

Contents

1	Introduction	17
1.1	The RailCab System.....	18
1.2	Problem Statement.....	19
1.3	Contribution	24
1.4	Overview	26
2	Foundations	29
2.1	Self-Adaptive Mechatronic Systems	29
2.1.1	Structuring.....	29
2.1.2	Operator-Controller-Module	30
2.1.3	Models@Runtime	32
2.2	Timed Model Checking.....	33
2.2.1	Timed Automata	33
2.2.2	Timed Computation Tree Logic.....	36
2.2.3	Model Checking Procedure	38
2.3	Graph-Based Specifications	38
2.3.1	Typed Attributed Graph Transformations Systems.....	39
2.3.2	Story Driven Modeling.....	41
2.4	MechatronicUML.....	45
2.4.1	Real-Time Coordination Protocols	45
2.4.2	Real-Time Statecharts	47
2.4.3	Assumptions on Quality-of-Service Characteristics	51
3	MechatronicUML Component Model	53
3.1	Modeling Components.....	54
3.1.1	Ports.....	55
3.1.2	Atomic Components	59
3.1.3	Structured Components	62
3.1.4	Connectors	66
3.1.5	Component Properties	67
3.2	Component Instances	68
3.3	Modeling Reconfiguration	71
3.3.1	Component Story Diagrams	71
3.3.2	Controller Exchange Nodes.....	73
3.3.3	Constraints for Multi Port Variables	74
3.3.4	Reconfiguration of Atomic Components	77
3.4	Instantiating Real-Time Coordination Protocols on System Level	78
3.4.1	Instantiating the RTCP ProtocolInstantiation.....	79
3.4.2	The RTCP ProtocolInstantiation	81
3.5	Modeling Component Properties by Architectural Constraints.....	83
3.6	Implementation	88

3.7	Related Work	89
3.7.1	Software Component Models	89
3.7.2	ADLs for Self-Adaptive Systems	91
3.7.3	Constraint Languages	92
3.8	Summary	93
4	Transactional Execution of Hierarchical Reconfigurations	95
4.1	MechatronicUML Reconfiguration Controller	97
4.2	Executing Reconfigurations	99
4.2.1	Single-Phase Execution	100
4.2.2	Three-Phase Execution	102
4.2.3	Quiescence	105
4.3	Declarative, Table-based Specification of the Reconfiguration Controller	109
4.3.1	Interface Specification of RM Ports	110
4.3.2	Manager Specification	111
4.3.3	Executor Specification	113
4.3.4	Interface Specification of RE Ports	114
4.4	Generating Operational Behavior Specifications	115
4.4.1	Manager Specification	115
4.4.2	Executor Specification	119
4.5	Verifying the Reconfiguration Specification	126
4.5.1	Consistency	128
4.5.2	Timing	130
4.6	Implementation	134
4.7	Assumptions and Limitations	134
4.8	Related Work	135
4.8.1	Approaches Supporting Reconfiguration of Hierarchical Components	135
4.8.2	Quiescence of Components	137
4.9	Summary	138
5	Verifying Refinements based on Test Automata	141
5.1	Refining Real-Time Coordination Protocols to Port Implementations	144
5.1.1	Real-Time Coordination Protocol EnterSection	144
5.1.2	Refined Port Real-Time Statecharts	145
5.2	Considered Refinement Definitions	149
5.3	Test automata-based Refinement Checking	154
5.3.1	Refinement Selection	155
5.3.2	Construction of the Test Automaton	156
5.3.3	Adjusting the Port Real-Time Statechart	163
5.3.4	Parallel Composition and Reachability Analysis	164
5.4	Implementation	164
5.5	Assumptions and Limitations	166

5.6	Case Study	166
5.6.1	Case Study Context	166
5.6.2	Setting the Hypothesis.....	166
5.6.3	Preparing the Input Models	167
5.6.4	Validating the Hypothesis	167
5.6.5	Analyzing the Results	169
5.7	Related Work.....	170
5.7.1	Refinement Checking.....	170
5.7.2	Test automata-based Verification	171
5.8	Summary	171
6	Simulating Self-Adaptive Mechatronic Systems in MATLAB/Simulink	173
6.1	MATLAB/Simulink and Stateflow.....	175
6.1.1	Simulink	175
6.1.2	Stateflow	177
6.2	MIL Simulation of MechatronicUML Models in Simulink and Stateflow	179
6.3	Translating Component Instance Configurations to Simulink Block Diagrams	182
6.3.1	Translating Atomic Component Instances.....	182
6.3.2	Translating Structured Component Instances.....	186
6.3.3	Using Message-Based Communication	190
6.3.4	Considering QoS Assumptions.....	193
6.4	Translating Real-Time Statecharts to Stateflow Charts	194
6.4.1	Basic Transformation Concepts.....	194
6.4.2	Message-Based Communication.....	196
6.4.3	Clock Concept.....	198
6.4.4	Urgency	199
6.4.5	Real-Time Statecharts of Multi Port Instances	199
6.4.6	Synchronizations.....	200
6.5	Translating Reconfiguration Specifications to Simulink and Stateflow... ..	204
6.5.1	Step 1: Compute Possible Configurations	205
6.5.2	Step 2: Create Integrated CIC for Component	207
6.5.3	Step 3: Generate the MATLAB-specific Reconfiguration Controller	207
6.5.4	Step 4: Encode Configurations and Generate Control Signals	214
6.5.5	Step 5: Create Integrated System CIC.....	216
6.5.6	Integrate MATLAB-specific reconfiguration controller into the Simulink Block Diagram	216
6.5.7	Realizing Port Reconfiguration in Stateflow Charts	218
6.6	Implementation	219
6.7	Limitations.....	221
6.8	Case Study	222
6.8.1	Case Study Context	222

6.8.2	Setting the Hypothesis.....	223
6.8.3	Preparing the Input Models	224
6.8.4	Validating the Hypothesis	224
6.8.5	Analyzing the Results	225
6.9	Related Work.....	225
6.9.1	Reconfiguration in MATLAB/Simulink	226
6.9.2	Reconfiguration in other Simulation Environments.....	226
6.9.3	Reconfiguration in AUTOSAR 3.x.....	227
6.9.4	Hybrid Verification	227
6.10	Summary	228
7	Conclusions	231
7.1	Summary	231
7.2	Future Work	233
	Own Publications	239
	Supervised Thesis	247
	Literature	249
	Appendix	
A	Complete RailCab Example	A-1
A.1	RTCPs.....	A-1
A.1.1	ConvoyEntry	A-2
A.1.2	ConvoyCoordination.....	A-4
A.1.3	ProfileDistribution.....	A-7
A.1.4	SpeedTransmission.....	A-9
A.1.5	StartExecution	A-10
A.1.6	StrategyExchange	A-11
A.1.7	NextSectionFree	A-12
A.2	Instantiating Real-Time Coordination Protocols on System Level	A-13
A.2.1	A Simple Discovery Protocol and Environment Model.....	A-13
A.2.2	Instantiating the RTCP ProtocolInstantiation.....	A-17
A.2.3	The RTCP ProtocolInstantiation	A-20
A.3	Components	A-22
A.3.1	RailroadCrossing	A-22
A.4	Component Instances	A-22
A.4.1	RailCab Driving as a Coordinator	A-23
A.4.2	RailCab Driving as a Member.....	A-24
A.5	Component RTSCs	A-25
A.5.1	RTSCs of the RailCab Components.....	A-25
A.5.2	RTSCs of the Section Components	A-37

A.6	Reconfiguration Behavior Specification of Components.....	A-42
A.6.1	Declarative, Table-based Reconfiguration Specification.....	A-42
A.6.2	Reconfiguration Rules.....	A-46
A.6.3	Generated RTSCs for Manager and Executor of RailCabDrive- Control	A-55
A.6.4	Specification of the Executor Operations.....	A-62
A.7	Component SDDs.....	A-68
A.7.1	RailCabDriveControl	A-70
A.7.2	ConvoyCoordination.....	A-71
A.7.3	VelocityController.....	A-73
A.7.4	OperationStrategy	A-76
A.7.5	RefGen	A-76
A.8	Excerpt of Generated MATLAB/Simulink Model.....	A-78
A.8.1	Simulink Model for Atomic Component Instance of Type Ref- Gen.....	A-78
A.8.2	Simulink Model for Structured Component Instance of Type ConvoyCoordination.....	A-79
B	Formalization of the Real-time Statechart Semantics	B-1
C	A Framework for Reachability Analyses	C-1
C.1	Reachability Analysis Framework.....	C-1
C.1.1	Metamodel	C-2
C.1.2	Reachability Analysis Algorithm.....	C-3
C.2	Story Diagram Reachability Analysis.....	C-5
C.2.1	Metamodel Extension	C-5
C.2.2	Functions of the Reachability Analysis	C-7
C.3	RTSC Reachability Analysis	C-10
C.3.1	Metamodel Extension	C-11
C.3.2	Functions of the Reachability Analysis	C-12
C.4	UDBM Library	C-12
D	Metamodels	D-1
D.1	MechatronicUML Component Model	D-1
D.1.1	Core.....	D-1
D.1.2	Components.....	D-4
D.1.3	Component Instances	D-6
D.1.4	Runtime Model.....	D-7
D.2	MechatronicUML Reconfiguration	D-9
D.2.1	Reconfigurable Components.....	D-9
D.2.2	Component Story Patterns.....	D-13
D.2.3	Component Story Diagrams	D-15
D.2.4	Component Story Decision Diagrams	D-16

D.3	MATLAB/Simulink and Stateflow.....	D-16
D.3.1	Simulink	D-18
D.3.2	Stateflow	D-19
D.3.3	Message-Based Communication.....	D-20
D.3.4	Reconfiguration	D-23