Book Review

Diagnosis and Fault-Tolerant Control — Mogens Blanke, Michel Kinnaert, Jan Lunze, and Marcel Staroswiecki (Berlin, Germany: Springer-Verlag, 2004). *Reviewed by Marian V. Iordache*

One of the major concerns in engineering is that the systems we design behave reasonably well in practice. We deal with imperfect models, model uncertainties, uncertainties in the interaction with the environment, and the finite dependability of the hardware and software components. There are various methods used in the engineering fields that account for such difficulties, including methods that check the dependability of designs by simulations and formal verification, methods for uncertainties in models such as worst case analysis and Monte Carlo analysis, and specific methods that can deal with certain faulty situations, such as in the areas of self-stabilization in Computer science and error-correcting codes in coding theory. In control systems, we have disciplines such as robust control, adaptive control and fault-tolerant control. While these three disciplines have similar goals, a careful look reveals the differences. Following the authors of the book, we notice that fault-tolerant control "aims at changing the control law so as to cancel the effects of the faults and or to attenuate them to an acceptable level." Compared to disturbances and model uncertainties, faults are more severe changes that cannot be suppressed by a fixed controller. This distinguishes fault-tolerant control from robust control, in which a fixed controller is designed as a tradeoff between performance and robustness. Further, the principle of adaptive control is "particularly efficient only for plants described by linear models with slowly varying parameters." However, fault-tolerant control is to deal also with systems of nonlinear behavior, while faults typically involve sudden Parameter changes.

A further distinction can be made between traditional fault tolerance and model-based fault-tolerant control, the latter being approached in the book. Traditional fault tolerance improves the dependability of the system based on physical redundancy: a component is replaced with a component of the Same type when it fails. Model-based fault tolerant control achieves dependability by means of analytical redundancy: In case of faults, changes are made in the control law and possibly also in the plant, by means of reconfigurations.

The field of fault-tolerant control is relatively new. Two surveys of the field are [2] and [3]. Note that fault diagnosis, which has been studied extensively in the literature, is required for the implementation of fault tolerant control. The book puts together several fault-tolerant control and fault diagnosis approaches, with an emphasis on the work of the authors. Application examples are also given, allowing the reader to compare the approaches proposed in the book. In the literature, there is another book on fault-tolerant control [I], which complements the material of the book with methods for systems with Markovian parameters.

The book is organized in ten chapters and six appendices. Chapters 1-3 are introductory, presenting an overview of the main ideas of the book, examples, and the various types of models used in the book. Chapters 4 and 5 present methods applicable at a higher-level of abstraction, in which the analytical details of the plant model are absent. Chapters 6 and 7 address fault diagnosis and fault-tolerant control for continuous variable systems. The Same problems are approached in Chapters 8 and 9 for quantized systems based on a discrete-event approach. Finally, the major approaches presented in the book are illustrated on several examples in Chapter 10. Appendices 1-3 present useful background in linear algebra, stochastic theory, and $\mathcal{H}_2/\mathcal{H}_\infty$ controller design. The other appendices include descriptions of the terminology of the book and a four-language technical dictionary.

Chapter 1 is an introduction to the field of fault-tolerant control. The main ideas are explained clearly and extensively.

Chapter 2 presents two examples that are referred in subsequent chapters of the book. The examples involve realistic models of a two-tank system and of a ship steering system.

Chapter 3, entitled *Models of Dynamical Systems*, presents the various formal models used in the book: Architecture based, structural, continuous variable, discrete-event, and hybrid.

Chapter 4 is titled *Analysis Based on Components and Architecture*. The chapter deals with methods relying on the information available from high-level descriptions of components and their interconnections. First, generic models are introduced, as the high-level description of components. Then, fault propagation analysis is presented. A generic model of a component consists mainly of a description of the services offered by the component, the modes under which the various services are available, and the transitions between modes. An interesting illustration of reconfigurations based on generic model analysis appears later, in Chapter 10. The analysis for fault propagation is algebraic, relying on a graph describing the interconnections between components. A graph-theoretic approach is also proposed for the identification of loops within the graph.

Chapter 5, entitled *Structural Analysis*, deals with methods on the structure graph, which is an abstraction of the equations describing the system. This structural approach can be used for both fault diagnosis and control reconfiguration. The structure graph is a bipartite graph, in which the two types of nodes correspond to variables and constraints, respectively. The links between the nodes are as follows: a variable is linked to a constraint if the variable participates in the constraint. The analysis on the structure graph can provide information on the observability, controllability and monitorability of the system.

Chapter 6 is titled *Fault Diagnosis of Continuous-Variable Systems*. It presents parity space, optimization-based, and Kalman filter approaches for fault-diagnosis. Both deterministic and stochastic models can be considered, as the first two approaches deal with deterministic models. In all cases the faults are modeled as additive signals. In each of the proposed methods, the problem is separated into the design of a *residual generator* and the design of a *residual evaluation* module. The goal of the residual generator is to produce a signal with certain desirable properties, such as sensitivity to the fault signal and no (or little) dependence on disturbances. This signal is then used by the evaluation module for fault detection, isolation and estimation. A brief description of the three approaches is as follows. In the parity space approach, the design of the residual generator corresponds to the design of transfer functions subject to certain equality constraints. The second approach uses suboptimal $\mathcal{H}_\infty$ design to obtain the residual generator. In the case of Kalman filtering, the focus is on change detection algorithms for the design of the residual evaluation, as the residual is a stochastic process in this case.

Chapter 7 is titled *Fault-Tolerant Control of Continuous Variable Systems*. This chapter considers active fault-tolerant control, that is,

The reviewer is with the Department of Electrical Engineering, University of Notre Dame, Notre Dame IN 46556 USA (e-mail: miordach@nd.edu).

Digital Object Identifier 10.1 109lTAC.2004.829648

0018-9286/04$20.00 © 2004 IEEE

fault accommodation and *system reconfiguration*. Fault accommodation is the situation in which only the controller is changed when a fault occurs. In the case of system reconfiguration, there are also sensors/actuators turned off or On. Four approaches are presented here: optimal control, model-matching, reconfiguration with virtual sensors and actuators, and controller redesign based on the Youla-Kucera parameterization. The optimal control approach considers a linear quadratic (LQ) problem. The model-matching method aims to obtain a closed-loop with the same transfer function as in the faultless case. The third method replaces faulty sensors/actuators by virtual sensors (Luenberger observers) and virtual actuators.

Chapter 8 is titled *Diagnosis und Reconfigurable Control of Discrete-Event Systems*. Here, the plant is described by a stochastic automaton and the faults are discrete (and unobservable) events. Note that a stochastic automaton is a nondeterministic automaton with inputs and outputs in which the transition relation is enhanced with a probability distribution. Note also that the output symbols are observable and the input symbols are generated by the controller. The stochastic process modeled by the automaton is assumed to satisfy the Markov property. As the state of the automaton is unknown, the chapter addresses first the state observation problem. The solution to the observation problem is then used for fault diagnosis. Fault diagnosis here involves computing conditional probabilities, namely, the probability that (specific) faults have occurred, given the sequence of inputs applied to the system and the sequence of observed outputs. Finally, tests evaluating the consistency of the observation with the automaton model are used for reconfigurations. In this context, a reconfiguration consists of removing the input/output associated to the faulty sensor/actuator from the estimation process. The approach of this chapter is clearly explained and extensively illustrated on examples.

Chapter 9, *Diagnosis und Reconfiguration of Quantized Systems*, applies the approach of the previous chapter to quantized systems. Quantized systems are continuous-variable systems that can be accessed only through quantizers, where the quantizers produce discrete events. The problem of abstracting a stochastic automaton from a quantized system is approached first. As the automaton can only approximate the real behavior of the system, special care is taken to ensure the automaton model is *complete*, that is, supports all possible input/output sequences of the quantized system. Then, the chapter applies the approach of Chapter 8 to fault diagnosis. Finally, the following reconfiguration problem is considered: moving the operation point back into the nominal region, after a fault has been detected.

Chapter 10 presents several interesting application examples: A three-tank system, a chemical process, a ship propulsion system, and a steam generator. The major approaches of the book are illustrated on these examples.

The book is a valuable resource for researchers from both academia and industry. It can also be used in a graduate-level Course. Even though the book Covers quite different diagnosis and fault-tolerant control methods, the authors have achieved a coherent presentation. I believe most readers will find the presentation self-contained. Overall, the material is readable and clearly presented. There are though typos and instances in which the point of a section is not very obvious (such as fault propagation in closed-loops in Chapter 4) or insufficiently elaborated (such as controller redesign based on the Youla-Kucera parameterization in Chapter 7). However, the reader can pursue further his topics of interest with the help of the detailed bibliographical notes at the end of each chapter.

REFERENCES

[1] M. M. Mahmoud, J. Jiang, and Y. Zhang, *Active Fault Tolerant Control Systems*. New York: Springer-Verlag, 2003.

[2] R. J. Patton, "Fault-tolerant control: The 1997 situation," in *Proc*. IFAC *Symp. Fault Detection, Supervision, Safety for Technical Processes* (*SAFEPROCESS'97*), 1997, pp. 1033-1055.

[3] R. F. Stengel, "Intelligent failure-tolerant control," *IEEE Cont~Syst. Mag.*, vol. 11, June 199 1.