

Table of Contents

Foreword	xiii
PART 1. GENERAL CONCEPTS AND PRINCIPLES	1
Chapter 1. Introduction	3
1.1. What is risk management?	3
1.2. Nature of risks	4
1.3. Evolution of risk management	6
1.4. Aims of this book	12
Chapter 2. Basic Notions	13
2.1. Formalization of the notion of risk	13
2.2. Hazard and sources of hazard	16
2.3. Stakes and targets	17
2.4. Vulnerability and resilience	18
2.5. Undesirable events and scenarios	18
2.6. Accidents and incidents	20
2.7. Safety	20
2.8. Likelihood, probability and frequency	21
2.9. Severity and intensity	22
2.10. Criticality	23
2.11. Reducing risk: prevention, protection and barriers	23
2.12. Risk analysis and risk management	25
2.13. Inductive and deductive approaches	26
2.14. Known risks and emerging risks	27
2.15. Individual and societal risks	27

2.16. Acceptable risk	28
2.17. The ALARP and ALARA principles	29
2.18. Risk maps	31
Chapter 3. Principles of Risk Analysis Methods	33
3.1. Introduction	33
3.2. Categories of targets and damages	35
3.3. Classification of sources and undesirable events	36
3.3.1. General points	36
3.3.2. Case of occupational risks	38
3.3.3. Case of major industrial risks	39
3.4. Causes of technical origin	40
3.4.1. Material failures	41
3.4.2. Failures in software and information systems	44
3.4.3. Failures linked to fluids and products	45
3.5. Causes linked to the natural or manmade environment	46
3.6. Human and organizational factors	46
3.6.1. Reason’s analysis of the human factor	48
3.6.2. Tripod classification of organizational failures	51
Chapter 4. The Risk Management Process (ISO31000)	53
4.1. Presentation	53
4.2. ISO31000 standard	55
4.2.1. Basic principles	55
4.2.2. The organizational framework	56
4.3. Implementation: the risk management process	61
4.3.1. Establishing the context	61
4.3.2. Risk assessment	65
4.3.3. Treatment of risk	66
4.3.4. Communication and consultation	67
4.3.5. Monitoring and review	68
4.3.6. Risk evaluation methods	68
PART 2. KNOWLEDGE REPRESENTATION	71
Chapter 5. Modeling Risk	73
5.1. Introduction	73
5.2. Degradation flow models	74

5.2.1. Source–target model	74
5.2.2. Reason’s model	75
5.2.3. From source–target to causal modeling	77
5.3. Causal modeling	77
5.3.1. Fishbone cause–effect diagram	78
5.3.2. Causal trees	79
5.3.3. Fault tree	80
5.3.4. Consequence or event trees	82
5.3.5. Bow-tie diagram	83
5.3.6. Scenario	84
5.3.7. Bayesian networks	84
5.4. Modeling dynamic aspects	87
5.4.1. Markov model	87
5.4.2. Dynamic fault tree	89
5.5. Summary	90
Chapter 6. Measuring the Importance of a Risk	93
6.1. Introduction	93
6.2. Assessing likelihood	96
6.2.1. Presentation	96
6.2.2. Quantitative scale	97
6.2.3. Qualitative scale	100
6.2.4. Determining likelihood values	101
6.3. Assessment of severity	102
6.3.1. Presentation	102
6.3.2. Quantitative indicators	104
6.3.3. Qualitative indicators	104
6.3.4. Determining a severity value	107
6.4. Risk assessment	109
6.4.1. Criticality	109
6.4.2. Risk matrices	110
6.4.3. Acceptability of a risk	112
6.5. Application to the case of occupational risks	113
6.5.1. Probability assessment	113
6.5.2. Severity assessment	116
6.5.3. Risk matrices	116
6.6. Application to the case of industrial risks	118
6.6.1. Probability assessment	118

6.6.2. Severity assessment	118
6.6.3. Risk matrices	120
Chapter 7. Modeling of Systems for Risk Analysis	123
7.1. Introduction	123
7.1.1. Why model a system?	123
7.1.2. The modeling process	124
7.2. Systemic or process modeling	126
7.2.1. Principle	126
7.2.2. Hierarchical breakdown	128
7.3. Functional modeling	128
7.3.1. Identifying functions	129
7.3.2. IDEF0 (SADT) representation	131
7.4. Structural modeling	131
7.5. Structuro-functional modeling	134
7.6. Modeling the behavior of a system	137
7.7. Modeling human tasks	140
7.7.1. Hierarchical task analysis (HTA)	141
7.7.2. Modeling using a decision/action flow diagram	144
7.7.3. Event tree modeling	144
7.8. Choosing an approach	145
7.9. Relationship between the system model and the risk model	146
PART 3. RISK ANALYSIS METHODS	151
Chapter 8. Preliminary Hazard Analysis	153
8.1. Introduction	153
8.2. Implementation of the method	155
8.2.1. Definition of context, information gathering and representation of the installation	156
8.2.2. Identification of hazards and undesirable events	158
8.2.3. Analysis of hazardous situations, consequences and existing barriers	159
8.2.4. Assessment of severity and frequency or likelihood	163
8.2.5. Proposing new barriers	163
8.2.6. Limitations	164
8.3. Model-driven PHA	165
8.4. Variations of PHA	166

8.4.1. Different forms of results tables	166
8.4.2. PHA in the chemical industry	167
8.5. Examples of application	169
8.5.1. Desk lamp	169
8.5.2. Chemical reactor	171
8.5.3. Automobile repair garage	172
8.5.4. Medication circuit	173
8.6. Summary	175
Chapter 9. Failure Mode and Effects Analysis	179
9.1. Introduction	179
9.2. Key concepts	181
9.2.1. Basic definitions	181
9.2.2. Causes of failure	181
9.2.3. The effects of a failure	183
9.2.4. Frequency or probability of a failure	184
9.2.5. The severity of a failure	185
9.2.6. Detection of a failure	185
9.2.7. Criticality of a failure and RPN	186
9.3. Implementation of the method	187
9.3.1. Analysis preparation	189
9.3.2. System modeling	189
9.3.3. Application of the analysis procedure	190
9.3.4. Review of the analysis and the measures to be taken	195
9.4. Model-based analysis	195
9.5. Limitations of the FMEA	197
9.5.1. Common cause failures	197
9.5.2. Other difficulties	197
9.6. Examples	198
9.6.1. Desk lamp	198
9.6.2. Chemical process	199
Chapter 10. Deviation Analysis Using the HAZOP Method	201
10.1. Introduction	201
10.2. Implementation of the HAZOP method	201
10.2.1. Preparing the study	202
10.2.2. Analysis of the study nodes	203
10.2.3. Causes and consequences of the deviation	206
10.2.4. Result tables	208

10.3. Limits and connections with other methods	208
10.4. Model-based analysis	209
10.5. Application example	210
Chapter 11. The Systemic and Organized Risk Analysis Method . . .	211
11.1. Introduction	211
11.2. Implementation of part A	214
11.2.1. Modeling of the installation	214
11.2.2. Identification of the hazard sources	215
11.2.3. Building the scenarios	220
11.2.4. Assessment of the severity of the scenarios	222
11.2.5. Negotiation of the objectives	222
11.2.6. Proposing the barriers	223
11.3. Implementing part B	224
11.3.1. Identifying the possible dysfunction	225
11.3.2. Building the fault tree	225
11.3.3. Negotiation of quantified objectives	226
11.3.4. Barrier quantification	226
11.4. Conclusion	228
Chapter 12. Fault Tree Analysis	229
12.1. Introduction	229
12.2. Method description	230
12.3. Useful notions	231
12.3.1. Definitions	231
12.3.2. Graphical representation of events and connections	232
12.4. Implementation of the method	234
12.5. Qualitative and quantitative analysis	237
12.5.1. MOCUS algorithm	238
12.5.2. Probability calculations	239
12.5.3. Importance measures	241
12.6. Connection with the reliability diagram	242
12.7. Model-based approach	243
12.8. Examples	244
12.8.1. Desk lamp	244
12.8.2. Chemical process	244
12.9. Common cause failure analysis	247
12.9.1. Introduction	247

12.9.2. Identification of common causes	248
12.9.3. Common cause analysis	249
12.9.4. The β -factor method	250
Chapter 13. Event Tree and Bow-Tie Diagram Analysis	253
13.1. Event tree	253
13.1.1. Description	253
13.1.2. Building the event tree	254
13.1.3. Conversion into a fault tree	257
13.1.4. Probability assessment	258
13.2. Bow-tie diagram	259
13.2.1. Description	259
13.2.2. Assessment of the probability	261
13.2.3. Conversion into a fault tree	262
Chapter 14. Human Reliability Analysis	263
14.1. Introduction	263
14.1.1. Objectives and context	263
14.1.2. Definitions	265
14.2. The stages of a probabilistic analysis of human reliability	267
14.3. Human error classification	269
14.3.1. Rasmussen's Skill – Rule – Knowledge (SRK) classification	270
14.3.2. The Reason classification	271
14.3.3. Errors of omission and commission	272
14.3.4. Pre-accidental and post-accidental errors	273
14.3.5. Classification based on a cognitive model of the activity	274
14.4. Analysis and quantification of human errors	274
14.4.1. Performance influencing factors	274
14.4.2. Error probability assessment	277
14.5. The SHERPA method	278
14.6. The HEART method	280
14.7. The THERP method	282
14.8. The CREAM method	288
14.9. Assessing these methods	291
Chapter 15. Barrier Analysis and Layer of Protection Analysis	293
15.1. Choice of barriers	293
15.2. Barrier classification	295

15.3. Barrier analysis based on energy flows	297
15.4. Barrier assessment	299
15.5. Safety instrumented systems	301
15.5.1. Introduction	301
15.5.2. IEC 61508 standard	303
15.5.3. Failures of an SIS	304
15.6. The LOPA method	307
15.6.1. Description	307
15.6.2. Scenario identification	311
15.6.3. Analysis of the scenarios	313
15.6.4. Identification of the frequency of initiating events	313
15.6.5. Identification of the safety barriers	315
15.6.6. Calculating the risk level of a scenario	316
15.6.7. Example	317
15.6.8. Conclusion	318
PART 4. APPENDICES	319
Appendix 1. Occupational Hazard Checklists	321
Appendix 2. Causal Tree Analysis	327
Appendix 3. A Few Reminders on the Theory of Probability	329
Appendix 4. Useful Notions in Reliability Theory	335
Appendix 5. Data Sources for Reliability	341
Appendix 6. A Few Approaches for System Modelling	347
Appendix 7. Case Study: Chemical Process	355
Appendix 8. XRisk Software	361
Bibliography	363
Index	369