Contents

Introduction xi

Part 1. Short Review of Petri Net Modeling 1

Introduction to Part 1 3

Chapter 1. Autonomous Petri Nets 5

1.1. Unmarked Petri nets 5
1.1.1. Definitions 5
1.1.2. Drawing 6
1.1.3. Other definitions 7
1.2. Marking of a PN 7
1.2.1. Order relation on markings 8
1.2.2. Enabled transition 9
1.3. Dynamics of autonomous PNs 9
1.3.1. Firing of a transition 9
1.3.2. Transition matrix 11
1.3.3. Firing sequence 11
1.3.4. Reachable marking 12
1.3.5. Fundamental equation 12
1.3.6. Properties of PN 14
1.3.7. Other properties 14
1.3.8. Invariants in a PN 15
1.3.9. Reachability graph 16

Chapter 2. Petri Nets and Event Languages 19
2.1. Labeled PNs 19
2.1.1. Formal definition 19
2.1.2. Generated and marked languages 20
2.2. Example 21

Chapter 3. Comparison Petri Nets – Finite State Automaton 25
3.1. Language expression 26
3.2. Building of the models 27
3.2.1. Synchronization of submodels 28
3.2.2. Resource sharing 29
3.2.3. Construction by refinement 30
3.3. Compactness of the model 32

Chapter 4. Some Extensions of Petri Nets 35
4.1. PN with inhibitor arcs 35
4.2. Timed PN 36
4.2.1. P-timed Petri nets 37
4.2.2. T-timed Petri nets 37
4.3. Synchronized PN 38
4.4. Timed synchronized PN 40
4.5. Interpreted PN 41
4.6. Colored PN 42
4.6.1. Introduction example 42
4.6.2. Formal definition 45
4.6.3. A dedicated software CPN Tools 46

Conclusion to Part 1 51

Part 2. A Formal Approach to Risk Assessment 53

Introduction to Part 2 51

Chapter 5. Ontology-based Accidental Process 61
5.1. Preliminary definitions 61
5.2. Elementary entities: HSE and VTE 63

5.2.1. Hazard supplier entity (HSE) 63
5.2.2. Vulnerable target entity (VTE) 63
5.3. Elementary situations and elementary events 64
5.3.1. State versus situation 64
5.3.2. Initial situation (IS) 64
5.3.3. Initiating event (IEv) 64
5.3.4. Hazard situation (HS) 65
5.3.5. Exposure event (EEv) 65
5.3.6. Exposure situation (ES) 65
5.3.7. Accident situation 65
5.3.8. Hazardous (feared) event (HEv) 65
5.4. Conclusion 66

Chapter 6. Petri Net Modeling of the Accidental Process 67

6.1. Elementary process 68
6.2. Sequence of elementary processes 71
6.3. Modeling the action of a safety barrier 71
6.4. Modeling of a cumulative process 73
6.5. PN as a support for risk assessment 75
6.5.1. Modeling of the damage 75
6.5.2. Modeling of the event frequencies 75
6.5.3. CPN Tools implementation 77
6.5.4. Evaluation rule of the risk 83
6.6. Conclusion 86

Chapter 7. Illustrative Example 87

7.1. Functional description 87
7.2. Building of an accidental process 88
7.2.1. First elementary process 88
7.2.2. Second elementary process 91
7.2.3. Parallel process 92
7.2.4. The whole model 92
7.3. Conclusion 94

Chapter 8. Design and Safety Assessment Cycle . . . 95
8.1. Five essential steps . . . 95
8.2. Ontological interest . . . 98

Conclusion to Part 2 . . . 101

Part 3. Stochastic Petri Nets . . . 103

Introduction to Part 3 . . . 105

Chapter 9. Basic Concept . . . 107
9.1. Introductory example . . . 107
9.2. Formal definition . . . 108

Chapter 10. Semantics, Properties and Evolution Rules of an SPN . . . 111
10.1. Conservatism properties . . . 112
10.1.1. Conservatism of the mean marking in steady state 112
10.1.2. Conservatism of the flow in steady state . . . 113
10.2. Mean sojourn time in a place of a SPN . . . 113
10.3. Equivalent Markov process . . . 114
10.4. Example of SPN for systems dependability modeling and assessment . . . 116

Chapter 11. Simplification of Complex Models . . . 121
11.1. Introduction . . . 121
11.2. System modeling . . . 122
11.3. Presentation of the quantitative analysis method . . . 124
11.3.1. Steps to obtain an aggregated Markov graph . . . 124
11.3.2. Toward a direct establishment of a reduced Markov graph . . . 137
11.4. Example . . . 137
11.4.1. Failure modeling . . . 138
11.4.2. Study of the different functional and hardware solutions . . . 139
11.4.3. Evaluation of the weighting coefficients from the Petri nets . . . 144
11.4.4. Conclusion . . . 147

Chapter 12. Extensions of SPN 149

12.1. Introduction 149
12.2. Relationship between stochastic Petri nets and stochastic processes 150
12.3. The transition firing policy 151
12.4. Associated stochastic processes 151
12.4.1. Temporal memory based on resampling 152
12.4.2. Temporal memory based on age memory or on enabling memory 153
12.4.3. Stochastic process underlying a stochastic PN . . . 154
12.4.4. Embedded Markov chain of the stochastic process 157
12.4.5. Application to a case study 159
12.5. Synchronization problem in generalized stochastic Petri nets 162
12.5.1. GSPN with internal synchronization 162
12.5.2. SPN with predicates and assertions 164
12.6. Conclusion 168

Part 4. Applications of Stochastic Petri Nets to Assessment Problems in Industrial Systems 169

Introduction to Part 4 171

Chapter 13. Application in Dynamic Reliability 175

13.1. Presentation of the system and hypothesis 175
13.2. System modeling with Petri net 177
13.3. Methodology application 179
13.4. Construction of an aggregated Markov graph 180
13.5. Conclusion 185

Chapter 14. Classical Dependability Assessment . . . 187

14.1. Availability study of a nuclear power plant subsystem 187
14.1.1. CPN modeling 188
14.1.2. Reliability and dependability assessment 192
14.1.3. Conclusion 196
14.2. Common causes failures in nuclear plants (safety oriented) 197

14.2.1. The Atwood model 197
14.2.2. Case study 199
14.2.3. Probabilistic dependability assessment 208
14.2.4. Conclusion 212

Chapter 15. Impact of Failures on System Performances 213

15.1. Reliability evaluation of networked control system . . 213
15.1.1. Statement of the problem 213
15.1.2. Reliability criteria of an NCS 215
15.1.3. Elements of modeling 216
15.1.4. Simulation and results 225
15.1.5. Evaluation of reliability 230
15.1.6. Conclusion 230
15.2. Railway signaling 231
15.2.1. Introduction 231
15.2.2. Interest 233
15.2.3. Signaling system specifications 234
15.2.4. Elements to be modeled 235
15.2.5. Architecture of the model 236
15.2.6. Example of an elementary model 237
15.2.7. Incident generation 239
15.2.8. Results 239
15.2.9. Conclusion 242

Conclusion 245

Appendix 247

Bibliography 251

Index 261