

Contents

<i>Introduction to the Fourth Edition</i>	xi
<i>Acknowledgements</i>	xiii

Part One Understanding Reliability Parameters and Costs	1
1 The history of reliability and safety technology	3
1.1 Failure data	3
1.2 Hazardous failures	4
1.3 Reliability and risk prediction	5
1.4 Achieving reliability	7
1.5 Major activities	8
1.6 Contractual pressures	8
2 Understanding terms and jargon	10
2.1 Defining Failure and failure modes	10
2.2 Failure Rate and Mean Time Between Failures	12
2.3 Interrelationships of terms	14
2.4 The Bathtub Distribution	16
2.5 Down Time and Repair Time	17
2.6 Availability	21
2.7 Hazard and risk-related terms	21
2.8 Choosing the appropriate parameter	22
3 A cost-effective approach to quality, reliability and safety	24
3.1 The cost of quality	24
3.2 Reliability and cost	27
3.3 Costs and safety	29

Part Two Interpreting Failure Rates	33
4 Realistic failure rates	35
4.1 Data accuracy	35
4.2 Microelectronics data	37
4.3 Overall data	41
4.4 Sources of failure rate data	43
5 Interpreting data and demonstrating reliability	50
5.1 The four cases	50
5.2 Inference and confidence levels	50
5.3 The Chi-square Test	52
5.4 Double-sided confidence limits	54
5.5 Summarizing the Chi-square Test	55
5.6 Reliability demonstration	55
5.7 Sequential testing	60
5.8 Setting up demonstration tests	61
Exercises	62
6 Variable failure rates and probability plotting	63
6.1 The Weibull Distribution	63
6.2 Using the Weibull Method	66
6.3 More complex cases of the Weibull Distribution	68
6.4 Continuous processes	70
Exercises	71
Part Three Predicting Reliability and Risk	73
7 Essential reliability theory	75
7.1 Why predict?	75
7.2 Probability theory	76
7.3 Reliability of series systems	78
7.4 Redundancy rules	79
7.5 General features of redundancy	86
Exercises	89
8 Methods of modelling	90
8.1 Markov Analysis	90

Exercises	101
8.2 Fault Tree Analysis	102
8.3 Common mode effects	107
8.4 Cause consequence diagrams	115
8.5 Simulation	119
8.6 Human factors	122
8.7 FMEA (Failure Mode and Effect Analysis)	126
9 Risk assessment	128
9.1 Frequency and consequence	128
9.2 Hazard identification	128
9.3 Factors to quantify	130
Part Four Achieving Reliability and Maintainability	135
10 Design and assurance techniques	137
10.1 Specifying and allocating the requirement	137
10.2 Stress analysis	138
10.3 Environmental stress protection	142
10.4 Failure mechanisms	143
10.5 Complexity and parts	145
10.6 Burn-in and screening	145
10.7 Maintenance strategies	150
11 Design review and test	152
11.1 Review techniques	152
11.2 Categories of testing	153
11.3 Reliability growth modelling	158
12 Field data collection and feedback	161
12.1 Reasons for data collection	161
12.2 Information and difficulties	161
12.3 Spreadsheets and databases	163
12.4 Analysis and presentation of results	164
12.5 Examples of failure report forms	166
13 Factors influencing down time	171
13.1 Key design areas	171
13.2 Maintenance strategies and handbooks	180

14 Predicting and demonstrating repair times	193
14.1 Prediction methods	193
14.2 Demonstration plans	204
15 Software quality/reliability	208
15.1 Programmable devices	208
15.2 Software failures	209
15.3 Software failure modelling	211
15.4 Software quality assurance	212
15.5 Modern/formal methods	219
15.6 Software checklists	221
Part Five Legal and Management Considerations	227
16 Project management	229
16.1 Setting objectives and specifications	229
16.2 Planning, feasibility and allocation	229
16.3 Programme activities	230
16.4 Responsibilities	232
16.5 Standards and guidance documents	232
17 Contract clauses and their pitfalls	234
17.1 Essential areas	234
17.2 Other areas	238
17.3 Pitfalls	239
17.4 Penalties	241
17.5 Subcontracted reliability assessments	243
17.6 Example	244
18 Product liability and safety legislation	246
18.1 The general situation	246
18.2 Strict liability	247
18.3 The Consumer Protection Act 1987	248
18.4 Health and Safety at Work Act 1974	249
18.5 Insurance and product recall	250
19 Safety-critical systems and major incidents	253
19.1 History of major incidents	253
19.2 Major incident legislation	254

19.3 Safety-critical systems	255
19.4 Current guidance	256
20 A case study	260
20.1 Introduction	260
20.2 The DATAMET Concept	260
20.3 Formation of the project group	263
20.4 Reliability requirements	263
20.5 First design review	265
20.6 Design and development	269
20.7 Syndicate study	270
20.8 Hints	270
Appendix 1 Glossary	271
Appendix 2 Percentage points of the Chi-square Distribution	280
Appendix 3 Microelectronics failure rates	284
Appendix 4 General failure rates	286
Appendix 5 Failure mode percentages	294
Appendix 6 Human error rates	297
Appendix 7 Fatality rates	299
Appendix 8 Answers to exercises	301
Appendix 9 Bibliography	305
Appendix 10 Software packages	308
Appendix 11 Simulation source code	311
Index	317

Fourth edition

Reliability Maintainability and Risk

Practical Methods for Engineers

David J. Smith
