Contents

1 Introduction **1**

1.1 Fault-tolerant control . . . 1

1.1.1 Motivation for fault-tolerant control . . . 1

1.1.2 Structure of the fault-tolerant control loop . . . 2

1.1.3 Fundamental questions . . . 3

1.2 Literature on fault-tolerant control of discrete event systems modeled by automata 4

1.2.1 Literature on controller design . . . 4

1.2.2 Literature on fault diagnosis . . . 5

1.2.3 Literature on controller reconfiguration . . . 7

1.2.4 Literature on integrated fault-tolerant control . . . 9

1.3 Main contributions of the thesis . . . 10

1.4 Structure of the thesis . . . 13

2 Formalization of the fault-tolerant control problem **15**

2.1 Notation . . . 15

2.2 Deterministic I/O automata . . . 15

2.2.1 Definition of deterministic I/O automata . . . 15

2.2.2 Complementary descriptions for deterministic I/O automata . . . 17

2.2.3 Automata graphs . . . 18

2.2.4 Properties of deterministic I/O automata . . . 20

2.3 Plant models . . . 21

2.3.1 General assumptions . . . 21

2.3.2 Relation between the faultless and the faulty plant . . . 22

2.3.3 Error relations . . . 22

2.3.4 Models of the faulty plant . . . 23

2.3.5 Plant model before and after the occurrence of a fault . . . 25

2.4 Problem statement . . . 26

2.4.1 Control aim: Reaching a desired final state . . . 26

2.4.2 Fault-tolerant control problem . . . 28

2.5 Running example: Automated warehouse . . . 29

3 Tracking control of deterministic I/O automata 33

3.1 Controllability analysis . . . 33

3.2 Structure of the tracking controller . . . 36

3.3 Controller for tracking a reference trajectory . . . 38

3.3.1 Definition of the controller . . . 38

3.3.2 Controller construction algorithm . . . 39

3.3.3 Properties of the controller . . . 40

3.3.4 Behavior of the controlled plant . . . 42

3.4 Planning a reference trajectory . . . 45

3.5 Fulfillment of the control aim in the closed-loop system . . . 48

3.6 Complexity of the tracking control method . . . 51

3.6.1 Complexity of the controllability analysis . . . 51

3.6.2 Complexity of the construction of the tracking controller . . . 52

3.6.3 Complexity of the online execution of the control method . . . 52

4 Active fault diagnosis 53

4.1 Consistency-based fault diagnosis settings . . . 53

4.2 Testing deterministic I/O automata . . . 55

4.2.1 Homing sequences . . . 56

4.2.2 Homing tree . . . 61

4.2.3 Construction of homing sequences from a homing tree . . . 63

4.3 Diagnosability analysis . . . 66

4.3.1 Detectability of a fault . . . 66

4.3.2 Identifiability of a fault . . . 67

4.3.3 Diagnosability with passive diagnosis . . . 73

4.3.4 Diagnosability with active diagnosis . . . 75

4.4 General approach for the fault diagnosis . . . 76

4.4.1 Fault detection . . . 76

4.4.2 Fault identification . . . 79

4.4.3 Fault diagnosis flowchart . . . 83

4.5 Generation of input sequences for active diagnosis . . . 86

4.5.1 Main idea for the generation of a homing sequence . . . 86

4.5.2 Selection of state pairs . . . 88

4.5.3 Computation of separating sequences . . . 90

4.5.4 Analysis of the resulting input sequence . . . 90

4.6 Properties of the diagnostic result . . . 94

4.6.1 Completeness and correctness of the diagnostic result . . . 94

4.6.2 Termination conditions for the fault identification 95
4.6.3 Diagnostic result at the diagnosis time 97
4.7 Complexity of the fault diagnosis methods 99
4.7.1 Complexity of the diagnosability analysis 100
4.7.2 Complexity of the online execution of the diagnosis methods 100
4.8 Active diagnosis avoiding illegal transitions 101
4.8.1 General approach for the active safe diagnosis 101
4.8.2 Safe diagnosability analysis 102
4.8.3 Adaptive safe homing sequence 104
4.8.4 Adaptive safe homing sequence for the closed-loop system 107
4.8.5 Active safe fault diagnosis 112
4.8.6 Complexity of the safe fault diagnosis method 117

5 Reconfiguration of the tracking controller 119

5.1 Reconfiguration setting 119
5.2 Reconfiguration with unambiguous diagnostic result 121
5.2.1 Reconfigurability analysis 121
5.2.2 Reconfiguration of the tracking controller by complete redefinition . . . 124
5.2.3 Partial redefinition of the trajectory planning unit 126
5.2.4 Partial redefinition of the controller 131
5.2.5 Reconfiguration of the tracking controller by partial redefinition 140
5.2.6 Complexity of the reconfiguration method 142
5.3 Reconfiguration with ambiguous diagnostic result 143
5.3.1 Main idea for the reconfiguration with ambiguous diagnostic result . . 144
5.3.2 Construction of the common model of the faulty plant 145
5.3.3 Reconfigurability analysis 148
5.3.4 Reconfiguration of the tracking controller by complete redefinition . . . 152
5.3.5 Partial redefinition of the trajectory planning unit and the controller . . 153
5.3.6 Reconfiguration of the tracking controller by partial redefinition 162
5.3.7 Complexity of the reconfiguration method 165
5.3.8 Discussion on reconfiguration with ambiguous diagnostic result 166

6 Integrated fault-tolerant control method 167

6.1 Fault-tolerant control flowchart 167
6.2 Fault-tolerant control without illegal transitions 170
6.2.1 Recoverability analysis 170
6.2.2 Definition of the fault-tolerant controller 175

6.2.3 Fulfillment of the control aim in the fault-tolerant control loop 183
6.3 Safe fault-tolerant control 187
6.3.1 Recoverability analysis 187
6.3.2 Definition of the safe fault-tolerant controller 191
6.3.3 Safe fulfillment of the control aim in the fault-tolerant control loop . . . 192

7 Example: Fault-tolerant control of a manufacturing process 195
7.1 Handling system HANS 195
7.1.1 Experimental setup 195
7.1.2 Implementation structure 196
7.2 Models of the Handling System HANS 197
7.2.1 General modeling information 197
7.2.2 Model of the faultless plant 198
7.2.3 Models of the faulty plant 200
7.3 Behavior in the faultless case 204
7.3.1 Controllability analysis 205
7.3.2 Definition of the tracking controller 205
7.3.3 Nominal control of the Handling System HANS 206
7.4 Recoverability analysis 210
7.5 Fault-tolerant control with unambiguous diagnostic result 213
7.5.1 Behavior of the fault-tolerant control loop 213
7.5.2 Fault diagnosis 215
7.5.3 Reconfiguration of the tracking controller 218
7.5.4 Time consumption 219
7.6 Fault-tolerant control with ambiguous diagnostic result 220
7.6.1 Termination of diagnosis with six elements in current state estimate . . 220
7.6.2 Termination of diagnosis with five elements in current state estimate . . 222
7.6.3 Discussion of different termination conditions 226
7.7 Safe fault-tolerant control 227
7.7.1 Safety constraints 227
7.7.2 Safe controllability analysis 227
7.7.3 Nominal safe control of the Handling System HANS 228
7.7.4 Safe recoverability analysis 229
7.7.5 Behavior of the fault-tolerant control loop 232
7.7.6 Time consumption 235

8 Conclusion **239**

8.1 Summary 239

8.2 Outlook 241

Bibliography **243**

Appendices **253**

A List of symbols **255**

B Compatibility partitions of the automated warehouse **261**

C Models of Handling System HANS **263**