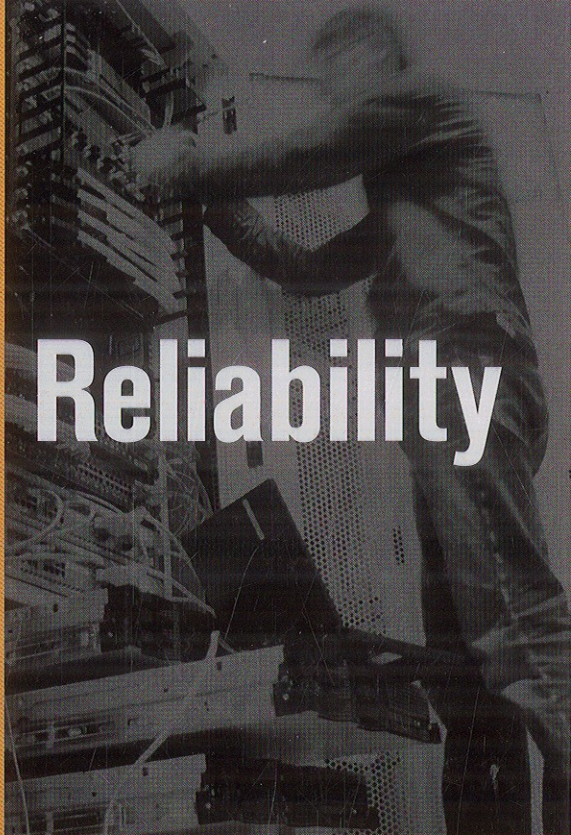
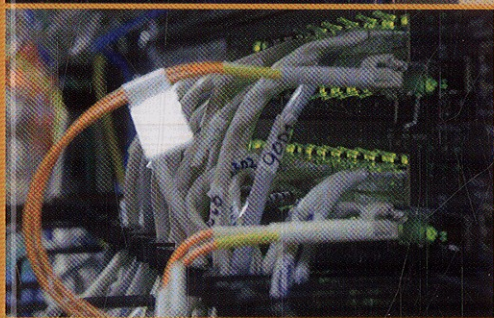
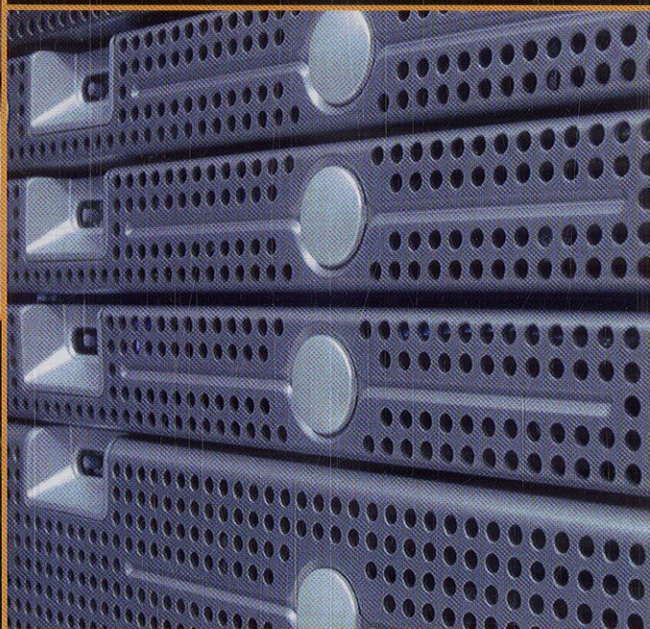
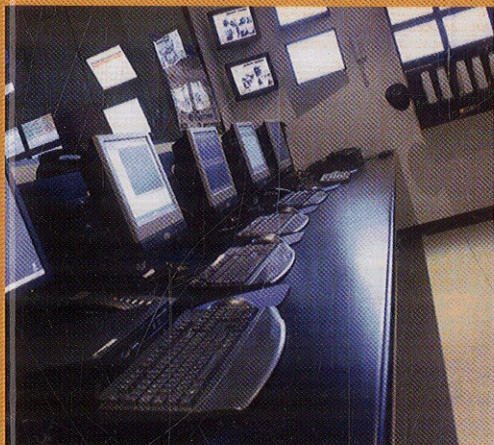


Design for Reliability

*Information and
Computer-Based
Systems*



ERIC BAUER



 **WILEY**

 **IEEE**
IEEE PRESS

Contents

Figures	xiii
Tables	xv
Preface	xvii
Acknowledgments	xxi

Part One Reliability Basics

1. Reliability and Availability Concepts	3
1.1 Reliability and Availability	3
1.2 Faults, Errors, and Failures	5
1.3 Error Severity	6
1.4 Failure Recovery	7
1.5 Highly Available Systems	9
1.6 Quantifying Availability	12
1.7 Outage Attributability	14
1.8 Hardware Reliability	16
1.9 Software Reliability	22
1.10 Problems	28
1.11 For Further Study	29
2. System Basics	31
2.1 Hardware and Software	31
2.2 External Entities	35
2.3 System Management	37
2.4 System Outages	43
2.5 Service Quality	47
2.6 Total Cost of Ownership	49
2.7 Problems	56

3. What Can Go Wrong

57

3.1	Failures in the Real World	57
3.2	Eight-Ingredient Framework	59
3.3	Mapping Ingredients to Error Categories	63
3.4	Applying Error Categories	66
3.5	Error Category: Field-Replaceable Unit (FRU) Hardware	68
3.6	Error Category: Programming Errors	70
3.7	Error Category: Data Error	71
3.8	Error Category: Redundancy	73
3.9	Error Category: System Power	74
3.10	Error Category: Network	75
3.11	Error Category: Application Protocol	76
3.12	Error Category: Procedures	77
3.13	Summary	79
3.14	Problems	80
3.15	For Further Study	80

Part Two Reliability Concepts

4. Failure Containment and Redundancy

85

4.1	Units of Design	85
4.2	Failure Recovery Groups	91
4.3	Redundancy	92
4.4	Summary	96
4.5	Problems	97
4.6	For Further Study	97

5. Robust Design Principles

99

5.1	Robust Design Principles	99
5.2	Robust Protocols	101
5.3	Robust Concurrency Controls	103
5.4	Overload Control	103
5.5	Process, Resource, and Throughput Monitoring	108
5.6	Data Auditing	109
5.7	Fault Correlation	110
5.8	Failed Error Detection, Isolation, or Recovery	111
5.9	Geographic Redundancy	112
5.10	Security, Availability, and System Robustness	114
5.11	Procedural Considerations	119
5.12	Problems	130
5.13	For Further Study	130

6. Error Detection	131
6.1 Detecting Field-Replaceable Unit (FRU) Hardware Faults	131
6.2 Detecting Programming and Data Faults	132
6.3 Detecting Redundancy Failures	134
6.4 Detecting Power Failures	139
6.5 Detecting Networking Failures	141
6.6 Detecting Application Protocol Failures	142
6.7 Detecting Procedural Failures	144
6.8 Problems	144
6.9 For Further Study	144
7. Analyzing and Modeling Reliability and Robustness	145
7.1 Reliability Block Diagrams	145
7.2 Qualitative Model of Redundancy	147
7.3 Failure Mode and Effects Analysis	149
7.4 Availability Modeling	151
7.5 Planned Downtime	165
7.6 Problems	168
7.7 For Further Study	168
 Part Three Design for Reliability	
8. Reliability Requirements	171
8.1 Background	171
8.2 Defining Service Outages	172
8.3 Service Availability Requirements	175
8.4 Detailed Service Availability Requirements	177
8.5 Service Reliability Requirements	180
8.6 Triangulating Reliability Requirements	181
8.7 Problems	182
9. Reliability Analysis	185
9.1 Step 1: Enumerate Recoverable Modules	186
9.2 Step 2: Construct Reliability Block Diagrams	191
9.3 Step 3: Characterize Impact of Recovery	193
9.4 Step 4: Characterize Impact of Procedures	198
9.5 Step 5: Audit Adequacy of Automatic Failure Detection and Recovery	200
9.6 Step 6: Consider Failures of Robustness Mechanisms	201
9.7 Step 7: Prioritizing Gaps	202
9.8 Reliability of Sourced Modules and Components	202
9.9 Problems	206

10. Reliability Budgeting and Modeling	207
10.1 Downtime Categories	208
10.2 Service Downtime Budget	209
10.3 Availability Modeling	212
10.4 Update Downtime Budget	213
10.5 Robustness Latency Budgets	215
10.6 Problems	218
11. Robustness and Stability Testing	219
11.1 Robustness Testing	219
11.2 Context of Robustness Testing	220
11.3 Factoring Robustness Testing	221
11.4 Robustness Testing in the Development Process	222
11.5 Robustness Testing Techniques	223
11.6 Selecting Robustness Test Cases	232
11.7 Analyzing Robustness Test Results	233
11.8 Stability Testing	234
11.9 Release Criteria	240
11.10 Problems	243
12. Closing the Loop	245
12.1 Analyzing Field Outage Events	245
12.2 Reliability Roadmapping	255
12.3 Problems	260
13. Design for Reliability Case Study	263
13.1 System Context	263
13.2 System Reliability Requirements	268
13.3 Reliability Analysis	270
13.4 Downtime Budgeting	283
13.5 Availability Modeling	284
13.6 Reliability Roadmap	286
13.7 Robustness Testing	287
13.8 Stability Testing	289
13.9 Reliability Review	290
13.10 Reliability Report	291
13.11 Release Criteria	292
13.12 Field Data Analysis	293
14. Conclusion	295
14.1 Overview of Design for Reliability	295
14.2 Concluding Remarks	299
14.3 Problems	300

15. Appendix: Assessing Design for Reliability Diligence 301

15.1	Assessment Methodology	302
15.2	Reliability Requirements	304
15.3	Reliability Analysis	306
15.4	Reliability Modeling and Budgeting	307
15.5	Robustness Testing	308
15.6	Stability Testing	310
15.7	Release Criteria	311
15.8	Field Availability	312
15.9	Reliability Roadmap	313
15.10	Hardware Reliability	313

Abbreviations 315**References 317****Photo Credits 319****About the Author 321****Index 323**