

Contents

- 1 Introduction 1**
 - 1.1 Challenges in the Design of Embedded Systems 1
 - 1.1.1 Issues in the Design of Embedded Systems..... 2
 - 1.1.2 Review of Traditional Methods to the Design
of Embedded Systems..... 3
 - 1.1.3 Weakness of the Traditional Design Methods 4
 - 1.2 Model-Based Design of Embedded Systems 6
 - 1.2.1 Related Work 11
 - 1.2.2 Discussion 11
 - 1.3 Brief Review of Simulink/Stateflow 12
 - 1.3.1 Simulink 12
 - 1.3.2 Stateflow 13
 - 1.4 Formalization of Simulink/Stateflow 14
 - 1.4.1 Necessity..... 14
 - 1.4.2 Overview of Our Approach 14
 - 1.4.3 Hybrid CSP..... 16
 - 1.4.4 Unifying Theories of Programming 16
 - 1.4.5 Hybrid Hoare Logic 17
 - 1.4.6 Differential Invariants 18
 - 1.4.7 MARS: A Toolchain to Support the Formalization..... 19
 - 1.5 Outline of This Book 20
- 2 Preliminaries 23**
 - 2.1 Continuous Dynamical System 23
 - 2.2 Stability and Feedback Control 24
 - 2.3 Polynomials and Polynomial Ideals 25
 - 2.4 First-Order Theory of Reals 27
 - 2.5 Summary..... 29

3	Unifying Theories of Programming (UTP)	31
3.1	Alphabetized Relational Calculus	31
3.2	Theory of Designs	33
3.3	Extending UTP to Higher-Order	35
3.4	Summary	36
4	Simulink	39
4.1	An Example	39
4.2	Modelling with Simulink	40
4.2.1	Blocks	41
4.2.2	Subsystems	44
4.2.3	Model Referencing	46
4.2.4	Block Library	46
4.3	Simulation and Analysis	50
4.3.1	Simulation Process	50
4.3.2	Solvers	51
4.3.3	Visualization of Simulation Results	52
4.4	Summary	53
5	Stateflow and Its Combination with Simulink	55
5.1	A Timer Example	55
5.2	Notations and Execution of Stateflow	56
5.2.1	Basic Notations	56
5.2.2	Execution of Stateflow	58
5.2.3	Advanced Features	59
5.3	Mealy and Moore Charts	60
5.3.1	Mealy and Moore Examples	60
5.3.2	Mealy and Moore Charts	62
5.4	Stateflow Languages	63
5.4.1	Events	63
5.4.2	Data	63
5.4.3	Message	64
5.4.4	Functions	64
5.4.5	Actions	67
5.5	How Stateflow Interacts with Simulink	68
5.5.1	An Example	69
5.6	Summary	69
6	Hybrid CSP	71
6.1	A Brief Introduction to CSP	71
6.1.1	Syntax of CSP	72
6.1.2	Operational Semantics of CSP	73
6.2	Syntax	75
6.2.1	Some Examples	79

6.3	Formal Semantics	80
6.3.1	Super-Dense Computation	80
6.3.2	Notations	80
6.3.3	Structural Operational Semantics.....	82
6.4	Summary and Related Work	86
6.4.1	Related Work	86
7	Hybrid Hoare Logic	91
7.1	History Formulas	92
7.2	Hoare Assertion	93
7.3	Proof System of HHL	95
7.4	Soundness	100
7.5	Summary and Related Work	104
7.5.1	Related Work	104
8	The HHL Prover	107
8.1	Isabelle/HOL	107
8.2	HHL Prover: Shallow Embedding	109
8.2.1	HCSP	109
8.2.2	Assertion Languages	110
8.2.3	Specification and Inference Rules	110
8.3	HHL Prover: Deep Embedding	113
8.3.1	Assertion Languages	114
8.4	A Case Study	116
8.4.1	Description of the Control Program	117
8.4.2	Verification in HHL Prover	117
8.5	Summary and Related Work	119
9	Invariant Generation	121
9.1	Differential Invariant	121
9.2	Semi-algebraic DI Generation	123
9.2.1	Topological Analysis of General DI.....	123
9.2.2	Predicting Continuous Evolution Using Lie Derivatives	126
9.2.3	Computing (Inverse) Inward Sets for Atomic Polynomial Formulas	129
9.2.4	Computing (Inverse) Inward Sets for SASs.....	132
9.2.5	A Necessary and Sufficient Criterion for Semi-algebraic DI	133
9.2.6	Automatic DI Generation	135
9.3	DI Generation Based on SOS-Relaxation	138
9.4	DI Generation for Non-polynomial Systems.....	139
9.4.1	Simulation of CCDSs	140
9.4.2	Polynomialization of Elementary ODEs	141
9.4.3	Constructing Polynomial Simulations of Elementary CCDSs	143

9.5	Summary and Related Work	147
9.5.1	Related Work	148
10	Translating Simulink Diagrams into HCSP	151
10.1	Translating Blocks	151
10.1.1	Continuous Blocks	153
10.1.2	Discrete Blocks	154
10.2	Translating Diagrams	156
10.2.1	Computing Inherited Sample Times	156
10.2.2	Translating Wires	157
10.2.3	Separating Diagrams	157
10.2.4	Translating Continuous Diagrams	158
10.2.5	Translating Discrete Diagrams	159
10.3	Translating Subsystems	160
10.3.1	Normal Subsystems	160
10.3.2	Triggered Subsystems	161
10.3.3	Enabled Subsystems	162
10.4	User Options for Translation	163
10.4.1	Options in Separating the Diagram	163
10.4.2	Options in Abstraction	164
10.5	Correctness of the Translation	164
10.5.1	UTP Semantics for Simulink	165
10.5.2	Diagrams	168
10.5.3	UTP Semantics for HCSP	171
10.5.4	Justification of Correctness	176
10.6	Summary and Related Work	179
10.6.1	Related Work	179
11	Translating Simulink/Stateflow Diagrams into HCSP	181
11.1	From Stateflow to HCSP	181
11.1.1	Transition Networks	181
11.1.2	Broadcasting and Monitor Process	184
11.1.3	Stateflow Diagrams	185
11.1.4	Other Features	186
11.1.5	Combination of Simulink and Stateflow	187
11.2	Correctness of the Translation	188
11.2.1	Abstract Syntax of Stateflow	188
11.2.2	UTP Semantics for Stateflow	189
11.2.3	Justification of Correctness	192
11.3	Summary and Related Work	195
11.3.1	Related Work	195
12	From HCSP to Simulink	199
12.1	Translating HCSP Constructs into Simulink	199
12.1.1	Expressions	200
12.1.2	skip Statement	202

12.1.3	Assignment	202
12.1.4	Continuous Evolution	203
12.1.5	Conditional Statement	204
12.1.6	Internal Choice	205
12.1.7	Sequential Composition.....	206
12.1.8	Recursion	206
12.1.9	Communication Events	207
12.1.10	Parallel	208
12.1.11	External Choice by Communications	209
12.1.12	Interruptions	210
12.2	Correctness of the Translation	210
12.3	A Two-Way Path between Informal and Formal Design of Embedded Systems.....	216
12.4	Summary and Related Work	217
12.4.1	Related Work	218
13	MARS: A Toolkit for Modelling, Analysis, and Verification of Hybrid Systems	219
13.1	The Sim2HCSP Translator.....	220
13.2	The HCSP2Sim Translator and Co-simulation	223
13.3	HHL Prover Revisited.....	224
13.4	Invariant Generator	225
13.4.1	Isabelle Oracle.....	225
13.4.2	QE-Based Invariant Generator.....	226
13.4.3	SOS-Based Invariant Generator	227
13.5	Summary and Related Work	228
13.5.1	Related Work	229
14	Case Studies	231
14.1	Chinese Train Control System at Level 3	231
14.1.1	Introduction of the Combined Scenario	232
14.1.2	Modelling and Simulation in Simulink/Stateflow	233
14.1.3	Formal Verification of the Simulink/Stateflow Model	235
14.2	The Guidance Control of a Lunar Lander	236
14.2.1	Description of the Verification Problem.....	237
14.2.2	Simulation and Verification	239
14.3	Summary and Related Work	240
14.3.1	Related Work	240
	References.....	243
	Index.....	255

Formal Verification of Simulink/Stateflow Diagrams

A Deductive Approach

Zhan, N.; Shuling, W.; Zhao, H.

2017, XV, 258 p. 74 illus., 60 illus. in color., Hardcover

ISBN: 978-3-319-47014-6