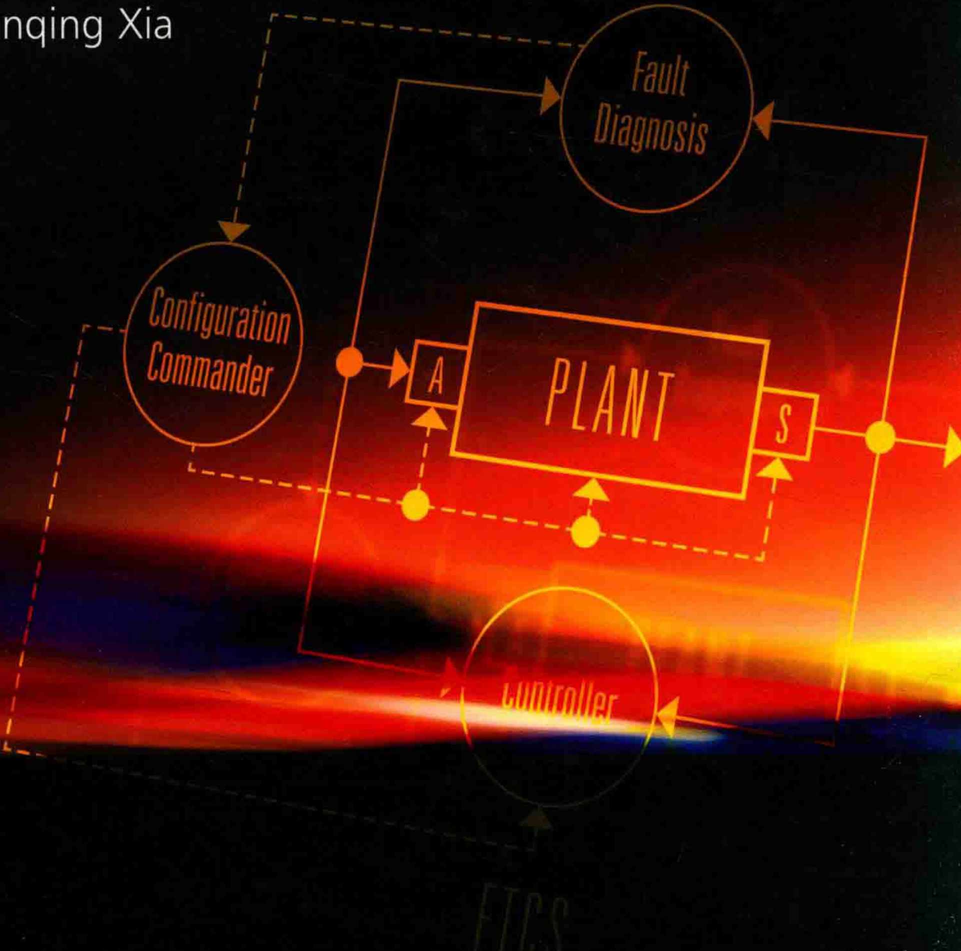
ANALYSIS AND SYNTHESIS OF FAULT-TOLERANT CONTROL SYSTEMS

Magdi S. Mahmoud

Yuanqing Xia



WILEY

ANALYSIS AND SYNTHESIS OF FAULT-TOLERANT CONTROL SYSTEMS

Magdi S. Mahmoud
King Fahd University of Petroleum and Minerals, Saudi Arabia

Yuanqing Xia
Beijing Institute of Technology, China

WILEY

This edition first published 2014

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

Mahmoud, Magdi S.
Analysis and synthesis of fault-tolerant control systems / Magdi S. Mahmoud, Yuanqing Xia.
pages cm
Includes bibliographical references and index.
ISBN 978-1-118-54133-3 (cloth)
1. Automatic control. 2. Fault tolerance (Engineering) 3. Control theory. I. Xia, Yuanqing. II. Title.
III. Title: Analysis and synthesis of FTCS.
TJ213.M268428 2013
629.8–dc23

2013023504

A catalogue record for this book is available from the British Library.

ISBN: 978-1-118-54133-3

Typeset in 10/12pt Times by Aptara Inc., New Delhi, India
Printed and bound in Singapore by Markono Print Media Pte Ltd

1 2014

To my loving wife, Salwa
To the 'M' family:
Medhat, Monda, Mohamed,
Menna, Malak, Mostafa
and Mohamed

MSM

To my honest and diligent
wife, Wang Fangyu
To my lovely daughter,
Xia Jingshu

YX

Preface

In recent years, we have been witnessing sophisticated control systems designed to meet increased performance and safety requirements for modern technological systems. Technical experience has indicated that conventional feedback control design for a complex system may result in an unsatisfactory performance, or even instability, in the event of malfunctions in actuators, sensors or other system components. In order to circumvent such weaknesses, new approaches to control system design have emerged with the goal of tolerating component malfunctions while maintaining desirable stability and performance properties. These types of control system are often known as "fault-tolerant control systems" (FTCS). The area of fault-tolerant control systems is a complex interdisciplinary research field that covers a diverse range of engineering disciplines, such as modeling and identification, applied mathematics, applied statistics, stochastic system theory, reliability and risk analysis, computer communications, control, signal processing, sensors and actuators, as well as hardware and software implementation techniques.

Modern technological systems rely on sophisticated control systems to meet performance and safety requirements. A conventional feedback control design for a complex system may result in unsatisfactory performance, or even instability, in the event of malfunctions in actuators, sensors or other system components. To overcome such weaknesses, new approaches to control system design have been developed in order to tolerate component malfunctions while maintaining the required levels of stability and performance. This is particularly important for safety-critical systems, such as aircraft, spacecraft, nuclear power plants, and chemical plants processing hazardous materials. In such systems, the consequences of a minor fault in a system component can be catastrophic. Therefore, the demand for reliability, safety and fault tolerance is generally high. It is necessary to design control systems which are capable of tolerating potential faults in these systems in order to improve the reliability and availability while providing desirable performance. More precisely, FTCS are control systems that possess the ability to accommodate component failures automatically. They are capable of maintaining overall system stability and acceptable performance in the event of such failures. In other words, a closed-loop control system which can tolerate component malfunctions, while maintaining desirable performance and stability properties is said to be a fault-tolerant control system [1].

The problem of fault monitoring has always been an area of much importance for research departments in industry. This becomes even more of a priority when we are dealing with nonlinear systems. Monitoring of uncommon behavior of plant and detecting unprecedented changes in systems are essential for maintaining the health of a system, followed by the removal of faulty components, replacement with the better ones, restructuring system architecture, and thus improving overall system reliability. However, with the increasing complexity of modern nonlinear systems, process engineers are facing tough challenges to understand and troubleshoot possible system problems. Highly efficient fault-monitoring methods have become a valuable asset in the life of large systems.

This book is about the analysis and design methods of fault-tolerant control systems. Particular consideration is given to covering wide topics that have been treated in the literature and presenting the results of typical case studies. The key feature is to provide a teaching-oriented volume supported by research.

The terminologies, conventions and notations that have been adopted throughout this book are explicitly presented in place to facilitate smooth readibilty of the different sections. They are quite standard in the scientific media and vary only in form or character.

Magdi S. Mahmoud
Dhahran, Saudi Arabia

Yuanqing Xia
Beijing, China
March 2013

Reference

[1] Zhang, Y., and Jiang, J. (2008) "Bibliographical review on reconfigurable fault-tolerant control systems", *Annual Reviews in Control* **32**, 229–252.

Acknowledgments

The subject matter of fault-tolerant control systems is perhaps one of the most attractive areas of contemporary reserarch and development. It embodies fault diagnosis, fault estimation, fault identification, and fault isolation, to name but a few topics. The topics discussed in this book have constituted an integral part of our academic research investigation over the past few years. The idea of writing the book arose and developed through communication with Dr Nigel Hollingworth. We would like to acknowledge the tireless effort and professional support from Wiley, particularly from Anne Hunt and Tom Carter.

In writing this volume, we have taken the approach of referring within the text to papers or books which we believe have taught us some concepts, ideas and methods. We have further complemented this by adding remarks and notes within and at the end of each chapter to shed light on other related results. We are indebted to the colleagues who introduced us to the subject of fault-tolerant control systems and to the people who made the writing of this book possible.

Magdi Mahmoud owes a measure of gratitude to the management of King Fahd University of Petroleum and Minerals (KFUPM, Saudi Arabia) for continuous encouragement and facilitating all sources of help. Particular appreciation goes to the deanship of scientific research (DSR) for providing a superb competitive environment for research activities through internal funding grants. It is a great pleasure to acknowledge the financial funding afforded by DSR through Project IN121003 and for providing overall support of research activities at KFUPM.

During the past five years, Magdi Mahmoud has had the privilege of teaching various graduate courses at KFUPM. The updated and organized course notes have been instrumental in generating chapters of this book. Valuable comments and suggestions by graduate students have been extremely helpful, particularly from those who attended the courses SE509, SE514, SE517, and SE650, offered by the Systems Engineering Department from 2007 to 2011.

Magdi Mahmoud deeply appreciates the efforts of Muhammad Sabih, Mirza H. Baig, Azhar M. Memon, Haris M. Khalid and Rohmat Widodo as well as Wen Xie from BIT for their unfailing help in preparing portions of the manuscript and performing numerous effective simulations.

The widely-recognized research work of Yuanqing Xia and his students on predictive control and related topics at the School of Automation, Beijing Institute of Technology (BIT) has contributed effectively to several sections of this volume.

Most of all however, we would like to express our deepest gratitude to all the members of our families and especially our wives, Salwa and Wang Fangyu, for their elegant style.

Without their constant love, incredible amount of patience and (mostly) enthusiastic support, this volume would not have been finished.

We would appreciate any comments, questions, criticisms, or corrections that readers may take the trouble of communicating to us at msmahmoud@kfupm.edu.sa, magdim@yahoo.com or yuanqing.xia@gmail.com.

Contents

1

Introduction

For more than three decades, the growing demand for safety, reliability, maintainability, and survivability in technical systems has created significant research interest in fault detection and diagnosis (FDD). Such efforts have led to the development of many FDD techniques. For a general exposure to the subject, the reader is directed to [1]–[5].

1.1 Overview

In the literature, fault detection and isolation or fault detection and identification are often used interchangeably and abbreviated as "FDI". To be precise and avoid further confusion, this book adopts the term "FDI" to stand for "fault detection and isolation"; "FDD" is used when the fault identification function is added to FDI. In FTCS designs, fault identification is important; therefore FDD is mainly used throughout this book to highlight the requirement of fault identification.

On a parallel path, research into reconfigurable fault-tolerant control systems has increased progressively since the initial research on restructurable control and self-repairing flight control systems began in the early 1980s (see [6]–[10]). More recently, fault-tolerant control has attracted more and more attention in both industry and academic communities due to increased demands for safety, high system performance, productivity and operating efficiency in wider engineering applications, not limited to traditional safety-critical systems. Several review or survey papers on FTCS have appeared since the 1990s including [11]–[16].

Fault tolerance is no longer limited to high-end systems and consumer products such as automobiles. However it is increasingly dependent on microelectronic and mechatronic systems, on-board communication networks, and software, thus requiring new techniques for achieving fault tolerance. Even though individual research on FTCS has been carried out extensively, systematic concepts, design methods, and even terminology are still not yet standardized. Recently, efforts have been made to unify some terminology [17]. In addition, for historical reasons and because of the complexity of the problem, most of the research on FDD and reconfigurable control (RC) has been treated as two separate fields. More specifically, most of the FDI techniques have been developed as a diagnostic or monitoring tool, rather

Analysis and Synthesis of Fault-Tolerant Control Systems, First Edition. Magdi S. Mahmoud and Yuanqing Xia.

than as an integral part of FTCS. As a result, some FDD methods may not satisfy the need of controller reconfiguration. On the other hand, most of the research on reconfigurable control is carried out assuming the availability of a perfect FDD. Little attention has been paid to analysis and design with the overall system structure and interaction between FDD and RC.

For example, the following questions are posed:

- From the viewpoint of RC design what are the needs and requirements for FDD?
- What information can be provided by existing FDD techniques for overall FTCS designs?
- How can we analyze systematically the interaction between FDD and RC?
- How can we design FDD and RC in an integrated manner for online and real-time applications?

Many other challenging issues still remain open for further research and development. One of the motivations of this book is to provide an overview of developments in FTCS and to address some challenging problems to attract the attention of future research.

1.2 Basic Concepts of Faults

The terminology used in this book is fairly standard. Below, some basic definitions of faults, failure, disturbances and uncertainties, fault detection, fault isolation, fault identification, and fault diagnosis are given. The interested reader is referred to [18, 19, 20] for more detailed explanation of the above mentioned terminology.

A "fault" is an unpermitted deviation of at least one characteristic property or parameter of a system from the acceptable (standard condition). The closely related term "failure" is regarded as a permanent interruption of a system's ability to perform a required function under specified operating conditions. *Failure* is used for the complete breakdown of a system, while *fault* is used to indicate a deviation from the normal characteristics. As far as detection is concerned, both faults and failures can be treated alike. Moreover, a fault can be treated as an external input or as a parameter deviation which changes the system characteristics. Similar to faults, "disturbances", "uncertainties", and "noises" can also be treated as external inputs. In fault detection and isolation (FDI) terminology, they are termed as "unknown inputs". Unlike faults, these unknown inputs are uncontrolled, unavoidable and are present during normal operation. The effect of the unknown inputs can be incorporated into the controller design and a process can perform well even in the presence of them. Faults, on the other hand, have very severe effects on the process and should be detected.

The process of *fault diagnosis* is referred to as the determination of the size, location, time of detection and type of fault in the process. Based on its performance, a fault diagnosis system (FDS) is regarded as a fault detection (FD), fault detection and isolation (FDI) or fault detection, isolation and analysis (FDIA) system [18]. An FD system is therefore the process of determining the fault in the process and its time of occurrence. An FDI system determines in addition the kind and location of the fault. Similarly, an FDIA, together with detection and isolation, also aims to determine the size and time behavior of the fault. It is worth noting that the existence conditions for fault isolation are more stringent than for fault detection, and even more so in the case of fault identification. Consequently, it is difficult to isolate or identify faults in most situations.