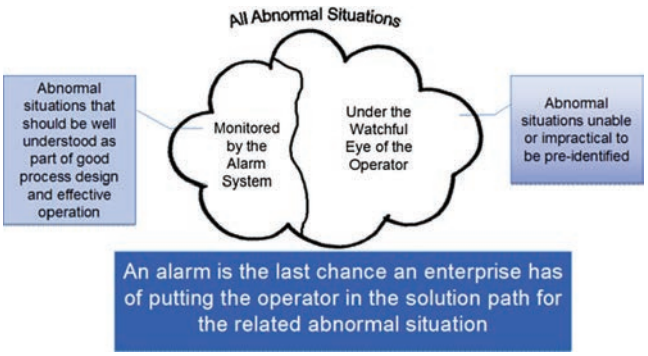

Figure 8-4. Alarms for abnormal situation identification are the primary responsibility of the process and equipment designers to build. All the other abnormal situations are left up to the operator to find, somehow.

9 Weak Signals

All things are easy to understand once they are discovered. The task is to discover them.

Galileo Galilei (Astronomer; Italy, 1564–1642)

In solving a problem of this sort, the grand thing is to be able to reason backwards.

Sir Arthur Conan Doyle (Author, creator of Sherlock Holmes)

When people stumble onto the truth they usually pick themselves up and hurry about their business.

Sir Winston Churchill (British Statesman)

Weak signals is a very new concept. It is new to the control room setting. It is new to our thinking in any situation. Properly understood and competently conducted, weak signals can provide a valuable and sharp tool for operators to identify situations that otherwise might have gone unnoticed and thus unappreciated. Certainly, operators have lots of other ways to identify things going amiss and potentially likely to cause trouble. Earlier chapters have covered many. Weak signals is another tool in the box. It is a very sharp one. You should find it extremely useful. Besides the obvious benefit of helping operators make sense of small indications of trouble or concern, the process works extremely well in getting around preconceived notions arising from biases (Chapter 7, "Awareness and Assessment Pitfalls"). It also makes sense of how the human-machine interface (HMI) screens are designed (Chapter 5, "The Human Machine Interface") to help find both large and small problems. We are now positioned to take full advantage of situation awareness.

Operators have the critical job to be on the lookout for problems in the making and find them early enough to prevent bad things from happening. These things can be hard to see. Operators need to be able to pick up early on operational clues and any suspicions about something not looking quite right. Qualified operators with proper training and experience are imperative. A purposeful, effective control room design and strong personnel access protocols are expected. High-quality supervision is essential. Success relies on a comprehensive human-machine interface (HMI) designed and built to provide an open window into the process. The HMI puts operators in the best position to focus their talents and actions for watching, evaluating, and managing. Using it, operators will sense things amiss and work out what might be going wrong. HMI design topics have been covered in earlier chapters. Now we are going to use them. This chapter lays out a powerful tool to help all operators find subtle plant operational issues and problems as they develop. But, as powerful as it is, and as useful as it is, please keep perspective. Without careful attention to all the earlier material in this book, even the best tools and talented operators cannot do well enough jobs. The single purpose of weak signals is to identify potential operating problems. *Weak signals* is not a tool used to diagnose. It is not used to remedy. It is simply used to identify and confirm.

Abnormal situations come in two parts: the ones that are alarmed and the ones that are not. Those that are well understood, are alarmed. Those that are not alarmed are the ones the operator must find pretty much on his own. Figure 9-1 illustrates this situation. Alarm system designers are responsible for ensuring that all abnormal situations they can uncover during equipment and process design, during the development of operating procedures and training, and during the operational safety analyses, including HAZOP and preoperation safety review (PREOP, also referred to as

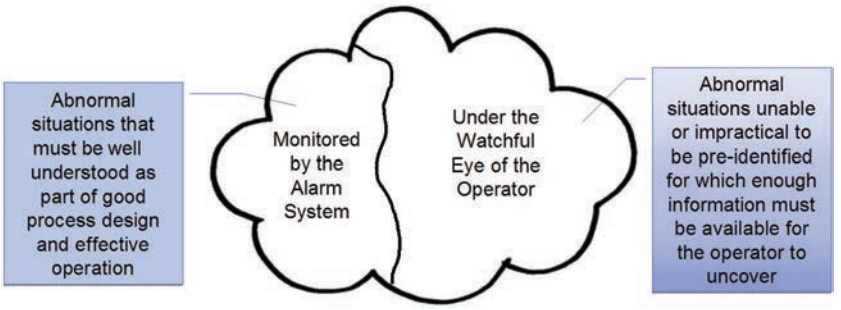

Figure 9-1. Abnormal situations are divided into the portion that competent designers must identify during the equipment and operations design process, including the HAZOP and process hazard analyses and other applicable design and operational safeguards. For the former, alarms are designed. All the rest are left up to operators to find using effective monitoring during operation. HMIs, plant operation guides, protocols, and procedures facilitate this task.

pre-startup safety review—PSSR), have proper alarms configured for them. The operator must discover all the remaining abnormal situations by his own effort. It is part of the job. Chapter 8, "Awareness and Assessment Tools," discussed the infrastructure tools operators rely on. Chapter 4, "High-Performance Control Rooms and Operation Centers," and Chapter 5, "The Human-Machine Interface," added to the building up of operators' support mechanisms to help. This chapter adds a new *situation awareness* tool called *weak signals* to the kit.

Weak signals are observable; suggestive but not definitive; and when examined properly, lead to the discovery of abnormal situations early enough to be valuable. Operators using this tool have a powerful skill to assist them. It helps operators focus on suspicions, clues, hunches, nagging issues, and the rest of those subtle nuances that might rightly be early (sometimes very early) indicators of things going amiss. It allows operators to separate them from noise. Weak signals as a tool moves the operator's capabilities from being useful to being effective and reliable. Its single purpose is to aid operators to find operational issues early. It is a true situation awareness tool. Using it, operators can more easily and effectively evaluate early irregularities and other puzzling concerns that they come across to determine which might be meaningful and which are likely not. The use of weak signals can be a game changer. Every operator who understands how to use it and uses it well can have a better chance of maintaining good operation. Every enterprise that successfully incorporates weak signals into its control room infrastructure can take advantage of the increased ability of operators to find potential operational problems and issues.

This is a tool that you will retrofit into your existing control room operations. It fits seamlessly into shift changes and periodic "walk-throughs" during the shift, and it can be used as needed when troublesome things seem to pop up. The chapter lays out the foundation and the work process. Operators who understand and incorporate weak signals into their shift activities will have a powerful methodology for increasing situation awareness. Be assured that there is nothing weak about using weak signals. It is a powerful capability. The term *weak* implies that subtle changes or cues provide relevant clues. These clues offer important avenues for assessment. But they first must be identified. According to Paul Schoemaker and George Day, a weak signal is:

> [a] seemingly random or disconnected piece of information that at first appears to be background noise but can be recognized as part of a significant pattern by viewing it through a different frame or connecting it with other pieces of information.[1]

---

1 Paul J. H. Schoemaker and George S. Day, "How to Make Sense of Weak Signals," *MIT Sloan Management Review* 50, no. 3 (2009), http://sloanreview.mit.edu/article/how-to-make-sense-of-weak-signals/.

This chapter is about how to identify and assess weak signals. Weak signal management has a single purpose: early identification of potential abnormal situations. Weak signals is a situation awareness tool. Once identified and confirmed, the rest of *situation management* takes over. It uses all the existing plant infrastructure and operations management tools. This work process builds seamlessly onto the technology and methodology of Chapter 8, "Awareness and Assessment Tools," and into the processes and work procedures you will find later on in Chapter 10, "Situation Management." Together, operators have a way to find the out-of-normal and abnormal, hopefully in time to make the difference. Weak signal management provides the ability to take something not well formed and provide confirmation (or disconfirmation) of its likely existence.

Weak signals have an interesting history. The term was coined by H. Igor Ansoff in 1975.[2] Ansoff recognized explicitly that almost no significant event emerges without some warning, although those warning signs can be extremely subtle and often indistinct. For the next 20 years, weak signals were an obscure label of something to look for. Bryan S. Coffman revisited them to extend and add structure to the concept in his MG Taylor monograph series in 1997 titled "Weak Signal Research."[3] Here was the beginning of a useful process. Some of the earliest uses were to make predictions about what new technology innovation might become a commercial success. Specifically, what might be the next big innovation to capture the market as a new product? The difficulty is that a real innovation does not build on something already there. The next innovative thing is not a continuation of an existing thing. It is an entirely new form. When people are asked what they would like to see in new things, they only see more wonderful versions of what is already there. So, to make the leap of insight, we must look for clues about what people do (as opposed to what they use to do it). We must ask what barriers might be in the way of doing it better. The clues, if any, are the weak signals.

This chapter lays out this tool for operators. Operators will use this tool differently. They will be looking for the next problem that they did not otherwise see coming. Besides the obvious utility of alarms, finding other potential problems is rather difficult. It is not so easy to be able to "keep an eye out" for things that could be amiss. The alarm system covers a really important part—everything that could be pre-identified for the enterprise design and operational requirements. But there is a lot left over that must be found. Weak signals fills a large part that gap. It provides an important tool

2 H. Igor Ansoff, "Managing Strategic Surprise by Response to Weak Signals," *California Management Review* 18, no. 2 (1975): 21–33 .

3 Bryan S. Coffman, *Weak Signal Research—Part I: Introduction* (Louisville, KY: MG Taylor Corporation, 1997).

for operator effectiveness. We will explain the technology and process. There is a lot to it. This discussion has been carefully laid out for you and the many supporting side threads examined. Try to keep this in perspective. The concept is simple. It is straightforward to use. Operators will actually use weak signals around 5% of their on-shift time. The rest of situation management is about the remaining 95%. Together they provide a game changer for your operator.

Before we get started, let us clarify how weak signals are to be used. There is a popular notion that we should call hunches, intuitions, clues, and the like weak signals. As if calling them that will make a difference and somehow elevate the situation. It does not. The term *weak signals* is used here to mean both a dependable way for observing them *and* a principled plan for using them to identify true implications. It is this dual activity that promises to be the value. Let us see how it works.

9.1 Key Concepts

Weak Signals	Weak signals are the foundation of a new technology that changes the operators' role from "hunting around hoping to find the problems" to an organized process for identifying likely ones. Weak signal analysis forms the core for simple yet powerful tools to expose abnormal process situations to the operator's view. Every off-normal condition is a weak signal. Weak signals (1) are observable; (2) are suggestive but not definitive; and (3) when examined properly, could lead to the discovery of an important abnormal situation early enough to be valuable.
Strong Knowledge	Weak signals are only useful in situations in which underlying knowledge of the function and inner workings of the process being managed is strong and used.
Solid Foundation Infrastructure	Effective weak signal management can build only on an existing solid foundation. The quality of the entire enterprise is the single highest influence on the operator's ability to find, understand, and manage operational threats.
Short-Term Strategic Tool	Weak signals is a short-term strategic tool providing a tactical look-ahead of likely developing abnormal situations, thus permitting operators to fully focus on the current task of maintaining regulation without blurring the need to find developing problems.
Do Not Escalate	Weak signals do not usually become stronger with time or worsening of the underlying off-normal situation; though it often becomes easier to backward-project them to look for evidence the longer they persist.
Confirmation and Disconfirmation	Weak signals evidence may exist as *confirming* (there is a real abnormal situation) or *disconfirming* (a real abnormal situation is unlikely here); both types must be sought and evaluated to guard against operator biases (Chapter 7, "Awareness and Assessment Pitfalls"). All confirmations must be clear, not vague.

Primary Situation Awareness Tool	Weak signals are the "front line" of situation awareness. To be useful, control rooms must be designed for their effective detection.
Weak Signals Question	"What is wrong with the current operation and my assessment of it that I may not be aware of now?"
Some Not Alarmed	Fast-evolving *transformative weak signals* can progress directly to consequences. If those situations could be anticipated in advance, alarms would have been designed for them. It is important, therefore, to identify and attempt to process transformative weak signals as soon as possible.
Alarms Plus Weak Signals	All process abnormalities worth knowing about that are not covered by appropriately configured alarms need to be available for exposure by weak signals. This is an *affirmative requirement* for HMI design, reporting protocols, and operating procedures. If they are neither, either the alarm system or weak signals need more work. This gap suggests a design failure in the understanding of process and operational risk.
"Soft" Observations	Weak signals can also arise from general observations of the process being managed or other sources surrounding that process.
Bottom Line	Weak signals is a powerful information noise processing algorithm.

9.2 Introduction

This chapter is about strengthening your operator's ability to figure out what might be going wrong. This is a daunting responsibility. It is difficult for an operator to be constantly on the lookout for anything and everything that might be amiss in his plant or operation. It is a task made all the more difficult because most of the time things are okay. Success depends on years of experience and on-the-job skills that vary considerably from operator to operator. Even for the same operator it depends on how the day is going. Your best operator is not on every shift. Even your best operator has limitations. Weak signals augment alarms to expose much that might be subtle, indistinct, elusive, insidious, indistinct, fuzzy, or otherwise inconspicuous to the operator working hard to achieve adequate situation awareness. Not too long ago, alarm management was not useful enough, and it often interfered with the operator assessing situations. Early alarm management was done intuitively and incrementally. This has all changed. Alarm systems now have a strong and powerful role in the management of abnormal situations. We understand their basic principles and know how to apply them. And when we do so, they work remarkably well. Weak signals is an important aid for finding the rest of what might be going wrong.

A Word to the Reader

Weak signals is a new topic. It takes some getting used to. This chapter will walk you through it. Mastering weak signals will allow you to relate what might be happening in the plant or operation with the other activities of operating in a control room.

To do this, the chapter is organized in layers. The layers begin at a concept level and progress deeper into the details and options. It is suggested that the reader read the entire chapter fully. This way, as important techniques and provisions are introduced and discussed, preliminary ideas can build into an understanding. As you read, it will become clear why this book carefully prepared the control room for getting ready to help this to work. The operating discipline of shift change both assists the leaving operator to make sense of his shift and at the same time orients the arriving operator to what to expect. The HMI is carefully designed to convey the critical functionality of the plant in a way that exposes as much of the irregularities (all those weak signals) as a good understanding of the plant will permit. Being able to understand and manage uniquely human thought and planning limitations keeps the operator better focused on finding out what might be amiss without getting in his way of keeping an open mind as he gathers confirming or disconfirming evidence for it.

This book could have been written almost the same had we not known about weak signals. In fact, this book was initially conceived without them. The entire frame of the book had been laid out without them. It was clear that for operators to do a good job, we needed them to be well trained with an in-depth understanding of the plant and equipment. We needed properly designed plants with strong management systems. We needed effective maintenance programs. We needed control rooms designed to facilitate the long shifts and the varied work going on inside them. We needed the HMI to fully engage the operator and allow him to fully open the windows to the process and provide the handles to adjust as needed to keep things on course. We needed a collaboration and operational charter as the tools of last resort. All of this puts situation management on as firm a footing as our best practices and experiences could provide. And that is where it was for a while.

Add weak signals to the mix and not much seems to change. But in reality, everything has changed. They give a clearheaded operator who is not fatigued and is looking at his HMI, the ability to see those subtle things that suggest something is amiss. And once they are seen, he has a process to evaluate their importance and significance. This is an extraordinary tool for finding abnormal operations early. Weak signals do not take the place of everything else. Rather, they build on everything else. Meaningful use of weak signals depends on those other things!

Before we look into this remarkable topic, I offer some advice. As you read how the concept of weak signals works and how the operator fits into its functionality, many of you are going to get a feeling that to do it well will be extremely taxing. Alarms are one thing. They sound when needed, gain the operator's attention, and provide most, if not all, the necessary guidance to manage the situation. Weak signals do not do any

Part III

Situation Management

10 Situation Management

Never mistake motion for action.

Ernest Hemmingway (Author)

We learn so little from experience because we often blame the wrong cause.

Joseph T. Hallinan (Author)

We must stop all this communication and start having a conversation.

Mark Twain (Author, Samuel Langhorne Clemens)

Now is the time to claim your prize! You did not win the lottery. Sorry. Anyway, relying on chance to keep things going well is not a dependable strategy. There are better ways. Here are some. In this concluding chapter on *situation management*, you will see the many ways you can change "chance" into competence. It is about ensuring that the job operators do will be beneficial. This chapter cements everything together so operators can deliver. It will help operators gain confidence in operations. To get the real prize, management must make changes, followed by operations, engineering, and maintenance. Everyone is part of this team. This team is going to work.

How the team works is everything. How the individual works will lay the framework for how the team works. We rely on a four-step process to keep everything clear and working.

1. **Observe** – See what about the enterprise might need attention and action.
2. **Confirm (or disconfirm) problem** – Understand everything that needs attention. Keep the parts that actually need clarification, attention, or action. Discard those that do not.
3. **Remediate** – Decide what intervention must be done and how to do it to manage everything that needs it. Carry out the needed actions and activities that were decided on.
4. **Confirm (or disconfirm) resolution** – Verify the effectiveness of actions and correct where needed.

The effectiveness and power of taking each step in order comes from knowing *only that step is being thought about and worked on*. Nothing is permitted to spill over into the next step before you are complete with this current step. Keeping everything distinct is effective in ensuring that each step is fully explored and understood in its own right. By not jumping ahead and by being careful, you can minimize those natural tendencies to succumb to biases that always lead down the wrong track; provide clear and structured opportunity to engage dual tools to work, including collaboration and delegation; and ensure enough information is at hand to prepare for the next step.

As you read into this chapter, you will come across many ideas and suggestions for changing the way your enterprise is designed and managed. As you find ideas you would like to use, please keep in mind that the best way to do so would be to design them into the fabric of your existing enterprise. Resist the temptation to add a new procedure, a new committee, or a new list of responsibilities. Doing it that way could be quick and less costly, but it is unlikely that it would be either efficient or sustainable. You want both. Work out how each new idea or concept should fit back into an existing procedure or training program. Design and modify the existing ones to include the new.

10.1 Key Concepts

Situation Management	Situation management is the ability to identify possible and potential threats to good operation of a plant or enterprise; confirm the validity, significance, and extent of the threats; undertake appropriate response to the threats to remediate or, if remediation is not possible, limit the extent of damage; and evaluate the results of those efforts.

Fundamental Concepts for Effective Situation Management	1. Explicitly *identify* what the current situation is. 2. Fully and independently *confirm* that situation is as identified. 3. *Remediate* or resolve only the situation identified and confirmed (no "changing horses in midstream"). 4. **Confirm** or disconfirm that current corrective actions are working.
Effective Situation Management Changes the Rules; New Rules Mean Better Outcomes	When an infrastructure is prepared for the unexpected as if it were "expected," the entire rules of the "game" become operations of competence. Managing shift workflow will significantly improve the operators' ability to detect and manage impending abnormal situations, and at the same time reduce uncertainty and stress.
Knowledge and Experience Should Rule	Operating in a major situation requires the active participation of individuals solely based on their expertise (demonstrated knowledge and experience) regardless of their immediate position in the organization hierarchy.
Design In Rather Than Add On	The best way for sustainable implementation is to design in rather than add on.
Control Room "Condition"	Use of specialized control room conditions can provide the environment where operator ability to focus is enhanced by explicitly managing distraction and simultaneously providing special targeted resources.
Goals versus Risk	When operational risk challenges operational goals, managing risk always comes first.
Escalation Is a Safeguard That Improves with Use	The ability to rapidly deploy competent escalation teams to the control room can make the difference between dangerous operations through inappropriate risk-taking or inability to recognize incipient danger and an orderly transition to a safe operating state. Enterprises will readily deploy escalation teams as often as needed to back up their culture for safe and effective operations.
Situation Management Bottom Line	Successful situation management requires operators to apply specific solutions to problems without specifically experiencing them beforehand. This requires competence training on how situation management tools and concepts are used.

10.2 Introduction

Automation today places the operator well above the minute-by-minute responsibility of watching process variable values and making manual adjustments to maintain proper regulation. Enterprises have sophisticated automation equipment to do that job. Whether it is a single-loop controller that measures a pressure to modulate the position of a control valve or a vast distributed control system that manages an entire plant, operators watch rather than manipulate. Only when proper operation might be at risk is the operator called on to act. In this new world of operations, the most important operator task is to know when things are going well and when they might not be. Every time an early abnormal operating situation is missed, valuable solution time is lost. When the abnormal situation gets worse and is also missed, much more is at risk. Often incidents, some very serious, are the result. And when intervention is called for, the skill of the operators and the performance of the supporting actors can make the difference.

Situation management is about finding and managing problems, not so much about resolving them. Once found, most of the solving is usually well understood. Most trouble comes from not finding the real problem, finding only a part and not finding those other parts, or failing to properly work a solution.

This chapter is about how things come together in the control room. Let us start by remembering the fundamental concepts for effective situation management. Everything in this book supports one of these four core concepts:

1. Explicitly *observe* what the current situation can be or is.
2. Fully and independently *confirm* or *disconfirm* that the actual situation is what you think it is.
3. *Remediate* or resolve only the situation identified and confirmed (no "changing horses in midstream").
    a. Factor in all *threats* present or on the horizon that can shape the solution.
    b. Always stay in *familiar* territory by never letting the process or operation take the operator to a place he has never been before (instead, shut down or safe park).
4. Make sure the resolution effectively *resolves the problem*.

A problem is not considered to be found until its potential risk (if not resolved) is fully understood.

The Situation Management Activity

Situation management is the competent execution of the four fundamental activities. Refer to Figure 10-1 (repeated from the Chapter 1, "Getting Started"). Everything in this book supports these activities.

Successful situation management requires operators to use specific solutions to problems without ever being trained or experiencing them specifically beforehand. That tool kit requires operators to be proficient at detecting early abnormal operations, evaluating those situations to identify all that must be addressed, and successfully addressing each. This is what the entire book is about. It is how you can ensure that what the operator needs gets successfully done. The shared understanding and acceptance of the principles of good operation protocols, competency training, and operational improvement

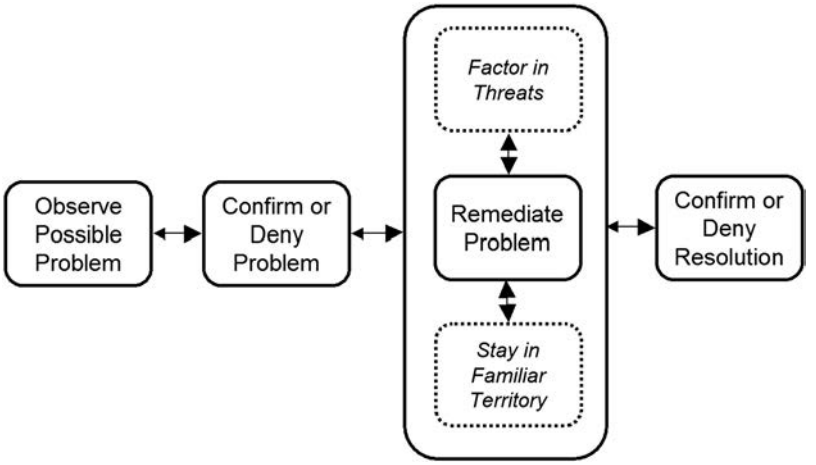

Figure 10-1. Four-part situation management activity process that requires appropriate tools and technology to be able to find all potential problems, specifically confirm or deny their presence, and resolve them if there. Note the importance of factoring in any threats that are near, keeping the remediation relevant, and making sure that everything done is familiar (not invented on the fly).

tools are the front line of success. Because these principles are so important, tools must be carefully designed, often following industry good practice guidelines or conforming to regulatory guidance and requirements. Operators and supervisors must be trained and refreshed in their use. Recommendations from incidents and accidents are carefully examined and folded back appropriately. Technology and equipment providers are ever-improving their offerings. Given proper management resourcing and direction, all of this should work to improve the control of operations.

Step-by-Step Working Process

Let us break this down into a nice, clean working process. Remember, for each bit of information, be sure to use the information fork (see Chapter 8, "Awareness and Assessment Tools") to identify the known parts and flag the unsure and assumptions parts. Only the known parts can be used.

Activity 1: Observe Possible Problem

- **Step 1**. Find all potential and reasonable problems that may be causing the process to be abnormal. *Make no evaluation* about how confident you feel about each or how plausible each might be.

  Here you are just making a list of cautionary clarifications for the step.

Activity 2: Confirm or Deny Problem

- **Step 2**. Find all evidence that tends to *confirm* each problem as being the right problem, and find all evidence that tends to *deny* each problem as being the

right one. Do not attempt to decide which problem might be the one causing the process to be abnormal.

Here you are making lists for each separate candidate problem.

- **Step 3**. Where some evidence confirming and/or denying one candidate problem is shared by another candidate problem found in step 2, then carefully and deliberately look for a larger or different problem that combines the two that share confirming and denying evidence. If you can, add that one to the list of potential problems found in step 2.

  Refine the list of problems to the smallest sensible number found.

- **Step 4**. Settle on the Step 3 list of problem(s) (abnormal situation observed and confirmed that needs active resolution).

  Make the list and arrange the items in order of operational risk. Make sure that none are moving too fast to manage.

Activity 3: Remediate Problem

- **Step 5**. Identify remediation protocols and procedures applicable to managing each problem.

  These must be established and approved procedures as well as trained-for activities.

- **Step 6**. Identify all threats that are outside the immediate problem but can affect either the choice of remediation method or the way the remediation is applied.

  Example threats include threat of loss of essential utilities, missing support manpower or other resources, problems in adjacent operating areas that might spill over into this one, and need for escalation or collaboration.

- **Step 7**. Execute the remediation activities making sure that all actions and activities, and all results and changes, are expected and understood. If not, at any time, immediately begin "permission to operate" activities and procedures.

Activity 4: Confirm or Deny Resolution

- **Step 8**. Continue monitoring and remediation activities until the situation is resolved. At any time where remediation activities fail to progress or achieve the needed results, and alternate activities are not a planned part of the remediation, immediately begin "permission to operate" activities and procedures.

At this point, the problem is resolved or the plant activities are in a safe place under established "permission to operate" activities and procedures. No other state is permitted.

10.3 Lessons from Air France Flight 447

In important respects, the tragic crash of Air France Flight 447, an Airbus A330-203, into the South Atlantic Ocean provides a rich experience in the value, *actually the necessity*, of proper operations management in the face of uncertainty—and the intimately related damaging effects of confusion.[1] It is precisely this that situation management is designed to detect and advise. To understand this event, we will use what has been pieced together from the various records of the flight and expert conclusions.

Background

On June 1, 2009, Flight 447 was at cruising altitude after a routine scheduled departure from Rio de Janeiro on its way to Paris. It crashed into the sea some 3.5 hours later with a loss of life of all 228 passengers and crew. The initiating event was inoperable air speed measurements caused by excessive icing of the Pitot tube measurement elements located on the outside skin of the fuselage. The proximate cause was aerodynamic stall caused by a too low airspeed. The too low airspeed was the direct result of pilot action. Predictably, the stall resulted in a complete loss of ability to fly. Although the problem of excessive icing of the Pitot tube airspeed sensors was well documented, Air France failed to upgrade the tubes on all fleet aircraft. This was compounded by the lack of proper training of Air France pilots in Airbus aircraft handling under full manual control. Training was deficient to the point that most current pilots would fail.

We examine the timeline of events leading up to the time of the crash. During an uneventful portion of Flight 447, the captain woke the second pilot for duty and left the cockpit for a routine nap. Later, within a few minutes after the airplane entered turbulent weather, the autopilot and auto-thrust systems disengaged. The airplane had flown into a thunderstorm with significant turbulence. It was one of several storms in the area, so it may have been difficult to avoid without extensive flight path deviation, although most pilots would choose flight path changes to avoid the storms. There was no indication that the pilot of Flight 447 made any effort to avoid this particular storm. The airspeed indicator increased sharply (for reasons unknown at the time, but later learned to be due to the failure of the airspeed sensors). The stall alarm sounded (an antithetical event; had airspeed actually increased, which it did not, the pilot neglected to process the true cause of this alarm). This led the pilot to erroneously assume that the aircraft was flying at too high a speed. The crew made consistent changes in flight surfaces designed to reduce airspeed. The actual airspeed eventually fell below stall, and the aircraft lost all ability to maintain flight. It has been estimated

1 "Air France Flight 447," Wikipedia, last modified June 20, 2018, https://en.wikipedia.org/wiki/Air_France_Flight_447.

Appendix: Definitions of Terms, Abbreviations, and Acronyms

"What's in a name?"

William Shakespeare

abnormal. The state of not being normal. See also *normal*.

abnormal situation. Any unexpected or unintended situation that differs from what is expected.

absolute alarm. Standard construction for most alarms. The present condition of a potential alarmed variable is compared against the preset alarm activation point. When crossed, the alarm becomes active.

Dynamic modification of the alarm activation point and/or priority is permitted.

See also *enhanced alarming*.

accident. An unforeseeable and unexpected turn of events that causes loss of value, injury, and increased liabilities.

ACK: acknowledge.

ACK'd: an alarm that has been acknowledged. See *acknowledge*.

acknowledge. The first operator action that indicates the recognition of an alarm to the alarm-managing portion of the control system.

action. The activity of doing something tangible (usually physical).

activate. An alarm that becomes "in alarm" by the monitored entity passing over the alarm activation point from the normal into the abnormal condition. See also *alarm activation point*.

active state. The status of a configured alarm being in alarm (the process or condition value on the alarm side of normal or within the alarm deadband).

adequate resources. Management is required to provide operators with accurate information and the training, tools, procedures, management support, and operating environment necessary for the operator to take action to help prevent accidents and minimize commodity losses.

advanced alarm. See *enhanced alarm*.

alarm. An audible or visible means of indicating to the operator an equipment or process malfunction or abnormal condition requiring a response.

alarm acknowledge. See *acknowledge*.

alarm activation. The state in which an alarm becomes active (enters the state of being in alarm).

alarm activation point. The threshold value or discrete state of a process variable that triggers the alarm into the active state.

alarm class. This is a misleading term. Dividing alarms into classes is not useful for operators or for designing alarm systems in general. Alarm priority should be used to assign a level of importance to alarms. See *alarm priority*.

alarm deadband. The range through which the alarmed variable must be varied away from the alarm activation point in order to clear the alarm.

alarm flood. The situation when the number of alarm activations exceeds the operator's ability to process them.

alarm group. The set of alarms associated within the alarm system. See also *plant area model*.

alarm historian. The database that contains the long-term record of all alarm (and other) activities associated with alarms. See also *alarm summary*.

alarm horn. Any type of audible sound (including voice response commands and warnings) that is initiated when an alarm activates and alerts the operator to the presence of an active alarm. The alarm horn will silence when the operator silences or acknowledges the alarm.

Some plants use different sounds and/or tones to distinguish between various operator positions and/or alarm priorities. This practice must be carefully designed to avoid confusion and unnecessary distraction during times of stress.

alarm indication. All means of indicating to the operator that an alarm has been activated.

alarm limit. Archaic term. See *alarm activation point*.

alarm log. The historical record of alarm indications and actions.

alarm management. The processes and practices for determining the need for, documenting, designing, monitoring, and maintaining alarm systems.

alarm message. The text message that is normally used to convey identification information about an alarm when it activates. This is an important part of the alarm summary.

alarm philosophy. The guiding document for design or redesign of the entire alarm system.

alarm points. The process conditions that are configured to be alarms. These are usually specific physical entities (pressure, temperature, purity, etc.).

alarm priority. The attribute of an alarm that defines a specific level of importance to the alarm to be used by the operator in deciding which alarms to work and in which order.

This is the primary way enterprises manage operational risk when alarms activate.

alarm rationalization. See *rationalization*.

alarm readiness state. The physical state of an alarm with regard to whether it is expected to activate when the alarm activation point is passed.

alarm response manual. The set of all alarm response sheets. See *alarm response sheet*.

alarm response sheet. A document (sheet) that contains all information about a given alarm and fully documents every operational aspect. It is extremely useful to both the operator and the alarm system designer.

The format may be a printed or online form, which may include dynamically assembled basic process control system (BPCS) screen information relevant to the alarm and plant states.

alarm set point. This is a misleading term. See *alarm activation point*.

alarm summary. See *alarm summary display*.

alarm summary display. A graphic human-machine interface (HMI) display that lists alarm indications over a period of time. The list includes the status of all active alarms and all recently cleared alarms.

In general, the BPCS manufacturer preconfigures the display and only facilitates minor customer customization.

alarm summary manual. See *alarm response manual*.

alarm summary sheet. See *alarm response sheet*.

alarm system. The entire construction (the collection of hardware, software, procedures, and protocols) that detects the alarm state, conveys that information and other supporting information to the operator, and archives all alarm information.

alarm trip point. Archaic term. See *alarm activation point*.

alert. A message or other visible and/or audible means of indicating to the operator a plant situation or equipment condition that does not require a response.

Alerts are useful in replacing old alarms that were used only for the purpose of notifying the operator of equipment status or condition. See also *message* and *notification*.

audit. The activity of examining status or performance by comparing the current conditions against the requirements. The audit results usually include recommendations for improvement.

auto shelve. An advanced alarm or enhanced alarm function that detects the need for shelving an alarm and does so without operator intervention, according to a preplanned procedure.

automation. The technology and equipment designed to operate mostly without undue operator attention.

backward-projection. The activity of identifying places to look for evidence of the most impactful implications that resulted from forward-extrapolation. See also *forward-extrapolation* and *weak signals*.

bad actors. Any alarm (usually thought of as a significant number of alarms) that activates too often to permit the proper operator actions. Taken as a class, these alarms result in a significant distraction to the operator who must acknowledge them, and because they can block or hide more useful alarms, even very important ones.

base load. Operator loading for all basic tasks and responsibilities when the plant or operation is functioning normally. See also *operator load*.

BATNEEC: best available technology not entailing excessive cost.

best practice. A recommended practice that is considered the most appropriate by those in the field of activity. See also *recommended practice*.

BPCS: basic process control system. See *primary controls platform*.

bypass. To manually modify a function to prevent its activation. The term is used to imply that some mechanical method (e.g., using jumper wires) has been employed to ensure that the affected alarm will not activate. See also *cutout, disable, inhibit,* and *suppress*.

(This term is not normally used to describe alarm readiness states.)

Index

Note: Page numbers followed by f or t indicate figures or tables, n refers to chapter footnotes.

A

ABB, operator effectiveness program, 53
Abnormal, 526
Abnormal operation region, 35–37
Abnormal situation, 472
  definition, 134
  plant actually abnormal, 135
  plant actually normal, 135
  weak signals, 518–519
Abnormal Situation Management (ASM) Consortium, 228
Abstract mimicry, screen, 278
Accident(s), 5, 136. *See also* Incident(s)
Accident-prone behavior, 455
Accommodation, 247
Acknowledging, communication, 657, 658
Acoustic, operator interaction, 278
Action notification, 507
Active lifetime, 509
Adams, Richard, 538
Administration, role in operations, 50
Advanced Operation Assistance Solutions, Yokogawa, 55
Advanced regulatory control, 108
Advanced technology control center(s), 239–241
Affecting operator, 160
Affordance, 245
Air and Space Operations Center, 236
Airbus 330–203, 552
Airbus A330, 421
Aircraft
  pilot training, 275–277, 276f
  See also Plane crashes
Air Florida Flight 90
  cockpit errors before takeoff, 676–677
  cockpit errors during takeoff, 677–678
  crash, 676–678
  crash into Potomac River Bridge, 677f
Air France Flight 421, 551–552, 647–649
AkzoNobel, 127
Alarm(s)
  abnormal situation identification, 477f
  definition, 506
  event data, 198
  excessively complicated dashboard for nuisance, 324f, 324–325
  line of defense, 40
  management, 66
  multitasking and, 453–454
  nuisance example gauge, 311–313
  operating region showing, 40f
  operation regions, 35–37
  overview display screen showing, 338f
  precedence of operator activity, 618
  process, 14f, 15f, 16f
  role of system, 472
  secondary display page showing, 341f
  something is wrong for sure, 40
  system, 402
  weak signals and, 617, 618
  See also Notification(s)

Alarm activations, weak signals from, 618–619
Alarm Management for Process Control, 498
Alarm rationalization, weak signals, 611
Alarm response sheet, 485–489, 486f
  abnormal situation, 486
  advanced alarm considerations, 489
  automatic actions, 488
  causes, 487
  configuration data, 485
  confirmatory actions, 487
  consequences of not acting, 487–488
  header information, 485
  manual corrective actions, 488
  online example, 489, 490f
  safety-related testing requirements, 489
Alarm system, 474
  alarm activation point, 491–493, 493f
  alarm fundamentals, 477–478, 478f
  alarm priority, 494–497
  alarm rationalization step-by-step, 497–499
  alarm response sheet, 485–489, 486f, 490f
  anatomy of, 478–479, 479f
  configuration metrics, 499–500
  management, 480–481
  metrics, 499–501
  operator alarm loading, 501–503
  performance metrics, 500–501, 501t
  philosophy, 479–480
  process abnormal, 475
  process fault, 475
  process normal, 474
  process trouble point, 489–490, 491f
  rationalization, 482–485
  time management, 491, 492f
Alignment failure, 465
Amagasaki rail crash, 425–427, 464
  aerial view of crash site, 426f
  setting up the fear, 426–427
  takeaway, 427
American National Standards Institute (ANSI), 43
American Petroleum Institute (API), 47
Analog, device technology, 277
Anchoring bias, 445–446
Annotation, 376
Announcements, HMI, 379–380
Ansoff, H. Igor, 520
Antonia, Rosa, 60
Aristotle, 461
Artificial intelligence, weak signal analysis, 631–632
Asiana Flight 214, 423–425, 447
  July 2013 crash, 423, 424f
  setting up the roles, 424
  takeaways from incident, 424–425
Asimov, Isaac, 527
Assessment situation, awareness and, 473–476
Audience of book, 10–11, 56, 58
Auditing, 514
Automated shutdown, 716
Automation, 643
  bias, 421–422
  ceasing operations during significant upsets, 114
  complacency, 420–421
  dangers from, 418–422
  generation effect, 422
  operating periodically without, 113–114
  plant, 112–115
  procedural, 110–112
  proper level of, 114–115
  selective, 113
  substitution myth, 419–420
  See also Selective automation
Awareness, 416
  alerts, messages and notifications, 506–511
  biases, 441–448
  concepts, 415
  definition, 392, 511
  doubt, 432–436
  geography of thought, 456–464
  inattention blindness, 448–450
  institutional culture versus individual responsibility, 464–469
  looking without seeing, 418
  making decisions, 436–441
  making mistakes, 416–418
  myth of multitasking, 452–454
  partial information, 450–451
  personalities, 454–456
  See also Notification(s); Situation awareness

B

Backward-projection
  confusing evidence from, 629
  illustration, 578f, 579–580
  no evidence from, 629
  potential problems, 631
  Texas City disaster, 615
  work process, 573–575, 574f
Bandwagon effect, bias, 446
Bank of England, 333, 334f
Baseline operational measures, 557–558
BATNEEC (best available technology not entailing excessive cost), 46–47
Beliefs, 416
Belonging, 215f, 216
Bender Treater, 351–352

Best available technology not entailing excessive cost (BATNEEC), 46–47
Best practice, 44
Beuthel, Carsten, 345
Biases, 441–448
  anchoring bias, 445–446
  automation, 421–422
  bandwagon effect, 446
  confirmation bias, 442–444
  continuation bias, 445
  diffusion of responsibility, 446–447
  halo effect, 446
  post hoc ergo propter hoc, 447–448
  "what then" question, 448
Boardroom, process safety beginning in, 87–88
Boeing 777–200ER airplane, 423
Boston Transit System, 369, 370f
BP, 93
  Toledo Refinery, 79
  Transocean *Deepwater Horizon* and, 467–469
BP Texas City disaster, 99–100, 403
  critical failure, 143f, 143–144, 147, 468
  operator's permission to operate, 685
  retrospective weak signal analysis of, 616t
  splitter process flow diagram, 614f
  weak signal case study, 612–613, 614f, 615
Brafman, Ori, 439
Brafman, Rom, 439
Brazerman auction, 439–440
Build-on-demand trends, 330
Bullemer, Peter, 273
Bystander effect, 447

C

Canadian Standards Association (CSA), 43
Carr, Nicholas, 419
Carrillo, Rosa Antonia, 567, 655
Carte blanche, permission to operate, 691
Cautions, conflict with protocols or statutory requirements, 9
  design and safety notice, 8–9
Center for Operator Performance, Wright State University, 54
Challenger Space Shuttle, 465–467
  prelaunch command and control management failures, 467
  prior-to-launch technology management failures, 466–467
Charles Schwab (SCHW), 80
Checklists, 182–183, 602
Chemical impairment, 169
Chemical Safety Board (CSB), 133
Chernobyl, 167, 167f
Cherry, Kendra, 162
Chevron Corporation, 217
Chevron Oil, tenets of operation, 660–661
China syndrome, 537–538
China Syndrome, The (movie), 537–538, 538f
Churchill, Winston, 223, 517
Circadian clock, 165, 166f
Circadian rhythm, 165, 166f
Clemens, Samuel Langhorne, 641
Coaching, escalation teams, 709–710
Code blue, 725–726
Code gray, 727–728
Code orange, 728
Coffman, Bryan S., 520, 567
Coherent view, 285
Collaboration, 402, 675–684
  10th man doctrine, 680–681
  Air Florida Flight 90 crash, 676–678
  control room, 740
  in control room, 679
  crew resource management (CRM), 678–679
  escalation in control room, 699–700
  red teams, 684
  shift handover, 186
  triangulation, 681–683
  using knowledge fork, 675f, 675–676
  weak signal management, 595–596
  work space, 243–244
  worst case, 680
Collaboration center(s), 237–239
  bring-your-own workstations, 238, 239f
  configurations, 238
  functional requirements, 237–238
  importance of, 238–239
  physical requirements, 237
Collective, term, 623
Color, 261
  blindness, 297–298
  display screen, 293, 294f, 295f
  excessive use of, 382f
  improved screen, 383f
Command and control
  control room, 713–715
  supervisor fully qualified as operator, 714–715
  supervisor not fully qualified as operator, 713–714
Commercial enterprise, term, 79
Communication
  escalation in control room, 698–699
  handover, 199
  hypothetical, 658
  mindful, 655–656
  mirroring, acknowledging and tracking, 656–657, 658

Communication (*Continued*)
mobile operator, 212–213
safe conversations, 652–658
shift handover, 186
word about safety, 653
Competency, training, 176–177
Complacency, automation, 420–421
Concept design, 261
Concept of scale, 74
Confirmation, situation management activity, 24, 25, 25f
Confirmation bias, 430, 442–444, 543, 649
illusion of skill, 444
loss of scale, 443–444, 444f
myside bias, 442
See also Biases
Consensus, weak signal management, 595–596
Content change management, 375
Continuation bias, 445, 649
Continuous improvement, 69
Contradictions, weak signals, 592
Control (magazine), 7
Control loop
flow control example, 106–107
magic of, 105–107
moving disturbances, 107
process control, 105–107
temperature control example, 105–106
Control measures, difficulty of, 554–555
Control room(s), 223–224, 233–235
in abnormal operations, 662
access management, 231
advanced technology control centers, 239–241
architect perspective, 256–257
architectural aspects, 235, 236f
automation complacency, 420–421
automation in, 643
building style, 251
code blue, 725–726
code gray, 727–728
code orange, 728
collaboration, 675–684, 740
command and control, 713–715
console design, 252–253
controls engineer, 738–739
crew resource management, 679
dangers from automation, 418–422
delegation, 674–675
design, 225, 226–227, 249–253, 257
design circa 1950, 226f
design circa 2014, 227f
design considerations, 252
design evolution, 234–235
directing operator, 724
environmental controls, 225, 229–230
escalation, 740
future of, 255–256
information support tools and technology, 230
key concepts, 224–225
layout, 251–252
life cycle, 253, 256–257
location, 250–251
management choices, 737–738
managing operator, 724
MBTA Boston Transit System, 369, 370f
meteorological, 228f
mobile, 253–254
mobile operator, 210–211
in normal operations, 661–662
observer evaluation, 695–696
operational conditions showing current primary structure in, 474f
operational conditions showing extended awareness structure in, 476f
operational support, 231
operations engineer, 739
operator redeployment, 720–725
operator self-evaluation, 696
permits, 232–233
personnel, 233
physical protection and security, 229
principles and ergonomics, 252
process and operational controls, 230
process engineer, 738
remoteness of, 234
requirements, 229–233
restricted, 661–663
role of, 254
scope, 228, 233
security, 251
situation codes, 725–728
special operating situations, 232
sterile, 664–665
upset operating situation, 723f
USS Seawolf submarine, 240f
video walls for, 366, 368–370
visitors, 233
Control room management, 19, 37
equipment, 21
essential components of, 20–22
framework of, 19f
maintenance, 21
management pillar, 20
operation interface, 21–22
operator training, 21
procedures, 21
Control room operators, 161. *See also* Operator(s)
Controls engineer, 738–739

Controls platform, formal notifications by, 510
Conversations
  mindful, 655–656
  safe communication, 653–655
Cooperation, situation awareness, 404, 405
Costa Concordia (cruise ship), 705
Costs
  best available technology not entailing, 46–47
  understanding, 59–60
Coveralls, 70
Crew resource management (CRM), 162, 170, 455
  collaboration, 678–679
  operators, 714
  training, 734
Crisis management, 12
Critical failures, 137–146
  BP Texas City, 143f, 143–144, 147
  chains, 138–140
  Deepwater Horizon, 144–145, 145f
  Milford Haven at Texaco refinery (UK), 140–142, 141f, 147
  Olympic pipeline in WA, 146, 146f
  Piper Alpha, 142–143
  See also Incident(s); Plane crashes
Critical variables, weak signals and, 619
Crossover(s), 159
  basic procedure framework, 159
  management, 159–161
  Piper Alpha lesson, 160
Cues, HMI, 378–379
Culture, 79–80, 416
  alignment failure, 465
  geography of thought, 456–464
  handling and reporting problems, 463–464
  individuality, 463
  institutional, versus individual responsibility, 464–469
  logic and reason, 460–462
  norms and conventions, 457–460
  visual perception, 459–460
  world map delineating East, West and blended frameworks, 457f

D

Darley, John, 163
Dashboards, 318–325
  better, 325
  clear and effective, 325f
  definition, 318
  design fundamentals, 326–327
  design fundamentals for, 325–329
  deviation diagram, 320–322
  excessively complicated, 324f, 324–325
  overloaded, 323f, 323–324
  pipeline system, 319–320
  salience requirements, 328–329
  social media users, 319
  unity of presentation, 322–325
Data versus information, 261
Da Vinci, Leonardo, 413
Day, George, 519
Dead reckoning, navigation, 302
Deception of two reasons, 430–431
Decisions
  Brazerman auction, 439–440
  loss aversion, 438–440
  making, 436–441
  over many shifts, 437–438
  short-term versus long-term, 436–438
  sixth sense, 440–441
  within a shift, 436–437
Decomposition, 127
  basics, 118
  concept, 78, 117
  illustration of typical boundaries, 118f
  input and output classification questions, 119f
  key repeated elements, 120–121, 121f
  key repeated subsystems of, 121–122, 122f
  looking for abnormal situations in repeated elements, 123–125
  looking for abnormal situations in repeated subsystems, 125–127
  structure of, 120–123
  subsystem boundary attributes, 118–119
  subsystem internal attributes, 119–120
  system, 123, 123f
  underlying situation management, 120–127
  using transformational analysis for, 130–131
Deepwater Horizon
  BP and Transocean, 467–469
  critical failure, 144–145, 145f
  during the incident, 468
  operation prior to incident, 468
  postscript, 468–469
De facto decisions, permission, 691
Defensive driving, Smith System, 32
Defensive operating, 32–35
  five principles of, 33–34
  lessons of, 665–666
  supplementary guidance, 34–35
  term, 32
Delegation
  of authority, 92
  control room, 674–675
  of responsibility, 92–93
Deming, W. Edwards, 77, 153

Design
concept of, 225
considerations, 252
console, 252–253
control room, 226–227, 249–253, 257
evolution, 234–235
high-reliability organizations, 88
safety notice and, 8–9
user-centered, 244–249
Development supervision, role in operations, 50
Deviation diagram
dashboard example, 320–322
operating area, 565f
Dials and gauges
design types, 327–328
nuisance alarms, 311f, 311–313
pipeline nominations tracking, 313–318
resolution-based display screens, 328
risk-based display screens, 327–328
Diffusion of responsibility, bias, 446–447
Digital
device technology, 277
smart devices, 559–560
Direct enter search, navigation, 302
Directing operator, 724
Direct measurements or observations, weak signals from, 542–545
Direct strong signals, 398–399
Disaster, 137. *See also* Critical failures; Incident(s)
Disaster management region, 531
Display screen(s)
attention-based principles, 268
building effective screens, 385–386
dashboards, 318–325
dials and gauges, 311–318
Engineering Equipment and Materials User Association (EEMUA) principles, 269–270
glyphs, 305–308, 308f
icons, 308–310
ISO 9241 principles, 271–272
large and small displays, 353–365
memory principles, 268–269
mental model principles, 268
mimicry concepts, 278
nomenclature for, 263–265
paper versus electronic screens, 370, 372–377
perception principles, 267–268
principles of design, 267–272
Wickens' 13 principles of, 267–269
See also Off-workstation (OWS)
Display screen design, 292–295
color, 293, 294f
color blindness, 297–298
construction, 281
display complexity and minimum view time, 297
dynamic page assembly, 295–296
examples, 286–290
flash, 291–292
hierarchy, 282–284, 283f
overview level, 283f, 283–284, 335–339
overview of, 281–290
principles of, 267–272
procedure tracking, 344f
screen arrangement and layout, 294–295, 296f
screen structure, 281, 282–291
secondary level, 283f, 284, 339–343
segmentation, 284–285
tertiary level, 283f, 284, 343–345
visibility and viewability, 290–291
Display screen examples, 334–345
overview identifying components, 337f
overview page, 335–339
overview showing alarms, 338f
overview showing operator's responsibility, 336f
secondary page, 339–343
secondary page for Riser/Regenerator, 340f
situationally based secondary pages, 340, 342–343
subordinate secondary pages, 339–340
tertiary page, 343–345
Display screen organization
geographically based, 290, 290f
hierarchy, 282–284, 283f
responsibility-based, 286f, 286–287
risk-based, 287f, 287–288
similarity-based, 289, 289f
situation-based, 304–305
task-based, 288, 288f
Documentation preparation, 198–199
Dodge, Wagner, 726–727
Doubt, 432–436
dealing with uncertainty, 434–435
lingering, 435
managing "truths," 435–436
possible, 433
probable, 433
reasonable, 433–434
shadow of a, 434
Douglas, Michael, 537
Doyle, Sir Arthur Conan, 517, 541
Ducommun, Jesse C., 153
Due diligence, 44
Dutch Safety Board, 133
Duty of care, 47
Dynamic page assembly, 295–296

E
EEMUA (Engineering Equipment and Materials User Association), 228, 269–270
Effective screens, 385–386
Electronic, device technology, 277
80:40 rule, 431–432, 432f
Electronic formats
  content change management, 375
  documents, 374–375
  following the thread, 374–376
  personalization and annotation, 376
  pros and cons, 372–373
  readability, 373–374
  related content, 375–376
Elements, 261, 263, 264f
Ellis, Graeme, 38n7, 61, 61n16
Email, informal notifications, 510–511
Emergency, alarm priority, 494, 496t
Emergency shutdown (ESD), 715–716
Emerson, 54
Emerson Automation Solutions, 382, 382f, 383f
Emotional impairment, 169
End of Eternity, The (Asimov), 527
Endsley, Mica, 378
Engaged handover interaction, 199–200
Engineer(s), 10–11, 59
Engineering Equipment and Materials User Association (EEMUA), 228, 269–270
Engineers' Creed, 155
Enough displays, 304
Enterprise(s), 77–78
  abnormal situation, 134–135
  accidents, 136–137
  automated plant, 112–115
  capabilities, 86–89
  commercial, 79
  communication between silos, 85–86
  component organization, 82–85
  control loop, 105–107
  critical failures, 137–146
  crossover management, 159–161
  culture, 79–80
  decomposition, 117–120
  decomposition underlying situation management, 120–127
  delegation of responsibility, 92–93
  hazard, 134
  key concepts, 78
  knowing what is right, 73–75
  learning from experiences, 133–134
  near miss, 135–136
  operational boundaries and responsibilities, 157–164
  operational integrity, 93–99
  plant area model, 115–117
  preparation, 199
  process hazard management, 146–148
  responsible engineering authority (REA), 103–105
  safety, 99–103
  selective automation, 107–112
  short-term versus long-term, 89–92
  silo concept, 82–86
  suits and coveralls, 70
  transformational analysis, 127–132
  understanding, 81
Enterprise design, concept, 78
Enterprise scale points, definitions, 98
Environmental controls, 225, 229–230
Epicycle, 74
Equipment, plant area model, 115–117
Equipment reliability indicators, 560–561
Escalation, 696–706
  collaboration, 699–700
  communication, 698–699
  control rooms, 740
  Costa Concordia cruise ship example, 705
  design, 706
  direction of, 703
  first duty of, 703
  operator recognizing, 700–702
  process of, 704, 704f
  resources, 702–703
  transfer of responsibility, 701–702
  when to escalate, 704–706
Escalation teams, 706–713
  abnormal situation management process model, 711–712
  activity, 709
  composition, 708
  frontline coaching and mentoring, 709–710
  readiness evaluation role, 710–711
  training, 711
Essential decomposition, concept, 78
Esteem, 215f, 216–217
European Agency for Safety and Health at Work (EU-OSHA), 133
European Organisation for the Exploitation of Meteorological Satellites, 228f
Evaluating effectiveness, HMI, 380–383
Evaluation, 261
Event notification, 507
Everyday situations
  fictional illustration, 666–667
  flow of operator activities, 670, 671f
  operator duties, 669
  operator intervention caution, 667–668

Everyday situations (*Continued*)
operators following the rules, 669–670
operators not being innovators, 668–669
situation management, 666–673
Evidence for confirmation
backward-projections, 578f, 579–580
confirming evidence, 575–576, 580
degrees of evidence, 577–578
disconfirming evidence, 575–576, 580
weight of evidence, 581
Expanse, work space, 243
Experience
benefiting from, 651–652
learning from, 75–76
operating, 67
Expertise, situation management, 651–652
Explicit, 38

F

Face-to-face handover, 200–201
Failures. *See* Critical failures
Fan charts, 332–333, 334f
Fate, logic versus, 462
Fatigue
causes of, 167
circadian rhythms, 165, 166f
impairment, 169
incidents and, 165–167
managing, 168
understanding, 164–167
See also Operator readiness
Fault-tolerance clock, 31
Federal Aviation Administration (FAA), 679
Few, Stephen, 318
Field operator, 162
handover, 202–203
handover timelines, 202f, 203f, 207f
Field shelters, 235
Flag, 198
Flags, weak signals as, 598–600
Flash
cycle, 291, 292f
screen display, 291–292
visibility, 291
Flow, control loop example, 106–107
Focus, navigation, 303
Fonda, Jane, 537
Formats, 261, 263, 264f, 332
Forward-extrapolation
problems of, 629
proper, 587
weak signals, 630
work process, 570–573, 571f, 572f
Four-corners tool, 409–411, 410f
Foxboro Company, 259, 320
Franklin, Benjamin, 463
Frontline supervisors, role in operations, 49–50
Functional silo, 84–85
Fundamental guide, 261
Fundamental tools, situation management, 24–30

G

Galilei, Galileo, 517
Gauges. *See* Dials and gauges
General observations, weak signals from, 534–537
Generation effect, 422
Geography of thought
eye flow on HMI page in West and East, 458f
handling and reporting problems, 463–464
individuality, 463
language construction, 460
logic and reason, 460–462
logic versus fate, 462
nailing down the issue, 462
normal visual flow directions, 457–459, 459f
norms and conventions, 457–460
simplicity as truth, 461–462
three postal codes, 464
visual perception, 459–460
world map delineating East, West and blended frameworks, 457f
Geometry, work space, 242
Georgia System Operations, video wall, 370, 371f
Gibran, Kahlil, 221
Gladwell, Malcolm, 598
Glass Cage, The (Carr), 419
Glass cockpit, 370
GlobalSantaFe Corporation, 467
Glyphs, 305–308
as navigation buttons, 307, 307f
social media, 308, 308f
tertiary page, 345f
tool tips combined with, 307f
traffic sign, 306f
Goals, short-term versus long-term, 89–92
Godell, Jack, 538
Good engineering practice, 65–69
alarm management, 66
maintenance, 67–69
operating experience, 67
operators on the job, 66
providing adequate information, 66
roles and responsibilities, 66
training, 67
Google, 373

Gould, Stephen Jay, 77
Graphics symbol library, 280–281
Gropius, Walter, 223
Ground rules, cautions and, 8–10
Guerlain, Stephanie, 273
Guideline(s), 44–45
  notifications, 509–511
  permission to operate, 691–692

H

Hallinan, Joseph T., 391, 641
Halo effect, bias, 446
Handover. *See* Shift handover
Hazard(s), 134
  definition, 134
  process hazard management, 146–148
Hazardous chemicals, OSHA 29 CFR 1910.119 for process safety management of, 45–46
Head-up displays, 363–365
  automobile example, 364f
  eyeglasses version of, 365f
Health and Safety Executive (HSE), United Kingdom, 44, 133, 686
Heat exchanger
  heat efficiencies of, 346–347
  mass data display, 346f
Helicobacter pylori, 428
Hemmingway, Ernest, 641
Herd mentality, 446
Hewlett, Bill, 80
Hewlett-Packard (HPQ), 80
Hierarchy
  display screen, 282–284, 283f
  geographically based organization, 290, 290f
  responsibility-based screen organization, 286f, 286–287
  risk-based screen organization, 287f, 287–288
  similarity-based organization, 289, 289f
  task-based organization, 288, 288f
High-reliability organizations (HROs), 81, 88–89
HMI. *See* Human-machine interface (HMI)
Holmes, Sherlock, 399
Honeywell, 54, 368, 369f
Hopkins, Andrew, 391
Hotton, Donald, 538
Human-machine interface (HMI), 5–6, 17, 47, 57, 64, 211, 259–260, 262–263, 274–281
  communication, 212
  components of, 277–278
  contemporary control room, 227f
  design philosophy, 278–279
  Emerson, 54
  evaluating effectiveness, 380–383
  fire, gas, safety instrumented systems and security systems, 377
  graphics library, 280–281
  high-performance, 53
  key concepts, 261
  mass data displays, 345–349
  multivariate process analysis, 349–353
  navigation, 298–305
  nomenclature for display screens and components, 263–265
  operation interface, 21–22, 27
  principles of display screen design, 267–272
  principles of workspace design, 272–274
  requirements for operator screens, 265–266
  Rockwell Automation, 54
  Schneider Electric, 55
  simple control design, 235, 236f
  sound, audio and video, 377–380
  style guide, 279–280
  trend plots, 329–334
  video walls, 365–370
  wartime story setting a stage, 275–277
  weak signals, 517–518
  See also Display screen

I

Icons, 308–310
  design fundamentals, 326–327
  design fundamentals for, 325–329
  progress, 310, 310f
  salience requirements, 328–329
  temperature, 309f, 309–310, 310f
Icons, dials, gauges and dashboards (IDGDVs), 564–565, 567
IDCON, root cause analysis, 148–149
Identification
  work process, 569–570
  situation management activity, 24, 25f
Illusion of skill, 444
Immature situation, 525, 526, 530, 531f
Immature weak signals, 532, 585
Impairment
  categories of, 169
  managing, 169
  understanding, 168–169
  See also Operator readiness
Imperial Chemical Industries (ICI), 127
Implicit, 38
Impulse control, 406
Impulsive behavior, 455
Inattention bias, 448–450
Inattention blindness, 448–450

Incident(s), 5, 137
Amagasaki rail crash, 425–427, 464
BP and Transocean *Deepwater Horizon*, 467–469
Challenger Space Shuttle, 465–467
costs of, 60
fatigue and, 165–167
literature, 133
Mann Gulch fire, 718, 726–727
near miss, 135–136
Piper Alpha, 142–143
"Swiss cheese" model of, 140f
weak signals and investigating, 633–634
See also Critical failures; Plane crashes
Independent protection layer (IPL), term, 150
Indirect measurements or observations
baseline operational measures, 557–558
difficulty of control measures, 554–555
equipment reliability indicators, 560–561
instrument condition monitoring, 558–560
key performance indicators, 561–562
mass and energy balances, 546–551
operational plausibility values, 551–554
statistical process control information, 555–557
weak signals from, 545–562
Indirect strong signals, 397
Individuality, 463
Inferential control, 110
Inflation report, Bank of England, 333, 334f
Inflections, weak signals, 592–593
Information
in-shift handover emulation, 506
intuition and "raw," 565–566
mobile operator, 212–213
partial, 450–451
receiving, 505
support tools and technology, 230
transferring for shift handover, 504f, 504–505
verifying and taking ownership, 505–506
Information fork, 434
Information silo, 84
Infrastructure, plant (enterprise) area model, 115–117
Inherent safety/complexity, definitions, 98
Insecurity, 406
Inspector(s), note to, 62
Instrument condition monitoring, 558–560
basic sensor validation, 558–559
smart field devices, 559–560
Instrument landing system (ILS), 423–424
Instrument panel, aircraft, 276f
InTech (magazine), 111–112
Integrity, operational, 63
International Association of Oil and Gas Producers (OGP), process safety, 86–87
International Electrochemical Commission (IEC), 43
International Society of Automation (ISA), 47
International Standards Organization (ISO), 43, 228
ISO 11064 (Ergonomic Design of Control Centres), 249, 252, 256
ISO 11064-5 (graphical displays), 263, 264f
ISO 9241 design principles, 271–272
Intervention actions, effectiveness of, 17–18
Introduction to Human Factors Engineering, An (Wickens), 267–269
Intuition, 261, 406, 565–566
iOps command center concept, 54
Irritability, 455

J

Jamieson, Greg, 273
Japan, Amagasaki rail crash, 425–427, 464
Joint operation, 199

K

Key performance indicators (KPIs), 561–562, 731–732
Key repeated elements, 482
alarm management, 611
decomposition, 120–121, 121f
looking for abnormal situations in, 123–125
Key repeated subsystems, 482
alarm management, 611
decomposition, 121–122, 122f
looking for abnormal situations in, 125–127
Kletz, Trevor, 3
Knowledge fork, 472, 473, 473f, 675–676
Kourti, Theodora, 349
Ko Wen-je, 29
Kroc, Ray, 81

L

Latané, Bibb, 163
Layers of protection, 150–151
Leadership
culture, 79–80
process safety beginning with, 87–88
situation awareness, 404–405
talking the talk, 81
walking the walk, 80–81
Leadership principles, 61

Lehrer, John, 440
Lemmon, Jack, 537
Liao Chien-tsung, 29
Life cycle, of weak signal, 608–609
Liu Tse-chung, 29
Logic
  reason and, 460–462
  versus fate, 462
Logic-tight compartments, 427–429
Logs, 196, 198, 511
Long-arm operations, 154, 213–214
Loss aversion, 438–440
Loss of scale, confirmation bias, 443–444, 444f
Loss of view, 383–385
Lowell, Elliott, 537

M

McDonald's (MCD), 81
MacGregor, John, 349
McMaster Advanced Control Consortium, 349
Maintenance, 21, 154
  good engineering practice, 67–69
  handback, 208
  shift handover for, 206, 208
Major situations
  managing, 719–725
  operator redeployment, 720–725
  See also Everyday situations
Malfunction, clear notice of, 558
Management
  alarm, 480–481
  control room, 20
  control room choices, 737–738
  fatigue, 168
  impairment, 169
  leadership principles, 61
  note to senior, 59–62
  operator workload, 171–172
  process hazard, 146–148
  role in permission to operate, 686
  role in situation management, 26
  role of, 47–48
  silo, 85
  See also Situation management; Weak signal management
Management of Change (MOC), 104, 375
Manager(s)
  bottom line, 5
  industrial setting, 38
  role of, 4
Managing operator, 724
Mann Gulch fire, 718, 726–727
Marshall, Barry, 428
Maslow's needs hierarchy diagram, 215f
Mass and energy balances, 546–551
  energy balance gauge, 550f, 551f
  mass balance gauge, 548f, 549f, 550f
  plant with area for calculation of balance, 547f
  showing imbalances to operator, 547–551
Mass data displays, 345–349
  departure from normal/expected value mode, 347
  departure from steady-state value mode, 347
  format in advanced control monitoring display, 348f
  heat exchanger example, 346f
Mastering, situation management, 739–740
MBTA Boston Transit System, 369, 370f
Measurement evaluation, operational integrity levels (OiL) as, 97–99
Mechanical engineering, 83f, 84–85
Mental model(s), 422, 622
  deception of two reasons, 430–431
  80:40 rule, 431–432, 432f
  expected roles, 423–425
  failure avoidance, 425–427
  good is not really good enough, 431–432
  logic-tight compartments, 427–429
  remembering, 431
  surrogate models, 429, 430
Mentoring, escalation teams, 709–710
Messages, role of, 472
Meteopole, Toulouse, France, 366, 367f
Metrics
  alarm configuration, 499–500
  alarm performance, 500–501
Meyer, Danny, 81
Milford Haven
  critical failure, 140–142, 147
  HSE report, 546
  operator's permission to operate, 686
Mindful organization, 81–82
Miracle on the Hudson, 732–735
Mirroring, communication, 657, 658
Mistakes
  looking without seeing, 418
  making, 416–418
Mobile operator(s)
  control room mobility, 210–211
  information and communication, 212–213
  large geographical mobility, 211–212
  plant area mobility, 211
  protocols and processes, 213
  requirements for mobility support, 212–213
  safeguards, 212
  tools, 212–213

Model(s)
accuracy, 622
fidelity, 622
inadequacies, 622–623
mental, 422–432
model-based reasoning, 109, 109f
plant (enterprise) area, 115–117
surrogate, 429
weak signal analysis, 566
See also Mental models
Model reference adaptive control (MRAC), 109–110, 110f
Moore-Ede, Martin, 164, 167
Morton Thiokol, 466, 467
Motivation
basics of, 215–217
belonging, 216
esteem, 216–217
physical needs hierarchy diagram, 215f
self-actualization, 217
Multitasking, 452–453
alarms and, 453–454
myth of, 415, 452–454
Multivariable process control (MPC), 110
Multivariate process analysis, 349–353
Myside bias, 442
Myth of multitasking, 415, 452–454

N

National Transportation Safety Board. *See* US National Transportation Safety Board (NTSB)
Navigation, 281, 298–305
definition, 298
navigating cycle, 299–302
product of, 303–305
purpose of, 298–299
tablet icons, 362f
tools, 302–303
Navigation tools
dead reckoning, 302
direct enter search, 302
focus, 303
table lookup, 302
targets, 303
yoking, 303
Near hits, 609
Near miss, 135–136, 609
News & Observer, The (newspaper), 29
New York Times (newspaper), 28
Nielsen, Jakob, 271
Nikkin Kyoiku, retraining program, 427
Noise, of weak signals, 605
Nomination, 564
gauge, 564f
process of, 313
Nominations gauge
design structure of, 314–315, 315f
explanation of symbols, 314f
flow changes, 315–318
natural gas and petroleum pipelines, 313–318
Noncontiguous shifts, 196
Nonpharmacological addiction, 169
Normal, 526
Normal operation region, 35–37
Notification(s)
action, 507
in combination, 508–509
event, 507
formal, 510
general design and implementation guidelines, 509–511
informal, 510–511
logs and, 511
properties of, 508–509
situation, 507–508
sorted, 509
as weak signals, 506–507
NTSB. *See* US National Transportation Safety Board (NTSB)
Nuisance alarms, example gauge, 311f, 311–313

O

Observation, possible meaning, 534, 535–536
Occam's razor, 74
Occupational Safety and Health Administration (OSHA), 45–46, 133, 715
Off-normal, 526, 530, 531f
Off-normal operation region, 35–37
Off-workstation (OWS)
ability to focus, 359–360
auditing, 360
benefits of, 362–363
display screen visibility, 359
formats, 361–362
illustrations of OWS large displays, 360–361
large displays, 356–358
OWS small displays, 361–363
physical analog mimic panel, 359f
physical design of large OWS displays, 358–359
problems of, 363
requirements for large OWS displays, 358–360
size, 353t

Operating displays
  weak signals from comparison, 544–545
  weak signals on, 543, 544f
Operating observations, weak signals from, 537
Operating situations, 686–687
  explosive events, 687
  operating in uncertainty, 686–687
  strong signals, 396–399
  unique events, 687
Operating values, deviation diagram, 565f
Operation(s)
  causes of poor, 71–73
  defensive principles, 665–666
  frontline supervisor's role, 49–50
  human operator in control room, 48–49
  management's role in, 47–48
  plants and, 156–157
  safety nets, 649–651
  tenets of, 217–218, 660–661, 689
  vendors, 53–55
Operational area
  boundaries and responsibilities, 157–158
  control room coordination with, 161–162
  crossing from one, to another, 159–160
  crossing to enterprise, 160
  crossing to universe, 160–161
Operational area division of responsibility, transformational analysis, 131
Operational drift, 658–661
Operational integrity, 63, 93–99
  equipment readiness, 96
  equipment suitability, 96
  levels (OiL), 95, 97t
  management competency, 95
  management effectiveness, 95–96
  measuring dial-type trend, 729f
  OiL as measurement evaluation, 97–99
  online risk management, 728–730
  plant complexity and inherent stability/safety, 96
  plant operability components, 95–96
  proper operation of enterprise, 94
  record, 96
  safety (SIL), 95
  staffing competency, 96
  staffing quality, 96
  staffing readiness, 96
Operational modes, 688–689
  definitions, 689
  plant state versus, 688f
Operational plausibility values, 545, 551–554
  model, 553, 554f
  plant showing identification of, 552f, 553f
Operational safety, 102
Operational success, key ingredients for, 70–71
Operational supervision, role in operations, 50
Operation center(s), 236–237
  concept of, 225
  environmental controls, 229–230
  information support tools and technology, 230
  permits, 232–233
  personnel, 233
  physical protection and security, 229
  process and operational controls, 230
  requirements, 229–233
  special operating situations, 232
  support, 231
  visitors, 233
Operation center controllers. *See* Operator(s)
Operation display, key operating parameters, 545f
Operation regions
  alarms, 40
  condenser and its, 124f
  illustration identifying, 394f
  for key repeated subsystem, 126f
  nested nature of, 39
  normal, off-normal and abnormal, 35–37
  overall setting, 39–42
  pump and its, 124f
  strong signals, 41
  weak signals, 41–42
Operations engineer, 739
Operator(s), 10–11
  active versus passive monitoring, 401
  alarm loading, 501–503, 502f
  alarms over weak signals, 618
  alarm system as line of defense, 40
  alertness, 172–173
  automation bias, 421–422
  basics of motivation, 215–217
  boundaries, 157–164
  creed, 155
  dealing with uncertainty, 434–435
  definition of, 155
  do list, 220–221
  don't list, 220
  duties, 669
  duty period plan and schedule, 52
  effectiveness pillars, 53
  flow of activities, 670, 671f
  following the rules, 669–670
  general flow of operator activities, 670–673
  goals, roles and culture, 214–222
  good engineering practice, 66
  human, in control room, 48–49
  improving performance, 173

Operator(s) (*Continued*)
interface, 21–22
intervention of, 4–6, 667–668
key concepts, 154
long arm of, 213–214
managing permission to operate, 694–696
mobile, 210–213
modality decisions, 693–694
not being innovators, 668–669
note to, 58
objectives of, 218–222
operational success, 7–8
operations and, 155–157
overview showing area of responsibility, 336f
ownership transfer at shift change, 503–506
permission to operate, 684–696
principles of effective, 33–34
qualification, 178–181
redeployment, 720–725
responsibilities of, 13–16, 51–52, 62, 162–164
role of, 4, 393f
self-evaluation, 696
situation awareness, 6
situation management by, 11–18, 153, 222
success of, 12
term, 3
training, 21, 173–178
See also Shift handover
Operator interface, 402. *See also* Human-machine interface (HMI)
Operator of the Future initiative, Honeywell, 54
Operator readiness
circadian rhythms, 165, 166f
improving operator performance, 173
managing fatigue, 168
managing impairment, 169
managing overload, 171–172
operator alertness, 172–173
understanding fatigue, 164–167
understanding impairment, 168–169
understanding overload, 170–171
Operator screens
requirements for, 265–266
See also Display screen(s)
Operator tools, 181–185
checklists, 182–183
procedures, 183–184
protocols, 183
reports, 185
simulators, 184–185
Organization(s), mindful, 81–82
Outcome based, 43
Outside operator, term, 161
Overload
management, 171–172
supervision, 171
understanding, 170–171
work complexity, 170–171
workload, 170
OWS. *See* Off-workstation (OWS)

P

Pacific Gas and Electric, diversion of funds, 403
Page, 261, 263, 264f
Parametric situation, 525, 526, 530, 531f
Parametric weak signals, 532–533, 585
Pareto Optimum, 431
Pathologic mental impairment, 169
Pay It Forward (Hyde), 220
Pay it forward illustration, 221
Peopleware, 65, 156
Perfect process understanding, 78
Performance, auditing, 514
Perishable skills, concept, 78
Permission to operate, 440, 684–696, 740
alternate methods for having, 691–694
BP Texas City operators, 685
de facto decisions, 691–692
diagram of formal flowchart, 697f
functionality, 684
guideline, 691–692
how it came to be, 689–690
how it works, 690–691
management's role, 686
managing operator's, 694–696
observer evaluation, 695–696
operating modality decisions, 693–694
operating situations, 686–687
operational modes, 688–689
operator self-evaluation, 696
operator's role, 684–686
qualifying abnormal, 694–695
safe operating limits, 694
withdrawn, 692
Permits, control room, 232–233
Personalities
accident-prone behavior, 455
quiet ones, 455
situation management points, 456
Personalization, 376
Personal safety, 101
Personal tools, 177–178
Personnel protective equipment (PPE), 101
PG&E San Bruno Pipeline, institutional failure, 87
Philosophy, HMI design, 278–279
Physical limitations, illness or, 169

Physical mimicry, screen, 278
Pilot training, 275–277, 276f
Pipeline, explosion at PG&E San Bruno, 87
Pipeline and Hazardous Materials Safety Administration (PHMSA), 47, 179, 180
Pipeline nominations tracking, example gauge, 313–318
Pipeline system, dashboard example, 319–320
Piper Alpha, 100
  critical failure, 142f, 142–143
  doubt, 432
  lesson learned, 160
  maintenance for, 206
Plane crashes
  Air Florida Flight 90, 676–678
  Air France Flight 447, 447, 421, 551–552, 647–649
  Asiana Flight 214, 423–425
  Miracle on the Hudson, 732–735
  TransAsia Flight 235, 28–30
  United Airlines Flight 173, 679
  US Airways Flight 1549, 732–734
Plant area model, 115–117
Plant operability components
  equipment readiness, 96
  equipment suitability, 96
  management competency, 95
  management effectiveness, 95–96
  plant complexity and inherent stability/safety, 96
  record, 96
  staffing competency, 96
  staffing quality, 96
  staffing readiness, 96
Polarity, 464–465
Pop-up, 345
Pop-up trends, 330
Portable document format (PDF), 374
Positive materials identification (PMI), 21, 104
Possible doubt, 433
Post hoc ergo propter hoc, bias, 447–448
Preoperation safety review (PREOP), 518
Prescriptive, 43
Pressure symbol, 280f
Pre-startup safety review (PSSR), 519
Pride and exceptionalism, 405
Principal component analysis (PCA), 350
Probable doubt, 433
Procedural automation, 110–112
Procedure(s), 183–184
Procedure gaps, weak signals, 633
Process control system (PCS), 105–107, 115
Process engineer, 738
Process hazard management, 146–148
Process safety
  beginning in boardroom, 87–88
  International Association of Oil and Gas Producers (OGP), 86–87
Process safety management, OSHA 29 CFR 1910.119, 45–46
Process trouble point, alarm system, 489–490, 491f
Production management, See-Understand-Decide-Act (SUDA), 30–32
Progressive abnormal situations, 617
Projection on least squares (PLS), 350
Protection layers of, 150–151
Protocols, 183
  conflicts with, 9
  mobile operator, 213
Proximate cause, 149–150
Psychological impairment, 169

Q

Qualified operator(s), 178–181
  glossary of, 179–181
  message of, 181
  resources, 179–180
  roles and responsibilities, 188
  See also Operator(s)
Quality of operation, concept, 78
Quick reference handbook (QRH), 733, 734

R

RAGAGEP. *See* Recognized and generally accepted good engineering practice (RAGAGEP)
Ratio control, 108
Rationalization
  alarm, 482–485
  step-by-step, 497–499
Raw information, 565–566
Readiness evaluation, situation management, 710–711
Reading suggestions, 56–57, 76, 151, 222, 386–387, 411, 470, 515, 637–638, 741
Reason, logic and, 460–462
Reasonable doubt, 433–435
Recognized and generally accepted good engineering practice (RAGAGEP), 45, 47, 103
Recommended practice, 44
Red teams, collaboration, 684
Reductio ad absurdum, 623
Regulator(s), note to, 62
Relative prime responsibility, 403
Remediation, situation management activity, 24, 25f, 25–26
Remembering, 431

Reports, 185, 197–198
Resistance, 455
Resolution, work process, 581–582
Resources, escalation, 702–703
Responsibility
  delegation of, 92–93
  maintaining, 162–164
  term, 158
  transfer of operational, 199
Responsible engineering authority (REA), 103–105
Responsive to proper operation, 728
Restricted control room, 661–663
  conditions, 663
  initiators of, 663
  termination of, 663
  See also Control room(s)
Retention, work space, 244
Retrospective weak signal analysis, Texas City disaster, 612–615, 616t
Riser/Regenerator, secondary display page, 339, 340f, 341f, 342
Risk assessment, using transformational analysis for, 129–130
Ritchie, Hugh, 29
Roberto, Michael, 655
Rockefeller Standard Oil, 93
Rockwell Automation, 54
Root cause/root cause analysis
  definition of, 148
  explanatory case for, 148–149
  weak signals, 610–611
Ruled-in problem, 399
Ruled-out problem, 399
Ruskin, John, 223
Russian nuclear power plant, 248–249

S

Safeguards, mobile operator, 212
Safe operating limits (SOLs), 104, 694
Safe operating modes
  alternatives to shutdowns, 716–718
  automated shutdown, 716
  Mann Gulch fire, 718, 726–727
  operator-initiated shutdown, 715–716
  safe park, 718–719
  USS Carl Vinson (aircraft carrier), 717
Safe park, 718–719
Safety, 9
  characteristics of, 100–101
  components of, 101–102
  conduct of personnel, 101
  definition, 99
  delivering, 103
  equipment and operational design, 102
  high-reliability organizations, 88
  importance of, 78
  inherent complexity and, 98
  International Association of Oil and Gas Producers (OGP) on process, 86–87
  management and, 38, 59–61
  performance of activities, 102
  personal, 101
  process safety time, 31f
  responsibility and, 23
  safe communication, 653–655
  word about, 653
Safety in numbers, 446
Safety instrumented systems (SISs), 377
Safety integrity level (SIL), 95
Safety nets, operations, 649–651
Safety notice, 8–9
Salas, Hector, 538
Salience, requirements, 328–329
Salk, Jonas, 471, 527
Salk vaccine, 527
Samuels, Neil, 60, 567
San Francisco International Airport, 423
Saving face, 463
Schneider Electric (Foxboro, Invensys), 55
Schoemaker, Paul, 519
Schwab, Chuck, 80
Security systems, 377
See-Understand-Decide-Act (SUDA), 30–32, 35, 492, 492f
Segmentation, display screen, 284–285
Selective attention, 448–450
Selective automation
  advanced basic control, 108
  advanced control, 108–110
  basic process control system (BPCS), 107
  concept of operator as coordinator, 111f
  models, 108–109
  MRAC (model reference adaptive control), 109–110
  procedural automation, 110–112
Self-actualization, 215f, 217
Senior management, note to, 59–62
Sensor validation, 558–559
Shadow of a doubt, 434
Shift assessments, 472
Shift change, operator ownership transfer at, 503–506
Shift handover, 154, 185–186, 198–201, 402, 741
  arriving operator, 185, 194, 503
  beginning the operator's shift role, 189–190
  ending of operator's shift role, 190–191
  engaged interaction, 199–200

face-to-face, 200–201
field operators' handover, 202f, 202–203, 203f, 207f
functional components of, 191–196
information and decision flow for, 504f, 504–505
information content of, 208–210
in-shift handover emulation, 506
leaving operator, 185, 194, 503
logs, 196, 198
for maintenance, 206, 208
noncontiguous shifts, 196
overlapped operation, 195–196
physical presence, 193–194
preparing full status report, 192–193
reasons for shift changes, 186–189
receiving information, 505
reports, 197–198
for supervisors, 204f, 204–206, 205f, 207f
taking operational control and ownership, 194
timelines, 188f, 202f, 203f, 204f, 205f, 207f
timing activities, 186f
tool tracking handover process, 201f
verifying information and taking ownership, 505–506
Shift progress reports, 402
Shirley, Richard S., 259
Short-term versus long-term
concept, 78
story of two enterprises, 89–92
Shutdown(s)
alternatives to, 716–718
automated, 716
operator-initiated, 715–716
Silo(s), 82
agricultural, 82f
communications between, 85–86
conceptual term, 82–84
functional silo, 84–85
information silo, 84
management of, 85
mentality, 82
pictorial design of mechanical engineering silo, 83f
Simplicity, 73
Simulations, 113
Simulators, 184–185
Situation assessment, 391, 649
question, 392, 406–407
region, 531
Situation awareness, 6, 64, 249, 391, 471, 472, 472–476, 531
accepting reality, 404
active versus passive monitoring, 401
alarms and weak signals for, 617
alarm system, 474, 477–503
assessment situation, 473–476
auditing, 514
cooperation, 404, 405
definition, 399–400
design and implementation, 513
interactive flow to situation management, 400f
intuition and raw information, 406
job capability, 513
key performance indicators, 561–562
knowledge fork, 473
leadership, 404–405
operational situations, 396
ownership, 403
problematic situations, 395–396
process of, 400
psychology of, 402–406
question, 392
relative prime responsibility, 403
requirements, 512
selling management, 513
tools, 401–402
triple package, 405–406
usability, 513
weak signals, 519
See also Alarm system
Situation-based display screens, 304–305, 340, 342f, 342–343
Situation codes of control room, 725–728
code blue, 725–726
code gray, 727–728
code orange, 728
Situation management, 4, 6, 11–18, 64–65, 260, 644, 741
abnormal, process model, 711–712
achieving, 735–739
activity, 644–645, 645f
alarm system, 22
basic four-activity process, 24–26, 25f
benefiting from experience, 651–652
changing the game, 35–39
collaboration, 675–684
command and control, 713–715
components of control room management, 20–22
contribution of alarms to, 503
cornerstones of, 4
decomposition underlying, 120–127
delegation, 674–675
diagram, 529f, 531f
doubts and concerns, 673–674

Situation management (*Continued*)
escalation, 696–706
escalation teams, 706–713
essential components of, 22–23
fitting process, 16–18
framework for, 19f
fundamental tools for, 24–30
general flow of operator activities, 670–673
importance, 23
interactive flow from solution awareness to, 400f
key concepts, 642–643
key performance indicators, 672, 673, 731–732
last opportunity, 5
layers of protection and, 150–151
lessons from Air France flight 447, 647–649
limitations of, 75
loss-of-view lesson, 383–385
managing biases, 730–731
managing everyday situations, 666–673
managing major situations, 719–725
operability integrity level for online risk management, 728–730
operational drift, 658–661
operational setting, 394–395
operations safety nets, 649–651
operator roles and responsibilities, 393f
overcoming pitfalls, 730–731
permission to operate, 22–23
premise, 78
preparation, 51
reality in function, 50–52
recommended structure of, 672f
region, 531
responsibilities of, 12–13
safe conversations, 652–658
safety and protective systems, 731
"situation," 393–395
step-by-step working process, 645–646
straightforward, 13–16
structure of, 18–24
success pathway, 650f
suits and coveralls, 70
training, practicing, evaluating and mastering, 739–740
TransAsia crash, 28–30
using experts, 651–652
weak signal analysis, 22
weak signals for, 520, 529–531
weak signals for abnormal, 712–713
See also Communication; Decomposition
Situation notification, 507–508
Sixth sense, 392, 416, 440–441, 511
Skiles, Jeffrey B., 732
Skills training, 176
Sleep deprivation, 167
Sleep disorders, 167
Smart field devices, 559–560
Smartphone screens, 361, 362f
Smith, Karen, 256–257
Smith System, defensive driving, 32
SMS (short message service), informal notifications, 510–511
Social media
dashboard example, 319, 319f
glyphs, 308, 308f
Sohio, 93
Solenoid valve icon, 281f
Sound, HMI, 377–378
Space
concept of, 241–242
See also Work spaces
Sparkline graphs, 562–563, 563f
Sparkline trend, 330, 333–334
Spatial introduction, work space, 242
Standard, 43
Standard Oil Company, 93
Statistical process control (SPC)
gauge, 555, 556f, 557f
information, 555–557
Statutory requirements, conflicts with, 9
Sterile control room
conditions, 664
initiators of, 665
termination of, 665
See also Control room(s)
Stimulant drug use, 167
StockCharts.com, 331, 331f
Stomach ulcers, 428
Strategic part, weak signal extrapolation, 610
Strategic weak signals, 620, 621
Stress, impairment, 169
Strong signals, 396–399, 402
direct, 398–399
indirect, 397
operating region showing, 41f
something is wrong but not sure what, 41
weak signals among, 605–606
Structural operational issues, transformational analysis for identifying, 131–132
Structured message, 509
Stumbling stone, 221
Style guide, screen design, 279–280
Substitution myth, automation, 419–420
SUDA (See-Understand-Decide-Act), 30–32, 35, 492, 492f
Suggestions for reading, 56–57
Suits, 70

Sullenberger, Chesley B. "Sully," 732–734
Supervision
  permission to operate, 171
  role in operations, 49–50
Supervisor(s)
  handover timelines, 204f, 205f, 207f
  note to, 59
  shift handover for, 204–206
Surrogate models, 407–409
  model test, 430
  from our immediate surroundings, 408
  from personal history or folklore, 409
  sources for surrogates, 408–409
Sustainability, 56, 92
Sustainable enterprise, 63
Sway (Brafman), 439
Symbols
  graphics library, 280–281
  icons, 308–310
  nominations gauge explanation, 314f
  pressure, 280f
  solenoid valve, 281f

T

Table lookup, navigation, 302
Tabletop simulations, 113
Tactical part, weak signal extrapolation, 609–610
Tactical weak signals, 620–621
Tactile, operator interaction, 277
Tags, plant area model, 116–117
Targets, navigation, 303
Task return point, 431
Teamwork, four-step process, 642
Technician(s), 10–11
Technologist(s), 59
Temperature, control loop example, 105–106
Templates, weak signals, 611–612
Tenets of operation, concept, 217–218
Tenth (10th) man doctrine, crew resource management, 680–681
Texaco Milford Haven
  alarms on previous unit, 540
  incident, 140–142, 141f, 539–540
  knock-out (KO) pot, 539
  stuck valve, 539
  weak signal example, 538–540
Texas City disaster
  retrospective weak signal analysis of, 616t
  weak signal case study, 612–613, 614f, 615
Theater Air Control System (TACS), 236
Things that go bump in the night, 606–607
Thinkware, 65
Three Mile Island, 167, 167f, 537–538
Time, 4
  power of, 30–32
  process safety, 30–32
Time-to-manage clock, 31
Tipping point
  after the, 598
  before the, 597
Tools, mobile operator, 212–213
Tracking, communication, 657, 658
Training, 154
  aircraft instrumentation, 275–277, 276f
  competency, 176–177
  escalation team, 711
  gaps and weak signals, 632
  good engineering practice, 67
  on-the-job (OJT), 177–178
  operator, 173–178
  personal tools, 177–178
  process understanding, 178
  situation management, 739
  skills and, 174–175
TransAsia crash, 28f, 28–30
Transfer of responsibility, escalation versus, 701–702
Transformational analysis, 127
  for decomposition, 130–131
  diagram, 128f, 130f
  identification of structural operational issues, 131–132
  for operational area division of responsibility, 131
  process, 127–129
  for risk assessment, 129–130
Transformative situation, 525, 526, 530, 531f
Transformative weak signals, 533, 585
Traveler's immunity, 416–417
Trend/trend plot, 329–334
  build-on-demand trends, 330
  complex trends, 331, 331f
  components, 332, 332f
  continuous trends, 330
  fan charts, 332–333, 334f
  pop-up trends, 330
  single, 329f
  sparkline charts, 333–334, 334f
  superimposed time-related trends, 333f
  weak signals from, 562–563, 563f
Trial and error, 43, 49
Trial by fire, 275
Triangulation, 681–683
  experience, 683
  job or task, 683
  questions, 682–683
Triple package, situation awareness, 405–406
Troubleshooting guide, weak signals, 628–631

Truth, 261
Tufte, Edward, 333
Twain, Mark, 471, 641
Two-cycle weak signal analysis, 600–601, 604
Two-reasons trap, 430–431

U
Union Square Café, 81
United Airlines Flight 173, 679
United Kingdom, Health and Safety Executive (HSE), 44, 133, 686
United Nations, 464
Unmanageable problem, 530
US Airways Flight 1549, 732–734
US Americans with Disability Act, 252
US Department of Transportation (DOT), 47, 187
US Department of Transportation Pipeline and Hazardous Materials Safety Administration (PHMSA), 714
User-centered design, 244–249
  affordance, 245
  compensation, 247
  environment, 245–246
  human factors, 245, 246f
  implementability, 248
  mixed technology, 248–249
  scaling, 246–247
  understandability, 247–248
  unified feel, 248
US Federal Aviation Administration (FAA), 134, 425, 463
US National Aeronautics and Space Administration (NASA), 236, 466–467
US National Transportation Safety Board (NTSB), 133, 678–679, 733, 734
US Occupational Safety and Health Administration, 45–46, 133, 715
USS Seawolf submarine, 240f

V
Vaccine, polio, 527
Vendors
  ABB, 53
  Emerson, 54
  Honeywell, 54
  Rockwell Automation, 54
  Schneider Electric, 55
  Yokogawa, 55
Video, HMI, 380
Video and animation, 261
Video walls, 365–370
  as augmentation to workstation HMI, 368–370
  as background, 365, 366f
  for control rooms, 366, 368–370
  conventional, 365–366
  futuristic display, 368, 368f
  main HMI, 366, 368
  as view into process, 367f
Viewability, screen display, 290–291
VigilantPlant initiative, Yokogawa, 55
Visibility, screen display, 290–291
Visitors, control room, 233
Visual, operator interaction, 277
Visual perception, 459–460

W
Walk the walk
  talking the talk, 81
  walking the walk, 80–81
Wal-Mart (WMT), 80
Walton, Sam, 80
Wang, Thomas, 29
Warren, Robin, 428
Weak signal(s), 402, 517–521, 524–541
  abnormal situation management, 712–713
  actively looking for, 591–593, 606–607
  from alarm activation, 618–619
  among strong signals, 605–606
  announce, 526–528
  artificial intelligence for analysis, 631–632
  building and displaying, 541–566
  categories of, 532–533, 597
  categories of trouble indicators, 588, 589f, 590f
  characteristics of, 541–542
  checklists and, 602
  China syndrome as example, 537–538
  classifying, 585
  clues something might be wrong, find out, 41–42
  collaboration and consensus, 595–596
  concepts, 533–534
  contradictions, 592
  critical variables and, 619
  design for, 587
  from direct measurements and observations, 542–545
  expectations interfering with, 540–541
  extrapolations, 609–611
  extremes, 593
  finding, 528, 625–626, 628–629
  as flags, 598–600
  gaps in training and procedures, 632–633
  from general observations, 534–537
  hunches and intuition, 540–541
  incident investigations and, 633–634
  inflections, 592–593
  intuition and "raw" information, 565–566

key concepts, 521–522
life cycle, 608–609
mastering, 740
model quality for analysis, 622–623
models for analysis, 566, 604
notifications as, 506–507
observation by experts, 595
off-normal operations, 526
from operating observations, 537
operating region showing, 42f
persistence of, 603, 607–609
prove true or prove false, 594–595
relationship between alarms and, 615, 617–619
retrospective case study, 612–615
role of icons, dials, gauges and dashboards (IDGDBs), 564–565
seeming to lead nowhere, 603–605
for situation management, 529–531
skipping over processing, 634–636
special case mapped to specific problem, 593–594
templates, 611–612
Texaco Milford Haven as example, 538–540
from trend plots, 562–563
troubleshooting guide, 628–631
two-cycle analysis, 600–601
without escalation, 596–598
working, 623–628
Weak signal extrapolations
alarm rationalization, 611
near hits, 609
near miss, 609
root cause analysis, 610–611
strategic part, 610
tactical part, 609–610
what-if and HAZOP, 610
Weak signal management, 566–587
accentuating negative and eliminating positive, 602
backward-projection, 573–575, 574f
before and after, 586–587
collaboration and consensus, 595–596
evidence for confirmation, 575–581
extrapolation and projection, 586
flowchart, 569f
forward-extrapolation, 570–573, 571f, 572f
identification, 569–570
indicators of problems, 626
model quality and, 622–623
no shortcuts for, 625–626
overload, 626–628
proper foundation, 624
recapping steps, 582–585
resolution, 581–582
selling, 628
work process, 567–569, 569f, 623
Webb, Amy, 592
Wells, Kimberly, 538
What-if, weak signal extrapolation, 610
What then question, bias, 448
Wickens, Christopher, 267–269
Wilkins, Maurice, 111–112, 112n26
Window, normal visual flow directions, 457–458, 458f
Windows, 261, 263, 264f, 345f
Wittgenstein, Ludwig, 3
Workload, 261
Work process, 567–569
backward-projection, 573–575, 579–580
evidence for confirmation, 575–579
forward-extrapolation, 570–573
identification, 569–570
recapping the steps, 582–585
resolution, 581–582
steps of, 567–568
tying up loose ends, 589–591
Work spaces
collaboration, 243–244
concept of space, 241–242
design of effective, 241–244
expanse, 243
geometry, 242
principles of design, 272–274
retention, 244
spatial introduction, 242
See also User-centered design
Workstation displays, 354–356
closely spaced, 356f
configuration options, 355f
entire plant floor status, 358f
head-up displays, 363–365
with large off-workstation (OWS), 357f
size, 353t
See also Off-workstation (OWS)
World War Z (movie), 681
Wright State University, 54

Y

Yoking, 376
construction details, 343f
navigation, 303
situationally based secondary page, 342f
Yokogawa, 55
Yom Kippur War (1973), 681