

# Contents

<b>Contributors</b>	<b>xiii</b>
<b>Foreword</b>	<b>xv</b>
<b>Preface</b>	<b>xvii</b>
<b>Introduction: What You Will Learn</b>	<b>xix</b>
<b>1 Design for Reliability Paradigms</b>	<b>1</b>
<hr/>	
<i>Dev Raheja</i>	
Why Design for Reliability?	1
Reflections on the Current State of the Art	2
The Paradigms for Design for Reliability	4
Summary	13
References	13
<b>2 Reliability Design Tools</b>	<b>15</b>
<hr/>	
<i>Joseph A. Childs</i>	
Introduction	15
Reliability Tools	19
Test Data Analysis	31
Summary	34
References	35
<b>3 Developing Reliable Software</b>	<b>37</b>
<hr/>	
<i>Samuel Keene</i>	
Introduction and Background	37
Software Reliability: Definitions and Basic Concepts	40
Software Reliability Design Considerations	44
Operational Reliability Requires Effective Change Management	48
Execution-Time Software Reliability Models	48
Software Reliability Prediction Tools Prior to Testing	49
References	51

---

## **4 Reliability Models** **53**

---

*Louis J. Gullo*

Introduction	53
Reliability Block Diagram: System Modeling	56
Example of System Reliability Models Using RBDs	57
Reliability Growth Model	60
Similarity Analysis and Categories of a Physical Model	60
Monte Carlo Models	62
Markov Models	62
References	64

---

## **5 Design Failure Modes, Effects, and Criticality Analysis** **67**

---

*Louis J. Gullo*

Introduction to FMEA and FMECA	67
Design FMECA	68
Principles of FMECA-MA	71
Design FMECA Approaches	72
Example of a Design FMECA Process	74
Risk Priority Number	82
Final Thoughts	86
References	86

---

## **6 Process Failure Modes, Effects, and Criticality Analysis** **87**

---

*Joseph A. Childs*

Introduction	87
Principles of P-FMECA	87
Use of P-FMECA	88
What Is Required Before Starting	90
Performing P-FMECA Step by Step	91
Improvement Actions	98
Reporting Results	100
Suggestions for Additional Reading	101

---

## **7 FMECA Applied to Software Development** **103**

---

*Robert W. Stoddard*

Introduction	103
Scoping an FMECA for Software Development	104

FMECA Steps for Software Development	106
Important Notes on Roles and Responsibilities with Software FMECA	116
Lessons Learned from Conducting Software FMECA	117
Conclusions	119
References	120

## **8 Six Sigma Approach to Requirements Development** **121**

---

*Samuel Keene*

Early Experiences with Design of Experiments	121
Six Sigma Foundations	124
The Six Sigma Three-Pronged Initiative	126
The RASCI Tool	128
Design for Six Sigma	129
Requirements Development: The Principal Challenge to System Reliability	130
The GQM Tool	131
The Mind Mapping Tool	132
References	135

## **9 Human Factors in Reliable Design** **137**

---

*Jack Dixon*

Human Factors Engineering	137
A Design Engineer's Interest in Human Factors	138
Human-Centered Design	138
Human Factors Analysis Process	144
Human Factors and Risk	150
Human Error	150
Design for Error Tolerance	153
Checklists	154
Testing to Validate Human Factors in Design	154
References	154

## **10 Stress Analysis During Design to Eliminate Failures** **157**

---

*Louis J. Gullo*

Principles of Stress Analysis	157
Mechanical Stress Analysis or Durability Analysis	158
Finite Element Analysis	158
Probabilistic vs. Deterministic Methods and Failures	159

## Contents

How Stress Analysis Aids Design for Reliability	159
Derating and Stress Analysis	160
Stress vs. Strength Curves	161
Software Stress Analysis and Testing	166
Structural Reinforcement to Improve Structural Integrity	167
References	167

## **11 Highly Accelerated Life Testing** **169**

---

*Louis J. Gullo*

Introduction	169
Time Compression	173
Test Coverage	174
Environmental Stresses of HALT	175
Sensitivity to Stresses	176
Design Margin	178
Sample Size	180
Conclusions	180
Reference	181

## **12 Design for Extreme Environments** **183**

---

*Steven S. Austin*

Overview	183
Designing for Extreme Environments	183
Designing for Cold	184
Designing for Heat	186
References	191

## **13 Design for Trustworthiness** **193**

---

*Lawrence Bernstein and C. M. Yuhas*

Introduction	193
Modules and Components	196
Politics of Reuse	200
Design Principles	201
Design Constraints That Make Systems Trustworthy	204
Conclusions	210
References and Notes	211

## **14 Prognostics and Health Management Capabilities to Improve Reliability** **213**

---

*Louis J. Gullo*

Introduction	213
PHM Is Department of Defense Policy	216
Condition-Based Maintenance vs. Time-Based Maintenance	216
Monitoring and Reasoning of Failure Precursors	217
Monitoring Environmental and Usage Loads for Damage Modeling	218
Fault Detection, Fault Isolation, and Prognostics	218
Sensors for Automatic Stress Monitoring	220
References	221

## **15 Reliability Management** **223**

---

*Joseph A. Childs*

Introduction	223
Planning, Execution, and Documentation	229
Closing the Feedback Loop: Reliability Assessment, Problem Solving, and Growth	232
References	233

## **16 Risk Management, Exception Handling, and Change Management** **235**

---

*Jack Dixon*

Introduction to Risk	235
Importance of Risk Management	236
Why Many Risks Are Overlooked	237
Program Risk	239
Design Risk	241
Risk Assessment	242
Risk Identification	243
Risk Estimation	244
Risk Evaluation	245
Risk Mitigation	247
Risk Communication	248
Risk and Competitiveness	249
Risk Management in the Change Process	249

## Contents

Configuration Management	249
References	251

## **17 Integrating Design for Reliability with Design for Safety** **253**

---

*Brian Moriarty*

Introduction	253
Start of Safety Design	254
Reliability in System Safety Design	255
Safety Analysis Techniques	255
Establishing Safety Assessment Using the Risk Assessment Code Matrix	260
Design and Development Process for Detailed Safety Design	261
Verification of Design for Safety Includes Reliability	261
Examples of Design for Safety with Reliability Data	262
Final Thoughts	266
References	266

## **18 Organizational Reliability Capability Assessment** **267**

---

*Louis J. Gullo*

Introduction	267
The Benefits of IEEE 1624-2008	269
Organizational Reliability Capability	270
Reliability Capability Assessment	271
Design Capability and Performability	271
IEEE 1624 Scoring Guidelines	276
SEI CMMI Scoring Guidelines	277
Organizational Reliability Capability Assessment Process	278
Advantages of High Reliability	282
Conclusions	283
References	284