Contents

1 Introduction **1**
- 1.1 The RailCab System . . . 2
- 1.2 Problem Statement . . . 3
- 1.3 Contribution . . . 7
- 1.4 Overview . . . 9

2 Foundations **11**
- 2.1 Self-Adaptive Mechatronic Systems . . . 11
  - 2.1.1 Structuring . . . 11
  - 2.1.2 Operator-Controller-Module . . . 12
  - 2.1.3 Models@Runtime . . . 14
- 2.2 Timed Model Checking . . . 14
  - 2.2.1 Timed Automata . . . 15
  - 2.2.2 Timed Computation Tree Logic . . . 18
  - 2.2.3 Model Checking Procedure . . . 19
- 2.3 Graph-Based Specifications . . . 19
  - 2.3.1 Typed Attributed Graph Transformations Systems . . . 20
  - 2.3.2 Story Driven Modeling . . . 22
- 2.4 MechatronicUML . . . 26
  - 2.4.1 Real-Time Coordination Protocols . . . 26
  - 2.4.2 Real-Time Statecharts . . . 27
  - 2.4.3 Assumptions on Quality-of-Service Characteristics . . . 31

3 MechatronicUML Component Model **33**
- 3.1 Modeling Components . . . 34
  - 3.1.1 Ports . . . 35
  - 3.1.2 Atomic Components . . . 38
  - 3.1.3 Structured Components . . . 41
  - 3.1.4 Connectors . . . 45
  - 3.1.5 Component Properties . . . 46
- 3.2 Component Instances . . . 46
- 3.3 Modeling Reconfiguration . . . 49
  - 3.3.1 Component Story Diagrams . . . 50
  - 3.3.2 Controller Exchange Nodes . . . 51
  - 3.3.3 Constraints for Multi Port Variables . . . 52
  - 3.3.4 Reconfiguration of Atomic Components . . . 55
- 3.4 Instantiating Real-Time Coordination Protocols on System Level . . . 56
  - 3.4.1 Instantiating the RTCP ProtocolInstantiation . . . 57

3.4.2 The RTCP ProtocolInstantiation . . . 58
3.5 Modeling Component Properties by Architectural Constraints . . . 61
3.6 Implementation . . . 65
3.7 Related Work . . . 66
3.7.1 Software Component Models . . . 66
3.7.2 ADLs for Self-Adaptive Systems . . . 68
3.7.3 Constraint Languages . . . 68
3.8 Summary . . . 70

4 Transactional Execution of Hierarchical Reconfigurations 71
4.1 MechatronicUML Reconfiguration Controller . . . 73
4.2 Executing Reconfigurations . . . 75
4.2.1 Single-Phase Execution . . . 76
4.2.2 Three-Phase Execution . . . 77
4.2.3 Quiescence . . . 81
4.3 Declarative, Table-based Specification of the Reconfiguration Controller . . . 84
4.3.1 Interface Specification of RM Ports . . . 85
4.3.2 Manager Specification . . . 85
4.3.3 Executor Specification . . . 87
4.3.4 Interface Specification of RE Ports . . . 88
4.4 Generating Operational Behavior Specifications . . . 89
4.4.1 Manager Specification . . . 89
4.4.2 Executor Specification . . . 93
4.5 Verifying the Reconfiguration Specification . . . 99
4.5.1 Consistency . . . 101
4.5.2 Timing . . . 102
4.6 Implementation . . . 106
4.7 Assumptions and Limitations . . . 107
4.8 Related Work . . . 107
4.8.1 Approaches Supporting Reconfiguration of Hierarchical Components 107
4.8.2 Quiescence of Components . . . 109
4.9 Summary . . . 110

5 Verifying Refinements based on Test Automata 111
5.1 Refining Real-Time Coordination Protocols to Port Implementations . . . 114
5.1.1 Real-Time Coordination Protocol EnterSection . . . 114
5.1.2 Refined Port Real-Time Statecharts . . . 115
5.2 Considered Refinement Definitions . . . 118
5.3 Test automata-based Refinement Checking . . . 123
5.3.1 Refinement Selection . . . 124
5.3.2 Construction of the Test Automaton . . . 125
5.3.3 Adjusting the Port Real-Time Statechart . . . 131
5.3.4 Parallel Composition and Reachability Analysis . . . 132
5.4 Implementation . . . 132
5.5 Assumptions and Limitations . . . 134

5.6 Case Study . . . 134
5.6.1 Case Study Context . . . 134
5.6.2 Setting the Hypothesis . . . 134
5.6.3 Preparing the Input Models . . . 135
5.6.4 Validating the Hypothesis . . . 135
5.6.5 Analyzing the Results . . . 137
5.7 Related Work . . . 138
5.7.1 Refinement Checking . . . 138
5.7.2 Test automata-based Verification . . . 138
5.8 Summary . . . 139

6 Simulating Self-Adaptive Mechatronic Systems in MATLAB/Simulink 141
6.1 MATLAB/Simulink and Stateflow . . . 143
6.1.1 Simulink . . . 143
6.1.2 Stateflow . . . 144
6.2 MIL Simulation of MechatronicUML Models in Simulink and Stateflow . . . 146
6.3 Translating Component Instance Configurations to Simulink Block Diagrams 149
6.3.1 Translating Atomic Component Instances . . . 149
6.3.2 Translating Structured Component Instances . . . 153
6.3.3 Using Message-Based Communication . . . 157
6.3.4 Considering QoS Assumptions . . . 159
6.4 Translating Real-Time Statecharts to Stateflow Charts . . . 160
6.4.1 Basic Transformation Concepts . . . 160
6.4.2 Message-Based Communication . . . 162
6.4.3 Clock Concept . . . 163
6.4.4 Urgency . . . 165
6.4.5 Real-Time Statecharts of Multi Port Instances . . . 165
6.4.6 Synchronizations . . . 166
6.5 Translating Reconfiguration Specifications to Simulink and Stateflow . . . 170
6.5.1 Step 1: Compute Possible Configurations . . . 170
6.5.2 Step 2: Create Integrated CIC for Component . . . 172
6.5.3 Step 3: Generate the MATLAB-specific Reconfiguration Controller . 172
6.5.4 Step 4: Encode Configurations and Generate Control Signals . . . 178
6.5.5 Step 5: Create Integrated System CIC . . . 180
6.5.6 Integrate MATLAB-specific reconfiguration controller into the Simulink Block Diagram . . . 180
6.5.7 Realizing Port Reconfiguration in Stateflow Charts . . . 182
6.6 Implementation . . . 183
6.7 Limitations . . . 184
6.8 Case Study . . . 185
6.8.1 Case Study Context . . . 186
6.8.2 Setting the Hypothesis . . . 187
6.8.3 Preparing the Input Models . . . 187
6.8.4 Validating the Hypothesis . . . 188
6.8.5 Analyzing the Results . . . 188

6.9 Related Work . . . 189
6.9.1 Reconfiguration in MATLAB/Simulink . . . 189
6.9.2 Reconfiguration in other Simulation Environments . . . 189
6.9.3 Reconfiguration in AUTOSAR 3.x . . . 190
6.9.4 Hybrid Verification . . . 190
6.10 Summary . . . 191

7 Conclusions **193**
7.1 Summary . . . 193
7.2 Future Work . . . 195

Appendix

A Complete RailCab Example **199**
A.1 RTCPs . . . 199
A.1.1 ConvoyEntry . . . 200
A.1.2 ConvoyCoordination . . . 202
A.1.3 ProfileDistribution . . . 203
A.1.4 SpeedTransmission . . . 207
A.1.5 StartExecution . . . 208
A.1.6 StrategyExchange . . . 209
A.1.7 NextSectionFree . . . 210
A.2 Instantiating Real-Time Coordination Protocols on System Level . . . 211
A.2.1 A Simple Discovery Protocol and Environment Model . . . 211
A.2.2 Instantiating the RTCP ProtocolInstantiation . . . 215
A.2.3 The RTCP ProtocolInstantiation . . . 217
A.3 Components . . . 219
A.3.1 RailroadCrossing . . . 219
A.4 Component Instances . . . 220
A.4.1 RailCab Driving as a Coordinator . . . 220
A.4.2 RailCab Driving as a Member . . . 222
A.5 Component RTSCs . . . 224
A.5.1 RTSCs of the RailCab Components . . . 224
A.5.2 RTSCs of the Section Components . . . 234
A.6 Reconfiguration Behavior Specification of Components . . . 238
A.6.1 Declarative, Table-based Reconfiguration Specification . . . 238
A.6.2 Reconfiguration Rules . . . 242
A.6.3 Generated RTSCs for Manager and Executor of RailCabDriveControl 252
A.6.4 Specification of the Executor Operations . . . 258
A.7 Component SDDs . . . 266
A.7.1 RailCabDriveControl . . . 266
A.7.2 ConvoyCoordination . . . 267
A.7.3 VelocityController . . . 267
A.7.4 OperationStrategy . . . 272
A.7.5 RefGen . . . 272

A.8 Excerpt of Generated MATLAB/Simulink Model 274
A.8.1 Simulink Model for Atomic Component Instance of Type RefGen . . 274
A.8.2 Simulink Model for Structured Component Instance of Type ConvoyCoordination 275

B Formalization of the Real-time Statechart Semantics 283

C A Framework for Reachability Analyses 289
C.1 Reachability Analysis Framework 290
C.1.1 Metamodel 290
C.1.2 Reachability Analysis Algorithm 291
C.2 Story Diagram Reachability Analysis 293
C.2.1 Metamodel Extension 293
C.2.2 Functions of the Reachability Analysis 294
C.3 RTSC Reachability Analysis 298
C.3.1 Metamodel Extension 298
C.3.2 Functions of the Reachability Analysis 299
C.4 UDBM Library 299

D Metamodels 301
D.1 MechatronicUML Component Model 301
D.1.1 Core 301
D.1.2 Components 304
D.1.3 Component Instances 304
D.1.4 Runtime Model 307
D.2 MechatronicUML Reconfiguration 309
D.2.1 Reconfigurable Components 309
D.2.2 Component Story Patterns 311
D.2.3 Component Story Diagrams 314
D.2.4 Component Story Decision Diagrams 316
D.3 MATLAB/Simulink and Stateflow 317
D.3.1 Simulink 317
D.3.2 Stateflow 319
D.3.3 Message-Based Communication 321
D.3.4 Reconfiguration 322

Own Publications 323

Supervised Thesis 331

Literature 333

List of Abbreviations 373

List of Figures 375