Mogens Blanke · Michel Kinnaert
Jan Lunze · Marcel Staroswiecki

Diagnosis and Fault-Tolerant Control

With contributions by Jochen Schröder

With 228 Figures

Springer

Contents

1. Introduction to diagnosis and fault-tolerant control 1

1.1 Technological processes subject to faults 1

1.2 Faults and fault tolerance 3

1.2.1 Faults 3

1.2.2 Requirements and properties of systems subject to faults 8

1.3 Elements of fault-tolerant control 10

1.3.1 Fault-tolerant control architecture 10

1.3.2 Main ideas of fault diagnosis 13

1.3.3 Main ideas of controller re-design 18

1.3.4 A practical view on fault-tolerant control 22

1.4 Survey of the book 23

Bibliographical notes 26

2. Examples 27

2.1 Two-tank system 27

2.2 Ship steering and track control 31

3. Models of dynamical systems 39

3.1 Fundamental notions 39

3.2 Modelling the system architecture 43

3.3 System behaviour – basic modelling features 46

3.4 Continuous-variable systems 47

3.5 System structure 51

3.6 Discrete-event systems 53

3.7 Hybrid systems 56

3.8 Links between the different models 57

Bibliographical notes 60

4. Analysis based on components and architecture 61

4.1 Introduction 61

4.2 Generic component models 63

4.2.1 Services 63

4.2.2 Introduction of the generic component model 65

4.2.3 Simple components 66

4.2.4 Complex components 69
4.2.5 Building systems from components 72
4.3 Faults in components and their consequences 75
4.4 Fault propagation analysis 77
4.5 Graph representation of component architecture 86
4.6 Fault propagation in closed loops 89
4.6.1 Cutting the closed fault propagation loop 90
4.6.2 Assessment of the severity of the fault effects 92
4.6.3 Decision about fault handling 92
4.7 Fault tolerance analysis 92
4.7.1 Relation between services and objectives 92
4.7.2 Management of service versions 95
4.7.3 Management of operation modes 96
Bibliographical notes 98

5. Structural analysis 99
5.1 Introduction 99
5.2 Structural model 100
5.2.1 Structure as a bi-partite graph 100
5.2.2 Subsystems 106
5.2.3 Structural properties 108
5.2.4 Known and unknown variables 109
5.3 Matching on a bi-partite graph 111
5.3.1 Definitions 112
5.3.2 Oriented graph associated with a matching 116
5.3.3 Alternated chains and reachability 118
5.3.4 Causal interpretation 119
5.3.5 Matching algorithm 127
5.4 System canonical decomposition 130
5.4.1 Definitions 130
5.4.2 Canonical subsystems 131
5.4.3 Interpretation of the canonical decomposition 133
5.5 Observability 136
5.5.1 Observability and computability 136
5.5.2 Structural observability conditions 138
5.5.3 Observability of linear systems 139
5.5.4 Graph-based interpretation and formal computation 142
5.6 Monitorability 144
5.6.1 Analytical redundancy-based fault detection and isolation 144
5.6.2 Structurally monitorable subsystems 147
5.6.3 Design of analytic redundancy relations 149
5.6.4 Parity space and observer-based approaches 156
5.6.5 Design of robust and structured residuals 158
5.6.6 Fault propagation and alarm filtering 161

5.7 Controllability ... 162
5.8 Structural analysis of fault tolerance ... 164
5.8.1 Faults and the system structure ... 165
5.8.2 Knowledge about faults ... 166
5.8.3 Fault tolerance with respect to non-structural faults ... 167
5.8.4 Fault tolerance with respect to structural faults ... 167
5.9 Conclusions ... 170
Bibliographical notes ... 171

6. Fault diagnosis of continuous-variable systems ... 173
6.1 Introduction ... 173
6.2 Deterministic model – parity space approach ... 176
6.2.1 Fault detection ... 176
6.2.2 Solution by the parity space approach ... 178
6.2.3 Fault isolation ... 186
6.2.4 Fault estimation ... 189
6.3 Deterministic model – optimisation-based approach ... 192
6.3.1 Problem statement ... 192
6.3.2 Solution using the standard setup formulation ... 196
6.3.3 Residual generation ... 199
6.4 Stochastic model – change detection algorithms ... 205
6.4.1 Introduction ... 205
6.4.2 Sequential change detection: the scalar case ... 205
6.4.3 Sequential change detection: the vector case ... 221
6.5 Stochastic model – Kalman filter approach ... 232
6.5.1 Model ... 232
6.5.2 Fault detection ... 233
6.5.3 Fault estimation ... 250
6.5.4 Fault isolation ... 252
Bibliographical notes ... 255

7. Fault-tolerant control of continuous-variable systems ... 259
7.1 Fault-tolerant control architecture ... 259
7.2 The fault-tolerant control problem ... 262
7.2.1 Standard control problem ... 262
7.2.2 Impacts of faults on the control problem ... 264
7.2.3 Passive versus active fault-tolerant control ... 266
7.2.4 Available knowledge ... 267
7.2.5 Active fault-tolerant control strategies ... 268
7.2.6 Supervision ... 269
7.3 An optimal control approach to fault-tolerant control with actuator faults ... 270
7.3.1 Control problem ... 270
7.3.2 Control of the nominal plant ... 271
7.3.3 Fault tolerance with respect to actuator faults ... 272

7.3.4 Fault accommodation . . . 274
7.3.5 Control reconfiguration . . . 277
7.3.6 Example . . . 278
7.3.7 Extension to a more general problem setting . . . 279
7.4 Model-matching approach to fault-tolerant control . . . 281
7.4.1 Reconfiguration problem . . . 281
7.4.2 Fault-tolerant control based on model-matching . . . 282
7.4.3 Model-matching control for sensor faults . . . 284
7.4.4 Model-matching control for actuator faults . . . 285
7.5 Control reconfiguration for actuator or sensor faults . . . 286
7.5.1 The idea of virtual sensors and virtual actuators . . . 286
7.5.2 Reconfiguration problem . . . 289
7.5.3 Virtual sensor . . . 290
7.5.4 Virtual actuator . . . 294
7.5.5 Duality between virtual sensors and virtual actuators . 299
7.6 Controller re-design in the general fault case . . . 303
7.6.1 System description . . . 303
7.6.2 Youla-Kucera parameterisation in coprime factorisation form . . . 305
7.6.3 Parametrisation in the state-space form . . . 307
7.6.4 Simultaneous design of the controller and the residual generator . . . 309
Bibliographical notes . . . 312

8. Diagnosis and reconfigurable control of discrete-event systems . . . 315
8.1 Motivation . . . 315
8.2 Models of discrete-event systems . . . 316
8.2.1 Deterministic and non-deterministic systems . . . 316
8.2.2 Non-deterministic automata and Petri nets . . . 319
8.2.3 Stochastic automata . . . 324
8.3 State observation of stochastic automata . . . 333
8.3.1 Observation problem . . . 333
8.3.2 Consistent input-output pairs . . . 334
8.3.3 Solution to the state observation problem . . . 335
8.3.4 Recursive form of the solution . . . 339
8.3.5 Discussion of the results . . . 341
8.3.6 Observation algorithm . . . 344
8.3.7 State observation of non-deterministic automata . . . 345
8.3.8 Observability of stochastic automata . . . 350
8.3.9 Distinguishing inputs . . . 354
8.4 Diagnosis of stochastic automata . . . 357
8.4.1 Principle of consistency-based diagnosis . . . 357
8.4.2 Model of the faulty automaton . . . 360
8.4.3 Consistency-based diagnosis of stochastic automata . . . 362

8.4.4 Diagnostic algorithm ... 365
8.4.5 Diagnosability of stochastic automata ... 369
8.5 Control reconfiguration for stochastic automata ... 373
8.5.1 Sensor and actuator fault isolation ... 373
8.5.2 Automatic substitution of faulty sensors ... 381
8.5.3 Automatic reconfiguration of diagnosis ... 382
Bibliographical notes ... 382

9. Diagnosis and reconfiguration of quantised systems ... 385
9.1 Introduction to quantised systems ... 385
9.1.1 Supervision of hybrid systems ... 385
9.1.2 The quantised system approach to supervisory control 388
9.2 Quantised systems ... 391
9.2.1 Continuous-variable system ... 391
9.2.2 Quantisation of the signal spaces ... 392
9.2.3 Example: two-tank system ... 393
9.2.4 Behaviour of quantised systems ... 395
9.2.5 Stochastic properties of quantised systems ... 399
9.3 A behavioural view on supervision problems ... 403
9.4 Discrete-event models of quantised systems ... 407
9.4.1 The modelling problem ... 407
9.4.2 Description of autonomous quantised systems by stochastic automata ... 408
9.4.3 Extensions to systems with input and output ... 415
9.4.4 Abstractions of faulty systems ... 416
9.5 State observation of quantised systems ... 419
9.5.1 Observation method ... 419
9.5.2 Discussion of the result ... 420
9.5.3 Observation algorithm ... 422
9.6 Diagnosis of quantised systems ... 425
9.6.1 Diagnostic method ... 425
9.6.2 Discussion of the result ... 425
9.6.3 Diagnostic algorithm ... 426
9.6.4 Automatic reconfiguration of diagnosis in case of sensor or actuator faults ... 428
9.6.5 Extensions and application examples ... 431
9.7 Fault-tolerant control of quantised systems ... 433
9.7.1 Reconfiguration problem ... 433
9.7.2 Graph-theoretic formulation of the control problem ... 435
9.7.3 A reconfiguration method ... 436
Bibliographical notes ... 437

10. Application examples ... 439
10.1 Fault-tolerant control of a three-tank system ... 439
10.1.1 The control problem ... 439
10.1.2 Generic component-based analysis of the three-tank system ... 443
10.1.3 Solution of the reconfiguration task ... 451
10.2 Diagnosis and fault-tolerant control of a chemical process ... 454
10.2.1 System description and control aims ... 454
10.2.2 Plant model for diagnosis ... 457
10.2.3 Experimental diagnostic results ... 457
10.2.4 Control reconfiguration in case of actuator faults ... 463
10.3 Diagnosis and control of a ship propulsion system ... 469
10.3.1 Structure of the ship propulsion system ... 469
10.3.2 Models of the propulsion system ... 471
10.3.3 Fault scenarios and requirements on the diagnosis ... 478
10.3.4 Structural analysis of the propulsion system ... 481
10.3.5 Fault diagnosis by using the parity space approach and state observation ... 485
10.3.6 Diagnosis of the pitch control loop by means of the quantised systems approach ... 489
10.3.7 Fault-tolerant propulsion ... 495
10.4 Supervision of a steam generator ... 496
10.4.1 Description of the process ... 496
10.4.2 Modeling of the steam generator ... 499
10.4.3 Design of the diagnostic system ... 504
10.4.4 Structural analysis ... 507
10.4.5 Fault signatures ... 513
10.4.6 Experimental results ... 515
10.4.7 Fault scenarios ... 516
10.4.8 Conclusions ... 519
10.5 Summary: A guideline for the design of fault-tolerant control ... 519
10.5.1 Architecture ... 519
10.5.2 Design procedure ... 520
Bibliographical notes ... 525

References ... 527

Appendices

Appendix 1: Some prerequisites on vectors and matrices ... 537

Appendix 2: Notions of probability theory ... 540

Appendix 3: $\mathcal{H}_2$ and $\mathcal{H}_\infty$controller design ... 552

Appendix 4: Nomenclature 558

Appendix 5: Terminology 559

Appendix 6: Dictionary 562

Subject index 566