

Contents

<i>Preface</i>	<i>xix</i>
<i>Acknowledgements</i>	<i>xxi</i>
Part 1: Understanding Reliability Parameters and Costs	1
<i>Chapter 1: The History of Reliability and Safety Technology</i>	3
1.1 Failure Data	3
1.2 Hazardous Failures	5
1.3 Predicting Reliability and Risk.....	5
1.4 Achieving Reliability and Safety-Integrity.....	8
1.5 The RAMS-Cycle	10
1.6 Contractual and Legal Pressures.....	12
1.7 Reliability versus Functional Safety.....	13
<i>Chapter 2: Understanding Terms and Jargon</i>	15
2.1 Defining Failure and Failure Modes	15
2.2 Failure Rate and Mean Time Between Failures	17
2.2.1 The Observed Failure Rate.....	17
2.2.2 The Observed Mean Time Between Failures.....	18
2.2.3 The Observed Mean Time to Fail	18
2.2.4 Mean Life	19
2.3 Interrelationships of Terms.....	19
2.3.1 Reliability and Failure Rate.....	19
2.3.2 Reliability and Failure Rate as an Approximation	21
2.3.3 Reliability and MTBF	22
2.4 The Bathtub Distribution	22
2.5 Down Time and Repair Time	24
2.6 Availability, Unavailability and Probability of Failure on Demand.....	26
2.7 Hazard and Risk-Related Terms.....	27
2.8 Choosing the Appropriate Parameter.....	28
Exercises	30
<i>Chapter 3: A Cost-Effective Approach to Quality, Reliability and Safety</i>	31
3.1 Reliability and Optimum Cost.....	31
3.2 Costs and Safety	35
3.2.1 The Need for Optimization	35
3.2.2 Costs and Savings Involved with Safety Engineering	35
3.3 The Cost of Quality	36

Part 2: Interpreting Failure Rates.....	41
Chapter 4: Realistic Failure Rates and Prediction Confidence.....	43
4.1 Data Accuracy	43
4.2 Sources of Data.....	45
4.2.1 Electronic Failure Rates	46
4.2.2 Other General Data Collections	48
4.2.3 Some Older Sources	50
4.3 Data Ranges.....	50
4.3.1 Using the Ranges.....	52
4.4 Confidence Limits of Prediction.....	54
4.5 Manufacturers' Data (Warranty Claims).....	56
4.6 Overall Conclusions	57
Chapter 5: Interpreting Data and Demonstrating Reliability.....	59
5.1 The Four Cases	59
5.2 Inference and Confidence Levels.....	59
5.3 The Chi-Square Test.....	61
5.4 Understanding the Method in More Detail	64
5.5 Double-Sided Confidence Limits	65
5.6 Reliability Demonstration.....	65
5.7 Sequential Testing	70
5.8 Setting Up Demonstration Tests.....	71
Exercises	72
Chapter 6: Variable Failure Rates and Probability Plotting.....	73
6.1 The Weibull Distribution.....	73
6.2 Using the Weibull Method	75
6.2.1 Curve Fitting to Interpret Failure Data.....	75
6.2.2 Manual Plotting	77
6.2.3 Using the COMPARE Computer Tool.....	80
6.2.4 Significance of the Result.....	81
6.2.5 Optimum Preventive Replacement.....	83
6.3 More Complex Cases of the Weibull Distribution	83
6.4 Continuous Processes	84
Exercises	85
PART 3: Predicting Reliability and Risk.....	87
Chapter 7: Basic Reliability Prediction Theory.....	89
7.1 Why Predict RAMS?	89
7.2 Probability Theory	90
7.2.1 The Multiplication Rule	90
7.2.2 The Addition Rule.....	90
7.2.3 The Binomial Theorem	91
7.2.4 Bayes Theorem.....	92

7.3 Reliability of Series Systems	93
7.4 Redundancy Rules	94
7.4.1 General Types of Redundant Configuration.....	94
7.4.2 Full Active Redundancy (Without Repair)	94
7.4.3 Partial Active Redundancy (Without Repair)	96
7.4.4 Conditional Active Redundancy	97
7.4.5 Standby Redundancy	98
7.4.6 Load Sharing	100
7.5 General Features of Redundancy	100
7.5.1 Incremental Improvement	100
7.5.2 Further Comparisons of Redundancy.....	102
7.5.3 Redundancy and Cost.....	103
Exercises	103

Chapter 8: Methods of Modeling 105

8.1 Block Diagrams and Repairable Systems.....	105
8.1.1 Reliability Block Diagrams	105
8.1.2 Repairable Systems (Revealed Failures).....	107
8.1.3 Repairable Systems (Unrevealed Failures)	110
8.1.4 Systems With Cold Standby Units and Repair.....	112
8.1.5 Modeling Repairable Systems with Both Revealed and Unrevealed Failures	112
8.1.6 Allowing for imperfect proof tests	113
8.1.7 Conventions for Labeling ‘Dangerous’, ‘Safe’, Revealed and Unrevealed Failures	113
8.2 Common Cause (Dependent) Failure	114
8.2.1 What is CCF?	114
8.2.2 Types of CCF Model.....	115
8.2.3 The BETAPLUS Model.....	117
8.3 Fault Tree Analysis.....	122
8.3.1 The Fault Tree	122
8.3.2 Calculations	123
8.3.3 Cutsets	126
8.3.4 Computer Tools.....	126
8.3.5 Allowing for Common Cause Failure	130
8.3.6 Fault Tree Analysis in Design.....	130
8.3.7 A Cautionary Note (Illogical Trees).....	130
8.4 Event Tree Diagrams	132
8.4.1 Why Use Event Trees?.....	132
8.4.2 The Event Tree Model.....	132
8.4.3 Quantification	134
8.4.4 Differences	134
8.4.5 Feedback Loops.....	135

Chapter 9: Quantifying the Reliability Models.....	137
9.1 The Reliability Prediction Method	137
9.2 Allowing for Diagnostic Intervals	139
9.2.1 Establishing Diagnostic Coverage	139
9.2.2 Modelling Diagnostic Coverage.....	139
9.2.3 Partial Stroke Testing	140
9.2.4 Safe Failure Fraction	141
9.3 FMEDA (Failure Mode and Diagnostic Analysis).....	142
9.4 Human Factors.....	145
9.4.1 Background	145
9.4.2 Models.....	145
9.4.3 HEART (Human Error Assessment and Reduction Technique)	146
9.4.4 THERP (Technique for Human Error Rate Prediction)	148
9.4.5 TESEO (Empirical Technique to Estimate Operator Errors)	148
9.4.6 Other Methods.....	149
9.4.7 Human Error Probabilities.....	149
9.4.8 Trends in Rigor of Assessment	151
9.5 Simulation.....	152
9.5.1 The Technique.....	152
9.5.2 Some Packages.....	154
9.6 Comparing Predictions with Targets	158
Exercises.....	158
 Chapter 10: Risk Assessment (QRA).....	 159
10.1 Frequency and Consequence	159
10.2 Perception of Risk, ALARP and Cost per Life Saved.....	160
10.2.1 Maximum Tolerable Risk (Individual Risk)	160
10.2.2 Maximum Tolerable Failure Rate	161
10.2.3 ALARP and Cost Per Life Saved.....	163
10.2.4 Societal Risk.....	167
10.2.5 Production/Damage Loss	170
10.2.6 Environmental Loss.....	170
10.3 Hazard Identification	171
10.3.1 HAZOP.....	171
10.3.2 HAZID	175
10.3.3 HAZAN (Consequence Analysis).....	175
10.4 Factors to Quantify	176
10.4.1 Reliability	176
10.4.2 Lightning and Thunderstorms	176
10.4.3 Aircraft Impact	178
10.4.4 Earthquake.....	179
10.4.5 Meteorological Factors.....	181
10.4.6 Other Consequences.....	181

PART 4: Achieving Reliability and Maintainability	183
<i>Chapter 11: Design and Assurance Techniques.....</i>	185
11.1 Specifying and Allocating the Requirement.....	185
11.2 Stress Analysis.....	186
11.3 Environmental Stress Protection	190
11.4 Failure Mechanisms.....	191
11.4.1 Types of Failure Mechanism.....	191
11.4.2 Failures in Semiconductor Components	192
11.4.3 Discrete Components	193
11.5 Complexity and Parts.....	193
11.5.1 Reduction of Complexity	193
11.5.2 Part Selection.....	194
11.5.3 Redundancy.....	195
11.6 Burn-In and Screening.....	195
11.7 Maintenance Strategies.....	196
<i>Chapter 12: Design Review, Test and Reliability Growth.....</i>	197
12.1 Review Techniques.....	197
12.2 Categories of Testing.....	198
12.2.1 Environmental Testing	199
12.2.2 Marginal Testing	200
12.2.3 High-Reliability Testing.....	201
12.2.4 Testing for Packaging and Transport	201
12.2.5 Multiparameter Testing	202
12.2.6 Step-Stress Testing	203
12.3 Reliability Growth Modeling.....	205
12.3.1 The CUSUM Technique.....	205
12.3.2 Duane Plots	206
Exercises	208
<i>Chapter 13: Field Data Collection and Feedback.....</i>	209
13.1 Reasons for Data Collection	209
13.2 Information and Difficulties	209
13.3 Times to Failure.....	211
13.4 Spreadsheets and Databases	212
13.5 Best Practice and Recommendations.....	214
13.6 Analysis and Presentation of Results.....	215
13.7 Manufacturers' data	216
13.8 Anecdotal Data	217
13.9 Examples of Failure Report Forms.....	217
13.10 No-Fault-Found (NFF)	217
<i>Chapter 14: Factors Influencing Down Time</i>	221
14.1 Key Design Areas.....	221
14.1.1 Access.....	221
14.1.2 Adjustment	221

14.1.3	Built-In Test Equipment.....	222
14.1.4	Circuit Layout and Hardware Partitioning	222
14.1.5	Connections	223
14.1.6	Displays and Indicators	224
14.1.7	Handling, Human and Ergonomic Factors	225
14.1.8	Identification.....	226
14.1.9	Interchangeability	226
14.1.10	Least Replaceable Assembly	227
14.1.11	Mounting	227
14.1.12	Component Part Selection	227
14.1.13	Redundancy	228
14.1.14	Safety.....	228
14.1.15	Software	228
14.1.16	Standardization.....	229
14.1.17	Test Points	229
14.2	Maintenance Strategies and Handbooks	229
14.2.1	Organization of Maintenance Resources.....	230
14.2.2	Maintenance Procedures	231
14.2.3	Tools and Test Equipment.....	232
14.2.4	Personnel Considerations	233
14.2.5	Maintenance Manuals	234
14.2.6	Spares Provisioning.....	236
14.2.7	Logistics	242
14.2.8	The User and the Designer	242
14.2.9	Computer Aids to Maintenance.....	243
Chapter 15:	<i>Predicting and Demonstrating Repair Times</i>	245
15.1	Prediction Methods	245
15.1.1	US Military Handbook 472 – Procedure 3	246
15.1.2	Checklist – Mil 472 – Procedure 3.....	247
15.1.3	Using a Weighted Sample	254
15.2	Demonstration Plans	254
15.2.1	Demonstration Risks	254
15.2.2	US Military Standard 471A (1973).....	255
15.2.3	Data Collection.....	257
Chapter 16:	<i>Quantified Reliability Centered Maintenance.....</i>	259
16.1	What is QRCM?	259
16.2	The QRCM Decision Process.....	260
16.3	Optimum Replacement (Discard).....	260
16.4	Optimum Spares	263
16.5	Optimum Proof Test	265
16.6	Condition Monitoring	266
Chapter 17:	<i>Systematic Failures, Especially Software</i>	269
17.1	Random versus Systematic Failures	269
17.2	Software-related Failures.....	270

17.3	Software Failure Modeling	273
17.4	Software Quality Assurance (Life Cycle Activities)	274
17.4.1	Organization of Software QA	275
17.4.2	Documentation Controls	275
17.4.3	Programming (Coding) Standards	278
17.4.4	Fault-Tolerant Design Features	279
17.4.5	Reviews	280
17.4.6	Integration and Test	280
17.5	Modern/Formal Methods	281
17.5.1	Requirements Specification and Design	282
17.5.2	Static Analysis	283
17.5.3	Test Beds	285
17.6	Software Checklists	285
17.6.1	Organization of Software QA	285
17.6.2	Documentation Controls	286
17.6.3	Programming Standards	286
17.6.4	Design Features	287
17.6.5	Code Inspections and Walkthroughs	288
17.6.6	Integration and Test	289
PART 5: Legal, Management and Safety Considerations		291
<i>Chapter 18: Project Management and Competence</i>		<i>293</i>
18.1	Setting Objectives and Making Specifications	293
18.2	Planning, Feasibility and Allocation	294
18.3	Program Activities	295
18.4	Responsibilities and Competence	297
18.5	Functional Safety Capability	299
18.6	Standards and Guidance Documents	300
<i>Chapter 19: Contract Clauses and Their Pitfalls.....</i>		<i>303</i>
19.1	Essential Areas	303
19.1.1	Definitions	304
19.1.2	Environment	305
19.1.3	Maintenance Support	305
19.1.4	Demonstration and Prediction	306
19.1.5	Liability	307
19.2	Other Areas	308
19.2.1	Reliability and Maintainability Program	308
19.2.2	Reliability and Maintainability Analysis	308
19.2.3	Storage	308
19.2.4	Design Standards	309
19.2.5	Safety-Related Equipment	309
19.3	Pitfalls	310
19.3.1	Definitions	310
19.3.2	Repair Time	310

19.3.3 Statistical Risks	310
19.3.4 Quoted Specifications.....	310
19.3.5 Environment	311
19.3.6 Liability	311
19.3.7 In Summary	311
19.4 Penalties	311
19.4.1 Apportionment of Costs During Guarantee	311
19.4.2 Payment According to Down Time.....	313
19.4.3 In Summary	313
19.5 Subcontracted Reliability Assessments	314
Chapter 20: Product Liability and Safety Legislation	317
20.1 The General Situation	317
20.1.1 Contract Law	317
20.1.2 Common Law	318
20.1.3 Statute Law.....	318
20.1.4 In Summary	319
20.2 Strict Liability	319
20.2.1 Concept.....	319
20.2.2 Defects.....	319
20.3 The Consumer Protection Act 1987	320
20.3.1 Background	320
20.3.2 Provisions of the Act	320
20.4 Health and Safety at Work Act 1974.....	321
20.4.1 Scope	321
20.4.2 Duties	321
20.4.3 Concessions	321
20.4.4 Responsibilities	321
20.4.5 European Community Legislation	322
20.4.6 Management of Health and Safety at Work Regulations 1992.....	322
20.4.7 COSHH	322
20.4.8 REACH	323
20.5 Insurance and Product Recall	323
20.5.1 The Effect of Product Liability Trends	323
20.5.2 Some Critical Areas	324
20.5.3 Areas of Cover	324
20.5.4 Product Recall	324
Chapter 21: Major Incident Legislation	327
21.1 History of Major Incidents.....	327
21.2 Development of major incident legislation.....	328
21.3 Safety reports	331
21.4 Offshore Safety Cases.....	334
21.5 Problem Areas	336
21.6 Rail.....	337
21.7 Corporate Manslaughter and Corporate Homicide.....	337

Chapter 22: Integrity of Safety-Related Systems	339
22.1 Safety-Related or Safety-Critical?	339
22.2 Safety-Integrity Levels (SILs)	340
22.2.1 Targets	340
22.2.2 Assessing Equipment Against the Targets	344
22.3 Programable electronic systems (PESs)	347
22.4 Current guidance.....	347
22.4.1 IEC International Standard 61508 (2010): <i>Functional safety of electrical/electronic/programmable electronic safety-related systems: 7 parts</i>	348
22.4.2 IEC International Standard 61511: <i>Functional safety – safety instrumented systems for the process industry sector</i>	348
22.4.3 Institution of Gas Engineers and Managers IGEN/SR/15: <i>Programmable equipment in safety-related applications – 5th edition</i>	348
22.4.4 European Standard EN 50126: <i>Railway applications – the specification and demonstration of dependability, reliability, maintainability and safety (RAMS)</i>	348
22.4.5 UK Defence Standard 00-56 (Issue 3.0): <i>Safety management requirements for defence systems</i>	349
22.4.6 RTCA DO-178B/(EUROCAE ED-12B): Software considerations in airborne systems and equipment certification	349
22.4.7 Documents related to machinery	349
22.4.8 Other industry sectors.....	350
22.5 Framework for Certification	350
22.5.1 Self-certification	350
22.5.2 Third-party assessment.....	350
22.5.3 Use of a Certifying Body	351
Chapter 23: A Case Study: The Datamet Project	353
23.1 Introduction	353
23.2 The Datamet Concept	353
23.3 The Contract	356
23.4 Detailed Design	357
23.5 Syndicate Study	358
23.6 Hints.....	358
Chapter 24: A Case Study: Gas Detection System	359
24.1 Safety-Integrity Target.....	359
24.2 Random Hardware Failures	360
24.3 ALARP	362
24.4 Architectures.....	363
24.5 Life-Cycle Activities	364
24.6 Functional Safety Capability	364

Chapter 25: A Case Study: Pressure Control System	365
25.1 The Unprotected System.....	365
25.2 Protection System	366
25.3 Assumptions	367
25.4 Reliability Block Diagram.....	367
25.5 Failure Rate Data	368
25.6 Quantifying the Model.....	368
25.7 Proposed Design and Maintenance Modifications	369
25.8 Modeling Common Cause Failure (Pressure Transmitters)	369
25.9 Quantifying the Revised Model.....	370
25.10 ALARP.....	370
25.11 Architectural Constraints.....	371
Chapter 26: Helicopter Incidents and Risk Assessment.....	373
26.1 Helicopter Incidents.....	373
26.2 Risk Assessment - Flootation Equipment.....	375
26.2.1 Assessment of the Scenario.....	375
26.2.2 ALARP.....	375
26.3 Effect of Pilot Experience on Incident Rate	377
Appendix 1: Glossary.....	379
A1.1 Terms Related to Failure.....	379
A1.1.1 Failure.....	379
A1.1.2 Failure Mode	379
A1.1.3 Failure Mechanism	379
A1.1.4 Failure Rate	380
A1.1.5 Mean Time Between Failures and Mean Time to Fail	380
A1.1.6 Common Cause Failure	380
A1.1.7 Common Mode Failure	380
A1.1.8 Dangerous Failure	380
A1.1.9 Safe Failure.....	380
A1.2 Reliability Terms	381
A1.2.1 Reliability	381
A1.2.2 Redundancy	381
A1.2.3 Diversity	381
A1.2.4 Failure Mode and Effect Analysis.....	381
A1.2.5 FMEDA (Failure Mode Effect and Diagnostic Analysis).....	381
A1.2.6 Fault Tree Analysis	381
A1.2.7 Cause Consequence Analysis (Event Trees).....	381
A1.2.8 Reliability Growth.....	382
A1.2.9 Reliability Centered Maintenance	382
A1.3 Maintainability Terms.....	382
A1.3.1 Maintainability	382
A1.3.2 Mean Time to Repair (MTTR).....	382
A1.3.3 Repair Rate	382

A1.3.4	Repair Time	382
A1.3.5	Down Time	382
A1.3.6	Corrective Maintenance	383
A1.3.7	Preventive Maintenance	383
A1.3.8	Least Replaceable Assembly (LRA)	383
A1.3.9	Second-Line Maintenance	383
A1.3.10	Maximum Repair Time	383
A1.4	Terms Associated With Software	383
A1.4.1	Software	383
A1.4.2	Programmable Device	383
A1.4.3	High-Level Language	383
A1.4.4	Assembler	384
A1.4.5	Compiler	384
A1.4.6	Diagnostic Software	384
A1.4.7	Simulation	384
A1.4.8	Emulation	384
A1.4.9	Load Test	384
A1.4.10	Functional Test	384
A1.4.11	Software Error	384
A1.4.12	Bit Error Rate	385
A1.4.13	Automatic Test Equipment (ATE)	385
A1.4.14	Data Corruption	385
A1.5	Terms Related to Safety	385
A1.5.1	Hazard	385
A1.5.2	Major Hazard	385
A1.5.3	Hazard Analysis	385
A1.5.4	HAZOP	385
A1.5.5	LOPA	385
A1.5.6	Risk	386
A1.5.7	Consequence Analysis	386
A1.5.8	Safe Failure Fraction	386
A1.5.9	Safety-Integrity	386
A1.5.10	Safety-Integrity level	386
A1.5.11	ALARP (As Low as Reasonably Practicable)	386
A1.5.12	Cost Per Life Saved	386
A1.5.13	GDF (Gross Disproportionality Factor)	386
A1.5.14	FAFR (Fatal Accident Frequency)	387
A1.6	General Terms	387
A1.6.1	Availability (Steady State)	387
A1.6.2	Unavailability (PFD)	387
A1.6.3	Burn-In	387
A1.6.4	Confidence Interval	387
A1.6.5	Consumer's Risk	387
A1.6.6	Derating	387

A1.6.7 Ergonomics.....	387
A1.6.8 Mean.....	388
A1.6.9 Median.....	388
A1.6.10 PFD.....	388
A1.6.11 Producer's Risk	388
A1.6.12 Quality	388
A1.6.13 Random	388
A1.6.14 FRACAS	388
A1.6.15 RAMS.....	388
Appendix 2: Percentage Points of the Chi-Square Distribution	389
Appendix 3: Microelectronic Failure Rates.....	397
Appendix 4: General Failure Rates	399
Appendix 5: Failure Mode Percentages.....	407
Appendix 6: Human Error Probabilities.....	411
Appendix 7: Fatality Rates	415
Appendix 8: Answers to Exercises.....	417
Chapter 2.....	417
Chapter 5.....	417
Chapter 6.....	418
Chapter 7.....	418
Chapter 9.....	419
Notes	420
Chapter 12.....	421
Chapter 25.....	422
25.2 Protection System	422
25.4 Reliability Block Diagram	422
25.6 Quantifying the Model	422
25.7 Revised diagrams	423
25.9 Quantifying the revised Model.....	424
25.10 ALARP	425
25.11 Architectural Constraints	426
Appendix 9: Bibliography.....	427
Appendix 10: Scoring Criteria for BETAPLUS Common Cause Model	429
A10.1 Checklist and Scoring for Equipment Containing Programable Electronics	429
A10.2 Checklist and Scoring for Non-Programable Equipment	431
For Programable Electronics	433
For Sensors and Actuators	433

Appendix 11: Example of HAZOP.....	435
A11.1 Equipment Details	435
A11.2 HAZOP Worksheets	435
A11.3 Potential Consequences	435
Worksheet	437
Appendix 12: HAZID Checklist.....	439
Appendix 13: Markov Analysis of Redundant Systems	443
Appendix 14: Calculating the GDF.....	449
Index.....	451