Contents

1 Introduction **1**

1.1 Motivation . . . 2

1.2 Framework of this Thesis . . . 4

1.3 Structure of this Thesis . . . 8

2 Basic Principles **9**

2.1 Technologies for studying Behavior . . . 10

2.2 Plants . . . 11

2.3 Controllers . . . 12

2.3.1 IEC 61131-3 . . . 12

2.3.2 IEC 61499-1 . . . 14

2.4 System Models . . . 14

2.4.1 Syntax . . . 15

2.4.2 Semantics . . . 20

2.5 Basics of Specifications . . . 23

2.5.1 Computation Tree Logic . . . 23

2.5.1.1 Syntax . . . 24

2.5.1.2 Semantics . . . 25

2.5.1.3 Equivalences . . . 26

2.5.1.4 Rules Of Precedence . . . 26

2.5.2 Extended Computation Tree Logic . . . 27

2.5.2.1 Syntax . . . 27

2.5.2.2 Semantics . . . 28

2.5.3 Timed Computation Tree Logic . . . 29

2.5.3.1 Syntax . . . 29

2.5.3.2 Semantics . . . 30

2.5.4 Symbolic Timing Diagrams . . . 30

2.6 Closed-Loop Composition . . . 32

2.7 Model Checking . . . 35

2.7.1 General Remarks . . . 35

2.7.2 Model Checking Algorithm . . . 36

2.8 Summary . . . 38

3 Formal Modeling of Plant, Controller, and the Closed Loop 39
3.1 Demonstration Example 40
3.2 Formal Plant Modeling 42
3.2.1 Modeling of Components 43
3.2.2 Semi-Automatic Model Generation 49
3.3 Formal Controller Modeling 54
3.3.1 Controller Modeling 55
3.3.2 Model Generation 60
3.4 Formal Closed-Loop Modeling 63
3.5 Summary 64

4 Specification 65
4.1 Safety-Oriented Technical Language 66
4.1.1 Syntax 67
4.1.2 Semantics 68
4.1.3 Compiler for SOTL 69
4.2 Symbolic Timing Diagrams 71
4.2.1 Modifications 72
4.2.2 Translation 73
4.2.3 STD Editor 74
4.3 Summary 78

5 Analysis of the Closed-Loop Behavior 79
5.1 Simulation in Closed Loop 79
5.1.1 Hardware-In-The-Loop Simulation 80
5.1.2 Software-In-The-Loop Simulation 86
5.2 Verification in Closed Loop 86
5.2.1 Hardware-In-The-Loop Verification 87
5.2.1.1 General Remarks 87
5.2.1.2 Case Study 90
5.2.2 Software-In-The-Loop Verification 97
5.2.2.1 General Remarks 97
5.2.2.2 Case Study 99
5.2.3 Limits of Verification 102
5.3 Summary 103

6 Conclusion and Outlook 105
6.1 Conclusion 105
6.2 Outlook 107

A Temporal Logics 109

B SOTL Grammar 111

C Algorithms 113

D Example for Model Checking 117

Bibliography 121

Index 127

Curriculum Vitae 129