

**HERBERT HECHT**



**SYSTEMS RELIABILITY  
AND FAILURE PREVENTION**

# Contents

<b>1</b>	<b><u>Introduction</u></b>	<b>1</b>
<b>2</b>	<b><u>Essentials of Reliability Engineering</u></b>	<b>5</b>
2.1	The Exponential Distribution	5
2.2	Parameter Estimation	8
2.3	Reliability Block Diagrams	9
2.4	State Transition Methods	12
2.5	The Devil Is In the Details	16
2.5.1	Numerator of the Failure Rate Expression	16
2.5.2	Denominator of the Failure Rate Expression	16
2.5.3	Repair Rate Formulations	18
2.6	Chapter Summary	19
	References	19
<b>3</b>	<b><u>Organizational Causes of Failures</u></b>	<b>21</b>
3.1	Failures Are Not Inevitable	21
3.2	Thoroughly Documented Failures	22
3.2.1	Mars Spacecraft Failures	23
3.2.2	Space Shuttle Columbia Accident	26

3.2.3	Chernobyl	27
3.2.4	Aviation Accidents	29
3.2.5	Telecommunications	31
3.3	Common Threads	32
	References	34
<b>4</b>	<b>Analytical Approaches to Failure Prevention</b>	<b>37</b>
4.1	Failure Modes and Effects Analysis	38
4.1.1	Overview of FMEA Worksheets	38
4.1.2	Organization of an FMEA Report	41
4.1.3	Alternative FMEA Approaches	46
4.1.4	FMEA as a Plan for Action	49
4.2	Sneak Circuit Analysis	52
4.2.1	Basics of SCA	52
4.2.2	Current SCA Techniques	55
4.3	Fault Tree Analysis	56
4.3.1	Basics of FTA	57
4.3.2	Example of FTA	58
4.4	Chapter Summary	61
	References	61
<b>5</b>	<b>Testing to Prevent Failures</b>	<b>63</b>
5.1	Reliability Demonstration	64
5.2	Design Margins	66
5.3	Reliability Relevance of Tests During Development	70
5.4	Reliability Relevance of Postdevelopment Tests	76
5.5	In-Service Testing	82
5.6	Chapter Summary	85
	References	85
<b>6</b>	<b>Redundancy Techniques</b>	<b>87</b>
6.1	Introduction to Redundancy at the Component Level	87

---

6.2	Dual Redundancy	91
6.2.1	Static and Dynamic Redundancy	91
6.2.2	Identical Versus Diverse Alternates	95
6.2.3	Active Versus Dormant Alternates	97
6.3	Triple Redundancy	98
6.3.1	TMR	99
6.3.2	Pair-and-Spare Redundancy	101
6.4	Higher-Order Redundant Configurations	102
6.5	Other Forms of Redundancy	105
6.5.1	Temporal Redundancy	105
6.5.2	Analytical Redundancy	105
6.6	Chapter Summary	106
	References	107
<b>7</b>	<b>Software Reliability</b>	<b>109</b>
7.1	The Nature and Statistical Measures of Software Failures	109
7.2	Software Testing	114
7.3	Failure Prevention Practices	120
7.3.1	Requirements	120
7.3.2	Test	122
7.3.3	UML-Based Software Development	126
7.4	Software Fault Tolerance	129
7.5	Software Reliability Models	132
7.6	Chapter Summary	132
	References	133
<b>8</b>	<b>Failure Prevention in the Life Cycle</b>	<b>137</b>
8.1	Life-Cycle Format and Terminology	138
8.2	Reliability Issues in Life-Cycle Phases	141
8.3	The Reliability Program Plan	148
8.4	Reviews and Audits	152

---

8.5	Monitoring of Critical Items	157
8.5.1	Monitoring Purchased Items	158
8.5.2	In-House Monitoring for Reliability Attainment	159
8.6	Chapter Summary	163
	References	164
<b>9</b>	<b>Cost of Failure and Failure Prevention</b>	<b>167</b>
9.1	Optimum Reliability	167
9.2	Time Considerations of Expenditures	170
9.3	Estimation of Cost Elements	174
9.4	A Generic Cost of Reliability Model	177
9.5	Chapter Summary	181
	References	182
<b>10</b>	<b>Cost Trade-offs</b>	<b>183</b>
10.1	Reliability Improvement to Meet QoS Requirements	183
10.1.1	Analysis of the Commercial Power Supply	184
10.1.2	Server Equipment Availability	187
10.2	Increasing Maintenance Effectiveness	192
10.3	Replacement of Communication Satellites	195
10.4	Chapter Summary	197
	References	198
<b>11</b>	<b>Applications</b>	<b>199</b>
11.1	Power Supply for Ground Communications	200
11.1.1	Framework for Power Supply Selection	200
11.1.2	Power Supply Alternatives	201
11.1.3	Evaluation of Alternatives	208
11.2	Reliability of Aircraft Electronics Bay	210
11.2.1	Primary Power Supply	210
11.2.2	Safety Critical Loads	211

11.2.3	Partial Improvement of a Function	213
11.3	Spacecraft Attitude Determination	215
11.3.1	Orthogonal Gyro Configurations	215
11.3.2	Nonorthogonal Gyro Orientation	217
11.4	Chapter Summary	219
	Reference	219
	<b>About the Author</b>	<b>221</b>
	<b>Index</b>	<b>223</b>

---