PRACTICAL SYSTEM RELIABILITY

Eric Bauer
Xuemei Zhang
Douglas A. Kimber
PRACTICAL SYSTEM
RELIABILITY
IEEE Press
445 Hoes Lane
Piscataway, NJ 08855

IEEE Press Editorial Board
Lajos Hanzo, Editor in Chief

R. Abari  T. Chen  B. M. Hammerli
J. Anderson  T. G. Croda  O. Malik
S. Basu  M. El-Hawary  S. Nahavandi
A. Chatterjee  S. Farshchi  W. Reeve

Kenneth Moore, Director of IEEE Book and Information Services (BIS)
Jeanne Audino, Project Editor

Technical Reviewers
Robert Hanmer, Alcatel-Lucent
Kime Tracy, Northeastern Illinois University
Paul Franklin, 2nd Avenue Subway Project
Simon Wilson, Trinity College, Ireland
PRACTICAL SYSTEM RELIABILITY

Eric Bauer
Xuemei Zhang
Douglas A. Kimber
For our families,
who have supported us in the writing of this book,
and in all our endeavors
## CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>xxi</td>
<td></td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>xiii</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>System Availability</td>
<td>5</td>
</tr>
<tr>
<td>2.1</td>
<td>Availability, Service and Elements</td>
<td>6</td>
</tr>
<tr>
<td>2.2</td>
<td>Classical View</td>
<td>8</td>
</tr>
<tr>
<td>2.3</td>
<td>Customers’ View</td>
<td>9</td>
</tr>
<tr>
<td>2.4</td>
<td>Standards View</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>Conceptual Model of Reliability and Availability</td>
<td>15</td>
</tr>
<tr>
<td>3.1</td>
<td>Concept of Highly Available Systems</td>
<td>15</td>
</tr>
<tr>
<td>3.2</td>
<td>Conceptual Model of System Availability</td>
<td>17</td>
</tr>
<tr>
<td>3.3</td>
<td>Failures</td>
<td>19</td>
</tr>
<tr>
<td>3.4</td>
<td>Outage Resolution</td>
<td>23</td>
</tr>
<tr>
<td>3.5</td>
<td>Downtime Budgets</td>
<td>26</td>
</tr>
<tr>
<td>4</td>
<td>Why Availability Varies Between Customers</td>
<td>31</td>
</tr>
<tr>
<td>4.1</td>
<td>Causes of Variation in Outage Event Reporting</td>
<td>31</td>
</tr>
<tr>
<td>4.2</td>
<td>Causes of Variation in Outage Duration</td>
<td>33</td>
</tr>
<tr>
<td>5</td>
<td>Modeling Availability</td>
<td>37</td>
</tr>
<tr>
<td>5.1</td>
<td>Overview of Modeling Techniques</td>
<td>38</td>
</tr>
<tr>
<td>5.2</td>
<td>Modeling Definitions</td>
<td>58</td>
</tr>
<tr>
<td>5.3</td>
<td>Practical Modeling</td>
<td>69</td>
</tr>
<tr>
<td>5.4</td>
<td>Widget Example</td>
<td>78</td>
</tr>
<tr>
<td>5.5</td>
<td>Alignment with Industry Standards</td>
<td>89</td>
</tr>
<tr>
<td>6</td>
<td>Estimating Parameters and Availability from Field Data</td>
<td>95</td>
</tr>
<tr>
<td>6.1</td>
<td>Self-Maintaining Customers</td>
<td>96</td>
</tr>
<tr>
<td>6.2</td>
<td>Analyzing Field Outage Data</td>
<td>96</td>
</tr>
<tr>
<td>6.3</td>
<td>Analyzing Performance and Alarm Data</td>
<td>106</td>
</tr>
</tbody>
</table>
6.4 Coverage Factor and Failure Rate 107
6.5 Uncovered Failure Recovery Time 108
6.6 Covered Failure Detection and Recovery Time 109

7 Estimating Input Parameters from Lab Data 111
  7.1 Hardware Failure Rate 111
  7.2 Software Failure Rate 114
  7.3 Coverage Factors 129
  7.4 Timing Parameters 130
  7.5 System-Level Parameters 132

8 Estimating Input Parameters in the Architecture/Design Stage 137
  8.1 Hardware Parameters 138
  8.2 System-Level Parameters 146
  8.3 Sensitivity Analysis 149

9 Prediction Accuracy 167
  9.1 How Much Field Data Is Enough? 168
  9.2 How Does One Measure Sampling and Prediction Errors? 172
  9.3 What Causes Prediction Errors? 173

10 Connecting the Dots 177
  10.1 Set Availability Requirements 179
  10.2 Incorporate Architectural and Design Techniques 179
  10.3 Modeling to Verify Feasibility 206
  10.4 Testing 208
  10.5 Update Availability Prediction 208
  10.6 Periodic Field Validation and Model Update 208
  10.7 Building an Availability Roadmap 209
  10.8 Reliability Report 210

11 Summary 213

Appendix A System Reliability Report outline 216
  1 Executive Summary 215
  2 Reliability Requirements 217
  3 Unplanned Downtime Model and Results 217
  Annex A Reliability Definitions 219
  Annex B References 219
  Annex C Markov Model State-Transition Diagrams 220

Appendix B Reliability and Availability Theory 221
  1 Reliability and Availability Definitions 221
  2 Probability Distributions in Reliability Evaluation 228
  3 Estimation of Confidence Intervals 237
THE RISE OF THE INTERNET, sophisticated computing and communications technologies, and globalization have raised customers’ expectations of powerful “always on” services. A crucial characteristic of these “always on” services is that they are highly available; if the customer cannot get a search result, or order a product or service, or complete a transaction instantly, then another service provider is often just one click away. As a result, highly available (HA) services are essential to many modern businesses, such as telecommunications and cable service providers, Web-based businesses, information technology (IT) operations, and so on.

Poor service availability or reliability often represents real operating expenses to service providers via costs associated with:

- **Loss of brand reputation and customer good will.** Verizon Wireless proudly claims to be “America’s most reliable wireless network” (based on low ineffective attempt and cutoff transaction rates), whereas Cingular proudly claims “Fewest dropped calls of any network.” Poor service availability can lead to subscriber churn, a tarnished brand reputation, and loss of customer good will.
- **Direct loss of customers and business.** Failure of an online provisioning system or order entry system can cause customers to be turned away because their purchase or order cannot be completed. For instance, if a retail website is unavailable or malfunctioning, many customers will simply go to a competitor’s website rather than bothering to postpone their purchase and retrying later.
- **Higher maintenance-related operating expenses.** Lower reliability systems often require more maintenance actions and raise
more alarms. More frequent failures often mean more maintenance staff must be available to address the higher volume of maintenance events and alarms. Repairs to equipment in unstaffed locations (e.g., outdoor base stations) require additional time and mileage expenses to get technicians and spare parts to those locations.

- **Financial penalties or liquidated damages** due to subscribers/customers for failing to meet service availability or “uptime” contractual requirements or service level agreements (SLAs).

This practical guide explains what system availability (including both hardware and software downtime) and software reliability are for modern server, information technology or telecommunications systems, and how to understand, model, predict and manage system availability throughout the development cycle. This book focuses on unplanned downtime, which is caused by product-attributable failures, rather than planned downtime caused by scheduled maintenance actions such as software upgrades and preventive maintenance. It should be noted that this book focuses on reliability of mission-critical systems; human-life-critical systems such as medical electronics, nuclear power operations, and avionics demand much higher levels of reliability and availability, and additional techniques beyond what is presented in this book may be appropriate.

This book provides valuable insight into system availability for anyone working on a system that needs to provide high availability. Product managers, system engineers, system architects, developers, and system testers will all see how the work they perform contributes to the ultimate availability of the systems they build.

**ERIC BAUER**
**XUEMEI ZHANG**
**DOUGLAS A. KIMBER**

*Freehold, New Jersey*
*Morganville, New Jersey*
*Batavia, Illinois*
*February 2009*
ACKNOWLEDGMENTS

We thank Abhaya Asthana, James Clark, Randee Adams, Paul Franklin, Bob Hanmer, Jack Olivieri, Meena Sharma, Frank Gruber, and Marc Benowitz for their support in developing, organizing and documenting the software reliability and system availability material included in this book. We also thank Russ Harwood, Ben Benison, and Steve Nicholls for the valuable insights they provided from their practical experience with system availability.

E.B.
X.Z.
D.K.