Functional Safety for Embedded Systems

Guoqi Xie
Yawen Zhang
Renfa Li
Kenli Li
Keqin Li

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Designed cover image: Guoqi Xie, Yawen Zhang, Renfa Li, Kenli Li, Keqin Li

Supported by the Key Projects of National Natural Science Foundation of China (NSFC) under the Grants 61932010 and 62133014.

First edition published 2023
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

Library of Congress Cataloging-in-Publication Data

ISBN: 978-1-032-48936-0 (hbk)
ISBN: 978-1-032-48938-4 (pbk)
ISBN: 978-1-003-39151-7 (ebk)

DOI: 10.1201/9781003391517

Typeset in Latin Modern font
by KnowledgeWorks Global Ltd.

Publisher's note: This book has been prepared from camera-ready copy provided by the authors.

Contents

SECTION II SAFETY-AWARE COST OPTIMIZATION

Foreword

Embedded systems are widely used in many consumer electronics, entertainment devices, home appliances, industrial equipment, medical instruments, military weapons, and research facilities. They are extensively used in application areas such as aerospace control systems, automobile industry, banking and finance, robotic systems, security and telecommunication, and traffic control.

Modern automobiles are typical safety-critical embedded systems, and development of self-driving systems is one of the hottest research areas in recent years. Meanwhile, the continuous advancement of embedded systems brings new functional safety requirements and design challenges. In recent years, some organizations have issued individual functional safety standards related to embedded systems, and the relevant functional safety research is gradually applied to practical applications. However, the functional safety assurance for embedded systems is a complex process, especially for parallel applications in distributed environments. There is an urgent need to design functional safety assurance techniques from the perspective of computing technology, thereby coping with respective characteristics and challenges of distributed embedded systems. The publication of this book satisfies this need in a timely manner.

The book introduces the functional safety standards related to embedded systems. It presents the design methods of functional safety assurance (including functional safety verification, enhancement, and validation), safety-aware hardware cost optimization, and safety-aware development cost optimization for embedded systems. The book combines the practical example of automotive embedded systems with the proposed functional safety design methods.

The book proposes various algorithms about functional safety assurance and safety-aware cost optimization for parallel applications of embedded systems. The book is rich in content and detailed in diagrams. A unique and effective feature of the book is to use appropriate motivational examples to clearly explain each proposed algorithm for the purpose of easier understanding. This book contains not only the basic knowledge and information, but also the latest research progress on the theory and methods of functional safety for embedded systems.

This book is the joint effort and endeavor of five scholars who have published very extensively in the fields of embedded computing, high-performance computing, embedded systems, and cyber-physical systems in the past few years. They are undoubtedly leading experts in the fields of embedded computing and high-performance computing. Their distinction and dedication make the book an important addition to the research community. The book is truly a significant contribution to the field of functional safety for embedded systems.

Finally, I would like to congratulate the authors for their solid work, and I look forward to seeing the book published.

Weimin Zheng
Member of the Chinese Academy of Engineering
Tsinghua University
Beijing, China

Preface

MOTIVATION OF THE BOOK

Ensuring functional safety is always a precondition in the realization of various embedded systems. However, the functional safety design of the system is challenged by multiple factors. Taking the automotive embedded system as an example, the complexity of the new generation automotive electrical and electronic (E/E) architecture, the continuous release and update of automotive functional safety standards, the publish of new AUTOSAR adaptive platform standard, and the increase in different kinds of costs bring challenges to functional safety design. Automotive systems are safety-critical embedded systems, consequences will be serious if functional safety cannot be guaranteed. Therefore, automobile manufacturers attach great importance to functional safety. In addition, the automobile industry is a cost-sensitive industry, so it is necessary to optimize costs while ensuring safety. This book uses the automotive embedded system as an example to introduce functional safety assurance and safety-aware cost optimization. The functional safety assurance integrates safety verification, enhancement, and validation. The safety-aware cost optimization divides cost types in terms of the essential differences of various costs in system design. The motivation of this book is to provide our recent research results on the aforementioned topics in recent years.

SUMMARY OF CONTENTS

Chapter 1 introduces functional safety for embedded systems. Most embedded systems are safety-critical systems, that must meet reliability and response time requirements simultaneously. This chapter takes the automotive embedded system as an example to introduce the functional design methods for ensuring functional safety, including functional safety verification, enhancement, and validation. The automotive industry is a cost-sensitive industry, and safety-aware cost optimization is a beneficial supplement to improve system design. Therefore, this chapter analyzes the necessities and challenges of hardware cost optimization and development cost optimization. Finally, this chapter lists the outline of this book.

Chapter 2 proposes a fast functional safety verification(FFSV) technique for parallel applications of embedded systems. First, this chapter presents the FFSV1 method to find the solution with the minimum response time under the reliability requirement. Second, this chapter presents the FFSV2 method to find the solution with the maximum reliability under the response time requirement. Finally, this chapter combines FFSV1 and FFSV2 to create the union FFSV (UFFSV). UFFSV is a fast heuristic method, and it can shorten the application's development lifecycle.

Chapter 3 studies functional safety enhancement techniques for parallel applications of embedded systems. This chapter presents forward safety enhancement(FFSE), repeated backward functional safety enhancement(RBFSE), and repeated FSE(RFFSE) algorithms to enhance the reliability values for a parallel application on automotive embedded systems. Considering that RBSE and RFSE could be invoked repeatedly until reaching a stable safety value, we propose the stable stopping-based safety enhancement (SSFSE) approach by combining the above algorithms. SSSE enhances the safety by using a stable stopping approach on the basis of the forward-and-backward recovery through primary-backup repetition.

Chapter 4 focuses on functional safety validation for parallel applications of embedded systems, this chapter proposes two effective reliability validation approaches, geometric mean-based non-fault-tolerant reliability pre-assignment (GMNRA) and geometric mean-based fault-tolerant reliability pre-assignment(GMFRA), for an automotive application based on geometric mean. These two approaches are used for the mechanisms of non-fault-tolerance and fault-tolerance, respectively.

Chapter 5 designs two hardware cost optimization methods. The first method proposes the progressive hardware cost optimization (PHCO), enhanced PHCO (EPHCO), and simplified EPHCO (SEPHCO) algorithms step by step for a distributed application while ensuring the functional safety requirement. The second approach proposes the cost-effectiveness-driven hardware cost optimization algorithm (CEHCO) for a distributed application while meeting the functional safety requirement.

Chapter 6 solves the problem of development cost optimization for an end-to-end embedded system function under ensuring the functional safety requirements based on the automotive safety integrity level (ASIL) decomposition defined in ISO 26262. First, this chapter proposes two heuristic algorithms, reliability calculation of scheme(RCS) and minimum development cost with reliability requirement(MDCRR) for parallel applications on distributed embedded systems. Second, this chapter presents FRA and DRA algorithms considering reliability and real-time requirements for real-time parallel applications on distributed embedded systems.

Chapter 7 summarizes the book and mentions future research.

AUDIENCE AND READERSHIP

This book should be a useful reference for researchers, engineers, and practitioners interested in embedded systems, Cyber-Physical Systems(CPSs), and functional safety of automotive embedded systems. This book can be used as a supplement to the advanced undergraduate or graduate courses of embedded computing, distributed computing, and CPSs in computer science, computing engineering, and electrical engineering. By reading this book, postgraduates and doctoral students will be familiar with the functional safety attributes of embedded systems, learn functional safety assurance and cost optimization algorithms, and find inspiration for their own research.

ACKNOWLEDGMENTS

This book was supported by the Key Projects of National Natural Science Foundation of China (NSFC) under the Grants 61932010 and 62133014, and the Outstanding Youth Fund of the Natural Science Foundation of Hunan Province under the Grant 2022JJ10021. The Grant 61932010 is titled “modeling theory and system design for safety- and security-critical automotive cyber-physical systems”, the Grant 62133014 is titled “intelligent interconnection of things and integrated safety and security in industrial cyber-physical systems”, and the Grant 2022JJ10021 is titled “real-time systems”. Part of the research in this book was done in conjunction with researchers Gang Zeng, Hao Peng, Jia Zhou, Jinlin Song, Na Yuan, Shiyan Hu, Wei Wu, Wenhong Ma, Yan Liu, Yanwen Li, Yong Xie, Yuekun Chen, Yunbo Han, Zhetao Li, and we are grateful for their contributions. The authors would like to express their gratitude to Professor Weimin Zheng, a member of the Chinese Academy of Engineering, for writing the foreword of this book. We also thank Ms. Joy Luo of Taylor & Francis Group for her efforts and support in helping to publish this book.

Contributors

Guoqi Xie
Key Laboratory for Embedded and Cyber-Physical Systems of Hunan Province, College of Computer Science and Electronic Engineering, Hunan University
Changsha, Hunan, China

Yawen Zhang
Key Laboratory for Embedded and Cyber-Physical Systems of Hunan Province, College of Computer Science and Electronic Engineering, Hunan University
Changsha, Hunan, China

Renfa Li
Key Laboratory for Embedded and Cyber-Physical Systems of Hunan Province, College of Computer Science and Electronic Engineering, Hunan University
Changsha, Hunan, China

Kenli Li
College of Computer Science and Electronic Engineering, Hunan University
Changsha, Hunan, China

Keqin Li
Department of Computer Science, State University of New York
New Paltz, NY, USA