## Contents

**Brief Introduction**  xiii  
**Preface**  xv  

1  **Introduction**  1  
1.1  Fundamental Concepts and Principles of Fault-tolerance Techniques  1  
1.1.1  Fundamental Concepts  1  
1.1.2  Reliability Principles  4  
1.1.2.1  Reliability Metrics  4  
1.1.2.2  Reliability Model  6  
1.2  The Space Environment and Its Hazards for the Spacecraft Control Computer  9  
1.2.1  Introduction to Space Environment  9  
1.2.1.1  Solar Radiation  9  
1.2.1.2  Galactic Cosmic Rays (GCRs)  10  
1.2.1.3  Van Allen Radiation Belt  10  
1.2.1.4  Secondary Radiation  12  
1.2.1.5  Space Surface Charging and Internal Charging  12  
1.2.1.6  Summary of Radiation Environment  13  
1.2.1.7  Other Space Environments  14  
1.2.2  Analysis of Damage Caused by the Space Environment  14  
1.2.2.1  Total Ionization Dose (TID)  14  
1.2.2.2  Single Event Effect (SEE)  15  
1.2.2.3  Internal/surface Charging Damage Effect  20  
1.2.2.4  Displacement Damage Effect  20  
1.2.2.5  Other Damage Effect  20  
1.3  Development Status and Prospects of Fault Tolerance Techniques  21  
**References**  25
2 Fault-Tolerance Architectures and Key Techniques 29
2.1 Fault-tolerance Architecture 29
2.1.1 Module-level Redundancy Structures 30
2.1.2 Backup Fault-tolerance Structures 32
2.1.2.1 Cold-backup Fault-tolerance Structures 32
2.1.2.2 Hot-backup Fault-tolerance Structures 34
2.1.3 Triple-modular Redundancy (TMR) Fault-tolerance Structures 36
2.1.4 Other Fault-tolerance Structures 40
2.2 Synchronization Techniques 40
2.2.1 Clock Synchronization System 40
2.2.1.1 Basic Concepts and Fault Modes of the Clock Synchronization System 40
2.2.1.2 Clock Synchronization Algorithm 41
2.2.2 System Synchronization Method 52
2.2.2.1 The Real-time Multi-computer System Synchronization Method 52
2.2.2.2 System Synchronization Method with Interruption 56
2.3 Fault-tolerance Design with Hardware Redundancy 60
2.3.1 Universal Logic Model and Flow in Redundancy Design 60
2.3.2 Scheme Argumentation of Redundancy 61
2.3.2.1 Determination of Redundancy Scheme 61
2.3.2.2 Rules Obeyed in the Scheme Argumentation of Redundancy 62
2.3.3 Redundancy Design and Implementation 63
2.3.3.1 Basic Requirements 63
2.3.3.2 FDMU Design 63
2.3.3.3 CSSU Design 64
2.3.3.4 IPU Design 65
2.3.3.5 Power Supply Isolation Protection 67
2.3.3.6 Testability Design 68
2.3.3.7 Others 68
2.3.4 Validation of Redundancy by Analysis 69
2.3.4.1 Hardware FMEA 69
2.3.4.2 Redundancy Switching Analysis (RSA) 69
2.3.4.3 Analysis of the Common Cause of Failure 69
2.3.4.4 Reliability Analysis and Checking of the Redundancy Power 70
2.3.4.5 Analysis of the Sneak Circuit in the Redundancy Management Circuit 72
2.3.5 Validation of Redundancy by Testing 73
2.3.5.1 Testing by Failure Injection 73
2.3.5.2 Specific Test for the Power of the Redundancy Circuit 74
2.3.5.3 Other Things to Note 74
References 74
3  Fault Detection Techniques  77
  3.1  Fault Model  77
    3.1.1  Fault Model Classified by Time  78
    3.1.2  Fault Model Classified by Space  78
  3.2  Fault Detection Techniques  80
    3.2.1  Introduction  80
    3.2.2  Fault Detection Methods for CPUs  81
      3.2.2.1  Fault Detection Methods Used for CPUs  82
      3.2.2.2  Example of CPU Fault Detection  83
    3.2.3  Fault Detection Methods for Memory  87
      3.2.3.1  Fault Detection Method for ROM  88
      3.2.3.2  Fault Detection Methods for RAM  91
    3.2.4  Fault Detection Methods for I/Os  95
  References  96

4  Bus Techniques  99
  4.1  Introduction to Space-borne Bus  99
    4.1.1  Fundamental Concepts  99
    4.1.2  Fundamental Terminologies  99
  4.2  The MIL-STD-1553B Bus  100
    4.2.1  Fault Model of the Bus System  101
      4.2.1.1  Bus-level Faults  103
      4.2.1.2  Terminal Level Faults  104
    4.2.2  Redundancy Fault-tolerance Mechanism of the Bus System  106
      4.2.2.1  The Bus-level Fault-tolerance Mechanism  107
      4.2.2.2  The Bus Controller Fault-tolerance Mechanism  108
      4.2.2.3  Fault-tolerance Mechanism of Remote Terminals  113
  4.3  The CAN Bus  116
    4.3.1  The Bus Protocol  117
      4.3.2  Physical Layer Protocol and Fault-tolerance  117
        4.3.2.1  Node Structure  117
        4.3.2.2  Bus Voltage  118
        4.3.2.3  Transceiver and Controller  119
        4.3.2.4  Physical Fault-tolerant Features  119
    4.3.3  Data Link Layer Protocol and Fault-tolerance  120
      4.3.3.1  Communication Process  120
      4.3.3.2  Message Sending  120
      4.3.3.3  The President Mechanism of Bus Access  120
      4.3.3.4  Coding  121
      4.3.3.5  Data Frame  121
      4.3.3.6  Error Detection  122
  4.4  The SpaceWire Bus  124
    4.4.1  Physical Layer Protocol and Fault-tolerance  126
4.4.1.1 Connector 126
4.4.1.2 Cable 126
4.4.1.3 Low Voltage Differential Signal 126
4.4.1.4 Data Filter (DS) Coding 128
4.4.2 Data Link Layer Protocol and Fault-tolerance 129
4.4.2.1 Packet Character 129
4.4.2.2 Packet Parity Check Strategy 131
4.4.2.3 Packet Structure 131
4.4.2.4 Communication Link Control 131
4.4.3 Networking and Routing 136
4.4.3.1 Major Technique used by the SpaceWire Network 136
4.4.3.2 SpaceWire Router 138
4.4.4 Fault-tolerance Mechanism 139
4.5 Other Buses 141
4.5.1 The IEEE 1394 Bus 141
4.5.2 Ethernet 143
4.5.3 The I²C Bus 145
References 148

5 Software Fault-Tolerance Techniques 151
5.1 Software Fault-tolerance Concepts and Principles 151
5.1.1 Software Faults 151
5.1.2 Software Fault-tolerance 152
5.1.3 Software Fault Detection and Voting 153
5.1.4 Software Fault Isolation 154
5.1.5 Software Fault Recovery 155
5.1.6 Classification of Software Fault-tolerance Techniques 156
5.2 Single-version Software Fault-tolerance Techniques 156
5.2.1 Checkpoint and Restart 157
5.2.2 Software-implemented Hardware Fault-tolerance 160
5.2.2.1 Control Flow Checking by Software Signatures (CFCSS) 161
5.2.2.2 Error Detection by Duplicated Instructions (EDDI) 164
5.2.3 Software Crash Trap 165
5.3 Multiple-version Software Fault-tolerance Techniques 165
5.3.1 Recovery Blocks (RcB) 165
5.3.2 N-version Programming (NVP) 167
5.3.3 Distributed Recovery Blocks (DRB) 168
5.3.4 N Self-checking Programming (NSCP) 169
5.3.5 Consensus Recovery Block (CRB) 172
5.3.6 Acceptance Voting (AV) 172
5.3.7 Advantage and Disadvantage of Multiple-version Software 172
5.4 Data Diversity Based Software Fault-tolerance Techniques 173
5.4.1 Data Re-expression Algorithm (DRA) 173
5.4.2 Retry Blocks (RtB) 174  
5.4.3 N-copy Programming (NCP) 174  
5.4.4 Two-pass Adjudicators (TPA) 175  
References 177

6 Fault-Tolerance Techniques for FPGA 179  
6.1 Effect of the Space Environment on FPGAs 180  
6.1.1 Single Event Transient Effect (SET) 181  
6.1.2 Single Event Upset (SEU) 181  
6.1.3 Single Event Latch-up (SEL) 182  
6.1.4 Single Event Burnout (SEB) 182  
6.1.5 Single Event Gate Rupture (SEGR) 182  
6.1.6 Single Event Functional Interrupt (SEFI) 183  
6.2 Fault Modes of SRAM-based FPGAs 183  
6.2.1 Structure of a SRAM-based FPGA 183  
6.2.2 Faults Classification and Fault Modes Analysis of SRAM-based FPGAs 186  
6.2.2.1 Faults Classification 186  
6.2.2.2 Fault Modes Analysis 186  
6.3 Fault-tolerance Techniques for SRAM-based FPGAs 190  
6.3.1 SRAM-based FPGA Mitigation Techniques 191  
6.3.1.1 The Triple Modular Redundancy (TMR) Design Technique 191  
6.3.1.2 The Inside RAM Protection Technique 193  
6.3.1.3 The Inside Register Protection Technique 194  
6.3.1.4 EDAC Encoding and Decoding Technique 195  
6.3.1.5 Fault Detection Technique Based on DMR and Fault Isolation Technique Based on Tristate Gate 198  
6.3.2 SRAM-based FPGA Reconfiguration Techniques 199  
6.3.2.1 Single Fault Detection and Recovery Technique Based on ICAP+FrameECC 199  
6.3.2.2 Multi-fault Detection and Recovery Technique Based on ICAP Configuration Read-back+RS Coding 205  
6.3.2.3 Dynamic Reconfiguration Technique Based on EAPR 210  
6.3.2.4 Fault Recovery Technique Based on Hardware Checkpoint 216  
6.3.2.5 Summary of Reconfiguration Fault-tolerance Techniques 217  
6.4 Typical Fault-tolerance Design of SRAM-based FPGA 219  
6.5 Fault-tolerance Techniques of Anti-fuse Based FPGA 227  
References 230

7 Fault-Injection Techniques 233  
7.1 Basic Concepts 233  
7.1.1 Experimenter 234
7.1.2 Establishing the Fault Model 234
7.1.3 Conducting Fault-injection 235
7.1.4 Target System for Fault-injection 235
7.1.5 Observing the System’s Behavior 235
7.1.6 Analyzing Experimental Findings 235
7.2 Classification of Fault-injection Techniques 236
7.2.1 Simulated Fault-injection 236
7.2.1.1 Transistor Switch Level Simulated Fault-injection 237
7.2.1.2 Logic Level Simulated Fault-injection 237
7.2.1.3 Functional Level Simulated Fault-injection 237
7.2.2 Hardware Fault-injection 238
7.2.3 Software Fault-injection 240
7.2.3.1 Injection During Compiling 240
7.2.3.2 Injection During Operation 241
7.2.4 Physical Fault-injection 242
7.2.5 Mixed Fault-injection 244
7.3 Fault-injection System Evaluation and Application 245
7.3.1 Injection Controllability 245
7.3.2 Injection Observability 246
7.3.3 Injection Validity 246
7.3.4 Fault-injection Application 247
7.3.4.1 Verifying the Fault Detection Mechanism 247
7.3.4.2 Fault Effect Domain Analysis 247
7.3.4.3 Fault Restoration 247
7.3.4.4 Coverage Estimation 247
7.3.4.5 Delay Time 247
7.3.4.6 Generating Fault Dictionary 248
7.3.4.7 Software Testing 248
7.4 Fault-injection Platform and Tools 248
7.4.1 Fault-injection Platform in Electronic Design Automation (EDA) Environment 249
7.4.2 Computer Bus-based Fault-injection Platform 252
7.4.3 Serial Accelerator Based Fault-injection Case 254
7.4.4 Future Development of Fault-injection Technology 256
References 258

8 Intelligent Fault-Tolerance Techniques 261
8.1 Evolvable Hardware Fault-tolerance 261
8.1.1 Fundamental Concepts and Principles 261
8.1.2 Evolutionary Algorithm 266
8.1.2.1 Encoding Methods 270
8.1.2.2 Fitness Function Designing 272
8.1.2.3 Genetic Operators 273
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.2.4</td>
<td>Convergence of Genetic Algorithm</td>
<td>277</td>
</tr>
<tr>
<td>8.1.3</td>
<td>Programmable Devices</td>
<td>277</td>
</tr>
<tr>
<td>8.1.3.1</td>
<td>ROM</td>
<td>278</td>
</tr>
<tr>
<td>8.1.3.2</td>
<td>PAL and GAL</td>
<td>279</td>
</tr>
<tr>
<td>8.1.3.3</td>
<td>FPGA</td>
<td>281</td>
</tr>
<tr>
<td>8.1.3.4</td>
<td>VRC</td>
<td>282</td>
</tr>
<tr>
<td>8.1.4</td>
<td>Evolvable Hardware Fault-tolerance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implementation Methods</td>
<td>285</td>
</tr>
<tr>
<td>8.1.4.1</td>
<td>Modeling and Organization of Hardware</td>
<td>286</td>
</tr>
<tr>
<td></td>
<td>Evolutionary Systems</td>
<td></td>
</tr>
<tr>
<td>8.1.4.2</td>
<td>Reconfiguration and Its Classification</td>
<td>289</td>
</tr>
<tr>
<td>8.1.4.3</td>
<td>Evolutionary Fault-tolerance Architectures and Methods</td>
<td>291</td>
</tr>
<tr>
<td>8.1.4.4</td>
<td>Evolutionary Fault-tolerance Methods at Various</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layers of the Hardware</td>
<td>293</td>
</tr>
<tr>
<td>8.1.4.5</td>
<td>Method Example</td>
<td>298</td>
</tr>
<tr>
<td>8.2</td>
<td>Artificial Immune Hardware Fault-tolerance</td>
<td>302</td>
</tr>
<tr>
<td>8.2.1</td>
<td>Fundamental Concepts and Principles</td>
<td>302</td>
</tr>
<tr>
<td>8.2.1.1</td>
<td>Biological Immune System and Its Mechanism</td>
<td>304</td>
</tr>
<tr>
<td>8.2.1.2</td>
<td>Adaptive Immunity</td>
<td>305</td>
</tr>
<tr>
<td>8.2.1.3</td>
<td>Artificial Immune Systems</td>
<td>307</td>
</tr>
<tr>
<td>8.2.1.4</td>
<td>Fault-tolerance Principle of Immune Systems</td>
<td>310</td>
</tr>
<tr>
<td>8.2.2</td>
<td>Fault-tolerance Methods with Artificial Immune System</td>
<td>314</td>
</tr>
<tr>
<td>8.2.2.1</td>
<td>Artificial Immune Fault-tolerance System</td>
<td>316</td>
</tr>
<tr>
<td>8.2.2.2</td>
<td>Immune Object</td>
<td>318</td>
</tr>
<tr>
<td>8.2.2.3</td>
<td>Immune Control System</td>
<td>321</td>
</tr>
<tr>
<td>8.2.2.4</td>
<td>Working Process of Artificial Immune Fault-tolerance System</td>
<td>325</td>
</tr>
<tr>
<td>8.2.3</td>
<td>Implementation of Artificial Immune Fault-tolerance</td>
<td>328</td>
</tr>
<tr>
<td>8.2.3.1</td>
<td>Hardware</td>
<td>328</td>
</tr>
<tr>
<td>8.2.3.2</td>
<td>Software</td>
<td>330</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>References</td>
<td>334</td>
</tr>
</tbody>
</table>

**Acronyms** 337

**Index** 343