


ontents

PREFACE xv

1 BASIC RISK CONCEPTS 1

1.1 Introduction 1

1.2 Formal Definition of Risk 1

- 1.2.1 Outcomes and Likelihoods 1
- 1.2.2 Uncertainty and Meta-Uncertainty 4
- 1.2.3 Risk Assessment and Management 6
- 1.2.4 Alternatives and Controllability of Risk 8
- 1.2.5 Outcome Significance 12
- 1.2.6 Causal Scenario 14
- 1.2.7 Population Affected 15
- 1.2.8 Population Versus Individual Risk 15
- 1.2.9 Summary 18

1.3 Source of Debates 18

- 1.3.1 Different Viewpoints Toward Risk 18
- 1.3.2 Differences in Risk Assessment 19
- 1.3.3 Differences in Risk Management 22
- 1.3.4 Summary 26

1.4 Risk-Aversion Mechanisms 26

- 1.4.1 Risk Aversion 27
- 1.4.2 Three Attitudes Toward Monetary Outcome 27
- 1.4.3 Significance of Fatality Outcome 30
- 1.4.4 Mechanisms for Risk Aversion 31
- 1.4.5 Bayesian Explanation of Severity Overestimation 31
- 1.4.6 Bayesian Explanation of Likelihood Overestimation 32

1.4.7 PRAM Credibility Problem 35

1.4.8 Summary 35

1.5 Safety Goals 35

1.5.1 Availability, Reliability, Risk, and Safety 35

1.5.2 Hierarchical Goals for PRAM 36

1.5.3 Upper and Lower Bound Goals 37

1.5.4 Goals for Normal Activities 42

1.5.5 Goals for Catastrophic Accidents 43

1.5.6 Idealistic Versus Pragmatic Goals 48

1.5.7 Summary 52

References 53

Problems 54

2 ACCIDENT MECHANISMS AND RISK MANAGEMENT 55

2.1 Introduction 55

2.2 Accident-Causing Mechanisms 55

2.2.1 Common Features of Plants with Risks 55

2.2.2 Negative Interactions Between Humans and the Plant 57

2.2.3 A Taxonomy of Negative Interactions 58

2.2.4 Chronological Distribution of Failures 62

2.2.5 Safety System and Its Malfunctions 64

2.2.6 Event Layer and Likelihood Layer 67

2.2.7 Dependent Failures and Management Deficiencies 72

2.2.8 Summary 75

2.3 Risk Management 75

2.3.1 Risk-Management Principles 75

2.3.2 Accident Prevention and Consequence Mitigation 78

2.3.3 Failure Prevention 78

2.3.4 Propagation Prevention 81

2.3.5 Consequence Mitigation 84

2.3.6 Summary 85

2.4 Preproduction Quality Assurance Program 85

2.4.1 Motivation 86

2.4.2 Preproduction Design Process 86

2.4.3 Design Review for PQA 87

2.4.4 Management and Organizational Matters 92

2.4.5 Summary 93

References 93

Problems 94

3 PROBABILISTIC RISK ASSESSMENT 95

3.1 Introduction to Probabilistic Risk Assessment 95

3.1.1 Initiating-Event and Risk Profiles 95

3.1.2 Plants without Hazardous Materials 96

- 3.1.3 Plants with Hazardous Materials 97
- 3.1.4 Nuclear Power Plant PRA: WASH-1400 98
- 3.1.5 WASH-1400 Update: NUREG-1150 102
- 3.1.6 Summary 104
- 3.2 Initiating-Event Search 104
 - 3.2.1 Searching for Initiating Events 104
 - 3.2.2 Checklists 105
 - 3.2.3 Preliminary Hazard Analysis 106
 - 3.2.4 Failure Mode and Effects Analysis 108
 - 3.2.5 FMECA 110
 - 3.2.6 Hazard and Operability Study 113
 - 3.2.7 Master Logic Diagram 115
 - 3.2.8 Summary 115
- 3.3 The Three PRA Levels 117
 - 3.3.1 Level 1 PRA—Accident Frequency 117
 - 3.3.2 Level 2 PRA—Accident Progression and Source Term 126
 - 3.3.3 Level 3 PRA—Offsite Consequence 127
 - 3.3.4 Summary 127
- 3.4 Risk Calculations 128
 - 3.4.1 The Level 3 PRA Risk Profile 128
 - 3.4.2 The Level 2 PRA Risk Profile 130
 - 3.4.3 The Level 1 PRA Risk Profile 130
 - 3.4.4 Uncertainty of Risk Profiles 131
 - 3.4.5 Summary 131
- 3.5 Example of a Level 3 PRA 132
- 3.6 Benefits, Detriments, and Successes of PRA 132
 - 3.6.1 Tangible Benefits in Design and Operation 132
 - 3.6.2 Intangible Benefits 133
 - 3.6.3 PRA Negatives 134
 - 3.6.4 Success Factors of PRA Program 134
 - 3.6.5 Summary 136
- References 136
- Chapter Three Appendices 138
- A.1 Conditional and Unconditional Probabilities 138
 - A.1.1 Definition of Conditional Probabilities 138
 - A.1.2 Chain Rule 139
 - A.1.3 Alternative Expression of Conditional Probabilities 140
 - A.1.4 Independence 140
 - A.1.5 Bridge Rule 141
 - A.1.6 Bayes Theorem for Discrete Variables 142
 - A.1.7 Bayes Theorem for Continuous Variables 143
- A.2 Venn Diagrams and Boolean Operations 143
 - A.2.1 Introduction 143
 - A.2.2 Event Manipulations via Venn Diagrams 144
 - A.2.3 Probability and Venn Diagrams 145
 - A.2.4 Boolean Variables and Venn Diagrams 146
 - A.2.5 Rules for Boolean Manipulations 147

A.3 A Level for 3 PRA—Station Blackout 148

- A.3.1 Plant Description 148
- A.3.2 Event Tree for Station Blackout 150
- A.3.3 Accident Sequences 152
- A.3.4 Fault Trees 152
- A.3.5 Accident-Sequence Cut Sets 153
- A.3.6 Accident-Sequence Quantification 155
- A.3.7 Accident-Sequence Group 156
- A.3.8 Uncertainty Analysis 156
- A.3.9 Accident-Progression Analysis 156
- A.3.10 Summary 163
- Problems 163

4 FAULT-TREE CONSTRUCTION 165

- 4.1 Introduction 165
- 4.2 Fault Trees 166
- 4.3 Fault-Tree Building Blocks 166
 - 4.3.1 Gate Symbols 166
 - 4.3.2 Event Symbols 172
 - 4.3.3 Summary 174
- 4.4 Finding Top Events 175
 - 4.4.1 Forward and Backward Approaches 175
 - 4.4.2 Component Interrelations and System Topography 175
 - 4.4.3 Plant Boundary Conditions 176
 - 4.4.4 Example of Preliminary Forward Analysis 176
 - 4.4.5 Summary 179
- 4.5 Procedure for Fault-Tree Construction 179
 - 4.5.1 Fault-Tree Example 180
 - 4.5.2 Heuristic Guidelines 184
 - 4.5.3 Conditions Induced by OR and AND Gates 188
 - 4.5.4 Summary 194
- 4.6 Automated Fault-Tree Synthesis 196
 - 4.6.1 Introduction 196
 - 4.6.2 System Representation by Semantic Networks 197
 - 4.6.3 Event Development Rules 204
 - 4.6.4 Recursive Three-Value Procedure for FT Generation 206
 - 4.6.5 Examples 210
 - 4.6.6 Summary 220
 - References 222
 - Problems 223

5 QUALITATIVE ASPECTS OF SYSTEM ANALYSIS 227

- 5.1 Introduction 227
- 5.2 Cut Sets and Path Sets 227
 - 5.2.1 Cut Sets 227
 - 5.2.2 Path Sets (Tie Sets) 227

5.2.3	Minimal Cut Sets	229
5.2.4	Minimal Path Sets	229
5.2.5	Minimal Cut Generation (Top-Down)	229
5.2.6	Minimal Cut Generation (Bottom-Up)	231
5.2.7	Minimal Path Generation (Top-Down)	232
5.2.8	Minimal Path Generation (Bottom-Up)	233
5.2.9	Coping with Large Fault Trees	234
5.3	Common-Cause Failure Analysis	240
5.3.1	Common-Cause Cut Sets	240
5.3.2	Common Causes and Basic Events	241
5.3.3	Obtaining Common-Cause Cut Sets	242
5.4	Fault-Tree Linking Along an Accident Sequence	246
5.4.1	Simple Example	246
5.4.2	A More Realistic Example	248
5.5	Noncoherent Fault Trees	251
5.5.1	Introduction	251
5.5.2	Minimal Cut Sets for a Binary Fault Tree	252
5.5.3	Minimal Cut Sets for a Multistate Fault Tree	257
	References	258
	Problems	259

6 QUANTIFICATION OF BASIC EVENTS 263

6.1	Introduction	263
6.2	Probabilistic Parameters	264
6.2.1	A Repair-to-Failure Process	265
6.2.2	A Repair-Failure-Repair Process	271
6.2.3	Parameters of Repair-to-Failure Process	274
6.2.4	Parameters of Failure-to-Repair Process	278
6.2.5	Probabilistic Combined-Process Parameters	280
6.3	Fundamental Relations	
	Among Probabilistic Parameters	285
6.3.1	Repair-to-Failure Parameters	285
6.3.2	Failure-to-Repair Parameters	289
6.3.3	Combined-Process Parameters	290
6.4	Constant-Failure Rate and Repair-Rate Model	297
6.4.1	Repair-to-Failure Process	297
6.4.2	Failure-to-Repair Process	299
6.4.3	Laplace Transform Analysis	299
6.4.4	Markov Analysis	303
6.5	Statistical Distributions	304
6.6	General Failure and Repair Rates	304
6.7	Estimating Distribution Parameters	309
6.7.1	Parameter Estimation	
	for Repair-to-Failure Process	309
6.7.2	Parameter Estimation	
	for Failure-to-Repair Process	318

6.8	Components with Multiple Failure Modes	322
6.9	Environmental Inputs	325
6.9.1	Command Failures	325
6.9.2	Secondary Failures	325
6.10	Human Error	326
6.11	System-Dependent Basic Event	326
	References	327
	Chapter Six Appendices	327
A.1	Distributions	327
A.1.1	Mean	328
A.1.2	Median	328
A.1.3	Mode	328
A.1.4	Variance and Standard Deviation	328
A.1.5	Exponential Distribution	329
A.1.6	Normal Distribution	330
A.1.7	Log-Normal Distribution	330
A.1.8	Weibull Distribution	330
A.1.9	Binomial Distribution	331
A.1.10	Poisson Distribution	331
A.1.11	Gamma Distribution	332
A.1.12	Other Distributions	332
A.2	A Constant-Failure-Rate Property	332
A.3	Derivation of Unavailability Formula	333
A.4	Computational Procedure for Incomplete Test Data	334
A.5	Median-Rank Plotting Position	334
A.6	Failure and Repair Basic Definitions	335
	Problems	335
7	CONFIDENCE INTERVALS	339
7.1	Classical Confidence Limits	339
7.1.1	Introduction	339
7.1.2	General Principles	340
7.1.3	Types of Life-Tests	346
7.1.4	Confidence Limits for Mean Time to Failure	346
7.1.5	Confidence Limits for Binomial Distributions	349
7.2	Bayesian Reliability and Confidence Limits	351
7.2.1	Discrete Bayes Theorem	351
7.2.2	Continuous Bayes Theorem	352
7.2.3	Confidence Limits	353
	References	354
	Chapter Seven Appendix	354
A.1	The χ^2 , Student's t , and F Distributions	354
A.1.1	χ^2 Distribution Application Modes	355
A.1.2	Student's t Distribution Application Modes	356

- A.1.3 F Distribution Application Modes 357
- Problems 359

8 QUANTITATIVE ASPECTS OF SYSTEM ANALYSIS 363

- 8.1 Introduction 363
- 8.2 Simple Systems 365
 - 8.2.1 Independent Basic Events 365
 - 8.2.2 AND Gate 366
 - 8.2.3 OR Gate 366
 - 8.2.4 Voting Gate 367
 - 8.2.5 Reliability Block Diagrams 371
- 8.3 Truth-Table Approach 374
 - 8.3.1 AND Gate 374
 - 8.3.2 OR Gate 374
- 8.4 Structure-Function Approach 379
 - 8.4.1 Structure Functions 379
 - 8.4.2 System Representation 379
 - 8.4.3 Unavailability Calculations 380
- 8.5 Approaches Based on Minimal Cuts or Minimal Paths 383
 - 8.5.1 Minimal Cut Representations 383
 - 8.5.2 Minimal Path Representations 384
 - 8.5.3 Partial Pivotal Decomposition 386
 - 8.5.4 Inclusion-Exclusion Formula 387
- 8.6 Lower and Upper Bounds for System Unavailability 389
 - 8.6.1 Inclusion-Exclusion Bounds 389
 - 8.6.2 Esary and Proschan Bounds 390
 - 8.6.3 Partial Minimal Cut Sets and Path Sets 390
- 8.7 System Quantification by KITT 391
 - 8.7.1 Overview of KITT 392
 - 8.7.2 Minimal Cut Set Parameters 397
 - 8.7.3 System Unavailability $Q_s(t)$ 402
 - 8.7.4 System Parameter $w_s(t)$ 404
 - 8.7.5 Other System Parameters 409
 - 8.7.6 Short-Cut Calculation Methods 410
 - 8.7.7 The Inhibit Gate 414
 - 8.7.8 Remarks on Quantification Methods 415
- 8.8 Alarm Function and Two Types of Failure 416
 - 8.8.1 Definition of Alarm Function 416
 - 8.8.2 Failed-Safe and Failed-Dangerous Failures 416
 - 8.8.3 Probabilistic Parameters 419
- References 420
- Problems 421

9	SYSTEM QUANTIFICATION FOR DEPENDENT EVENTS	425
9.1	Dependent Failures	425
9.1.1	Functional and Common-Unit Dependency	425
9.1.2	Common-Cause Failure	426
9.1.3	Subtle Dependency	426
9.1.4	System-Quantification Process	426
9.2	Markov Model for Standby Redundancy	427
9.2.1	Hot, Cold, and Warm Standby	427
9.2.2	Inclusion-Exclusion Formula	427
9.2.3	Time-Dependent Unavailability	428
9.2.4	Steady-State Unavailability	439
9.2.5	Failures per Unit Time	442
9.2.6	Reliability and Repairability	444
9.3	Common-Cause Failure Analysis	446
9.3.1	Subcomponent-Level Analysis	446
9.3.2	Beta-Factor Model	449
9.3.3	Basic-Parameter Model	456
9.3.4	Multiple Greek Letter Model	461
9.3.5	Binomial Failure-Rate Model	464
9.3.6	Markov Model	467
	References	469
	Problems	469
10	HUMAN RELIABILITY	471
10.1	Introduction	471
10.2	Classifying Human Errors for PRA	472
10.2.1	Before an Initiating Event	472
10.2.2	During an Accident	472
10.3	Human and Computer Hardware System	474
10.3.1	The Human Computer	474
10.3.2	Brain Bottlenecks	477
10.3.3	Human Performance Variations	478
10.4	Performance-Shaping Factors	481
10.4.1	Internal PSFs	481
10.4.2	External PSFs	484
10.4.3	Types of Mental Processes	487
10.5	Human-Performance Quantification by PSFs	489
10.5.1	Human-Error Rates and Stress Levels	489
10.5.2	Error Types, Screening Values	491
10.5.3	Response Time	492
10.5.4	Integration of PSFs by Experts	492
10.5.5	Recovery Actions	494
10.6	Examples of Human Error	494
10.6.1	Errors in Thought Processes	494
10.6.2	Lapse/Slip Errors	497

- 10.7 SHARP: General Framework 498
- 10.8 THERP: Routine and Procedure-Following Errors 499
 - 10.8.1 Introduction 499
 - 10.8.2 General THERP Procedure 502
- 10.9 HCR: Nonresponse Probability 506
- 10.10 Wrong Actions due to Misdiagnosis 509
 - 10.10.1 Initiating-Event Confusion 509
 - 10.10.2 Procedure Confusion 510
 - 10.10.3 Wrong Actions due to Confusion 510
- References 511
- Chapter Ten Appendices 513
- A.1 THERP for Errors During a Plant Upset 513
- A.2 HCR for Two Optional Procedures 525
- A.3 Human-Error Probability Tables from Handbook 530
- Problems 533

11 UNCERTAINTY QUANTIFICATION 535

- 11.1 Introduction 535
 - 11.1.1 Risk-Curve Uncertainty 535
 - 11.1.2 Parametric Uncertainty and Modeling Uncertainty 536
 - 11.1.3 Propagation of Parametric Uncertainty 536
- 11.2 Parametric Uncertainty 536
 - 11.2.1 Statistical Uncertainty 536
 - 11.2.2 Data Evaluation Uncertainty 537
 - 11.2.3 Expert-Evaluated Uncertainty 538
- 11.3 Plant-Specific Data 539
 - 11.3.1 Incorporating Expert Evaluation as a Prior 539
 - 11.3.2 Incorporating Generic Plant Data as a Prior 539
- 11.4 Log-Normal Distribution 541
 - 11.4.1 Introduction 541
 - 11.4.2 Distribution Characteristics 541
 - 11.4.3 Log-Normal Determination 542
 - 11.4.4 Human-Error-Rate Confidence Intervals 543
 - 11.4.5 Product of Log-Normal Variables 545
 - 11.4.6 Bias and Dependence 547
- 11.5 Uncertainty Propagation 549
- 11.6 Monte Carlo Propagation 550
 - 11.6.1 Unavailability 550
 - 11.6.2 Distribution Parameters 552
 - 11.6.3 Latin Hypercube Sampling 553
- 11.7 Analytical Moment Propagation 555
 - 11.7.1 AND Gate 555
 - 11.7.2 OR Gate 556
 - 11.7.3 AND and OR Gates 557
 - 11.7.4 Minimal Cut Sets 558

11.7.5 Taylor Series Expansion	560
11.7.6 Orthogonal Expansion	561
11.8 Discrete Probability Algebra	564
11.9 Summary	566
References	566
Chapter Eleven Appendices	567
A.1 Maximum-Likelihood Estimator	567
A.2 Cut Set Covariance Formula	569
A.3 Mean and Variance by Orthogonal Expansion	569
Problems	571

12 LEGAL AND REGULATORY RISKS 573

12.1 Introduction	573
12.2 Losses Arising from Legal Actions	574
12.2.1 Nonproduct Liability Civil Lawsuits	575
12.2.2 Product Liability Lawsuits	575
12.2.3 Lawsuits by Government Agencies	576
12.2.4 Worker's Compensation	577
12.2.5 Lawsuit-Risk Mitigation	578
12.2.6 Regulatory Agency Fines: Risk Reduction Strategies	579
12.3 The Effect of Government Regulations on Safety and Quality	580
12.3.1 Stifling of Initiative and Abrogation of Responsibility	581
12.3.2 Overregulation	582
12.4 Labor and the Safe Workplace	583
12.4.1 Shaping the Company's Safety Culture	584
12.4.2 The Hiring Process	584
12.5 Epilogue	587

INDEX 589