Design for Trustworthy Software

Tools, Techniques, and Methodology of Developing Robust Software

Bijay K. Jayaswal
Peter C. Patton
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADR Method</td>
</tr>
<tr>
<td>Seven Components of the Robust Software Development Process</td>
</tr>
<tr>
<td>Robust Software Development Model</td>
</tr>
<tr>
<td>Sidebar 1.2: Mission-Critical Aircraft Control Software</td>
</tr>
<tr>
<td>Key Points</td>
</tr>
<tr>
<td>Additional Resources</td>
</tr>
<tr>
<td>Internet Exercises</td>
</tr>
<tr>
<td>Review Questions</td>
</tr>
<tr>
<td>Discussion Questions and Projects</td>
</tr>
<tr>
<td>Endnotes</td>
</tr>
</tbody>
</table>

**CHAPTER 2  The Challenge of Trustworthy Software: Robust Design in Software Context**  
35

Software Reliability: Myth and Reality  
- Similarities and Differences Between Software and Manufactured Products 37
- Comparing Software and Hardware Reliability 39
- Causes of Software Unreliability 41

Japanese Quality Management Systems and the Taguchi Approach 43
Sidebar 2.1: The Life and Times of Dr. Genichi Taguchi 43
Sidebar 2.2: Quality Engineering Methodology at a Glance 45
Sidebar 2.3: Taguchi on Taguchi Methods 46
Sidebar 2.4: The Essence of Deming’s 14 Points 48

The Nitty-Gritty of Taguchi Methods for Robust Design 51
- The Concept of Signal-to-Noise Ratio 52
- The Concept of Quality Loss Function 53
- The Concept of Robust Design 55

The Challenge of Software Reliability: Design for Trustworthy Software 56
A Robust Software Development Model: DFTS Process in Practice 61
Key Points 63
Additional Resources 65
Internet Exercises 65
Review Questions 66
Discussion Questions and Projects 67
Endnotes 67
CHAPTER 3  Software Quality Metrics

Measuring Software Quality 71
Classic Software Quality Metrics 71
Total Quality Management 73
Generic Software Quality Measures 74
  Metrics Methodology 74
  In-Process Quality Metrics for Software Testing 76
  Software Complexity Metrics 77
  Software Science 78
  Cyclomatic Complexity 79
  Function Point Metrics 80
  Availability and Customer Satisfaction Metrics 82
Sidebar 3.1: A Software Urban Legend 83
Current Metrics and Models Technology 84
New Metrics for Architectural Design and Assessment 86
Common Architectural Design Problems 87
Pattern Metrics in OOAD 89
Key Points 90
Additional Resources 91
Internet Exercises 91
Review Questions 91
Discussion Questions and Projects 92
Endnotes 92

CHAPTER 4  Financial Perspectives on Trustworthy Software

Why DFTS Entails Different Financial Analyses 97
Cost and Quality: Then and Now 98
Cost of Software Quality 102
  Benefits of Cost-of-Quality Analysis 102
  Cost of Quality Tasks 103
  Classification of Cost of Software Quality 105
  Establishing a CoSQ Reporting System 109
  Payback from Investment in Quality 116
  Value of CoSQ Analysis 117
  Pitfalls of a CoSQ Program 118
Cost of Software Quality Over the Life Cycle 118
CHAPTER 5   Organizational Infrastructure and Leadership for DFTS  139

Organizational Challenges of a DFTS Deployment 141
DFTS Implementation Framework 141
  Step 1: Creating Management Awareness and Buy-in 144
  Step 2: Communicating Top Management’s Consensus and Commitment 147
  Step 3: Recognizing Potential Pitfalls of a DFTS Initiative 147
Sidebar 5.1: Virtuous Teaching Cycle and TPOV 156
  Step 4: Laying Foundations for a Quality-Focused Enterprise 157
  Step 5: Building the Organizational Infrastructure 160
  Step 6: Understanding the Roles of the Key Players 161
  Step 7: Designing a Supportive Organizational Structure 170
  Step 8: Establishing Effective Communication 172
  Step 9: Creating an Appropriate Reward System 174
  Step 10: Establishing Cost of Software Quality 175
  Step 11: Planning and Launching Organization-Wide Learning 176
  Step 12: Implementing the DFTS Model 177
  Step 13: Monitoring and Feedback for Learning and Improvement 180
  Step 14: Freezing the Improvements and Gains 180
  Step 15: Integrating and Expanding the Initiative 181
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Putting It All Together</td>
<td>181</td>
</tr>
<tr>
<td>Key Points</td>
<td>182</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>186</td>
</tr>
<tr>
<td>Internet Exercises</td>
<td>186</td>
</tr>
<tr>
<td>Review Questions</td>
<td>187</td>
</tr>
<tr>
<td>Discussion Questions and Projects</td>
<td>188</td>
</tr>
<tr>
<td>Endnotes</td>
<td>189</td>
</tr>
<tr>
<td><strong>PART II TOOLS AND TECHNIQUES OF DESIGN FOR TRUSTWORTHY SOFTWARE</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CHAPTER 6 The Seven Basic (B7) Tools of Quality</strong></td>
<td>193</td>
</tr>
<tr>
<td>The Seven Basic (B7) Tools</td>
<td>196</td>
</tr>
<tr>
<td>Sidebar 6.1: Kaoru Ishikawa: Developing a SpecificallyJapanese Quality Strategy</td>
<td>198</td>
</tr>
<tr>
<td>B7 in a DFTS Context</td>
<td>200</td>
</tr>
<tr>
<td>Other DFTS Tools, Techniques, and Methodologies</td>
<td>201</td>
</tr>
<tr>
<td>Flowcharts</td>
<td>202</td>
</tr>
<tr>
<td>High-Level Flowcharts</td>
<td>204</td>
</tr>
<tr>
<td>Detailed Flowcharts</td>
<td>204</td>
</tr>
<tr>
<td>Swim Lane Flowcharts</td>
<td>205</td>
</tr>
<tr>
<td>Pareto Charts</td>
<td>205</td>
</tr>
<tr>
<td>Cause-and-Effect Diagrams</td>
<td>206</td>
</tr>
<tr>
<td>Creating Cause-and-Effect-Diagrams to Identify Causes</td>
<td>208</td>
</tr>
<tr>
<td>Cause-and-Effect-Diagrams for Process Classification</td>
<td>210</td>
</tr>
<tr>
<td>Scatter Diagrams</td>
<td>212</td>
</tr>
<tr>
<td>Check Sheets</td>
<td>214</td>
</tr>
<tr>
<td>Histograms</td>
<td>215</td>
</tr>
<tr>
<td>Determining the Distribution Pattern</td>
<td>216</td>
</tr>
<tr>
<td>Determining Whether Specifications Are Satisfied</td>
<td>217</td>
</tr>
<tr>
<td>Comparing Data by Stratifying</td>
<td>217</td>
</tr>
<tr>
<td>Graphs</td>
<td>218</td>
</tr>
<tr>
<td>Control Charts</td>
<td>219</td>
</tr>
<tr>
<td>Key Points</td>
<td>222</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>223</td>
</tr>
<tr>
<td>Review Questions</td>
<td>223</td>
</tr>
<tr>
<td>Discussion Questions</td>
<td>224</td>
</tr>
<tr>
<td>Endnotes</td>
<td>225</td>
</tr>
</tbody>
</table>
# CHAPTER 7  The 7 MP Tools: Analyzing and Interpreting Qualitative and Verbal Data

- The N7 and 7 MP Tools
- Typical Applications of 7 MP Tools
- Affinity Diagram
- Interrelationship Diagraph (I.D.)
- Tree Diagram
- Prioritization Matrices
- Matrix Diagram
- Process Decision Program Chart (PDPC)
- Activity Network Diagram
- Behavioral Skills for 7 MP Tools
- Key Points
- Additional Resources
- Review Questions
- Discussion Questions and Projects
- Endnotes

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>227</td>
</tr>
<tr>
<td>The 7 MP Tools</td>
<td></td>
</tr>
<tr>
<td>Typical Applications of 7 MP Tools</td>
<td></td>
</tr>
<tr>
<td>Affinity Diagram</td>
<td></td>
</tr>
<tr>
<td>Interrelationship Diagraph (I.D.)</td>
<td></td>
</tr>
<tr>
<td>Tree Diagram</td>
<td></td>
</tr>
<tr>
<td>Prioritization Matrices</td>
<td></td>
</tr>
<tr>
<td>Matrix Diagram</td>
<td></td>
</tr>
<tr>
<td>Process Decision Program Chart (PDPC)</td>
<td></td>
</tr>
<tr>
<td>Activity Network Diagram</td>
<td></td>
</tr>
<tr>
<td>Behavioral Skills for 7 MP Tools</td>
<td></td>
</tr>
<tr>
<td>Key Points</td>
<td></td>
</tr>
<tr>
<td>Additional Resources</td>
<td></td>
</tr>
<tr>
<td>Review Questions</td>
<td></td>
</tr>
<tr>
<td>Discussion Questions and Projects</td>
<td></td>
</tr>
<tr>
<td>Endnotes</td>
<td></td>
</tr>
</tbody>
</table>

# CHAPTER 8  The Analytic Hierarchy Process

- Prioritization, Complexity, and the Analytic Hierarchy Process
- Multiobjective Decision-Making and AHP
- Terminology
  - Structuring an Objectives Hierarchy
  - Decision Hierarchy
- Case Study 8.1: MIS Director's IT Dilemma
- Case Study 8.1 Solution Using Expert Choice
  - Step 1: Brainstorm and Construct a Hierarchical Model of the Problem
  - Step 2: Derive Ratio Scale Priorities for the Objectives
  - Step 3: Derive Priorities for the Alternatives with Respect to Each Objective
  - Step 4: Synthesis
- Approximations to AHP with Manual Calculations
  - Approximate Solution Method 1
  - Approximate Solution Method 2: Brassard's Full Analytical Criteria Method for Prioritization
Contents

Conclusion 289
Key Points 289
Additional Resources 290
Internet Exercises 290
Review Questions 290
Discussion Questions and Projects 291
Problems 292

Problem 1: Managing Complexity in System Conversion 292
Problem 2: Managing Software Complexity in a High-Tech Start-up Enterprise 294
Problem 3: Complexity in Patient Record Systems 296
Problem 4: Oil Well Drilling Decision System 297
Problem 5: The ROI Issue 299
Problem 6: An Abstract Complexity Analysis 299
Problem 7: Sensitivity to Complexity 300

Endnotes 300

CHAPTER 9  Complexity, Mistakes, and Poka Yoke in Software Development Processes 303

Poka Yoke as a Quality Control System 305
Principles of Poka Yoke 306
Causes of Defects: Variation, Mistakes, and Complexities 307
Situations in Which Poka Yoke Works Well 309
Mistakes as Causes of Defects 310
Controlling Complexity in Software Development 312
Mistakes, Inspection Methods, and Poka Yoke 316
Deploying a Poka Yoke System 317
Identifying a Poka Yoke Solution 321
Key Points 322
Additional Resources 324
Internet Exercises 325
Review Questions 325
Discussion Questions and Projects 326
Endnotes 326
CHAPTER 10  5S for Intelligent Housekeeping in Software Development  329
5S: A Giant Step Toward a Productive Workplace Environment  331
Implementation Phases of the 5S System  332
  Phase 1: Sorting/Cleaning Up  332
  Phase 2: Straightening/Orderliness  332
  Phase 3: Shine/Cleanliness  333
  Phase 4: Standardize  333
  Phase 5: Sustain/Discipline  333
The 5S System and the DFTS Process  334
Sidebar 10.1: From 5S to the Lean DFTS Process  335
Overcoming Resistance  338
Implementing 5S  339
  Step 1: Management Buy-in  340
  Step 2: Training and Implementation  340
  Step 3: Link to a Reward System  340
  Step 4: Follow-up and Continuous Improvement  340
Key Points  341
Additional Resources  342
Internet Exercises  342
Review Questions  343
Discussion Questions and Projects  343
Endnotes  344

CHAPTER 11  Understanding Customer Needs: Software QFD and
the Voice of the Customer  345
QFD: Origin and Introduction  347
  What's Different about QFD as a Quality System?  348
  The History of QFD  350
  The History of Software QFD  350
  So, What Is QFD and Why Do We Need It?  352
A Focus on Priority  354
QFD Defined  355
QFD Deployments  356
The Four-Phase Model of QFD  357
The “House of Quality” Matrix  359
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems with Traditional QFD Applied to Software</td>
<td></td>
</tr>
<tr>
<td>Traditional QFD Failures</td>
<td></td>
</tr>
<tr>
<td>“The Matrix Is Too Big”</td>
<td></td>
</tr>
<tr>
<td>“It Takes Too Long”</td>
<td></td>
</tr>
<tr>
<td>“We Knew That Already”</td>
<td></td>
</tr>
<tr>
<td>Modern QFD for Software</td>
<td></td>
</tr>
<tr>
<td>Blitz QFD</td>
<td></td>
</tr>
<tr>
<td>The Seven Management and Planning (7 MP) Tools</td>
<td></td>
</tr>
<tr>
<td>Customer Satisfaction and Value</td>
<td></td>
</tr>
<tr>
<td>The Blitz QFD Process</td>
<td></td>
</tr>
<tr>
<td>Step 1: Key Project Goal</td>
<td></td>
</tr>
<tr>
<td>Step 2: Key Customer Segment</td>
<td></td>
</tr>
<tr>
<td>Step 3: Key Process Steps</td>
<td></td>
</tr>
<tr>
<td>Step 4: Go to Gemba</td>
<td></td>
</tr>
<tr>
<td>Step 5: What Are the Customer Needs?</td>
<td></td>
</tr>
<tr>
<td>Step 6: Structure the Customer Needs</td>
<td></td>
</tr>
<tr>
<td>Step 7: Analyze Customer Needs Structure</td>
<td></td>
</tr>
<tr>
<td>Step 8: Prioritize the Customer Needs</td>
<td></td>
</tr>
<tr>
<td>Step 9: Deploy Prioritized Customer Needs</td>
<td></td>
</tr>
<tr>
<td>Downstream Deployments: Analyze (Only) Important Relationships in Detail</td>
<td></td>
</tr>
<tr>
<td>The “House of Quality” and Beyond</td>
<td></td>
</tr>
<tr>
<td>Six Sigma Projects</td>
<td></td>
</tr>
<tr>
<td>Follow-Up: Apply, Evolve, and Improve the Process</td>
<td></td>
</tr>
<tr>
<td>Rapid Development</td>
<td></td>
</tr>
<tr>
<td>Schedule Deployment with Critical Chain Project Management</td>
<td>386</td>
</tr>
<tr>
<td>Implementing Software QFD</td>
<td></td>
</tr>
<tr>
<td>The People Side of QFD</td>
<td>386</td>
</tr>
<tr>
<td>QFD Challenges and Pitfalls</td>
<td>387</td>
</tr>
<tr>
<td>How to Implement Software QFD</td>
<td>390</td>
</tr>
<tr>
<td>Conclusion</td>
<td>391</td>
</tr>
<tr>
<td>Modern QFD in the DFTS Process</td>
<td></td>
</tr>
<tr>
<td>Key Points</td>
<td>393</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>394</td>
</tr>
<tr>
<td>Internet Exercises</td>
<td>395</td>
</tr>
<tr>
<td>Review Questions</td>
<td>396</td>
</tr>
<tr>
<td>Discussion Questions</td>
<td>397</td>
</tr>
<tr>
<td>Endnotes</td>
<td>399</td>
</tr>
<tr>
<td>About the Author</td>
<td>404</td>
</tr>
</tbody>
</table>
CHAPTER 12  Creativity and Innovation in the Software Design Process:  
TRIZ and Pugh Concept Selection Methodology  405

The Need for Creativity in DFTS  407
Creativity and TRIZ  407
Sidebar 12.1: What Is Serendipity?  408
Sidebar 12.2: Being There When the Page Was Blank  411
TRIZ in Software Development  411
Sidebar 12.3: Lingua Latina Non Mortus Est  412
TRIZ, QFD, and Taguchi Methods  419
Brainstorming  421
Pugh Concept Selection Methodology  423
Software as Intellectual Property  425
Sidebar 12.4: A Picture Is Worth…  427
Key Points  428
Additional Resources  428
Internet Exercises  428
Review Questions  429
Discussion Questions and Projects  429
Endnotes  429

CHAPTER 13  Risk Assessment and Failure Modes and Effects Analysis in Software  431

FMEA: Failure Modes and Effects Analysis  433
Upstream Application of FMEA  437
Software Failure Tree Analysis  440
Software Failure Modes and Their Sources  443
Risk Assignment and Evaluation at Each Stage of DFTS  445
Key Points  446
Additional Resources  447
Internet Exercises  447
Review Questions  447
Discussion Questions and Projects  447
Endnotes  448
CHAPTER 16  Robust Software in Context  499

The Software Specification Process  501
Sidebar 16.1: A Precise Functional Specification  503
What Is Robust Software?  504
Requirements for Software to Be Robust  505
Sidebar 16.2: Getting the End User’s Input  506
Specifying Software Robustness  506
Sidebar 16.3: An Example of Parameter Design  508
Key Points  508
Additional Resources  509
Internet Exercises  509
Review Questions  509
Discussion Questions and Projects  509
Problems  510
Endnotes  510

CHAPTER 17  Taguchi Methods and Optimization for Robust Software  511

Taguchi Methods for Robust Software Design  513
An Example from Engineering Design  517
An Example from Software Design and Development  521
Orthogonal Matrices for Taguchi Parameter Design Experiments  526
Applications to the Design of Trustworthy Software  529
Key Points  529
Additional Resources  530
Internet Exercises  530
Review Questions  530
Discussion Questions  530
Problems  531
Endnotes  531
CHAPTER 18 Verification, Validation, Testing, and Evaluation for Trustworthiness 533
Continuing the Development Cycle 535
Sidebar 18.1: An Urban Legend About Business Software 536
Verification 537
Case Study 18.1: Taguchi Methods for RTOS Design Verification 537
Validation 541
Case Study 18.2: Taguchi Methods for Software Validation 541
Testing and Evaluation 544
Sidebar 18.2: Testing and Debugging Anomalies 545
Key Points 549
Additional Resources 550
Internet Exercises 550
Review Questions 550
Discussion Questions and Projects 550
Problems 551
Endnotes 551

CHAPTER 19 Integration, Extension, and Maintenance for Trustworthiness 553
Completing the Development Cycle 555
Integration 555
Sidebar 19.1: The Supermarine Spitfire 556
Extension 556
Case Study 19.1: Extending the Capability of an Electronic Warfare System 557
Maintenance 558
Case Study 19.2: Field Maintenance of Software Systems 559
Sidebar 19.2: Maintaining Sophisticated Software Functionality Out of Existence 560
Key Points 561
Additional Resources 561
Internet Exercises 562
Review Questions 562
Discussion Questions and Projects 562
Problems 562
Endnotes 563
PART IV  PUTTING IT ALL TOGETHER: DEPLOYMENT OF A DFTS PROGRAM

CHAPTER 20  Organizational Preparedness for DFTS  567

Time to Ponder  569
Case Study 20.1: Striving for a Perfect Production Process  569
Case Study 20.2: Institutionalizing Six Sigma at GE  572
Leadership Challenges for Transformational Initiatives  577
Assessing Key Organizational Elements  577
  Creating Leadership Commitment  578
  Understanding the Leadership Role  579
  Assessing Strategic Linkages  580
  Ensuring Organization-Wide Participation  580
  Understanding the Need for Customer Focus  581
  Assessing Current Quality Management Capability  582
Key Points  583
Additional Resources  584
Internet Exercises  585
Review Questions  585
Discussion Questions and Projects  585
Endnotes  586

CHAPTER 21  Launching a DFTS Initiative  587

DFTS and the PICS Framework  589
Plan  589
Implement  592
  Step 11: Launching Organization-Wide Learning  592
  Designing Learning Curricula: Customization and Differentiation  593
  Training Support Personnel  593
  Step 12: Implementing DFTS Technology: Learning and Application Process  595
Control  600
  Step 13: Feedback Control Systems  603
Case Study 21.1: GE's Operating System for Continual Learning and Enrichment  606
  Project Management  610
Secure  611
  Step 14: Freezing the Improvements and Gains  611
  Step 15: Integrating and Expanding the Initiative  612
CHAPTER 24 Defining Customer Needs for Brand-New Products:
QFD for Unprecedented Software

Introduction
- Definition of Value
- Why Not Ask?
- Unprecedented Products
Defining Brand-New Needs
- Methods for Defining Customer Needs
Tools
- QFD's Seven Management and Planning (7MP) Tools
Sidebar 24.1: What Is the Theory of Constraints (TOC)?
- TOC's Thinking Processes
Last Steps
- Marketing Brand-New Products
Layers of Resistance
Conclusion
Acknowledgments
References
About the Author

CHAPTER 25 Jurassic QFD: Integrating Service and Product Quality
Function Deployment

Company Profile of MD Robotics
Why QFD?
- History of QFD
- Kano's Requirements
Triceratops Encounter at Universal Studios Florida Island of Adventure
- QFD Template
- Voice of Customer Analysis
- Emotion Deployment
Contents

de Bono 738
Deming 738
Gemba Visit/Voice of Customer Analysis 738
Hoshin Planning 739
Kano Model 739
Kansei Engineering 739
Lead User Research 739
Lean Manufacturing 740
New Lanchester Strategy 740
Neural Linguistic Programming (NLP) 740
Project Management 740
Pugh Concept Selection 740
QFD (Comprehensive) 740
Reliability 741
Seeds to Needs QFD 741
Seven Management and Planning (7 MP) Tools 741
Seven Product Planning (7PP) Tools 741
Seven Quality Control (7QC) Tools 741
Six Sigma, SPC 742
Software Engineering 742
Stage-Gate 742
Strategic Information Systems (SIS) 742
Supply Chain Management 742
Taguchi Methods 742
Theory of Constraints 742
Total Quality Management (TQM) 743
TRIZ 743
Value Engineering 743
About the Author 743
References 744

Glossary of Technical Terms 745

Name Index 753

Index 759