

# Contents

## About the authors — v

### 1 Risk management is not only a matter of financial risk — 1

References — 7

### 2 Introduction to engineering and managing risks — 9

- 2.1 Managing risks and uncertainties – an introduction — 9
- 2.2 The complexity of risks and uncertainties — 13
- 2.3 Hazards and risks — 17
- 2.4 Simplified interpretation of (negative) risk — 19
- 2.5 Hazard and risk mapping — 22
- 2.6 Risk perception and risk attitude — 25
- 2.7 ERM – main steps — 27
- 2.8 Objectives and importance of ERM — 33
- 2.9 The Black Swan (type III events) — 34
- 2.10 Conclusions — 36

References — 36

### 3 Risk management principles — 39

- 3.1 Introduction to risk management — 39
- 3.2 Integrated risk management — 41
- 3.3 Risk management models — 43
  - 3.3.1 Model of the accident pyramid — 43
  - 3.3.2 The P2T model — 46
  - 3.3.3 The Swiss cheese model and the domino theory — 46
- 3.4 The anatomy of an accident: SIFs and SILs — 49
- 3.5 Individual risk, societal risk, physical description of risk — 57
  - 3.5.1 Location-based (individual) risk — 57
  - 3.5.2 Societal risk or group risk — 58
  - 3.5.3 Physical description of risk — 62
    - 3.5.3.1 Static model of an accident — 64
    - 3.5.3.2 Dynamic model of an accident — 64
  - 3.6 Safety culture and safety climate — 66
    - 3.6.1 Organizational culture and climate — 66
    - 3.6.2 Safety culture models — 68
    - 3.6.3 The P2T model revisited and applied to safety and security culture — 71

3.6.4	The Egg Aggregated Model (TEAM) of safety culture — 73
3.7	Strategic management concerning risks and continuous improvement — 75
3.8	The IDEAL S&S model — 77
3.8.1	Performance indicators — 82
3.9	Continuous improvement of organizational culture — 86
3.10	High reliability organizations and systemic risks — 88
3.10.1	Systems thinking — 88
3.10.1.1	Reaction time or retardant effect — 88
3.10.1.2	Law of communicating vessels — 88
3.10.1.3	Non-linear causalities — 89
3.10.1.4	Long-term vision — 89
3.10.1.5	Systems thinking conclusions — 89
3.10.2	Normal accident theory (NAT) and high reliability theory (HRT) — 90
3.10.3	High reliability organization (HRO) principles — 92
3.10.3.1	HRO principle 1: targeted at disturbances — 93
3.10.3.2	HRO principle 2: reluctant for simplification — 93
3.10.3.3	HRO principle 3: sensitive towards implementation — 93
3.10.3.4	HRO principle 4: devoted to resiliency — 94
3.10.3.5	HRO principle 5: respectful for expertise — 94
3.10.4	Risk and reliability — 94
3.11	Accident reporting — 96
3.12	Conclusions — 98
	References — 99
<b>4</b>	<b>Risk diagnostic and analysis — 103</b>
4.1	Introduction to risk assessment techniques — 103
4.1.1	Inductive and deductive approaches — 104
4.1.2	General methods for risk analysis — 105
4.1.3	General procedure — 111
4.1.4	General process for all analysis techniques — 113
4.2	SWOT — 114
4.3	Preliminary hazard analysis — 117
4.4	Checklist — 119
4.4.1	Methodology — 119
4.4.2	Example — 120
4.4.2.1	Step 1a: Critical difference, effect of energies failures — 121
4.4.2.2	Step 1b: Critical difference, deviation from the operating procedure — 121
4.4.2.3	Step 2: Establish the risk catalogue — 122
4.4.2.4	Step 3: risk mitigation — 123
4.4.3	Conclusion — 123

4.5	HAZOP — 123
4.5.1	HAZOP inputs and outputs — 124
4.5.2	HAZOP process — 125
4.5.3	Example — 126
4.5.4	Conclusions — 128
4.6	FMECA — 131
4.6.1	FMECA inputs and outputs — 132
4.6.2	FMECA process — 132
4.6.2.1	Step 1: Elaboration of the hierarchical model, functional analysis — 134
4.6.2.2	Step 2: Failure mode determination — 135
4.6.2.3	Step 3: The criticality determination — 136
4.6.3	Example — 137
4.6.4	Conclusions — 140
4.7	Fault tree analysis and event tree analysis — 141
4.7.1	Fault tree analysis — 141
4.7.2	Event tree analysis — 146
4.7.3	Cause-consequence-analysis (CCA): a combination of FTA and ETA — 147
4.8	The risk matrix — 151
4.9	Quantitative risk assessment (QRA) — 156
4.10	Layer of protection analysis — 158
4.11	Bayesian networks — 161
4.12	Conclusion — 165
	References — 166

5	Risk treatment/reduction — 169
5.1	Introduction — 169
5.2	Prevention — 174
5.2.1	Seveso Directive as prevention means for chemical plants — 175
5.2.2	Seveso company tiers — 179
5.3	Protection and mitigation — 180
5.4	Risk treatment — 184
5.5	Risk control — 189
5.6	STOP principle — 192
5.7	Resilience — 195
5.8	Conclusion — 198
	References — 199

6	Event analysis — 201
6.1	Traditional analytical techniques — 202
6.1.1	Sequence of events — 203

6.1.2	Multilinear events sequencing — 203
6.1.3	Root cause analysis — 204
6.2	Causal tree analysis — 205
6.2.1	Method description — 205
6.2.2	Collecting facts — 207
6.2.3	Event investigation good practice — 209
6.2.4	Building the tree — 210
6.2.5	Example — 213
6.2.6	Building an action plan — 214
6.2.7	Implementing solutions and follow-up — 215
6.3	Conclusions — 215
	References — 216

## 7 Major industrial accidents and learning from accidents — 217

7.1	Link between major accidents and legislation — 217
7.2	Major industrial accidents: examples — 219
7.2.1	Feyzin, France, January 1966 — 219
7.2.2	Flixborough, UK, June 1974 — 220
7.2.3	Seveso, Italy, July 1976 — 221
7.2.4	Los Alfaques, Spain, July 1978 — 221
7.2.5	Mexico City, Mexico, November 1984 — 222
7.2.6	Bhopal, India, December 1984 — 222
7.2.7	Chernobyl, Ukraine, April 1986 — 223
7.2.8	Piper Alpha, North Sea, July 1988 — 223
7.2.9	Pasadena, Texas, USA, October 1989 — 224
7.2.10	Enschede, The Netherlands, May 2000 — 224
7.2.11	Toulouse, France, September 2001 — 224
7.2.12	Ath, Belgium, July 2004 — 225
7.2.13	Houston, Texas, USA, March 2005 — 225
7.2.14	St Louis, Missouri, USA, June 2005 — 225
7.2.15	Buncefield, UK, December 2005 — 226
7.2.16	Port Wenworth, Georgia, USA, February 2008 — 226
7.2.17	Deepwater Horizon, Gulf of Mexico, April 2010 — 227
7.2.18	Fukushima, Japan, March 2011 — 227
7.2.19	West, Texas, USA, April, 2013 — 228
7.2.20	La Porte, Texas, USA, November, 2014 — 228
7.2.21	Tianjin, China, August, 2015 — 229
7.3	Learning from accidents — 229
7.4	Conclusions — 232
	References — 232

<b>8</b>	<b>Crisis management — 235</b>
8.1	Introduction — 236
8.2	The steps of crisis management — 238
8.2.1	What to do when a disruption occurs — 239
8.2.2	Business continuity plan — 244
8.3	Crisis evolution — 245
8.3.1	The pre-crisis stage or creeping crisis — 246
8.3.2	The acute-crisis stage — 247
8.3.3	The post-crisis stage — 247
8.3.4	Illustrative example of a crisis evolution — 247
8.4	Proactive or reactive crisis management — 249
8.5	Crisis communication — 250
8.6	Conclusions — 251
	References — 252
<b>9</b>	<b>Economic issues of safety — 253</b>
9.1	Accident costs and hypothetical benefits — 255
9.2	Prevention costs — 259
9.3	Prevention benefits — 260
9.4	The degree of safety and the minimum total cost point — 261
9.5	Safety economics and the two different types of risks — 262
9.6	Cost-effectiveness analysis and cost-benefit analysis for occupational (type I) accidents — 264
9.6.1	Cost-effectiveness analysis — 264
9.6.2	Cost-benefit analysis — 265
9.6.2.1	Decision rule, present values and discount rate — 267
9.6.2.2	Disproportion factor — 270
9.6.2.3	Different cost-benefit ratios — 271
9.6.2.4	Cost-benefit analysis for safety measures — 271
9.6.3	Risk acceptability — 272
9.6.4	Using the event tree to decide about safety investments — 276
9.6.5	Advantages and disadvantages of analyses based on costs and benefits — 277
9.7	Optimal allocation strategy for the safety budget — 278
9.8	Loss aversion and safety investments – safety as economic value — 279
9.9	Conclusions — 280
	References — 280
<b>10</b>	<b>Risk governance — 283</b>
10.1	Introduction — 283
10.2	Risk management system — 285

10.3	A framework for risk and uncertainty governance — 290
10.4	The risk governance model (RGM) — 296
10.4.1	The “considering?” layer of the risk governance model — 297
10.4.2	The “results?” layer of the risk governance model — 299
10.4.3	The risk governance model — 299
10.5	A risk governance PDCA — 300
10.6	Risk governance deficits — 302
10.7	Conclusions — 304
	References — 305
<b>11</b>	<b>Examples of practical implementation of risk management — 307</b>
11.1	The MICE concept — 308
11.1.1	The management step — 309
11.1.2	The information and education step — 309
11.1.3	The control step — 310
11.1.4	The emergency step — 310
11.2	Application to chemistry research and chemical hazards — 310
11.3	Application to physics research and physics hazards — 312
11.3.1	Hazards of liquid cryogens — 313
11.3.2	Asphyxiation — 316
11.4	Application to emerging technologies — 317
11.4.1	Nanotechnologies as illustrative example — 320
11.5	Conclusions — 323
	References — 325
<b>12</b>	<b>Concluding remarks — 327</b>
	<b>Index — 331</b>