

Ajit Kumar Verma · Srividya Ajit
Durga Rao Karanki

Reliability and Safety Engineering

Second Edition



Contents

1	Introduction	1
1.1	Need for Reliability and Safety Engineering	1
1.2	Exploring Failures	2
1.3	Improving Reliability and Safety	3
1.4	Definitions and Explanation of Some Relevant Terms	4
1.4.1	Quality	4
1.4.2	Reliability	5
1.4.3	Maintainability	5
1.4.4	Availability	6
1.4.5	Risk and Safety	6
1.4.6	Probabilistic Risk Assessment/Probabilistic Safety Assessment	7
1.5	Resources	7
1.6	History	8
1.7	Present Challenges and Future Needs for the Practice of Reliability and Safety Engineering	12
	References	15
2	Basic Reliability Mathematics	19
2.1	Classical Set Theory and Boolean Algebra	19
2.1.1	Operations on Sets	19
2.1.2	Laws of Set Theory	21
2.1.3	Boolean Algebra	21
2.2	Concepts of Probability Theory	22
2.2.1	Axioms of Probability	24
2.2.2	Calculus of Probability Theory	24
2.2.3	Random Variables and Probability Distributions	28
2.3	Reliability and Hazard Functions	31

2.4	Distributions Used in Reliability and Safety Studies	34
2.4.1	Discrete Probability Distributions	34
2.4.2	Continuous Probability Distributions	40
2.4.3	Summary	59
2.5	Failure Data Analysis	59
2.5.1	Nonparametric Methods	59
2.5.2	Parametric Methods	63
	References	72
3	System Reliability Modeling	75
3.1	Reliability Block Diagram (RBD)	75
3.1.1	Procedure for System Reliability Prediction Using RBD	75
3.1.2	Different Types of Models	78
3.1.3	Solving RBD	87
3.2	Markov Models	92
3.2.1	Elements of Markov Models	92
3.3	Fault Tree Analysis	104
3.3.1	Procedure for Carrying Out Fault Tree Analysis	104
3.3.2	Elements of Fault Tree	107
3.3.3	Evaluations of Fault Tree	109
3.3.4	Case Study	115
	References	122
4	Reliability of Complex Systems	123
4.1	Monte Carlo Simulation	123
4.1.1	Analytical versus Simulation Approaches for System Reliability Modeling	123
4.1.2	Elements of Monte Carlo Simulation	125
4.1.3	Repairable Series and Parallel System	127
4.1.4	Simulation Procedure for Complex Systems	132
4.1.5	Increasing Efficiency of Simulation	139
4.2	Dynamic Fault Tree Analysis	140
4.2.1	Dynamic Fault Tree Gates	141
4.2.2	Modular Solution for Dynamic Fault Trees	143
4.2.3	Numerical Method	144
4.2.4	Monte Carlo Simulation	147
	References	158
5	Electronic System Reliability	161
5.1	Importance of Electronic Industry	161
5.2	Various Components Used and Their Failure Mechanisms	162
5.2.1	Resistors	162
5.2.2	Capacitors	162

5.2.3	Inductors	163
5.2.4	Relays	163
5.2.5	Semiconductor Devices	163
5.2.6	Microcircuits (ICs)	164
5.3	Reliability Prediction of Electronic Systems	165
5.3.1	Parts Count Method	166
5.3.2	Parts Stress Method	166
5.4	PRISM	167
5.5	Sneak Circuit Analysis (SCA)	169
5.5.1	Definition of SCA	169
5.5.2	Network Tree Production	170
5.5.3	Topological Pattern Identification	170
5.6	Case Study	171
5.6.1	Total Failure Rate	172
5.7	Physics of Failure Mechanisms of Electronic Components	174
5.7.1	Physics of Failures	174
5.7.2	Failure Mechanisms for Resistors	174
5.7.3	Failure Mechanisms for Capacitor	176
5.7.4	MOS Failure Mechanisms	176
5.7.5	Field Programmable Gate Array	180
	References	182
6	Software Reliability	183
6.1	Introduction to Software Reliability	183
6.2	Past Incidences of Software Failures in Safety Critical Systems	184
6.3	The Need for Reliable Software	187
6.4	Difference Between Hardware Reliability and Software Reliability	188
6.5	Software Reliability Modeling	189
6.5.1	Software Reliability Growth Models	191
6.5.2	Black Box Software Reliability Models	191
6.5.3	White Box Software Reliability Models	192
6.6	How to Implement Software Reliability	192
6.7	Emerging Techniques in Software Reliability Modeling—Soft Computing Technique	199
6.7.1	Need for Soft Computing Methods	201
6.7.2	Environmental Parameters	201
6.7.3	Anil-Verma Model	208
6.8	Future Trends of Software Reliability	215
	References	216

7	Mechanical Reliability	219
7.1	Reliability Versus Durability	220
7.2	Failure Modes in Mechanical Systems	221
7.2.1	Failures Due to Operating Load	222
7.2.2	Failure Due to Environment	226
7.3	Reliability Circle	226
7.3.1	Specify Reliability	228
7.3.2	Design for Reliability	231
7.3.3	Test for Reliability	245
7.3.4	Maintain the Manufacturing Reliability	250
7.3.5	Operational Reliability	252
	References	255
8	Structural Reliability	257
8.1	Deterministic versus Probabilistic Approach in Structural Engineering	257
8.2	The Basic Reliability Problem	258
8.2.1	First Order Second Moment (FOSM) Method	259
8.2.2	Advanced First Order Second Moment Method (AFOSM)	263
8.3	First Order Reliability Method (FORM)	264
8.4	Reliability Analysis for Correlated Variables	268
8.4.1	Reliability Analysis for Correlated Normal Variables	269
8.4.2	Reliability Analysis for Correlated Non-normal Variables	270
8.5	Second Order Reliability Methods (SORM)	271
8.6	System Reliability	282
8.6.1	Classification of Systems	282
8.6.2	Evaluation of System Reliability	284
	References	292
9	Maintenance of Large Engineering Systems	293
9.1	Introduction	293
9.2	Peculiarities of a Large Setup of Machinery	294
9.3	Prioritizing the Machinery for Maintenance Requirements	296
9.3.1	Hierarchical Level of Machinery	299
9.3.2	FMECA (Failure Mode Effect and Criticality Analysis)	301
9.4	Maintenance Scheduling of a Large Setup of Machinery	309
9.4.1	Introduction	309
9.4.2	Example	311

9.4.3	Example—MOOP of Maintenance Interval Scheduling	314
9.4.4	Use of NSGA II—Elitist Genetic Algorithm Program	316
9.4.5	Assumptions and Result.	317
9.5	Decision Regarding Maintenance Before an Operational Mission	321
9.5.1	Introduction	321
9.5.2	The Model.	322
9.5.3	Assumptions	323
9.5.4	Result	329
9.6	Summary	331
	References.	332
10	Probabilistic Safety Assessment	333
10.1	Introduction	333
10.2	Concept of Risk and Safety	333
10.3	An Overview of Probabilistic Safety Assessment Tasks	336
10.4	Identification of Hazards and Initiating Events	339
10.4.1	Preliminary Hazard Analysis	339
10.4.2	Master Logic Diagram (MLD)	339
10.5	Event Tree Analysis	340
10.6	Importance Measures.	346
10.7	Common Cause Failure Analysis	349
10.7.1	Treatment of Dependent Failures	350
10.7.2	The Procedural Framework for CCF Analysis.	352
10.7.3	Treatment of Common Cause Failures in Fault Tree Models.	352
10.7.4	Common Cause Failure Models	357
10.8	Human Reliability Analysis	365
10.8.1	HRA Concepts	365
10.8.2	HRA Process, Methods, and Tools	366
	References.	370
11	Dynamic PSA	373
11.1	Introduction to Dynamic PSA.	373
11.1.1	Need for Dynamic PSA.	373
11.1.2	Dynamic Methods for Risk Assessment.	374
11.2	Dynamic Event Tree Analysis	376
11.2.1	Event Tree versus Dynamic Event Tree	376
11.2.2	DET Approach—Steps Involved.	376
11.2.3	DET Implementation—Comparison Among Tools.	379

11.3	Example—Depleting Tank	382
11.3.1	Description on Depleting Tank Problem	382
11.3.2	Analytical Solution	383
11.3.3	Discrete DET Solution.	385
11.4	DET Quantification of Risk—Practical Issues and Possible Solutions.	388
11.4.1	Challenges in Direct Quantification of Risk with DET.	388
11.4.2	Uncertainties and Dynamics in Risk Assessment.	389
	References.	390
12	Applications of PSA	393
12.1	Objectives of PSA	393
12.2	PSA of Nuclear Power Plant	394
12.2.1	Description of PHWR	394
12.2.2	PSA of Indian NPP (PHWR Design).	396
12.3	Technical Specification Optimization.	410
12.3.1	Traditional Approaches for Technical Specification Optimization	410
12.3.2	Advanced Techniques for Technical Specification Optimization	413
12.4	Risk Monitor	420
12.4.1	Necessity of Risk Monitor?	421
12.4.2	Different Modules of Risk Monitor.	421
12.4.3	Applications of Risk Monitor	423
12.5	Risk Informed In-Service Inspection	425
12.5.1	RI-ISI Models	426
12.5.2	ISI and Piping Failure Frequency	434
	References.	454
13	Uncertainty Analysis in Reliability/Safety Assessment.	457
13.1	Mathematical Models and Uncertainties	457
13.2	Uncertainty Analysis: An Important Task of PRA/PSA	459
13.3	Methods of Characterising Uncertainties	461
13.3.1	The Probabilistic Approach	461
13.3.2	Interval and Fuzzy Representation.	462
13.3.3	Dempster-Shafer Theory Based Representation.	463
13.4	Bayesian Approach	465
13.5	Expert Elicitation Methods.	470
13.5.1	Definition and Uses of Expert Elicitation	470
13.5.2	Treatment of Expert Elicitation Process	470
13.5.3	Methods of Treatment	471

13.6	Uncertainty Propagation.	474
13.6.1	Method of Moments	474
13.6.2	Monte Carlo Simulation.	480
13.6.3	Interval Analysis.	484
13.6.4	Fuzzy Arithmetic	486
	References.	491
14	Advanced Methods in Uncertainty Management.	493
14.1	Uncertainty Analysis with Correlated Basic Events	493
14.1.1	Dependency: Common Cause Failures versus Correlated Epistemic Parameters	494
14.1.2	Methodology for PSA Based on Monte Carlo Simulation with Nataf Transformation	496
14.1.3	Case Study.	499
14.2	Uncertainty Importance Measures	506
14.2.1	Probabilistic Approach to Ranking Uncertain Parameters in System Reliability Models	507
14.2.2	Method Based on Fuzzy Set Theory	508
14.2.3	Application to a Practical System	511
14.3	Treatment of Aleatory and Epistemic Uncertainties	514
14.3.1	Epistemic and Aleatory Uncertainty in Reliability Calculations	515
14.3.2	Need to Separate Epistemic and Aleatory Uncertainties	516
14.3.3	Methodology for Uncertainty Analysis in Reliability Assessment Based on Monte Carlo Simulation.	517
14.4	Dempster-Shafer Theory	521
14.4.1	Belief and Plausibility Function of Real Numbers. . .	524
14.4.2	Dempster's Rule of Combination	525
14.4.3	Sampling Technique for the Evidence Theory.	526
14.5	Probability Bounds Approach.	529
14.5.1	Computing with Probability Bounds	530
14.5.2	Two-Phase Monte Carlo Simulation	535
14.5.3	Uncertainty Propagation Considering Correlation Between Variables	540
14.6	Case Study to Compare Uncertainty Analysis Methods	541

14.6.1	Availability Assessment of MCPS Using Fault Tree Analysis	542
14.6.2	Uncertainty Propagation in MCPS with Different Methods	543
14.6.3	Observations from Case Study	549
	References.	551
	Appendix	555
	Index	567