Modeling and Verification Using UML Statecharts

A Working Guide to Reactive System Design, Runtime Monitoring and Execution-Based Model Checking

Doron Drusinsky

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Newnes is an imprint of Elsevier

Contents

Preface ..... **ix**
Acknowledgments ..... **xi**
What's on the CD-ROM? ..... **xii**
Chapter 1: Formal Requirements and Finite Automata Overview ..**1**
1.1. Terms 1
1.2. Finite Automata: The Basics 2
1.3 Regular Expressions 7
1.4. Deterministic Finite Automata and Finite State Diagrams 8
1.5. Nondeterministic Finite Automata 15
1.6. Other Forms of FA 19
1.7. FA Conversions and Lower Bounds 26
1.8. Operations on Regular Requirements 34
1.9. Succinctness of FA 35
1.10. Specifications as Zipped Requirements 38
1.11. Finite State Machines 39
1.12. Normal Form and Minimization of FA and FSMs 40
Chapter 2: Statecharts **43**
2.1. Transformational vs. Reactive Components 43
2.2. Statecharts in Brief 44
2.3. A Related Tool 45
2.4. Basic Elements of Statecharts 46
2.5. Code Generation and Scheduling 72
2.6. Event-Driven Statecharts, Procedural Statecharts, and Mixed Flowcharts and Statecharts 84
2.7. Flowcharts inside Statecharts: Workflow within Event-Driven Controllers 85
2.8. Nonstandard Elements of Statecharts 87
2.9. Passing Data to a Statechart Controller 95
2.10. JUnit Testing of Statechart Objects 95
2.11. Statecharts vs. Message Sequence Charts and Scenarios 98
2.12. Probabilistic Statecharts 98
Chapter 3: Academic Specification Languages for Reactive Systems **103**
3.1. Natural Language Specifications 104
3.2. Using Specification Languages for Runtime Monitoring 106
3.3. Linear-time Temporal Logic (LTL) 108

3.4. Other Formal Specification Languages for Reactive Systems 134
Chapter 4: Using Statechart Assertions for Formal Specification . 141
4.1. Statechart Specification Assertions 141
4.2. Nondeterministic Statechart Assertions. 163
4.3. Operations on Assertions. 196
4.4. Quantified Distributed Assertions 200
4.5. Runtime Recovery for Assertion Violations 202
4.6. The Language Dog-Fight: Statechart Assertions vs. LTL and ERE. 203
4.7. Succinctness of Pure Statechart Assertions. 209
4.8. Temporal Assertions vs. JML and Java Assertions 211
4.9. Commonly Used Assertions 213
Chapter 5: Creating and Using Temporal Statechart Assertions . . 217
5.1. Motivation, or Why Use Temporal Assertions?. 217
5.2. Applying Assertions: Three Uses 229
5.3. Writing Assertions. 230
5.4. Runtime Execution Monitoring—Runtime Verification 243
5.5. Runtime Recovery from Requirement Violations 245
5.6. Automatic Test Generation 247
5.7. Execution-Based Model Checking 248
Chapter 6: Application of Formal Specifications and Runtime Monitoring to the Ballistic Missile Defense Project. 261
6.1. Abstract 262
6.2. Context 263
6.3. Formal Specification and Verification Approach. 263
6.4. Overall Value 276
6.5. Challenges 278
Appendix: TLCharts: Syntax and Semantics. 279
A.1. About TLCharts 279
A.2. Syntax. 281
A.3. Semantics without Temporal Conditions 282
A.4. Semantics with Temporal Conditions. 285
A.5. TLCharts with Overlapping States 289
Bibliographical Notes 295
About the Author. 302
Index. 303