Contents

Abstract VIII

1 Introduction 1

2 Paradigms for Automation Applications 10
2.1 Approaches related to Industrial Automation . . . 10
2.2 Object-Orientation . . . 13
2.3 Component-based Development . . . 14
2.4 Function Block Paradigm . . . 15
2.4.1 Concepts of Function Blocks . . . 15
2.4.2 Current Function Block Paradigm . . . 17
2.4.3 Why Function Blocks . . . 18
2.4.4 Considerations of Improving the Present FB Paradigm . . . 19
2.5 Summary . . . 20

3 Merging Paradigms 22
3.1 Merging Principles . . . 22
3.2 Safety Constraints . . . 23
3.3 Requirement Analysis . . . 24
3.4 Design . . . 26
3.4.1 Design of *SafeFB* . . . 27
3.4.2 Design of FB Networks . . . 30
3.5 Architecture Design . . . 33
3.6 Implementation: Coding . . . 34
3.7 Verification and Validation . . . 35

4 Function Block Metamodel 36
4.1 FB Interface . . . 37
4.2 Basic Module . . . 39
4.2.1 Behavioural Elements . . . 39
4.3 Composition of Modules . . . 40
4.3.1 Structure of a Composition . . . 40
4.3.2 Event-driven Modelling . . . 41
4.4 Summary . . . 42

5 Formal Models of SafeFBs and Applications 43
5.1 Foundations of Formal Methodology . . . 43
5.1.1 Transition System . . . 44
5.1.2 FSM/EFSMs . . . 44
5.1.3 Clocked Transition Systems . . . 45
5.1.4 Petri-Nets . . . 45
5.2 Formal Model of SafeFB . . . 45
5.3 Formal Model of FB Network . . . 49
5.3.1 Computational Models . . . 50
5.3.2 Abstraction . . . 51
5.3.3 From *FBNetwork* to CL^2TS . . . 53
5.3.4 Transformation Algorithm and Summary . . . 58
5.4 Comparison with Related Work . . . 59

6 Verification via Model Checking 61
6.1 Temporal Logic . . . 61
6.2 Checking EFSM . . . 63
6.3 Checking the Computational Model of an Integration . . . 65
6.3.1 Safety-related Properties . . . 65
6.4 Summary . . . 69

7 Verification by Testing 70
7.1 Overview on Software Testing . . . 70
7.1.1 Testing Methods . . . 71
7.1.2 Techniques to Derive Test Cases . . . 72
7.2 Test Design . . . 74
7.2.1 Specification and Testing . . . 75
7.2.2 Testing Criteria . . . 75
7.3 Preparation for Test Case Generation . . . 77
7.3.1 Execution Analysis Diagram . . . 77
7.3.2 Basic FBs . . . 78
7.3.3 Execution Analysis of an Integration . . . 79
7.3.4 Timed EAD . . . 82
7.3.5 Describing the Execution of an Integration with an TEAD . . . 83
7.4 Test Case Generation . . . 84
7.4.1 Test Case Specification . . . 84
7.4.2 Test Cases for Integration Testing . . . 85
7.5 Summary . . . 88

8 A Case Study Supported by a Tool 89
8.1 A Demonstrator Process . . . 90
8.2 Requirement Analysis . . . 91
8.2.1 Subprocess Distribute . . . 91

8.2.2 The Other Three Subprocesses 92
8.3 Design 93
8.4 Specification and Implementation 95
8.4.1 Implementation Model and Implementation 95
8.4.2 Test Cases 99
8.5 Execution of Testings 101
8.6 Summary 103

9 Conclusion **104**

A Additional Figures **106**

B Metaclass Definitions of FB Metamodel **112**

References **114**