Contents

Preface *page* xiv

Part I Introduction 1

1 Dependability 3
1.1 Definition 3
1.2 Dependability Measures and Metrics 4
1.3 Examples of System Dependability Evaluation 7
1.3.1 Pure Reliability Evaluation 7
1.3.2 Safety Analysis of Critical Systems 8
1.3.3 Availability and Maintainability Evaluation 8
1.3.4 Software Dependability 8
1.3.5 Service-Oriented Dependability 9
1.3.6 Task-Oriented Dependability 9
1.4 Predictive Dependability Assessment 10
1.5 Further Reading 11
References 11

2 Dependability Evaluation 15
2.1 Quantitative Evaluation of Dependability 15
2.1.1 Measurement-Based Evaluation 16
2.1.2 Model-Based Evaluation 17
2.1.3 Interplay between Measurement and Modeling 19
2.2 The Modeling Process 20
2.2.1 Studying/Understanding the System Being Modeled 21
2.2.2 Development of a Conceptual Model 23
2.2.3 Translation into an Operational Computerized Model 24
2.2.4 Parametrization of the Operational Model 24
2.2.5 Solution of the Operational Model and Presentation of the Results 25
2.2.6 Verification, Validation and Improvement of the Model 25
2.2.7 Use of the Model 26
2.3 Modeling Formalisms 27
2.4 Model Verification and Validation 29
2.4.1 Model Verification 29
2.4.2 Model Validation 31

2.5 Errors in Models 32
2.5.1 Errors in the Construction of the Conceptual Model 32
2.5.2 Errors in the Construction of the Operational Computerized Model 32
2.5.3 Errors in Model Solution 33
2.6 The Probabilistic Approach 33
2.7 Statistical Dependence 34
2.8 Further Reading 36
References 36

Dependability Metrics Defined on a Single Unit 41
3.1 Non-Repairable Unit 41
3.2 Common Probability Distribution Functions 46
3.2.1 Exponential Distribution 46
3.2.2 Shifted Exponential Distribution 50
3.2.3 Weibull Distribution 50
3.2.4 Normal and Lognormal Distributions 52
3.2.5 Phase-Type Distribution 54
3.2.6 Gamma Distribution 61
3.2.7 Log-Logistic Distribution 61
3.2.8 Bernoulli Distribution 62
3.2.9 Poisson Distribution 63
3.2.10 Mass at Origin 63
3.2.11 Defective Distribution 64
3.3 Minimum and Maximum of Random Variables 66
3.3.1 The Cdf of the Minimum of Random Variables 66
3.3.2 The Cdf of the Maximum of Random Variables 68
3.4 Epistemic Uncertainty Propagation 69
3.4.1 Distribution for Rate Parameter of an Exponential Distribution 70
3.4.2 Reliability Distribution 70
3.5 Repairable Unit 72
3.5.1 Measures for Repairable Systems 73
3.5.2 Renewal Processes 74
3.5.3 The Exponential Case: Poisson Process 77
3.5.4 Modified Renewal Process 81
3.5.5 Availability Analysis: Alternating Renewal Process 81
3.5.6 Availability Analysis: State Transition Diagram 87
3.5.7 Sensitivity of Steady-State Availability 91
3.5.8 Scaled Sensitivity of Steady-State Availability 92
3.5.9 Cumulative Downtime Distribution 93
3.6 Interval Reliability 94
3.7 Task-Oriented Measures 96
3.7.1 No Failure and No Repair 96
3.7.2 Failure and Repair 96
3.7.3 Failure and Constrained Repair 98

3.8 Improving Dependability 99
3.9 Further Reading 99
References 99

Part II Non-State-Space (Combinatorial) Models 103

4 **Reliability Block Diagram** 105
4.1 Series Systems 105
4.1.1 Reliability of Series Systems 106
4.1.2 Importance (Sensitivity) Analysis of Series Systems 110
4.1.3 The Parts Count Method 111
4.1.4 Other Measures for Series Systems 112
4.2 Systems with Redundancy 115
4.2.1 Parallel Redundancy 115
4.2.2 Reliability of a Parallel System 116
4.2.3 Parallel System: The Exponential Case 118
4.2.4 Importance (Sensitivity) Analysis of Parallel Systems 118
4.2.5 Parallel Systems: Availability 119
4.2.6 Series-Parallel Systems 119
4.2.7 Importance (Sensitivity) Analysis of Series-Parallel Systems 125
4.2.8 System Redundancy vs. Component Redundancy 126
4.2.9 Is Redundancy Always Useful? 131
4.3 *k*-out-of-*n* Majority Voting Systems 133
4.3.1 The Exponential Case 136
4.3.2 Application of *k*-out-of-*n* Redundancy 137
4.3.3 The Consecutive *k*-out-of-*n* System 140
4.4 Factoring for Non-Series-Parallel Systems 141
4.5 Non-Identical *k*-out-of-*n* System 143
4.5.1 *k*-out-of-*n* System with Two Groups of Components 144
4.6 Further Reading 147
References 148

5 **Network Reliability** 150
5.1 Networks and Graphs 151
5.2 Binary Probabilistic Networks 151
5.2.1 Basic Properties of a Binary Decision Diagram 152
5.2.2 Network Reliability Based on Minpath Analysis 154
5.2.3 Network Reliability Based on Mincut Analysis 159
5.2.4 Network Reliability Based on Factoring 162
5.2.5 Graph-Visiting Algorithm 163
5.2.6 Deriving Minpaths and Mincuts from BDD 167
5.3 Binary Probabilistic Weighted Networks 173
5.3.1 Definition of BPWN 174
5.3.2 Weight as Cost 175
5.3.3 Weight as Capacity 178

5.4 Multi-State Networks 183
5.4.1 Weighted Multi-State Networks 185
5.4.2 Multi-Valued Decision Diagrams 185
5.4.3 Basic Operations for MDD Manipulation 186
5.4.4 Algorithmic Implementation and Probability Evaluation 189
5.5 Limitation of the Exact Algorithm 192
5.6 Computing Upper and Lower Bounds of Reliability 193
5.7 Further Reading 196
References 196

Fault Tree Analysis 201
6.1 Motivation for and Application of FTA 201
6.2 Construction of the Fault Tree 203
6.2.1 The OR Logic Gate 203
6.2.2 The AND Logic Gate 205
6.2.3 Fault Trees with OR and AND Gates 206
6.2.4 Fault Trees with Repeated Events 206
6.2.5 The *k*-out-of-*n* Node 207
6.3 Qualitative Analysis of a Fault Tree 208
6.3.1 Logical Expression through Minimal Cut Sets 208
6.3.2 Logical Expression through Graph-Visiting Algorithm 212
6.3.3 Qualitative Analysis of FTRE 213
6.3.4 Fault Tree and Success Tree 216
6.3.5 Structural Importance 217
6.4 Quantitative Analysis 219
6.4.1 Probability of Basic Events 219
6.4.2 Quantitative Analysis of an FT without Repeated Events 221
6.4.3 Quantitative Analysis of an FT with Repeated Events 226
6.5 Modularization 228
6.6 Importance Measures 229
6.6.1 Birnbaum Importance Index 230
6.6.2 Criticality Importance Index 231
6.6.3 Vesely–Fussell Importance Index 232
6.7 Case Studies 234
6.8 Attack and Defense Tree 243
6.8.1 Countermeasures 243
6.8.2 Weighted Attack Tree (WAT) 244
6.9 Multi-State Fault Tree 247
6.10 Mapping Fault Trees into Bayesian Networks 250
6.10.1 Bayesian Network Definition 250
6.10.2 Mapping an Algorithm from FT to BN 252
6.10.3 Probabilistic Gates: Common Cause Failures 255
6.10.4 Noisy Gates 256
6.10.5 Multi-State Variables 257
6.10.6 Sequentially Dependent Failures 259
6.10.7 Dependability Analysis through BN Inference 261
6.11 Further Reading 264
6.12 Useful Properties of Boolean Algebra 265
References 266

7 State Enumeration 271
7.1 The State Space 271
7.1.1 Characterization of System States: Truth Table and Structure Function 274
7.1.2 Structural Importance and Frontier States 275
7.1.3 Boolean Expression of the Structure Function 275
7.2 The Failure Process Defined on the State Space 278
7.2.1 Dependability Measures Defined on the State Space 279
7.3 System Reliability with Independent Components 280
7.4 Repairable Systems with Independent Components 284
References 285

8 Dynamic Redundancy 286
8.1 Cold Standby Case 286
8.2 Warm Standby 289
8.3 Hot Standby and *k*-out-of-*n* 291
8.4 Imperfect Fault Coverage 292
8.5 Epistemic Uncertainty Propagation 295
8.5.1 Cold Standby with Identical Components 296
8.5.2 Warm Standby 298
8.5.3 Hot Standby and *k*-out-of-*n* 299
References 300

Part III State-Space Models with Exponential Distributions 303

9 Continuous-Time Markov Chain: Availability Models 305
9.1 Introduction 305
9.1.1 Chapman–Kolmogorov Equations 306
9.1.2 The Infinitesimal Generator Matrix 308
9.1.3 Kolmogorov Differential Equation 309
9.1.4 Distribution of the Sojourn Time in a Given State 312
9.2 Classification of States and Stationary Distribution 313
9.2.1 Irreducible Markov Chain 313
9.2.2 Expected State Occupancy 315
9.3 Dependability Models Defined on a CTMC 317
9.3.1 Expected Uptime and Expected Downtime 318

9.4 Markov Reward Models 329
9.4.1 MRM with Reward Rates 330
9.4.2 MRM with Impulse Reward 332
9.5 Availability Measures Defined on an MRM 333
9.5.1 Instantaneous, Steady-State, and Interval Availability 333
9.5.2 Expected Uptime and Expected Downtime 333
9.5.3 Expected Number of Transitions 334
9.5.4 Expected Number of Visits 334
9.5.5 Expected Number of System Failures/Repairs 335
9.5.6 Equivalent Failure and Repair Rate 337
9.5.7 Defects per Million 340
9.6 Case Study: IBM Blade Server System 342
9.7 Parametric Sensitivity Analysis 349
9.7.1 Parametric Sensitivity Analysis for a CTMC 351
9.8 Numerical Methods for Steady-State Analysis of Markov Models 352
9.8.1 Power Method 352
9.8.2 Successive Over-Relaxation 353
9.9 Further Reading 353
References 354

10 Continuous-Time Markov Chain: Reliability Models 357
10.1 Continuous-Time Markov Chain Reliability Models 357
10.1.1 Convolution Integration Method for Transient Probabilities 363
10.1.2 Solution with Laplace Transforms 364
10.1.3 Other Dependability Measures Defined on a CTMC 373
10.2 Continuous-Time Markov Chains with Absorbing States 374
10.2.1 Single Absorbing State: Cdf of Time to Absorption 375
10.2.2 Single Absorbing State: Expected Time to Absorption 376
10.2.3 Single Absorbing State: Moments of Time to Absorption 381
10.2.4 Multiple Absorbing States 388
10.2.5 Expected First-Passage Time 397
10.3 Continuous-Time Markov Chains with Self-Loops 405
10.3.1 Uniformization of a CTMC 409
10.4 Transient Solution Methods 412
10.4.1 Fully Symbolic and Semi-Symbolic Methods 412
10.4.2 Transient Solution via Series Expansion 413
10.4.3 Transient Solution via Uniformization (Jensen's method) 415
10.4.4 ODE-Based Solution Methods 416
10.5 Further Reading 419
References 419

11 Continuous-Time Markov Chain: Queuing Systems 423
11.1 Continuous-Time Markov Chain Performance Models 424
11.2 The Birth–Death Process 424
11.3 The Single Queue 427
11.3.1 $M/M/1$ Queue 428
11.4 $M/M/m$: Single Queue with m Servers 433
11.4.1 $M/M/\infty$: An Infinite Number of Servers 435
11.5 $M/M/1/K$: Finite Storage 435
11.5.1 $M/M/m/m$ Queue 438
11.6 Closed $M/M/1$ Queue 441
11.7 Queues with Breakdown 442
11.8 Further Reading 450
References 451

12 Petri Nets 453
12.1 Introduction 453
12.2 From Petri Nets to Stochastic Reward Nets 455
12.2.1 Petri Nets 455
12.2.2 Structural Extensions to Petri Nets 458
12.2.3 Stochastic Petri Nets 460
12.2.4 Generalized Stochastic Petri Nets 463
12.3 Stochastic Reward Nets 469
12.4 Computing the Dependability and Performance Measures 476
12.5 Further Reading 482
References 482

Part IV State-Space Models with Non-Exponential Distributions 487

13 Non-Homogeneous Continuous-Time Markov Chains 489
13.1 Introduction 489
13.1.1 Kolmogorov Differential Equation 489
13.2 Illustrative Examples 490
13.3 Piecewise Constant Approximation 494
13.4 Queuing Examples 498
13.5 Reliability Growth Examples 501
13.6 Numerical Solution Methods for NHCTMCs 503
13.6.1 Ordinary Differential Equation Method 503
13.6.2 Uniformization Method 504
13.7 Further Reading 505
References 505

14 Semi-Markov and Markov Regenerative Models 509
14.1 Introduction 509
14.2 Steady-State Solution 510

14.3 Semi-Markov Processes with Absorbing States 528
14.3.1 Mean Time to Absorption 528
14.3.2 Variance of the Time to Absorption 535
14.3.3 Probability of Absorption in SMPs with Multiple Absorbing States 538
14.4 Transient Solution 539
14.5 Markov Regenerative Process 542
14.5.1 Transient and Steady-State Analysis of an MRGP 543
14.6 Further Reading 546
References 547

Phase-Type Expansion 551
15.1 Introduction 551
15.1.1 Definition 552
15.2 Properties of the PH Distribution 556
15.3 Phase-Type Distributions in System Modeling 558
15.4 Task Completion Time under a PH Work Requirement 563
15.5 Phase-Type Distribution in Queuing Models 566
15.6 Comparison of the Modeling Power of Different Model Types 569
15.7 Further Reading 570
References 570

V Multi-Level Models 575

Hierarchical Models 577
16.1 Introduction 577
16.2 Hierarchical Modeling 578
16.2.1 Import Graph 579
16.3 Availability Models 580
16.4 Reliability Models 586
16.4.1 Phased Mission Systems 590
16.4.2 Behavioral Decomposition 592
16.5 Dynamic Fault Tree 599
16.6 Performance Models 604
16.7 Performability Models 608
16.8 Survivability Models 619
16.9 Further Reading 624
References 624

Fixed-Point Iteration 631
17.1 Introduction 631
17.1.1 Revisiting the Import Graph 632
17.2 Availability Models 632
17.3 Reliability Models 635
17.4 Performance Models 636
17.5 Further Reading 640
References 640

Part VI Case Studies 643

18 Modeling Real-Life Systems 645
18.1 Availability Models 645
18.2 Reliability Models 669
18.3 Combined Performance and Reliability Models 675
18.4 Further Reading 689
References 690

Author Index 695
Subject Index 704