

Contents

Abstract	v
German abstract (Kurzfassung)	ix
1. Introduction	1
1.1. Discrete-event control reconfiguration problem	2
1.2. Motivation	3
1.2.1. Missing methods for fault-tolerant control with I/O automata	3
1.2.2. Practical motivation	5
1.2.3. Fundamental issues of fault-tolerant control	6
1.3. Application examples	7
1.3.1. Examples used in this thesis	7
1.3.2. Examples from the literature	11
1.4. Literature overview	12
1.4.1. Fault tolerance paradigms	12
1.4.2. Fault-tolerant control of discrete-event systems	15
1.4.3. Comparative study of literature	16
1.5. Main results of the thesis	19
1.5.1. Formalism for fault-tolerant control of I/O automata	19
1.5.2. Modeling of faults and failures	20
1.5.3. Nominal controller design method	21
1.5.4. Off-line and On-line reconfiguration method	22
1.5.5. Simulation and experimental results	25
1.6. Structure of the thesis	25
 I. Theory of discrete-event systems for fault-tolerant control	 27

2. Modeling and analysis methods for discrete-event systems	28
2.1. Description of discrete-event systems	28
2.1.1. Autonomous automata	28
2.1.2. Nondeterministic I/O automata	29
2.1.3. Autonomous behavior of a system	30
2.1.4. Asynchronous networks of I/O automata	31
2.2. Analysis tools for discrete-event fault-tolerant control	36
2.2.1. Active input, active output and active next state sets	36
2.2.2. Output and transition degrees	37
2.2.3. Adjacency matrices	37
2.2.4. W -determinism	41
2.2.5. I/O trellis automata	41
2.3. Discrete-event modeling issues	44
2.3.1. Controllable and observable events	44
2.3.2. State space explosion	44
3. Discrete-event fault modeling	47
3.1. Faulty behavior and diagnosis approach	47
3.2. Motivation	48
3.3. Fault definition and classification	49
3.3.1. Definitions	49
3.3.2. Fault classification	50
3.4. Case study: a fluid level control process subject to faults	50
3.5. Modeling of faults and failures	52
3.5.1. Main idea	52
3.5.2. Actuator faults and failures	52
3.5.3. Sensor faults and failures	53
3.5.4. System internal faults and failures	53
3.6. Construction of the model of a system subject to faults and failures	54
3.6.1. Input failure	54
3.6.2. Output failure	54
3.6.3. State failure	55
3.6.4. Computation of the faulty behavior	55
3.7. Application on a fluid level control process subject to faults	56
3.7.1. Blocking valve V_2	57
3.7.2. Sensor failure	57

3.7.3. Internal fault: leakage in tank T_1	58
3.8. Literature review	59
4. Control design	61
4.1. Basic notions of the discrete-event control design	61
4.1.1. Problem statement	61
4.1.2. Model of the control loop	62
4.1.3. Execution cycle of a control loop	63
4.1.4. Control loop analysis	65
4.2. Specification of a process	68
4.2.1. Different types of specifications	68
4.2.2. Interpretation of the specification automaton	69
4.2.3. Pseudo-specification automaton	71
4.2.4. Exact specification automaton	72
4.2.5. Specification automaton design	73
4.2.6. State sequences set extraction	74
4.2.7. Test automaton computation from a set of state sequences	76
4.2.8. Feasibility of a specification	77
4.2.9. Completeness and exactness of the specification	80
4.3. Feedback control design	81
4.3.1. Main idea	81
4.3.2. Procedural description of the design method	81
4.3.3. Realization of the feedback controller	88
4.3.4. Controllability conditions	89
4.3.5. Complexity analysis	90
4.4. Application of the control design method	91
4.4.1. Nominal fluid level control process	92
4.4.2. Control design method with I/O trellis automata	94
4.5. Usability of the control design method	100
4.5.1. Implementation issues of the control law and control devices	100
4.5.2. Application of the controller design approach to standard automata	101
4.6. Literature review	102
5. Fault-tolerant control of discrete-event systems	107
5.1. Discrete-event control reconfiguration schemes	107
5.1.1. Off-line reconfiguration concept	107
5.1.2. Formalized off-line reconfiguration	108

5.1.3.	On-line reconfiguration concept	110
5.1.4.	Forward and backward reconfiguration paradigm	111
5.2.	Degrees of freedom and redundancies	112
5.2.1.	Degrees of freedom of a specification	112
5.2.2.	Redundancy degree of a controller	113
5.3.	Forward and backward on-line reconfiguration of a controller	117
5.4.	Reconfigurability of a controller	120
5.5.	Complexity analysis of the reconfiguration	123
5.6.	Control reconfiguration of the fluid process	125
5.6.1.	Faulty behavior after an actuator failure: broken outflow valve . . .	125
5.6.2.	Application of the off-line control reconfiguration	126
5.6.3.	Discussion	128

II. Application examples 129

6.	Virtual manufacturing process: Pick-and-place system	130
6.1.	Modeling and nominal control design of the pick-and-place system	130
6.2.	Forward control reconfiguration after an internal system fault: random workpiece supply	133
6.3.	Backward reconfiguration after a sensor fault: damaged visual sensor . . .	134
7.	Experimental manufacturing process	137
7.1.	Structure of the manufacturing cell	137
7.2.	Component-oriented modeling of the manufacturing cell	140
7.3.	Nominal manufacturing process	147
7.4.	Control reconfiguration after an actuator failure	153
7.4.1.	Nominal subprocess SP1	153
7.4.2.	Actuator failure	155
7.4.3.	Fault-tolerant control with a deflector failure	157
7.5.	Control reconfiguration after a system internal fault	162
7.5.1.	Nominal subprocess SP2	162
7.5.2.	System internal fault	165
7.5.3.	Fault-tolerant control despite an occupied position	166
7.6.	Experimental limitations and sketches of solutions	171
8.	Conclusion	177

8.1. Summary	177
8.2. Discussion and open problems	179
Bibliography	183
 III. Appendices	 201
A. Nomenclature	202
B. Proofs	207
C. MATLAB/Simulink programs: IDEFICS	211
C.1. Modeling of discrete-event systems	211
C.2. Discrete-event control design	225
C.3. Analysis operators	231
C.4. Specific features	249
D. Models of the components of the pilot manufacturing cell	259
D.1. Pusher	259
D.2. Buffer rail	260
D.3. Magazine	263
D.4. Horizontal handler	266
D.5. Horizontal handling gripper	267
D.6. Positions in blocks	269
D.7. Conveyor belt	270
D.8. Deflectors	273
D.9. Slides	275
D.10. Vertical handler	278
D.11. Vertical handling gripper	279
D.12. Encoding tables of all control laws of the pilot manufacturing cell	282