

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

© 2023 Guoqi Xie, Yawen Zhang, Renfa Li, Kenli Li, Keqin Li

Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact mpkbookspermissions@tandf.co.uk

Trademark notice: Product or corporate names may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe.

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

Foreword	xi
Preface	xiii
Contributors	xvii
CHAPTER 1 ■ Introduction	1

1.1	AUTOMOTIVE EMBEDDED SYSTEMS	1
1.2	FUNCTIONAL SAFETY	2
1.2.1	Functional Safety Standard	2
1.2.2	Automotive Safety Integrity Level (ASIL) Determination	3
1.3	CHALLENGES OF FUNCTIONAL SAFETY DESIGN	5
1.4	STRUCTURE OF THE RESEARCH	6
1.5	FUNCTIONAL SAFETY ASSURANCE	6
1.5.1	Functional Safety Verification	6
1.5.2	Functional Safety Enhancement	7
1.5.3	Functional Safety Validation	7
1.6	SAFETY-AWARE COST OPTIMIZATION	7
1.6.1	Hardware Cost Optimization	8
1.6.2	Development Cost Optimization	8
1.7	OUTLINE OF THE BOOK	8
1.8	CONCLUDING REMARKS	9

SECTION I ■ FUNCTIONAL SAFETY ASSURANCE

CHAPTER 2 ■ Functional Safety Verification	13
---	-----------

2.1	INTRODUCTION	13
2.2	RELATED WORK	15
2.3	MODELS AND PRELIMINARIES	16

2.3.1	System Model	16
2.3.2	Reliability Model	18
2.3.3	Reliability Requirement Assessment	20
2.3.4	Real-Time Requirement Assessment	20
2.3.5	Problem Statement	22
2.4	RESPONSE TIME MINIMIZATION UNDER RELIABILITY REQUIREMENT	23
2.4.1	Satisfying Reliability Requirement	23
2.4.2	Response Time Minimization	25
2.4.3	Example of the FFSV1	27
2.5	RELIABILITY MAXIMIZATION UNDER REAL-TIME REQUIREMENT	28
2.5.1	Satisfying Real-Time Requirement	28
2.5.2	Reliability Maximization	30
2.5.3	Example of the FFSV2	32
2.5.4	Union Verification	32
2.6	EXPERIMENTS FOR FUNCTIONAL SAFETY VERIFICATION ALGORITHMS FFSV2, FFSV2, AND UFFSV	33
2.6.1	Real-Life Parallel Application	33
2.6.2	Synthetic Parallel Application	36
2.7	CONCLUDING REMARKS	37
CHAPTER 3	Functional Safety Enhancement	39
<hr/>		
3.1	INTRODUCTION	39
3.2	RELATED WORK	41
3.3	MODELS AND PROBLEM STATEMENT	42
3.3.1	Lower Bound of Application	42
3.3.2	Problem Statement	44
3.4	BACKWARD AND FORWARD SAFETY ENHANCEMENT	44
3.4.1	Existing BFSE Algorithm	44
3.4.2	FFSE Algorithm	45
3.5	REPEATED SAFETY ENHANCEMENT	49
3.5.1	RBFSE Algorithm	49
3.5.2	RFFSE Algorithm	51
3.5.3	Stable Stopping-Based Functional Safety Enhancement	52
3.6	EXPERIMENTS FOR FUNCTIONAL SAFETY ENHANCEMENT TECHNIQUE SSFSE	56

3.6.1	Real-Life Parallel Application	56
3.6.2	Synthetic Parallel Application	59
3.7	CONCLUDING REMARKS	60
CHAPTER	4 ■ Functional Safety Validation	61
<hr/>		
4.1	INTRODUCTION	61
4.2	RELATED WORK	62
4.3	MODELS	63
4.3.1	System Architecture	63
4.3.2	Reliability Model	64
4.3.3	Problem Statement	65
4.4	NON-FAULT TOLERANT FUNCTIONAL SAFETY VALIDATION	66
4.4.1	Non-Fault Tolerant Reliability Requirement Assessment	66
4.4.2	Existing Non-Fault Tolerant Functional Safety Validation Algorithms	66
4.4.3	Example of the MRTRR Algorithm	68
4.4.4	Use of Geometric Mean under Non-Fault Tolerance	70
4.4.5	GMNRA Algorithm	72
4.4.6	Example of the GMNRA Algorithm	74
4.5	FAULT TOLERANT RELIABILITY REQUIREMENT VALIDATION	75
4.5.1	Fault Tolerant Reliability Requirement Assessment	75
4.5.2	Existing Fault Tolerant Functional Safety Validation Algorithms	75
4.5.3	Use of Geometric Mean under Fault Tolerance	76
4.5.4	Optimizing Response Time	77
4.5.5	GMFRA Algorithm	78
4.5.6	Example of the GMFRA Algorithm	80
4.6	EXPERIMENTS FOR FUNCTIONAL SAFETY VALIDATION ALGORITHMS GMNRA AND GMFRA	81
4.6.1	Real-Life Parallel Application	81
4.6.2	Synthetic Parallel Application	84
4.7	CONCLUDING REMARKS	85

SECTION II SAFETY-AWARE COST OPTIMIZATION

CHAPTER 5 ■ Hardware Cost Optimization	89
5.1 INTRODUCTION	89
5.1.1 Progressive Hardware Cost Optimization	89
5.1.2 Cost-Effectiveness-Driven Hardware Cost Optimization	90
5.2 RELATED WORK	91
5.3 MODELS AND PROBLEM STATEMENT	92
5.3.1 Hardware Cost Model	92
5.3.2 Problem Statement	93
5.4 PROGRESSIVE HARDWARE COST OPTIMIZATION	93
5.4.1 IHCO Algorithm	93
5.4.2 PHCO Algorithm	94
5.4.3 Example of the PHCO Algorithm	96
5.5 ENHANCED PROGRESSIVE HARDWARE COST OPTIMIZATION	96
5.5.1 EPHCO Algorithm	96
5.5.2 RE Algorithm	97
5.5.3 Real-time Requirement of Tasks	99
5.5.4 Reliability Enhancement of Tasks	101
5.5.5 Example of the EPHCO Algorithm	102
5.5.6 SEPHCO Algorithm	103
5.5.7 Optimal Solutions of the Motivational Parallel Application	104
5.6 HARDWARE COST OPTIMIZATION BY CLOSED-TO-OPENED	104
5.6.1 CEHCO1 Algorithm	104
5.6.2 Iteration Process of CEHCO1	106
5.7 HARDWARE COST OPTIMIZATION BY OPENED-TO-CLOSED	108
5.7.1 CEHCO2 Algorithm	108
5.7.2 Iteration Process of CEHCO2	108
5.7.3 CEHCO Algorithm	109
5.8 EXPERIMENTS FOR HARDWARE COST OPTIMIZATION ALGORITHMS	111
5.8.1 Experimental Conditions and Instructions	111
5.8.2 Experimental Details and Analyses	111
5.9 CONCLUDING REMARKS	116

CHAPTER 6 ■ Development Cost Optimization	117
<hr/>	
6.1 INTRODUCTION	117
6.1.1 Development Cost Optimization with Reliability Requirement	117
6.1.2 Safety Assurance and Development Cost Optimization	118
6.2 RELATED WORK	119
6.3 ASIL DECOMPOSITION	120
6.3.1 Exposure and Reliability Requirement	121
6.4 MODEL AND PROBLEM STATEMENT	122
6.4.1 Systems Model	122
6.4.2 Motivational Example	123
6.4.3 Development Cost Model	124
6.4.4 Reliability Model	125
6.4.5 Problem Statement	126
6.5 RELIABILITY CALCULATION OF SCHEMES	127
6.5.1 Reliability Calculation	127
6.5.2 RCS Algorithm	128
6.6 MINIMIZING DEVELOPMENT COST WITH RELIABILITY REQUIREMENT	128
6.6.1 Task Prioritization	129
6.6.2 Satisfying Reliability Requirement	130
6.6.3 Minimizing Development Cost	132
6.6.4 Example of MDCRR Algorithm	133
6.7 FUNCTIONAL SAFETY RISK ASSESSMENT	134
6.7.1 Reliability Risk Assessment	134
6.7.2 Real-Time Risk Assessment	135
6.7.3 FRA Algorithm	137
6.7.4 Example of FRA Algorithm	138
6.8 DEVELOPMENT COST OPTIMIZATION WITH FUNCTIONAL SAFETY REQUIREMENTS	139
6.8.1 Reliability Requirement Assurance	139
6.8.2 Real-Time Requirement Assurance	140
6.8.3 Optimizing Development Cost	141
6.8.4 Example of DRA Algorithm	142
6.9 EXPERIMENTS FOR DEVELOPMENT COST OPTIMIZATION ALGORITHM MDCRR	143

x ■ Contents

6.9.1	Experimental Metrics	143
6.9.2	Real-Life Parallel Application	143
6.9.3	Synthetic Parallel Application	146
6.10	EXPERIMENTAL FOR DEVELOPMENT COST OPTIMIZATION ALGORITHMS FRA AND DRA	147
6.10.1	Real-Life Parallel Application	147
6.10.2	Synthetic Parallel Application	150
6.11	CONCLUDING REMARKS	151
CHAPTER	7 ■ Summary and Future Research	153
<hr/>		
7.1	SUMMARY	153
7.2	FUTURE RESEARCH	154
	Bibliography	157

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