

# Contents

Foreword	xi
Preface	xiii
Acknowledgements	xvii
About the Authors	xix

## 1 Preliminaries 1

1.1 Fault Classification	2
1.2 Types of Redundancy	3
1.3 Basic Measures of Fault Tolerance	4
1.3.1 Traditional Measures	5
1.3.2 Network Measures	6
1.4 Outline of This Book	7
1.5 Further Reading	9
References	10

## 2 Hardware Fault Tolerance 11

2.1 The Rate of Hardware Failures	11
2.2 Failure Rate, Reliability, and Mean Time to Failure	13
2.3 Canonical and Resilient Structures	15
2.3.1 Series and Parallel Systems	16
2.3.2 Non-Series/Parallel Systems	17
2.3.3 <i>M</i> -of- <i>N</i> Systems	20
2.3.4 Voters	23
2.3.5 Variations on <i>N</i> -Modular Redundancy	23
2.3.6 Duplex Systems	27
2.4 Other Reliability Evaluation Techniques	30
2.4.1 Poisson Processes	30
2.4.2 Markov Models	33

2.5	Fault-Tolerance Processor-Level Techniques	36
2.5.1	Watchdog Processor	37
2.5.2	Simultaneous Multithreading for Fault Tolerance	39
2.6	Byzantine Failures	41
2.6.1	Byzantine Agreement with Message Authentication	46
2.7	Further Reading	48
2.8	Exercises	48
	References	53

### **3 Information Redundancy 55**

3.1	Coding	56
3.1.1	Parity Codes	57
3.1.2	Checksum	64
3.1.3	<i>M-of-N</i> Codes	65
3.1.4	Berger Code	66
3.1.5	Cyclic Codes	67
3.1.6	Arithmetic Codes	74
3.2	Resilient Disk Systems	79
3.2.1	RAID Level 1	79
3.2.2	RAID Level 2	81
3.2.3	RAID Level 3	82
3.2.4	RAID Level 4	83
3.2.5	RAID Level 5	84
3.2.6	Modeling Correlated Failures	84
3.3	Data Replication	88
3.3.1	Voting: Non-Hierarchical Organization	89
3.3.2	Voting: Hierarchical Organization	95
3.3.3	Primary-Backup Approach	96
3.4	Algorithm-Based Fault Tolerance	99
3.5	Further Reading	101
3.6	Exercises	102
	References	106

### **4 Fault-Tolerant Networks 109**

4.1	Measures of Resilience	110
4.1.1	Graph-Theoretical Measures	110
4.1.2	Computer Networks Measures	111
4.2	Common Network Topologies and Their Resilience	112
4.2.1	Multistage and Extra-Stage Networks	112
4.2.2	Crossbar Networks	119
4.2.3	Rectangular Mesh and Interstitial Mesh	121
4.2.4	Hypercube Network	124

4.2.5	Cube-Connected Cycles Networks	128
4.2.6	Loop Networks	130
4.2.7	Ad hoc Point-to-Point Networks	132
4.3	Fault-Tolerant Routing	135
4.3.1	Hypercube Fault-Tolerant Routing	136
4.3.2	Origin-Based Routing in the Mesh	138
4.4	Further Reading	141
4.5	Exercises	142
	References	145

## 5 Software Fault Tolerance 147

5.1	Acceptance Tests	148
5.2	Single-Version Fault Tolerance	149
5.2.1	Wrappers	149
5.2.2	Software Rejuvenation	152
5.2.3	Data Diversity	155
5.2.4	Software Implemented Hardware Fault Tolerance (SIHFT)	157
5.3	<i>N</i> -Version Programming	160
5.3.1	Consistent Comparison Problem	161
5.3.2	Version Independence	162
5.4	Recovery Block Approach	169
5.4.1	Basic Principles	169
5.4.2	Success Probability Calculation	169
5.4.3	Distributed Recovery Blocks	171
5.5	Preconditions, Postconditions, and Assertions	173
5.6	Exception-Handling	173
5.6.1	Requirements from Exception-Handlers	174
5.6.2	Basics of Exceptions and Exception-Handling	175
5.6.3	Language Support	177
5.7	Software Reliability Models	178
5.7.1	Jelinski–Moranda Model	178
5.7.2	Littlewood–Verrall Model	179
5.7.3	Musa–Okumoto Model	180
5.7.4	Model Selection and Parameter Estimation	182
5.8	Fault-Tolerant Remote Procedure Calls	182
5.8.1	Primary-Backup Approach	182
5.8.2	The Circus Approach	183
5.9	Further Reading	184
5.10	Exercises	186
	References	188

<b>6</b>	<b>Checkpointing</b>	<b>193</b>
6.1	What is Checkpointing?	195
6.1.1	Why is Checkpointing Nontrivial?	197
6.2	Checkpoint Level	197
6.3	Optimal Checkpointing—An Analytical Model	198
6.3.1	Time Between Checkpoints—A First-Order Approximation	200
6.3.2	Optimal Checkpoint Placement	201
6.3.3	Time Between Checkpoints—A More Accurate Model	202
6.3.4	Reducing Overhead	204
6.3.5	Reducing Latency	205
6.4	Cache-Aided Rollback Error Recovery (CARER)	206
6.5	Checkpointing in Distributed Systems	207
6.5.1	The Domino Effect and Livelock	209
6.5.2	A Coordinated Checkpointing Algorithm	210
6.5.3	Time-Based Synchronization	211
6.5.4	Diskless Checkpointing	212
6.5.5	Message Logging	213
6.6	Checkpointing in Shared-Memory Systems	217
6.6.1	Bus-Based Coherence Protocol	218
6.6.2	Directory-Based Protocol	219
6.7	Checkpointing in Real-Time Systems	220
6.8	Other Uses of Checkpointing	223
6.9	Further Reading	223
6.10	Exercises	224
	References	226
<b>7</b>	<b>Case Studies</b>	<b>229</b>
7.1	NonStop Systems	229
7.1.1	Architecture	229
7.1.2	Maintenance and Repair Aids	233
7.1.3	Software	233
7.1.4	Modifications to the NonStop Architecture	235
7.2	Stratus Systems	236
7.3	Cassini Command and Data Subsystem	238
7.4	IBM G5	241
7.5	IBM Sysplex	242
7.6	Itanium	244
7.7	Further Reading	246
	References	247
<b>8</b>	<b>Defect Tolerance in VLSI Circuits</b>	<b>249</b>
8.1	Manufacturing Defects and Circuit Faults	249

8.2	Probability of Failure and Critical Area	251
8.3	Basic Yield Models	253
8.3.1	The Poisson and Compound Poisson Yield Models	254
8.3.2	Variations on the Simple Yield Models	256
8.4	Yield Enhancement Through Redundancy	258
8.4.1	Yield Projection for Chips with Redundancy	259
8.4.2	Memory Arrays with Redundancy	263
8.4.3	Logic Integrated Circuits with Redundancy	270
8.4.4	Modifying the Floorplan	272
8.5	Further Reading	276
8.6	Exercises	277
	References	281
<b>9</b>	<b>Fault Detection in Cryptographic Systems</b>	<b>285</b>
9.1	Overview of Ciphers	286
9.1.1	Symmetric Key Ciphers	286
9.1.2	Public Key Ciphers	295
9.2	Security Attacks Through Fault Injection	296
9.2.1	Fault Attacks on Symmetric Key Ciphers	297
9.2.2	Fault Attacks on Public (Asymmetric) Key Ciphers	298
9.3	Countermeasures	299
9.3.1	Spatial and Temporal Duplication	300
9.3.2	Error-Detecting Codes	300
9.3.3	Are These Countermeasures Sufficient?	304
9.3.4	Final Comment	307
9.4	Further Reading	307
9.5	Exercises	307
	References	308
<b>10</b>	<b>Simulation Techniques</b>	<b>311</b>
10.1	Writing a Simulation Program	311
10.2	Parameter Estimation	315
10.2.1	Point Versus Interval Estimation	315
10.2.2	Method of Moments	316
10.2.3	Method of Maximum Likelihood	318
10.2.4	The Bayesian Approach to Parameter Estimation	322
10.2.5	Confidence Intervals	324
10.3	Variance Reduction Methods	328
10.3.1	Antithetic Variables	328
10.3.2	Using Control Variables	330
10.3.3	Stratified Sampling	331
10.3.4	Importance Sampling	333

10.4	Random Number Generation	341
10.4.1	Uniformly Distributed Random Number Generators	342
10.4.2	Testing Uniform Random Number Generators	345
10.4.3	Generating Other Distributions	349
10.5	Fault Injection	355
10.5.1	Types of Fault Injection Techniques	356
10.5.2	Fault Injection Application and Tools	358
10.6	Further Reading	358
10.7	Exercises	359
	References	363
	Subject Index	365