

CONTENTS

Foreword	xiii
Preface	xvii
1 Fundamentals of Component and System Reliability and Review of Software Reliability	1
1.1 Functions of Importance in Reliability, 1	
1.2 Hazard Rate Functions in Reliability, 6	
1.3 Common Distributions and Random Number Generations, 8	
1.3.1 Uniform (Rectangular) p.d.f, 8	
1.3.2 Triangular p.d.f., 10	
1.3.3 Negative Exponential p.d.f., Pareto, and Power Functions, 11	
1.3.4 Gamma, Erlang, and Chi-Square p.d.f.'s, 13	
1.3.5 Student's <i>t</i> -Distribution, 16	
1.3.6 Fisher's <i>F</i> -Distribution, 16	
1.3.7 Two- and Three-Parameter (Sahinoglu–Libby) Beta p.d.f.'s, 17	
1.3.8 Poisson p.m.f., 20	
1.3.9 Bernoulli, Binomial, and Multinomial p.m.f.'s, 20	
1.3.10 Geometric p.m.f., 21	
1.3.11 Negative Binomial and Pascal p.m.f.'s, 22	
1.3.12 Weibull p.d.f., 23	
1.3.13 Normal p.d.f., 25	
1.3.14 Lognormal p.d.f., 27	
1.3.15 Logistic p.d.f., 28	
1.3.16 Cauchy p.d.f., 29	
1.3.17 Hypergeometric p.m.f., 29	

- 1.3.18 Extreme Value (Gumbel) p.d.f.'s, 30
- 1.3.19 Summary of the Distributions and Relationships Most Commonly Used, 31
- 1.4 Life Testing for Component Reliability, 33
 - 1.4.1 Estimation Methods for Complete Data, 33
 - 1.4.2 Estimation Methods for Incomplete Data, 36
- 1.5 Redundancy in System Reliability, 40
 - 1.5.1 Series System Reliability, 40
 - 1.5.2 Active Parallel Redundancy, 41
 - 1.5.3 Standby Redundancy, 42
 - 1.5.4 Other Redundancy Limitations: Common-Mode Failures and Load Sharing, 44
- 1.6 Review of Software Reliability Growth Models, 45
 - 1.6.1 Software Reliability Models in the Time Domain, 48
 - 1.6.2 Classification of Reliability Growth Models, 49
- Appendix 1A: 500 Computer-Generated Random Numbers, 65
- References, 66
- Exercises, 71

2 Software Reliability Modeling with Clustered Failure Data and Stochastic Measures to Compare Predictive Accuracy of Failure-Count Models

78

- 2.1 Software Reliability Models Using the Compound Poisson Model, 78
 - 2.1.1 Notation and Introduction, 79
 - 2.1.2 Background and Motivation, 80
 - 2.1.3 Maximum Likelihood Estimation in the Poisson[^]Geometric Model, 81
 - 2.1.4 Nonlinear Regression Estimation in the Poisson[^]Geometric Model, 82
 - 2.1.5 Calculation of Forecast Quality and Comparison of Methods, 91
 - 2.1.6 Discussion and Conclusions, 96
- 2.2 Stochastic Measures to Compare Failure-Count Reliability Models, 99
 - 2.2.1 Introduction and Motivation, 99
 - 2.2.2 Definitions and Notation, 100
 - 2.2.3 Model, Data, and Computational Formulas, 101
 - 2.2.4 Prior Distribution Approach, 104
 - 2.2.5 Applications to Data Sets and Computations, 106
 - 2.2.6 Discussion and Conclusions, 110
- References, 113
- Exercises, 116

3	Quantitative Modeling for Security Risk Assessment	119
3.1	Decision Tree Model to Quantify Risk, 119	
3.1.1	Motivation, 119	
3.1.2	Risk Scenarios, 120	
3.1.3	Quantitative Security Meter Model, 122	
3.1.4	Model Application and Results, 124	
3.1.5	Modifying the Quantitative Model for Qualitative Data, 127	
3.1.6	Hybrid Security Meter Model for Both Quantitative and Qualitative Data, 127	
3.1.7	Simulation Study and Conclusions, 129	
3.2	Bayesian Applications for Prioritizing Software Maintenance, 131	
3.2.1	Motivation, 131	
3.2.2	Bayesian Rule in Statistics and Applications for Software Maintenance, 132	
3.2.3	Another Bayesian Application for Software Maintenance, 135	
3.2.4	Monte Carlo Simulation to Verify the Bayesian Analysis Proposed, 137	
3.2.5	Discussion and Conclusions, 137	
3.3	Quantitative Risk Assessment for Nondisjoint Vulnerabilities and Nondisjoint Threats, 138	
3.3.1	Motivation Behind the Disjoint Notion of Vulnerabilities and Threats, 138	
3.3.2	Fundamental Probability Laws of Independence, Conditionality, and Disjointness, 138	
3.3.3	Security Meter Modified for Nondisjoint Vulnerabilities and Disjoint Threats, 139	
3.3.4	Security Meter Modified for Nondisjoint Vulnerabilities and Nondisjoint Threats, 141	
3.3.5	Discussion and Conclusions, 142	
3.4	Simple Statistical Design to Estimate the Security Meter Model Input Data, 142	
3.4.1	Estimating the Input Parameters in the Security Meter Model, 143	
3.4.2	Statistical Formulas Used to Estimate Inputs in the Security Meter Model, 144	
3.4.3	Numerical Example of the Statistical Design for the Security Meter Model, 145	
3.4.4	Discrete Event (Dynamic) Simulation, 147	
3.4.5	Monte Carlo (Static) Simulation, 147	
3.4.6	Risk Management Using the Security Meter Model, 148	

- 3.4.7 Discussion and Conclusions, 149
- 3.5 Statistical Inference to Quantify the Likelihood of Lack of Privacy, 150
 - 3.5.1 Introduction: What Is Privacy?, 150
 - 3.5.2 How to Quantify Lack of Privacy, 151
 - 3.5.3 Numerical Applications for a Privacy Risk Management Study, 152
 - 3.5.4 Discussion and Conclusions, 154
- Appendix 3A: Comparison of Various Risk Assessment Approaches and CINAPEAAA, 154
- Appendix 3B: Brief Introduction to Encryption, Decryption, and Types, 156
- Appendix 3C: Attack Trees, 159
- Appendix 3D: Capabilities-Based Attack Tree Analysis, 161
- Appendix 3E: Time-to-Defeat Model, 162
- References, 164
- Exercises, 167

4 Stopping Rules in Software Testing 172

- 4.1 Effort-Based Empirical Bayesian Stopping Rule, 173
 - 4.1.1 Stopping Rule in Test Case–Based (Effort) Models, 173
 - 4.1.2 Introduction and Motivation, 174
 - 4.1.3 Notation, Compound Poisson Distribution, and Empirical Bayes Estimation, 177
 - 4.1.4 Stopping Rule Proposed for Use in Software Testing, 182
 - 4.1.5 Applications and Results, 185
 - 4.1.6 Discussion and Conclusions, 188
- Appendix 4A: Analysis Tables, 191
- Appendix 4B: Comparison of the Proposed CP Rule with Other Stopping Rules, 193
- Appendix 4C: MESAT-1 Output Screenshots and Graphs, 200
- 4.2 Stopping Rule for High-Assurance Software Testing in Business, 205
 - 4.2.1 Introduction, 205
 - 4.2.2 EVM Methodology, 205
 - 4.2.3 Typical SDLC Testing Management, 206
 - 4.2.4 New View of Testing, 206
 - 4.2.5 Case Study, 208
 - 4.2.6 Discussion and Conclusions, 213
- 4.3 Bayesian Stopping Rule for Testing in the Time Domain, 215
 - 4.3.1 Introduction, 215
 - 4.3.2 Review of the Compound Poisson Process, 216

4.3.3	Stopping Rule, 217	
4.3.4	Bayes Analysis for the Poisson [^] Geometric Model, 218	
4.3.5	Empirical Bayesian Stopping Rule, 220	
4.3.6	Computational Example, 220	
4.3.7	Discussion and Conclusions, 221	
	Appendix 4D: MESAT-2 Applications and Results, 221	
	References, 225	
	Exercises, 229	
5	Availability Modeling Using the Sahinoglu–Libby Probability Distribution Function	231
5.1	Nomenclature, 232	
5.2	Introduction and Motivation, 233	
5.3	Sahinoglu–Libby Probability Model Formulation, 234	
5.4	Bayes Estimators for Various Informative Priors and Loss Functions, 235	
5.4.1	Squared-Error Loss Function, 236	
5.4.2	Absolute-Error Loss Function, 236	
5.4.3	Weighted Squared-Error Loss Function, 237	
5.5	Availability Calculations for Simple Parallel and Series Networks, 239	
5.6	Discussion and Conclusions, 243	
	Appendix 5A: Derivation of the Sahinoglu–Libby p.d.f., 247	
	Appendix 5B: Derivation of the Bayes Estimator for Weighted Squared-Error Loss, 251	
	References, 252	
	Exercises, 253	
6	Reliability Block Diagramming in Complex Systems	257
6.1	Introduction and Motivation, 258	
6.2	Simple Illustrative Example, 259	
6.3	Compression Algorithm and Various Applications, 260	
6.4	Hybrid Tool to Compute Reliability for Complex Systems, 265	
6.5	More Supporting Examples for the Hybrid Form, 268	
6.6	New Polish Decoding (Decompression) Algorithm, 268	
6.7	Overlap Technique, 271	
6.7.1	Overlap Ingress–Egress Reliability Method, 271	
6.7.2	Overlap Ingress–Egress Reliability Algorithm, 274	
6.8	Multistate System Reliability Evaluation, 275	
6.8.1	Simple Series System, 276	
6.8.2	Active Parallel System, 277	
6.8.3	Simple Parallel–Series System, 278	

6.8.4	Simple Parallel System, 279	
6.8.5	Combined System, 279	
6.9	Discussion and Conclusions, 281	
	Appendix 6A: Overlap Algorithm Described, 282	
	Appendix 6B: Overlap Ingress–Egress Reliability Algorithm Applied, Example 1, 285	
	Appendix 6C: Overlap Ingress–Egress Reliability Algorithm Applied, Example 2, 298	
	References, 303	
	Exercises, 306	
Index		309