CONTENTS

 Preface xxv
 List of Contributors xxvii

 1 INTRODUCTION 1
 Niklas Möller, Sven Ove Hansson, Jan-Erik Holmberg, and Carl Rollenhagen
 1.1 Competition, Overlap, and Conflicts 1
 1.2 A New Level in the Study of Safety Principles 2
 1.3 Metapriniciples of Safety 3
 1.4 Other Ways to Characterize Safety Principles 5
 1.5 Conflicts Between Safety Principles 7
 1.6 When Can Safety Principles Be Broken? 8
 1.7 Safety in Context 9
 References 10

 2 PREVIEW 11
 Niklas Möller, Sven Ove Hansson, Jan-Erik Holmberg, and Carl Rollenhagen
 2.1 Part I: Safety Reserves 12
 2.2 Part II: Information and Control 13
 2.3 Part III: Demonstrability 16
 2.4 Part IV: Optimization 17
 2.5 Part V: Organizational Principles and Practices 20
# Part I  Safety Reserves

## 3 RESILIENCE ENGINEERING AND THE FUTURE OF SAFETY MANAGEMENT

*Erik Hollnagel*

- **3.1 On the Origins of Resilience** 25
- **3.2 The Resilience Engineering Understanding of “Resilience”** 27
- **3.3 The Four Potentials for Resilience Performance** 29
- **3.4 Safety Management Systems** 31
- **3.5 Developing Definitions of Resilience** 33
- **3.6 Managing the Potentials for Resilient Performance** 34
  - 3.6.1 Organizations of the First Kind 35
  - 3.6.2 Organizations of the Second Kind 36
  - 3.6.3 Organizations of the Third Kind 36
  - 3.6.4 Organizations of the Fourth Kind 37
- **3.7 Resilience Management: LP-HI OR HP-LI?** 37
  
## References 39

## 4 DEFENSE-IN-DEPTH

*Jan-Erik Holmberg*

- **4.1 Introduction** 42
- **4.2 Underlying Theory and Theoretical Assumptions** 43
  - 4.2.1 Definitions and Terminology 43
- **4.3 Redundancy, Diversity, and Separation Principles** 44
  - 4.3.1 Principle of Successive Barriers and Reducing Consequences 46
  - 4.3.2 Principle of Accident Prevention and Mitigation 47
  - 4.3.3 Classification of Barriers 49
  - 4.3.4 Safety Classification 50
  - 4.3.5 Overall Safety Goals and Risk Acceptance Criteria vs. Defense-in-Depth 51
- **4.4 Use and Implementation** 53
  - 4.4.1 Nuclear Power Plant Safety 53
  - 4.4.2 Chemical Industry 54
  - 4.4.3 Information Technology Security 55
  - 4.4.4 Railway Safety 56
  - 4.4.5 Automobile Safety 57
CONTENTS

4.5 Empirical Research on use and Efficiency 57
4.6 Weaknesses, Limitations, and Criticism 57
4.7 Relations to Other Safety Principles 59
References 60
Further Reading 61

5 SAFETY BARRIERS 63
Lars Harms-Ringdahl and Carl Rollenhagen
5.1 Introduction 63
5.1.1 Classical and Radical Definitions of Barriers 64
5.1.2 Examples 64
5.2 Origin and Theoretical Background 65
5.2.1 Energy and Sequence Models 65
5.2.2 Extended Models 66
5.3 Definitions and Terminology 67
5.3.1 Examples of Barrier Definitions 67
5.3.2 Barriers and Barrier Systems 68
5.3.3 Alternatives to the Barrier Concept 69
5.3.4 Safety Functions 70
5.3.5 Conclusion 71
5.4 Classification of Barriers 71
5.4.1 General Considerations 71
5.4.2 System Level Classification 72
5.4.3 Classification Related to Accident Sequence 72
5.4.4 Physical and Non-physical Barriers 72
5.4.5 Administrative and Human Barriers 73
5.4.6 Passive and Active Barriers 73
5.4.7 Combined Models 74
5.4.8 Purpose of Barriers 75
5.5 Methods for Analysis of Safety Barriers 75
5.5.1 Energy Analysis 76
5.5.2 Event Tree Analysis 76
5.5.3 Fault Tree Analysis 77
5.5.4 Safety Barrier Diagrams 77
5.5.5 Management Oversight and Risk Tree 78
CONTENTS

Part II Information and Control 115

7 EXPERIENCE FEEDBACK 117

Urban Kjellén

7.1 Introduction 117
  7.1.1 Example 117
7.2 Origin and History 118
7.3 Definitions 121
7.4 Underlying Theories and Assumptions 122
  7.4.1 Feedback Cycle for the Control of Anything 122
  7.4.2 Safety Information Systems 124
  7.4.3 The Diagnostic Process 125
  7.4.4 Knowledge Management 126
7.5 Use and Implementation 127
  7.5.1 Safety Practice in an Operational Setting 127
  7.5.2 Risk Assessment 131
  7.5.3 Transfer of Experience to New Construction Projects 132
  7.5.4 Transfer of Experience from the Users to Design 133
7.6 Empirical Research on Use and Efficiency 135
7.7 Relations to Other Safety Principles 137
  7.7.1 Safety Management 137
  7.7.2 Resilience Engineering 138
  7.7.3 Safety Indicators 138
  7.7.4 Safety Culture 138
References 138
  Further Reading 141

8 RISK AND SAFETY INDICATORS 142

Drew Rae

8.1 Introduction 142
8.2 Origin and History 143
8.3 Definitions and Terminology 145
8.4 Underlying Theory and Theoretical Assumptions 146
  8.4.1 Past, Present, and Future Safety 146
  8.4.2 Outcome Indicators 147
  8.4.3 Risk Models and Precursor Events 148
8.4.4 Status of Physical and Procedural Controls
8.4.5 Safe Behaviors
8.4.6 Amount and Quality of Safety Activity
8.4.7 Organizational Drivers and Attributes
8.4.8 Variability
8.5 Use and Implementation
  8.5.1 Metrics Collection
  8.5.2 Incentives and Accountability
  8.5.3 Benchmarking and Comparison
  8.5.4 Safety Management System Performance Monitoring
8.6 Empirical Research on Use and Efficacy
  8.6.1 Usage of Indicators
  8.6.2 Efficacy of Indicators
8.7 Weaknesses, Limitations, and Criticism
  8.7.1 Underreporting and Distortion
  8.7.2 The Regulator Paradox and Estimation of Rare Events
  8.7.3 Confusion Between Process Safety and Personal Safety Indicators
  8.7.4 Unintended Consequences of Indirect Measurement
8.8 Relations to Other Safety Principles
  8.8.1 Ensurance Principles
  8.8.2 Assessment and Assurance Principles
References

9 PRINCIPLES OF HUMAN FACTORS ENGINEERING
Leena Norros and Paula Savioja
9.1 Introduction
9.2 Principle 1: HFE is Design Thinking
  9.2.1 Description
  9.2.2 Theoretical Foundation
  9.2.3 Use and Implementation
  9.2.4 Empirical Research on Use and Efficiency
9.3 Principle 2: HFE Studies Human as a Manifold Entity
  9.3.1 Description
  9.3.2 Theoretical Foundations
  9.3.3 Use and Implementation
  9.3.4 Empirical Research on Use and Efficiency
CONTENTS

9.4 Principle 3: HFE Focuses on Technology in Use 177
   9.4.1 Description 177
   9.4.2 Theoretical Foundations 177
   9.4.3 Use and Implementation 180
   9.4.4 Empirical Research on Use and Efficiency 181

9.5 Principle 4: Safety is Achieved Through Continuous HFE 182
   9.5.1 Description 182
   9.5.2 Theoretical Foundation 182
   9.5.3 Use and Implementation 183
   9.5.4 Empirical Research on Use and Efficiency 185

9.6 Relation to Other Safety Principles 187

9.7 Limitations 188

9.8 Conclusions 189

References 190

Further Reading 195

10 SAFETY AUTOMATION 196

Björn Wahlström

10.1 Introduction 196
   10.1.1 Purpose of Safety Automation 197
   10.1.2 Functions of I&C Systems 199
   10.1.3 Allocation of Functions between Humans and Automation 200

10.2 Origin and History 201
   10.2.1 Roots of Safety Automation 201
   10.2.2 Systems Design 202
   10.2.3 Typical Design Projects 203
   10.2.4 Analog and Digital I&C 204

10.3 Definitions and Terminology 205
   10.3.1 System Life Cycles 205
   10.3.2 Process and Product 206
   10.3.3 Phases of Design 206
   10.3.4 Operations 210

10.4 Underlying Theories and Assumptions 211
   10.4.1 Systems of Systems 212
   10.4.2 Building Reliability with Unreliable Parts 213
CONTENTS

10.4.3 Reusability of Designs 213
10.4.4 Vendor Capability 213
10.4.5 Project Management 214
10.4.6 Regulatory Oversight 215

10.5 Use and Implementation 215
10.5.1 From Systems Design to I&C Design 215
10.5.2 Physical Realizations of I&C 216
10.5.3 Initial Considerations 216
10.5.4 I&C Design 217
10.5.5 Practices in Different Domains 220

10.6 Research on Use and Efficiency 220
10.6.1 Estimates of Project Cost and Duration 220
10.6.2 Support Systems for Design and Construction 221
10.6.3 Benefits of Using Safety Principles 221

10.7 Weaknesses, Limitations, and Criticism 222
10.7.1 What is Safe Enough? 222
10.7.2 Quality of Design 224
10.7.3 Field Programmable Gate Arrays 224
10.7.4 Cyber Security 224
10.7.5 Regulatory Acceptance 225

10.8 Relations to Other Safety Principles 225
10.8.1 Safety Reserves 226
10.8.2 Information and Control 226
10.8.3 Demonstrability 227
10.8.4 Optimization 227
10.8.5 Organizational Principles and Practices 228

10.9 Summary and Conclusions 228
References 229

11 RISK COMMUNICATION 235

Jan M. Gutteling

11.1 Introduction 235
11.1.1 Example 1 236
11.1.2 Risk Perception, Awareness, and Communication 236
11.1.3 This Chapter 238
CONTENTS

11.2 The Origin and History of Risk Communication as Academic Field 238
  11.2.1 Example 2 239
  11.2.2 Changing Notions about Communication 239
  11.2.3 Example 3 241
  11.2.4 Conclusion 241
11.3 Underlying Assumptions, Concepts and Empirical Data on Risk Communication Models 241
  11.3.1 Information versus Communication 241
  11.3.2 Risk Communication Aims 243
  11.3.3 Diagnostic Risk Communication Studies 244
  11.3.4 Social Amplification of Risk 245
  11.3.5 Trust in Risk Communication 246
  11.3.6 Socio-Cognitive Models 247
  11.3.7 Risk Information Seeking Models 247
  11.3.8 Risk Communication and Social Media 249
  11.3.9 Conclusion 250
11.4 Weaknesses, Limitations, and Criticism 250
11.5 Final Word 252
References 252
Further Reading 257

12 THE PRECAUTIONARY PRINCIPLE 258
Sven Ove Hansson
12.1 Introduction 258
12.2 History and Current Use 259
12.3 Definitions 263
12.4 Underlying Theory 267
12.5 Research on Use and Efficiency 271
12.6 Weaknesses, Limitations, and Criticism 271
  12.6.1 Is the Principle Asymmetric? 271
  12.6.2 Strawman Criticism 273
12.7 Relation to Expected Utility and Probabilistic Risk Assessment 273
12.8 Relations to Other Safety Principles 276
  12.8.1 Maximin 276
  12.8.2 A Reversed Burden of Proof 278
  12.8.3 Sound Science 278
CONTENTS

14.7 Demands on the Environment 322
    14.7.1 Organization 322
    14.7.2 Communication 324
14.8 Handling Complexity 327
    References 329

Part III Demonstrability 331

15 QUALITY PRINCIPLES AND THEIR APPLICATIONS TO SAFETY 333
    Bo Bergman
    15.1 Introduction 333
    15.2 Improvement Knowledge and its Application to Safety 338
        15.2.1 Understanding Variation 338
        15.2.2 Knowledge Theory 345
        15.2.3 Psychology 348
        15.2.4 System Thinking 348
    15.3 Health-Care Improvement and Patient Safety 349
    15.4 Weaknesses, Limitations, and Criticism 351
    15.5 Some Personal Experiences 352
    15.6 Relations to Other Safety Principles 353
        References 355
        Further Reading 360

16 SAFETY CASES 361
    Tim Kelly
    16.1 Introduction 361
    16.2 Origins and History 361
        16.2.1 Windscale 362
        16.2.2 Flixborough 362
        16.2.3 Piper Alpha 363
        16.2.4 Clapham 363
        16.2.5 The Introduction of Safety Cases—A Shift in Emphasis 364
    16.3 Definitions and Terminology 364
        16.3.1 Safety Cases vs. Safety Case Reports 366
        16.3.2 Other Terminology 367
CONTENTS

16.4 Underlying Theory
   16.4.1 Safety Case Argumentation 367
   16.4.2 Types of Safety Case Argument 369
   16.4.3 Safety Case Lifecycle 372
   16.4.4 Incremental Safety Case Development 373
   16.4.5 Safety Case Maintenance 374
   16.4.6 Safety Case Evaluation 375
   16.4.7 Safety Case Confidence 376
16.5 Empirical Research on Use and Efficiency 377
16.6 Weaknesses, Limitations, and Criticisms
   16.6.1 Other Criticisms 381
16.7 Relationship to Other Principles

References 383
Further Reading 385

17 INHERENTLY SAFE DESIGN
   Rajagopalan Srinivasan and Mohd Umair Iqbal
   17.1 Introduction 386
   17.2 Origin and History of the Principle 387
   17.3 Definitions and Terminology 388
   17.4 Use and Implementation
      17.4.1 Examples of Minimization 390
      17.4.2 Examples of Substitution 391
      17.4.3 Examples of Simplification 391
      17.4.4 Example of Moderation 391
   17.5 Empirical Research on Use and Efficiency 392
   17.6 Weaknesses, Limitation, and Criticism 393
   17.7 Relation to Other Principles

References 394

18 MAINTENANCE, MAINTAINABILITY, AND INSPECTABILITY
   Torbjörn Ylipää, Anders Skoogh, and Jon Bokrantz
   18.1 Introduction 397
      18.1.1 The Piper Alpha Disaster 398
   18.2 Origin and History 399
CONTENTS

18.3 Underlying Theory, Theoretical Assumptions, Definition, and Terminology 400
18.4 Use and Implementation 405
18.5 Empirical Research on Use and Efficiency 408
18.6 Weaknesses, Limitations, and Criticism 409
18.7 Relations to Other Safety Principles 410
References 410
Further Reading 413

Part IV Optimization 415

19 ON THE RISK-INFORMED REGULATION FOR THE SAFETY AGAINST EXTERNAL HAZARDS 417
Pieter van Gelder
19.1 Introduction 417
19.2 Risk-Regulation in Safety Against Environmental Risks 421
19.3 Dealing with Uncertainties in Risk-Informed Regulation 422
19.4 Limitations of the Current Risk Measures 424
19.5 Spatial Risk 426
19.6 Temporal Risk 429
19.7 Conclusions and Recommendations 431
Acknowledgment 432
References 432

20 QUANTITATIVE RISK ANALYSIS 434
Jan-Erik Holmberg
20.1 Introduction 434
20.2 Origin and History 435
20.3 Underlying Theory and Theoretical Assumptions 438
20.3.1 Risk 438
20.3.2 Probability 438
20.3.3 Uncertainty 439
20.3.4 Expected Value and Utility Principle 441
20.3.5 Risk Criteria 442
20.3.6 ALARP 442
20.3.7 Subsidiary Risk Criteria 443
| 20.3.8 | Event Tree–Fault Tree Modeling | 445 |
| 20.3.9 | Bayesian Belief Network | 448 |
| 20.3.10 | Bow-Tie Method | 449 |
| 20.3.11 | Monte Carlo Simulation | 449 |
| 20.4 | Use and Implementation | 449 |
| 20.4.1 | National Risk Criteria | 449 |
| 20.4.2 | IEC 61508 and Safety Integrity Levels | 450 |
| 20.4.3 | Nuclear Power Plants | 452 |
| 20.4.4 | Oil and Gas Industry in Europe | 453 |
| 20.4.5 | Railway Safety in Europe | 455 |
| 20.4.6 | Other Industries | 455 |
| 20.5 | Empirical Research on Use and Efficiency | 456 |
| 20.6 | Weaknesses, Limitations, and Criticism | 456 |
| 20.7 | Relations to Other Safety Principles | 458 |
| References | 458 |
| Further Reading | 460 |

### QUALITATIVE RISK ANALYSIS

*Risto Tiisanen*

| 21.1 | Introduction | 463 |
| 21.2 | Origin and History of the Principle | 464 |
| 21.3 | Definitions | 465 |
| 21.4 | Underlying Theory and Theoretical Assumptions | 466 |
| 21.4.1 | Brainstorming | 467 |
| 21.4.2 | Preliminary Hazard Analysis | 468 |
| 21.4.3 | Scenario Analysis | 468 |
| 21.4.4 | Operating Hazard Analysis | 468 |
| 21.4.5 | HAZOP Studies | 469 |
| 21.4.6 | Risk Matrixes | 470 |
| 21.5 | Use and Implementation | 471 |
| 21.5.1 | Systems Engineering Approach to Risk Assessment | 472 |
| 21.5.2 | System-Safety Engineering | 473 |
| 21.5.3 | Industrial Safety Engineering | 476 |
| 21.5.4 | Machinery-Safety Engineering | 477 |
| 21.5.5 | Functional Safety Engineering | 478 |
| 21.6 | Strengths, Weaknesses, Limitations and Criticism | 480 |
CONTENTS

21.7 Experiences of Preliminary Hazard Identification Methods 482
21.8 Experiences of Hazop Studies 482
21.9 Experiences of Risk Estimation Methods 483
21.10 Summary of Strengths and Limitations 484
21.11 Experiences from Complex Machinery Applications 484
21.11.1 Change from Machines to Automated Machine Systems 484
21.11.2 Case Studies on Qualitative Methods 489
21.11.3 Case Study Results 490
21.12 Relations to Other Safety Principles 491
References 491

22 PRINCIPLES AND LIMITATIONS OF COST–BENEFIT ANALYSIS FOR SAFETY INVESTMENTS 493
Genserik Reniers and Luca Talarico
22.1 Introduction 493
22.2 Principles of Cost–Benefit Analysis 495
22.3 CBA Methodologies 497
22.3.1 CBA for Type I Accidents 499
22.3.2 CBA for Type II Safety Investments 504
22.3.3 Disproportion Factor 505
22.4 Conclusions 511
References 512

23 RAMS OPTIMIZATION PRINCIPLES 514
Yan-Fu Li and Enrico Zio
List of Acronyms 514
23.1 Introduction to Reliability, Availability, Maintainability, and Safety (RAMS) Optimization 515
23.2 Multi-Objective Optimization 516
23.2.1 Problem Formulation 517
23.2.2 Pareto Optimality 518
23.3 Solution Methods 519
23.3.1 Weighted-Sum Approach 519
23.3.2 $\varepsilon$-Constraint Approach 520
23.3.3 Goal Programming 521
23.3.4 Evolutionary Algorithms 521
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.4  Performance Measures</td>
<td>523</td>
</tr>
<tr>
<td>23.5  Selection of Preferred Solutions</td>
<td>524</td>
</tr>
<tr>
<td>23.5.1 “Min–Max” Method</td>
<td>524</td>
</tr>
<tr>
<td>23.6  Guidelines for Implementation and Use</td>
<td>525</td>
</tr>
<tr>
<td>23.7  Numerical Case Study</td>
<td>527</td>
</tr>
<tr>
<td>23.8  Discussion</td>
<td>536</td>
</tr>
<tr>
<td>23.9  Relations to Other Principles</td>
<td>536</td>
</tr>
<tr>
<td>References</td>
<td>537</td>
</tr>
<tr>
<td>Further Reading</td>
<td>539</td>
</tr>
<tr>
<td>24    MAINTENANCE OPTIMIZATION AND ITS RELATION TO SAFETY</td>
<td>540</td>
</tr>
<tr>
<td>Roger Flage</td>
<td></td>
</tr>
<tr>
<td>24.1  Introduction</td>
<td>540</td>
</tr>
<tr>
<td>24.2  Related Principles and Terms</td>
<td>541</td>
</tr>
<tr>
<td>24.2.1 Key Terms</td>
<td>541</td>
</tr>
<tr>
<td>24.2.2 Maintenance Optimization Models as Special Types of Cost–Benefit Analysis</td>
<td>542</td>
</tr>
<tr>
<td>24.2.3 Risk Assessment and Risk Management</td>
<td>543</td>
</tr>
<tr>
<td>24.2.4 The ALARP Principle and Risk Acceptance Criteria</td>
<td>545</td>
</tr>
<tr>
<td>24.3  Maintenance Optimization</td>
<td>547</td>
</tr>
<tr>
<td>24.3.1 Theory</td>
<td>547</td>
</tr>
<tr>
<td>24.3.2 Use and Implementation</td>
<td>550</td>
</tr>
<tr>
<td>24.4  Discussion and Conclusions</td>
<td>556</td>
</tr>
<tr>
<td>References</td>
<td>559</td>
</tr>
<tr>
<td>Further Reading</td>
<td>561</td>
</tr>
<tr>
<td>25    HUMAN RELIABILITY ANALYSIS</td>
<td>565</td>
</tr>
<tr>
<td>Luca Podofillini</td>
<td></td>
</tr>
<tr>
<td>25.1  Introduction With Examples</td>
<td>565</td>
</tr>
<tr>
<td>25.2  Origin and History of the Principle</td>
<td>569</td>
</tr>
<tr>
<td>25.3  Underlying Theory and Theoretical Assumptions</td>
<td>572</td>
</tr>
<tr>
<td>25.4  Use and Implementation</td>
<td>576</td>
</tr>
<tr>
<td>25.5  Empirical Research on Use and Efficiency</td>
<td>578</td>
</tr>
<tr>
<td>25.6  Weaknesses, Limitations, and Criticism</td>
<td>583</td>
</tr>
<tr>
<td>25.7  Relationship with Other Principles</td>
<td>585</td>
</tr>
<tr>
<td>References</td>
<td>586</td>
</tr>
</tbody>
</table>
CONTENTS

26  ALARA, BAT, AND THE SUBSTITUTION PRINCIPLE 593
Sven Ove Hansson

26.1  Introduction 593
26.2  Alara
   26.2.1  History and Current Use 594
   26.2.2  Definitions and Terminology 596
   26.2.3  Theory and Interpretation 596
   26.2.4  Effects of Applying the Principle 600
   26.2.5  Weaknesses and Criticism 601
26.3  Best Available Technology 601
   26.3.1  History and Current Use 601
   26.3.2  Definitions and Terminology 603
   26.3.3  Theory and Interpretation 603
   26.3.4  Effects of Applying the Principle 605
   26.3.5  Weaknesses and Criticism 605
26.4  The Substitution Principle 606
   26.4.1  History and Current Use 606
   26.4.2  Definitions and Terminology 609
   26.4.3  Theory and Interpretation 612
   26.4.4  Effects of Applying the Principle 613
   26.4.5  Weaknesses and Criticism 614
26.5  Comparative Discussion 615
   26.5.1  Comparisons Between the Three Principles 615
   26.5.2  Comparisons with Other Principles 616
Acknowledgment 618
References 618
Further Reading 624

Part V  Organizational Principles and Practices 625

27  SAFETY MANAGEMENT PRINCIPLES 627
Gudela Grote

27.1  Introduction 627
27.2  Origin and History of the Principle 629
27.3  Definitions 629
27.4  Underlying Theory and Theoretical Assumptions 630
27.5  Use and Implementation 633
CONTENTS

27.6 Empirical Research on Use and Efficiency 634
   27.6.1 Contextual factors 635
   27.6.2 Examples for the effects of context on safety management 638
27.7 Weaknesses, Limitations, and Criticism 640
27.8 Relations to Other Safety Principles 642
   References 642
   Further Reading 646

28 SAFETY CULTURE 647
   Teemu Reiman and Carl Rollenhagen
   28.1 Introduction 647
   28.2 Origin and History 652
      28.2.1 The Chernobyl Accident 652
      28.2.2 Organizational Culture and Organizational Climate: The Broader Context 653
      28.2.3 Safety Climate 654
      28.2.4 Organizational Culture and Safety Culture 655
   28.3 Definitions and Terminology 656
   28.4 Underlying Theory and Theoretical Assumptions 658
      28.4.1 Some Common Features of Safety Culture Models 658
      28.4.2 Theoretical Frameworks 659
   28.5 Empirical Research 662
   28.6 Use and Implementation 663
      28.6.1 When and Where to Use the Concept? 663
      28.6.2 Safety Culture as an Evaluation Framework 664
      28.6.3 Developing Safety Culture 666
   28.7 Weaknesses and Critique 667
   28.8 Main Messages and What the Concept Tells About Safety 670
      References 671

29 PRINCIPLES OF BEHAVIOR-BASED SAFETY 677
   Steve Roberts and E. Scott Geller
   29.1 Introduction 677
   29.2 Origin and History of BBS 678
   29.3 Leadership 680
   29.4 Physical Environment/Conditions 683
   29.5 Systems 683
CONTENTS

29.6  Behaviors 689  
29.7  Employee Involvement and Ownership 695  
29.8  Person States 699  
29.9  The Benefits of Behavior-Based Safety 701  
29.10  Weaknesses, Limitations, and Criticisms 703  
29.11  Relationship with Other Principles 705  
References 707  
Further Reading 710  

30  PRINCIPLES OF EMERGENCY PLANS AND CRISIS MANAGEMENT 711  
Ann Enander  
30.1  Introduction 711  
    30.1.1  Components in an Emergency Plan 712  
    30.1.2  Emergency Planning as a Process 713  
    30.1.3  Crisis Management in Theory and Practice 714  
    30.1.4  Crisis Leadership 715  
30.2  Origin and History 716  
30.3  Definitions and Terminology 717  
    30.3.1  Classifications and Typologies 719  
30.4  Underlying Theory and Theoretical Assumptions 720  
    30.4.1  The Emergency Response Cycle 720  
30.5  Use and Implementation 721  
30.6  Empirical Research on Use and Efficiency 722  
30.7  Weaknesses, Limitations, and Criticism 723  
    30.7.1  Myths and Misconceptions 724  
    30.7.2  Success or Failure 725  
30.8  Relations to Other Safety Principles 726  
References 726  
Further Reading 731  

31  SAFETY STANDARDS: CHRONIC CHALLENGES AND EMERGING PRINCIPLES 732  
Ibrahim Habli  
31.1  Introduction 732  
31.2  Definitions and Terminology 734  
31.3  Organization of Safety Standards 734  
    31.3.1  Safety Lifecycle Models 735  

CONTENTS

31.4 Domain Specific Principles 736
  31.4.1 Software Safety Assurance Principles 737
  31.4.2 Automotive Functional Safety Principles 741
31.5 Development of Standards 742
31.6 Rationale in Standards 743
31.7 Chapter Summary 744
    References 744
    Further Reading 746

32 MANAGING THE UNEXPECTED 747
Jean-Christophe Le Coze
32.1 Introduction 747
32.2 Defining the Unexpected 750
  32.2.1 The Unexpected, What Are We Dealing With? 750
    Three Examples 750
  32.2.2 Were These Disasters Unexpected, Surprising? 751
  32.2.3 The Unexpected, a Highly Relative Category 752
32.3 Thirty Years of Research on the Unexpected 754
  32.3.1 Conceptualizing the Unexpected: Four Different Threads 754
  32.3.2 Charles Perrow and Normal Accident 756
  32.3.3 Barry Turner and Man-Made Disaster: A “Kuhnian” Thread 758
  32.3.4 Jens Rasmussen and Complexity: An Ashbyan Thread 760
  32.3.5 Four Threads, Four Sensitivities, But Not Exclusive: A Synthesis 764
32.4 Managing the Unexpected 766
  32.4.1 Building Favorable Power Configurations (vs. Marxian Thread) 767
  32.4.2 Confronting Our Fallible (Cultural) Constructs (vs. Kuhnian Thread) 769
  32.4.3 Keeping Sight of the Relation Between Parts and Whole (vs. Ashbyan Thread) 770
  32.4.4 Limitations and Opening 771
32.5 Relation to Other Principles: Further Reading 771
32.6 Conclusion 772
    References 772

Index 777