Contents

LIST OF FIGURES xvii

LIST OF TABLES. xxiii

FOREWORD. xxv
Patrick MILLOT

INTRODUCTION xxvii

PART 1. GENERAL APPROACHES FOR CRISIS MANAGEMENT 1

CHAPTER 1. DEALING WITH THE UNEXPECTED 3
Guy A. BOY

1.1. Introduction 3
1.2. From mechanics to software to computer network 5
1.3. Handling complexity: looking for new models 7
1.4. Risk taking: dealing with nonlinear dynamic systems 10
1.5. Discussion 15
1.6. Conclusion 17
1.7. Bibliography 18

CHAPTER 2. VULNERABILITY AND RESILIENCE ASSESSMENT OF INFRASTRUCTURES AND NETWORKS: CONCEPTS AND METHODOLOGIES 21
Eric CHÂTELET

2.1. Introduction 21
2.2. Risk and vulnerability 22
2.2.1. Concept of risk 22
2.2.2. Concept of vulnerability 26
2.3. Vulnerability analysis and assessment 27
2.4. Resilience and main associated concepts 29
2.4.1. Resilience: a multifaceted concept 29
2.4.2. Main resilience components 30
2.5. Paradigms as consequence of risk analysis extension 32
2.5.1. Risk analysis extension and systemic approaches 32
2.5.2. Paradigms emerging from risk analysis extension 33
2.6. Resilience analysis and assessment 35
2.7. Conclusion: new challenges. 36
2.8. Bibliography 36

CHAPTER 3. THE GOLDEN HOUR CHALLENGE: APPLYING SYSTEMS ENGINEERING TO LIFE-CRITICAL SYSTEM OF SYSTEMS 41
Jean-René RUAULT

3.1. Introduction 41
3.2. The Golden hour: toward a resilient life-critical system of systems 42
3.2.1. Accident technical reports: getting experience feedback 42
3.2.2. Resilience: reducing the damage 43

3.2.3. The Golden hour: managing serious accidents as soon as possible 44
3.2.4. The challenge 47
3.3. Systems of systems engineering 48
3.3.1. The systems of systems engineering principles 48
3.3.2. Applying systems of systems engineering to life-critical systems 50
3.4. Next steps forward 54
3.5. Bibliography 54

CHAPTER 4. SITUATED RISK VISUALIZATION IN CRISIS MANAGEMENT 59
Lucas STÉPHANE

4.1. Introduction 59
4.2. Crisis management, emergency management and business continuity 60
4.2.1. Crisis management 60
4.2.2. Emergency management 61
4.2.3. Business continuity and disaster recovery 63
4.3. Risk management in critical operations 65
4.3.1. Human systems integration risk perspective 65
4.3.2. Effectiveness of risk definitions in critical operations 66
4.4. Situated risk visualization in critical operations 68
4.4.1. Rationale and requirements 68
4.4.2. Integrated structure and ontology 69
4.4.3. Interactive 3D visual scene 71
4.4.4. Evaluation results 72
4.5. Conclusions and perspectives 72
4.6. Bibliography 73

CHAPTER 5. SAFETY CRITICAL ELEMENTS OF THE RAILWAY SYSTEM: MOST ADVANCED TECHNOLOGIES AND PROCESS TO DEMONSTRATE AND MAINTAIN HIGHEST SAFETY PERFORMANCE 79
Stéphane ROMEI

5.1. Railways demonstrate the highest safety performance for public transportation 79
5.2. Key success factors 79
5.3. The European very high-speed rail technology: a safety concept with more than 30 years of experience and continuous innovation in the technology 81
5.3.1. Guidance and dynamic behavior 81
5.3.2. Environment with avoidance of external events 82
5.3.3. Velocity with capacity to guarantee the emergency braking 83
5.3.4. Lifetime spanning several decades: operation and maintenance 84
5.4. Project management and system integration 85
5.4.1. Robust industry standards in project management 85
5.4.2. System integration 85
5.5. Procedure for risk management 86
5.5.1. The regulatory framework 86
5.5.2. The EC common safety method 88
5.5.3. High technical and safety standards 88
5.5.4. Independent safety assessment 90
5.5.5. Significant change 90
5.5.6. Safety management system 91
5.5.7. Safety authorization and safety management system 92
5.6. Conclusion 93

CHAPTER 6. FUNCTIONAL MODELING OF COMPLEX SYSTEMS 95
Morten LIND

6.1. Introduction 95
6.1.1. Dimensions of system complexity 95

6.2. The modeling paradigm of MFM 97
6.2.1. The concept of function 97
6.2.2. The means-end relation 100
6.2.3. Means-end structure 101
6.3. Uses of functional modeling 102
6.3.1. Operator support systems 102
6.3.2. Control systems design 103
6.4. Multilevel flow modeling 103
6.4.1. MFM concepts 104
6.4.2. A modeling example 105
6.4.3. Modeling safety functions 109
6.5. Conclusions 110
6.6. Bibliography 111

PART 2. RISK MANAGEMENT AND HUMAN FACTORS 115

CHAPTER 7. DESIGNING DRIVER ASSISTANCE SYSTEMS IN A RISK-BASED PROCESS 117
Pietro Carlo CACCIABUE

7.1. Risk-based design in perspective 117
7.1.1. Risk-based design principles 117
7.1.2. Short historical review of the RBD process 121
7.2. Human factors in risk-based design 123
7.2.1. Human reliability assessment 124
7.2.2. Models of human behavior 126
7.2.3. Models of error and taxonomies 130
7.2.4. Dynamic nature of needs 132
7.3. A quasi-static methodology 134
7.3.1. The methodology 134
7.3.2. The expanded human performance event-tree 137
7.3.3. Evaluation of consequences and risk assessment 139

7.4. Implementation on board vehicles for driver assistance 142
7.5. A case study 145
7.5.1. Scenario definition 145
7.5.2. Initiating event 146
7.5.3. Development of the expanded event tree 147
7.5.4. Probability assessment 149
7.5.5. Consequence evaluation 151
7.5.6. Risk evaluation 152
7.6. Conclusions 152
7.7. Bibliography 153

CHAPTER 8. DISSONANCE ENGINEERING FOR RISK ANALYSIS: A THEORETICAL FRAMEWORK 157
Frédéric VANDERHAEGEN

8.1. Introduction 157
8.2. The concept of dissonance 157
8.2.1. Dissonance engineering and risk analysis. 157
8.2.2. Dissonance reduction and knowledge reinforcement 158
8.3. A theoretical framework for risk analysis 162
8.3.1. The DIMAGE model 162
8.3.2. The human–machine learning process 165
8.3.3. The behavior analysis for dissonance identification 167
8.3.4. The knowledge-based analysis for dissonance evaluation 168
8.3.5. The knowledge-based analysis for dissonance reduction 170
8.4. Examples of application of the theoretical framework 172
8.4.1. An application of the automated dissonance identification 172
8.4.2. An application of the automated dissonance evaluation 174

8.4.3. An application of the automated dissonance reduction 176
8.5. Conclusion 178
8.6. Bibliography 179

CHAPTER 9. THE FADING LINE BETWEEN SELF AND SYSTEM 183
René VAN PASSEN

9.1. Introduction 183
9.2. Four events 186
9.2.1. Turkish Airlines 1951 186
9.2.2. Night charter with a Piper Seneca 187
9.2.3. Air France Flight 447 187
9.2.4. US Airways Flight 1549 189
9.3. Development, drama 189
9.4. Views on human error 191
9.5. Peirce's triadic semiotic system 193
9.6. Abduction, or how do humans form conclusions 197
9.7. Heidegger and Descartes. 200
9.8. Designing the signs 203
9.9. Consequences 204
9.10. Conclusions 207
9.11. Bibliography 208

CHAPTER 10. RISK MANAGEMENT: A MODEL FOR PROCEDURE USE ANALYSIS 211
Kara SCHMITT

10.1. Introduction 211
10.2. Procedures in nuclear power 213
10.3. Description of the model 215
10.3.1. Description 215
10.3.2. Assumptions 221
10.3.3. Peer review of the model 222
10.4. Application of the model 223
10.4.1. Generic applications 223

10.4.2. Specific applications 223
10.4.3. Real-world application of the model 224
10.5. Significance 227
10.6. Conclusions 229
10.7. Acknowledgements 230
10.8. Bibliography 230

CHAPTER 11. DRIVER-ASSISTANCE SYSTEMS FOR ROAD SAFETY IMPROVEMENT 233
Serge BOVERIE

11.1. Introduction 233
11.2. Driver's vigilance diagnostic 236
11.2.1. Diagnostic of driver hypovigilance 238
11.2.2. Diagnostic of driver impairment. 241
11.3. Driver distraction diagnostic 242
11.4. Human–machine interaction concept 245
11.5. Conclusions 247
11.6. Bibliography 249

PART 3. MANAGING RISK VIA HUMAN–MACHINE COOPERATION 253

CHAPTER 12. HUMAN–MACHINE COOPERATION PRINCIPLES TO SUPPORT LIFE-CRITICAL SYSTEMS MANAGEMENT 255
Marie-Pierre PACAUX-LEMOINE

12.1. Context 255
12.2. Human–machine cooperation model 256
12.2.1. The "know-how" or the abilities to control the process 257
12.2.2. Know-how-to-cooperate or the agent's ability to cooperate 258
12.3. Common work space 260
12.4. Multilevel cooperation 263

12.5. Towards a generic modeling of human–machine cooperation 266
12.5.1. Cooperation to decide combination of tasks 267
12.5.2. Cooperation to decide authority 268
12.6. Conclusion and perspectives 270
12.7. Bibliography 272

CHAPTER 13. COOPERATIVE ORGANIZATION FOR ENHANCING SITUATION AWARENESS 279
Patrick MILLOT

13.1. Introduction 279
13.2. Procedure-based behavior versus innovative behavior 281
13.3. Situation awareness: between usefulness and controversy 283
13.3.1. Situation awareness: several controversial definitions 283
13.3.2. Several SA definitions suffer from a lack of assessment methods 284
13.3.3. Collective situation awareness: an incomplete framework 285
13.4. Collective SA: how to take the agent's organization into account? 287
13.4.1. Examples of task distribution and SA distribution among the agents 287
13.4.2. Collective SA: the distribution of roles among the agents 289
13.4.3. SA distribution according to the generic forms of task distribution 291
13.5. Enhancing collective SA with a support tool issued of cooperation concepts: the common work space 292
13.5.1. Cooperation model: a similitude with collective SA 292
13.5.2. Common work space for collective SA 295
13.6. Conclusion 296
13.7. Bibliography 297

CHAPTER 14. A COOPERATIVE ASSISTANT FOR DEEP SPACE EXPLORATION 301
Donald PLATT

14.1. Introduction 301
14.1.1. Previous human space exploration 301
14.1.2. Deep space situation awareness 302
14.2. The virtual camera 303
14.2.1. Motivation 303
14.2.2. Design method 309
14.2.3. Implementation 311
14.3. Evaluation 314
14.3.1. Preliminary testing 314
14.3.2. Further testing 315
14.4. Future work 316
14.5. Conclusion 316
14.6. Bibliography 317

CHAPTER 15. MANAGING THE RISKS OF AUTOMOBILE ACCIDENTS VIA HUMAN–MACHINE COLLABORATION 319
Makoto ITOH

15.1. Introduction 319
15.2. Trust as human understanding of machine 320
15.3. Machine understanding of humans 323
15.3.1. Drowsiness detection 323
15.3.2. Inference of driver intent and detecting distraction 325
15.4. Design of attention arousal and warning systems 326
15.4.1. Attention arousal for distracted drivers 326
15.4.2. Individual adaptation of a rear-end collision warning system for reducing the possibility of driver overreliance 327
15.5. Trading of authority for control from the driver to the machine under time-critical situations 329

15.6. Conclusions 330
15.7. Bibliography 331

CHAPTER 16. HUMAN–MACHINE INTERACTION IN AUTOMATED VEHICLES: THE ABV PROJECT 335
Chouki SENTOUH and Jean Christophe POPIEUL

16.1. Introduction 335
16.2. The ABV project 337
16.2.1. Objectives. 337
16.2.2. Structure of the ABV project 338
16.3. Specifications of the human–machine cooperation 339
16.3.1. Operating modes of the ABV system 339
16.3.2. ABV system HMI. 340
16.3.3. Driver monitoring. 342
16.4. Cooperation realization. 343
16.4.1. Mechanisms for operating mode switching 343
16.4.2. Shared control architecture 345
16.5. Results 346
16.6. Conclusion. 348
16.7. Bibliography 349

CHAPTER 17. INTERACTIVE SURFACES, TANGIBLE INTERACTION: PERSPECTIVES FOR RISK MANAGEMENT 351
Christophe KOLSKI, Catherine GARBAY, Yoann LEBRUN, Fabien BADEIG, Sophie LEPREUX, René MANDIAU and Emmanuel ADAM

17.1. Introduction 351
17.2. State of the art 352
17.2.1. Supports for risk management 352
17.2.2. Interactive surfaces, tangible interaction 354
17.3. Proposition: distributed UI on interactive tables and other surfaces for risk management 355
17.4. Case studies 358
17.4.1. Distributed road traffic management 358

17.4.2. Distributed risk game 361
17.5. Conclusion. 366
17.6. Acknowledgments 366
17.7. Bibliography 367

CONCLUSION 375

LIST OF AUTHORS 381

INDEX 383