

Contents

- 1 Introduction 1**
 - 1.1 Motivation 1
 - 1.2 Approach 3
 - 1.2.1 Outline 5
 - References 6
- 2 Background 9**
 - 2.1 Introduction 9
 - 2.1.1 Structure of This Chapter 10
 - 2.2 Reliability and Safety 10
 - 2.2.1 Reliability 10
 - 2.2.2 Safety 11
 - 2.2.3 Safety vs. Reliability 12
 - 2.3 Software in Safety-Critical Systems 13
 - 2.3.1 Software Safety and Reliability 13
 - 2.4 The Safety Life-Cycle for Critical Systems 15
 - 2.5 Traditional Safety Analysis Techniques 17
 - 2.5.1 Hazard Analysis 17
 - 2.5.2 Risk Assessment and Safety Integrity 21
 - 2.5.3 Safety Integrity and Assurance 21
 - 2.6 Traditional System Engineering Approach 22
 - 2.6.1 The Software Safety Life-Cycle 23
 - 2.7 Standard Design Methodologies 24
 - 2.7.1 Design for Reliability 25
 - 2.8 Safety Standards 26
 - 2.9 Regulations for Medical Devices 28
 - 2.9.1 Device Classification 29
 - 2.9.2 Regulation Issues 30
 - 2.10 Industrial Application of Formal Methods 31
 - 2.10.1 IBM’s Customer Information Control System 31

| | | |
|----------|--|-----------|
| 2.10.2 | The Central Control Function Display Information System (CDIS) | 31 |
| 2.10.3 | The Paris Métro Signalling System (SACEM) | 32 |
| 2.10.4 | The Traffic Collision Avoidance System (TCAS) | 32 |
| 2.10.5 | The Rockwell AAMP5 Microprocessor | 33 |
| 2.10.6 | The VIPER Microprocessor | 33 |
| 2.10.7 | INMOS Transputer | 33 |
| 2.10.8 | The Mondex Electronic Purse | 33 |
| 2.10.9 | Darlington: Trip Computer Software | 34 |
| 2.10.10 | The BOS Control System | 34 |
| 2.10.11 | NIST Token-Based Access Control System (TBACS) | 35 |
| 2.10.12 | The Intel® Core™ i7 Processor Execution Cluster | 35 |
| 2.11 | Formal Methods for Safety-Critical Systems | 36 |
| 2.11.1 | Why Formal Methods? | 36 |
| 2.11.2 | Motivation for Their Use | 36 |
| | References | 40 |
| 3 | The Modelling Framework: Event-B | 47 |
| 3.1 | Introduction | 47 |
| 3.1.1 | Overview of B | 47 |
| 3.1.2 | Proof-Based Development | 48 |
| 3.1.3 | Scope of the B Modelling | 49 |
| 3.1.4 | Structure of This Chapter | 49 |
| 3.2 | Related Techniques | 49 |
| 3.3 | The Event-B Modelling Notation | 50 |
| 3.3.1 | Contexts | 51 |
| 3.3.2 | Machines | 51 |
| 3.4 | Modelling Actions over States | 52 |
| 3.5 | Proof Obligations | 53 |
| 3.6 | Model Refinement | 54 |
| 3.7 | Decomposition | 56 |
| 3.8 | Tools Environments for Event-B | 57 |
| | References | 58 |
| 4 | Critical System Development Methodology | 61 |
| 4.1 | Introduction | 61 |
| 4.1.1 | Structure of This Chapter | 63 |
| 4.2 | Related Work | 63 |
| 4.3 | Overview of the Methodology | 66 |
| 4.3.1 | Informal Requirements | 66 |
| 4.3.2 | Formal Specification | 67 |
| 4.3.3 | Formal Verification | 68 |
| 4.3.4 | Formal Validation | 69 |
| 4.3.5 | Real-Time Animation Phase | 69 |
| 4.3.6 | Code Generation | 70 |
| 4.3.7 | Acceptance Testing | 71 |

| | | |
|----------|---|------------|
| 4.4 | Benefits of Proposed Approach | 71 |
| 4.4.1 | Improving Requirements | 72 |
| 4.4.2 | Reducing Error Introduction | 72 |
| 4.4.3 | Improving Error Detection | 72 |
| 4.4.4 | Reducing Development Cost | 72 |
| 4.5 | Evaluation with Existing Tools | 73 |
| 4.6 | Summary | 73 |
| | References | 74 |
| 5 | Real-Time Animator and Requirements Traceability | 79 |
| 5.1 | Introduction | 79 |
| 5.1.1 | Structure of This Chapter | 81 |
| 5.2 | Motivation | 81 |
| 5.2.1 | Traceability | 83 |
| 5.3 | Related Work | 84 |
| 5.4 | Animation | 86 |
| 5.4.1 | Benefits of Animation | 86 |
| 5.4.2 | Limitations of Animation | 86 |
| 5.5 | Proposed Architecture | 87 |
| 5.5.1 | Data Acquisition & Preprocessing | 88 |
| 5.5.2 | Feature Extraction | 88 |
| 5.5.3 | Database | 89 |
| 5.5.4 | Graphical Animations Tool: Macromedia Flash | 89 |
| 5.5.5 | Animator: Brama Plug-in | 89 |
| 5.5.6 | Formal Modelling Language: Event-B | 90 |
| 5.6 | Applications and Case Studies | 90 |
| 5.7 | Limitations | 91 |
| 5.8 | Summary | 91 |
| | References | 93 |
| 6 | Refinement Chart | 97 |
| 6.1 | Introduction | 97 |
| 6.1.1 | Structure of This Chapter | 98 |
| 6.2 | Related Work | 98 |
| 6.3 | Refinement Chart | 99 |
| 6.4 | Applications and Case Studies | 102 |
| 6.5 | Summary | 103 |
| | References | 103 |
| 7 | EB2ALL: An Automatic Code Generation Tool | 105 |
| 7.1 | Introduction | 105 |
| 7.1.1 | Structure of This Chapter | 107 |
| 7.2 | Related Work | 107 |
| 7.3 | A Basic Framework of Translator | 109 |
| 7.3.1 | Selection of a Rodin Project | 109 |
| 7.3.2 | Introduction of a Context File | 110 |

| | | |
|----------|--|------------|
| 7.3.3 | Generated Proof Obligations | 113 |
| 7.3.4 | Filter Context and Concrete Machine Modules | 113 |
| 7.3.5 | Basic Principles of Code Generation | 114 |
| 7.3.6 | Events Scheduling | 132 |
| 7.3.7 | External Code Injection and Code Verification | 135 |
| 7.3.8 | Compiling and Running the Code | 137 |
| 7.4 | How to Use Code Generator Plug-ins | 137 |
| 7.4.1 | Assessment of the Translation Tool | 137 |
| 7.5 | Limitations | 138 |
| 7.6 | Summary | 139 |
| | References | 139 |
| 8 | Formal Logic Based Heart-Model | 143 |
| 8.1 | Introduction | 143 |
| 8.1.1 | Motivation | 144 |
| 8.1.2 | Structure of This Chapter | 145 |
| 8.2 | Related Work | 145 |
| 8.3 | Background | 147 |
| 8.3.1 | The Heart System | 147 |
| 8.3.2 | Basic Overview of Electrocardiogram (ECG) | 147 |
| 8.3.3 | ECG Morphology | 148 |
| 8.4 | Proposed Idea | 149 |
| 8.4.1 | Heart Block | 154 |
| 8.4.2 | Cellular Automata Model | 155 |
| 8.5 | Functional Formal Modelling of the Heart | 158 |
| 8.5.1 | The Context and Initial Model | 158 |
| 8.5.2 | Abstract Model | 159 |
| 8.5.3 | Refinement 1: Introducing Steps in the Propagation | 161 |
| 8.5.4 | Refinement 2: Impulse Propagation | 162 |
| 8.5.5 | Refinement 3: Perturbation in the Conduction | 165 |
| 8.5.6 | Refinement 4: Getting a Cellular Model | 168 |
| 8.5.7 | Model Validation and Analysis | 171 |
| 8.6 | Discussion | 172 |
| 8.7 | Summary | 172 |
| | References | 173 |
| 9 | The Cardiac Pacemaker | 177 |
| 9.1 | Introduction | 177 |
| 9.1.1 | Why Model-Checker? | 179 |
| 9.1.2 | Related Work for the Cardiac Pacemaker | 179 |
| 9.1.3 | Structure of This Chapter | 180 |
| 9.2 | Basic Overview of Pacemaker System | 180 |
| 9.2.1 | The Heart System | 181 |
| 9.2.2 | The Pacemaker System | 182 |
| 9.2.3 | Bradycardia Operating Modes | 183 |
| 9.3 | Event-B Patterns for Modelling the Cardiac Pacemaker | 184 |

| | | |
|-----------|---|------------|
| 9.3.1 | Action-Reaction Pattern | 184 |
| 9.3.2 | Time-Based Pattern | 184 |
| 9.4 | Refinement Structure of a Cardiac Pacemaker | 185 |
| 9.5 | Development of the Cardiac Pacemaker Using Refinement Chart | 186 |
| 9.6 | Cardiac Pacemaker Control Requirements | 189 |
| 9.7 | Formal Development of the One-Electrode Cardiac Pacemaker | 191 |
| 9.7.1 | Context and Initial Model | 191 |
| 9.7.2 | First Refinement: Threshold | 196 |
| 9.7.3 | Second Refinement: Hysteresis | 198 |
| 9.7.4 | Third Refinement: Rate Modulation | 199 |
| 9.8 | Formal Development of the Two-Electrode Cardiac Pacemaker | 201 |
| 9.8.1 | Context and Abstract Model | 201 |
| 9.8.2 | First Refinement: Threshold | 211 |
| 9.8.3 | Second Refinement of DDD Mode: Hysteresis | 217 |
| 9.8.4 | Third Refinement: Rate Modulation | 218 |
| 9.9 | Model Validation and Analysis | 220 |
| 9.10 | Closed-Loop Model of Heart and Cardiac Pacemaker | 222 |
| 9.10.1 | The Context and Initial Model | 223 |
| 9.10.2 | Chain of Refinements | 227 |
| 9.10.3 | Proof Statistics | 229 |
| 9.11 | Closed-Loop Modelling Requirements | 230 |
| 9.11.1 | Patient Safety in Closed-Loop | 230 |
| 9.11.2 | Behavioural Requirements | 230 |
| 9.11.3 | Clinical Requirements with Closed-Loop | 230 |
| 9.11.4 | To Discover Essential Safety Properties | 231 |
| 9.12 | Real-Time Animation Using Pacemaker Case Study | 231 |
| 9.13 | Code Generation Using EB2ALL Tool | 233 |
| 9.14 | Discussion | 236 |
| 9.15 | Summary | 237 |
| | References | 240 |
| 10 | Formalisation of Electrocardiogram (ECG) | 243 |
| 10.1 | Introduction | 243 |
| 10.1.1 | Structure of This Chapter | 245 |
| 10.2 | Related Work | 245 |
| 10.3 | Selection of Medical Protocol | 248 |
| 10.4 | Basic Overview of Electrocardiogram (ECG) | 249 |
| 10.4.1 | Differentiating the P-, QRS- and T-waves | 249 |
| 10.5 | Formal Development of the ECG Interpretation | 250 |
| 10.5.1 | Abstract Model: Assessing Rhythm and Rate | 250 |
| 10.5.2 | First Refinement: Assess Intervals and Blocks | 256 |
| 10.5.3 | Second Refinement: Assess for Nonspecific Intraventricular Conduction Delay and Wolff-Parkinson- White Syndrome | 259 |
| 10.5.4 | Third Refinement: Assess for ST-segment Elevation or Depression | 262 |

| | | |
|-----------|---|------------|
| 10.5.5 | Fourth Refinement: Assess for Pathologic Q-wave | 266 |
| 10.5.6 | Fifth Refinement: P-wave | 272 |
| 10.5.7 | Sixth Refinement: Assess for Left and Right Ventricular Hypertrophy | 274 |
| 10.5.8 | Seventh Refinement: Assess T-wave | 277 |
| 10.5.9 | Eighth Refinement: Assess Electrical Axis | 285 |
| 10.5.10 | Ninth Refinement: Assess for Miscellaneous Conditions . | 289 |
| 10.5.11 | Tenth Refinement: Assess Arrhythmias | 291 |
| 10.5.12 | Proof Statistics | 294 |
| 10.6 | Lesson Learnt | 296 |
| 10.6.1 | Ambiguous | 297 |
| 10.6.2 | Inconsistencies | 297 |
| 10.6.3 | Incompleteness | 298 |
| 10.7 | Summary | 298 |
| | References | 299 |
| 11 | Conclusion | 303 |
| 11.1 | Introduction | 303 |
| 11.2 | Life-Cycle Methodology | 304 |
| 11.3 | Techniques and Tools | 305 |
| 11.4 | Applications | 306 |
| 11.5 | Medical Protocol | 307 |
| | References | 308 |
| | Appendix Certification Standards | 311 |
| A.1 | What Are Standards? | 311 |
| A.2 | ISO/IEC Standards | 312 |
| A.2.1 | IEC 61508—Software Safety in E/E/EP Systems | 313 |
| A.2.2 | IEC 62304—Process Requirements for Medical Device Software | 314 |
| A.3 | IEEE Standards Association | 315 |
| A.3.1 | IEEE Standard 1012 | 316 |
| A.3.2 | IEEE Standard 730 | 316 |
| A.3.3 | IEEE Standard 1074 | 316 |
| A.4 | FDA | 317 |
| A.5 | Common Criteria | 318 |
| A.5.1 | CC Evaluation Assurance Level (EAL) | 319 |
| | References | 320 |
| | Index | 323 |



<http://www.springer.com/978-1-4471-5259-0>

Using Event-B for Critical Device Software Systems

Singh, N.K.

2013, XVIII, 326 p., Hardcover

ISBN: 978-1-4471-5259-0