



国防科技图书出版基金

“十二五”国家重点出版规划项目

航天器和导弹制导、导航与控制

航天器控制计算机容错技术

Fault Tolerance Techniques
for Spacecraft Control Computer

杨孟飞 华更新 冯彦君 龚健 © 编著



国防工业出版社
National Defense Industry Press



国防科技图书出版基金

杨孟飞 华更新 冯彦君

航天器控制计算机容错技术

Fault Tolerance Techniques for Spacecraft Control Computer

Introduction

Fault Tolerance Architecture and Key Techniques

Fault Detection Techniques

Bus Techniques

Software Fault Tolerance Techniques

Fault Tolerant Techniques of FPGA

Fault Injection Techniques

Intelligence Fault Tolerance Techniques



国防工业出版社
National Defense Industry Press

图书在版编目(CIP)数据

航天器控制计算机容错技术 / 杨孟飞等编著. —北京:
国防工业出版社, 2014. 3

(航天器和导弹制导、导航与控制丛书)

ISBN 978 - 7 - 118 - 09074 - 1

I. ①航... II. ①杨... III. ①航天器 - 飞行控制 -
电子计算机 - 容错技术 IV. ①V448. 2②TP302. 8

中国版本图书馆 CIP 数据核字(2014)第 031262 号

航天器控制计算机容错技术

编 著 者 杨孟飞 华更新 冯彦君 龚 健

责 任 编 辑 王 华

出 版 发 行 国防工业出版社(010 - 88540717 010 - 88540777)

地 址 邮 编 北京市海淀区紫竹院南路 23 号, 100048

经 售 新华书店

印 刷 北京嘉恒彩色印刷有限责任公司

开 本 710 × 960 1/16

印 张 20½

印 数 1 - 2500 册

字 数 305 千字

版 印 次 2014 年 3 月第 1 版第 1 次印刷

定 价 98.00 元

(本书如有印装错误, 我社负责调换)



致读者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分,又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展,加强社会主义物质文明和精神文明建设,培养优秀科技人才,确保国防科技优秀图书的出版,原国防科工委于1988年初决定每年拨出专款,设立国防科技图书出版基金,成立评审委员会,扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是:

1. 在国防科学技术领域中,学术水平高,内容有创见,在学科上居领先地位的基础科学理论图书;在工程技术理论方面有突破的应用科学专著。
2. 学术思想新颖,内容具体、实用,对国防科技和武器装备发展具有较大推动作用的专著;密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。
3. 有重要发展前景和有重大开拓使用价值,密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。
4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作,负责掌握出版基金的使用方向,评审受理的图书选题,决定资助的图书选题

和资助金额,以及决定中断或取消资助等。经评审给予资助的图书,由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就,积累和传播科技知识的使命。在改革开放的新形势下,原国防科工委率先设立出版基金,扶持出版科技图书,这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物,是对出版工作的一项改革。因而,评审工作需要不断地摸索、认真地总结和及时地改进,这样,才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授,以及社会各界朋友的热情支持。

让我们携起手来,为祖国昌盛、科技腾飞、出版繁荣而共同奋斗!

国防科技图书出版基金

评审委员会

国防科技图书出版基金

第七届评审委员会组成人员

主任委员 王 峰

副主任委员 吴有生 蔡 镭 杨崇新

秘 书 长 杨崇新

副 秘 书 长 邢海鹰 贺 明

委员（按姓氏笔画排序）

才鸿年	马伟明	王小谟	王群书	甘茂治
甘晓华	卢秉恒	巩水利	刘泽金	孙秀冬
陆 军	芮筱亭	李言荣	李德仁	李德毅
杨 伟	肖志力	吴宏鑫	张文栋	张信威
陈良惠	房建成	赵万生	赵凤起	郭云飞
唐志共	陶西平	韩祖南	傅惠民	魏炳波

《航天器和导弹制导、导航与控制》

丛书编委会

顾 问 陆元九* 屠善澄* 梁思礼*

主任委员 吴宏鑫*

副主任委员 房建成
(执行主任)

委员 (按姓氏笔画排序)

马广富	王 华	王 辉	王 巍*	王子才*
王晓东	史忠科	包为民*	邢海鹰	任 章
任子西	刘 宇	刘良栋	刘建业	汤国建
孙承启	孙柏林	孙敬良*	孙富春	孙增圻
严卫钢	李俊峰	李济生*	李铁寿	杨树兴
杨维廉	吴 忠	吴宏鑫*	吴森堂	余梦伦*
张广军*	张天序	张为华	张春明	张弈群
张履谦*	陆宇平	陈士橹*	陈义庆	陈定昌*

陈祖贵	周 军	周东华	房建成	孟执中 *
段广仁	侯建文	姚 郁	秦子增	夏永江
徐世杰	殷兴良	高晓颖	郭 雷 *	郭 雷
唐应恒	黄 琳 *	黄培康 *	黄瑞松 *	曹喜滨
崔平远	梁晋才 *	韩 潮	曾广商 *	樊尚春
魏春岭				

常务委员 (按姓氏笔画排序)

任子西	孙柏林	吴 忠	吴宏鑫 *	吴森堂
张天序	陈定昌 *	周 军	房建成	孟执中 *
姚 郁	夏永江	高晓颖	郭 雷	黄瑞松 *
魏春岭				

秘 书	全 伟	宁晓琳	崔培玲	孙津济	郑 丹
-----	-----	-----	-----	-----	-----

注:人名有*者均为院士。

总 序

航天器(Spacecraft)是指在地球大气层以外的宇宙空间(太空),按照天体力学的规律运行,执行探索、开发或利用太空及天体等特定任务的飞行器,例如人造地球卫星、飞船、深空探测器等。导弹(Guided Missile)是指携带有效载荷,依靠自身动力装置推进,由制导和导航系统导引控制飞行航迹,导向目标的飞行器,如战略/战术导弹、运载火箭等。

航天器和导弹技术是现代科学技术中发展最快、最引人注目的高新技术之一。它们的出现使人类的活动领域从地球扩展到太空,无论是从军事还是从和平利用空间的角度都使人类的认识发生了极其重大的变化。

制导、导航与控制(Guidance Navigation and Control, GNC)是实现航天器和导弹飞行性能的系统技术,是飞行器技术最复杂的核心技术之一,是集自动控制、计算机、精密机械、仪器仪表以及数学、力学、光学和电子学等多领域于一体的前沿交叉科学技术。

中国航天事业历经 50 多年的努力,在航天器和导弹的制导、导航与控制技术领域取得了辉煌的成就,达到了世界先进水平。这些成就不仅为增强国防实力和促进经济发展起了重大作用,而且也促进了相关领域科学技术的进步和发展。

1987 年出版的《导弹与航天丛书》以工程应用为主,体现了工程的系统性和实用性,是我国航天科技队伍 30 年心血凝聚的精神和智慧成果,是多种专业技术工作者通力合作的产物。此后 20 余年,我国航天器和导弹的制导、导航与控制技术又有了突飞猛进的发展,取得了许多创新性成果,这些成果是航天器和导弹的制导、导航与控制领域的新理论、新方法和新技术的集中体现。为适应新形势的需要,我们决定组织撰写出版《航天器

和导弹制导、导航与控制》丛书。本丛书以基础性、前瞻性和创新性研究成果为主,突出工程应用中的关键技术。这套丛书不仅是新理论、新方法、新技术的总结与提炼,而且希望推动这些理论、方法和技术在工程中推广应用,更希望通过“产、学、研、用”相结合的方式使我国制导、导航与控制技术研究取得更大进步。

本丛书分两个部分:第一部分是制导、导航与控制的理论和方法;第二部分是制导、导航与控制的系统和器件技术。

本丛书的作者主要来自北京航空航天大学、哈尔滨工业大学、西北工业大学、国防科学技术大学、清华大学、北京理工大学、华中科技大学和南京航空航天大学等高等学校,中国航天科技集团公司和中国航天科工集团公司所属的研究院所,以及“宇航智能控制技术”、“空间智能控制技术”、“飞行控制一体化技术”、“惯性技术”和“航天飞行力学技术”等国家级重点实验室,而且大多为该领域的优秀中青年学术带头人及其创新团队的成员。他们根据丛书编委会总体设计要求,从不同角度将自己研究的创新成果,包括一批获国家和省部级发明奖与科技进步奖的成果撰写成书,每本书均具有鲜明的创新特色和前瞻性。本丛书既可为从事相关专业技术研究和应用领域的工程技术人员提供参考,也可作为相关专业的高年级本科生和研究生的教材及参考书。

为了撰写好该丛书,特别聘请了本领域德高望重的陆元九院士、屠善澄院士和梁思礼院士担任丛书编委会顾问。编委会由本领域各方面的知名专家和学者组成,编著人员在组织和技术工作上付出了很多心血。本丛书得到了中国人民解放军总装备部国防科技图书出版基金资助和国防工业出版社的大力支持。在此一并表示衷心感谢!

期望这套丛书能对我国航天器和导弹的制导、导航与控制技术的人才培养及创新性成果的工程应用发挥积极作用,进一步促进我国航天事业迈向新的更高的目标。

丛书编委会

2010年8月

前 言

控制计算机是航天器控制系统的核心部件之一,随着空间技术的发展,其功能日趋复杂,加之在空间应用中空间环境尤其是辐射环境的影响,对计算机的可靠性提出了更高的要求。因此,在实际的航天器设计中,为了提高控制计算机的可靠性,需要采用多种容错技术。美国 NASA 从 20 世纪 60 年代开始在航天器上采用容错计算机系统,例如 STAR(Self-Testing And Repairing)容错计算机。我国从 20 世纪 70 年代开始研制航天器容错计算机,并于 20 世纪 80 年代由北京控制工程研究所首次在卫星上采用容错控制计算机,成功实现在轨飞行。此后,容错技术在控制计算机中大量采用,并为航天器型号任务的成功做出了巨大的贡献。

本书针对容错技术在航天领域的重要性,介绍了我国航天器控制计算机研究和设计中所用到的容错技术,既涵盖了基本理论知识,也包括了工程实践中采用的方法和案例。全书共分为 8 章:第 1 章为绪论,概述了容错技术的基本概念和理论,针对航天器控制计算机的特点分析了空间环境及其影响,介绍了容错技术的发展历史并进行了展望。第 2 章结合我国的航天器型号和工程实践介绍了容错计算机的体系结构以及关键技术。第 3 章给出了常用的故障模型,在此基础上介绍了计算机关键部件的故障检测技术。第 4 章介绍了航天器控制计算机中几种常用总线的容错技术,主要包括 1553B 总线、CAN 总线、SpaceWire 总线等。第 5 章介绍了软件容错的概念和基本原理,并重点讨论了单版本容错、多版本容错和基于数据多样性容错等多种具体软件容错方法。第 6 章针对空间辐射对 FPGA 的影响,重点介绍了 SRAM 型 FPGA 的故障模型和动态容错方法。第 7 章结合实际的工程实践介绍了故障注入相关技术,主要包括几类故障注入方法、故障

注入评价方法及故障注入工具。第8章智能容错技术,是容错技术的最新进展,重点介绍了以可进化硬件容错和人工免疫硬件容错为代表的两种智能容错技术的基本概念和原理,以及具体的实现方法。

本书由杨孟飞、华更新、冯彦君和龚健进行策划。杨孟飞、龚健和冯彦君参加了第1章的编著,杨孟飞、冯彦君和龚健参加了第2章的编著,杨孟飞和龚健参加了第3章的编著,华更新、杨孟飞、冯彦君和龚健参加了第4章的编著,冯彦君和杨孟飞参加了第5章的编著,刘鸿瑾、杨孟飞和龚健参加第6章的编著,华更新和宫经刚参加了第7章的编著,龚健、杨孟飞和董暘参加了第8章的编著。全书由龚健和冯彦君进行格式和图表整理,最后由杨孟飞负责审校和定稿。

在本书的编著过程中,得到了北京控制工程研究所领导、专家和同事的大力支持和帮助,在此表示衷心感谢。同时,衷心感谢吴宏鑫院士的鼓励和帮助,衷心感谢张笃周、袁利、王大铁、丁诚、顾斌、吴一帆、杨桦、刘波、陈朝晖、刘淑芬、陆晓野、王磊、赵卫华、王嵘、袁艺、张少林等领导和同事的支持。本书的出版得到了国防科技图书出版基金的资助,在此表示衷心感谢。

本书内容不仅是作者对实际工作的总结,也融入了作者的研究心得,力图全面反映我国在航天器控制计算机容错技术领域的先进水平。本书理论联系实际,专业性较强,可作为从事各种高可靠计算机,特别是航天器计算机和电子系统研究和设计人员的参考用书,也可作为从事该方向研究的研究生教材。

限于作者的水平,书中难免存有欠妥和谬误之处,敬请读者指正。

编著者

2013年6月

目 录

CONTENTS

第 1 章 绪论	1	1 Introduction	1
1.1 容错技术的基本概念和理论	1	1.1 Fundamental Concept and Principle of Fault Tolerance Techniques	1
1.1.1 基本概念	1	1.1.1 Fundamental concept	1
1.1.2 可靠性理论	4	1.1.2 Reliability principle	4
1.2 航天器控制计算机面临的 空间环境	9	1.2 Space Environment of Spacecraft Control Computer	9
1.2.1 空间环境介绍	9	1.2.1 Introduction to space environment	9
1.2.2 空间环境的损伤效应分析	13	1.2.2 Analysis on damage effect in space environment	13
1.3 容错技术发展状况及其展望	19	1.3 Development Status and Prospect of Fault Tolerance Techniques	19
第 2 章 容错系统结构及其关键技术	23	2 Fault Tolerance Architecture and Key Techniques	23
2.1 容错系统结构	23	2.1 Fault Tolerance Architecture	23
2.1.1 模块级冗余结构	23	2.1.1 Module-level redundancy structures	23
2.1.2 备份容错结构	26	2.1.2 Backup fault tolerance structures	26
2.1.3 三机容错结构	29	2.1.3 Triple-module fault tolerance structures	29
2.1.4 其他容错结构	32	2.1.4 Other fault tolerance structures	32
2.2 同步技术	32	2.2 Synchronization Techniques	32
2.2.1 同步时钟系统	33	2.2.1 Clock synchronization system	33
2.2.2 系统同步方法	45	2.2.2 System synchronization method	45
2.3 硬件冗余容错设计	52	2.3 Fault Tolerance Designe with Hardware Redundancy	52
2.3.1 冗余设计的通用逻辑 模型和流程	52	2.3.1 Universal logic model and flow in redundancy design	52
2.3.2 冗余的方案论证	53	2.3.2 Scheme argumentation of redundancy	53
2.3.3 冗余的设计实现	54	2.3.3 Redundancy Design and Implementation	54
2.3.4 冗余的分析验证	59	2.3.4 Validation of redundancy by analysis	59
2.3.5 冗余的测试验证	63	2.3.5 Validation of redundancy by testing	63

第3章 故障检测技术	64	3 Fault Detection Techniques	64
3.1 故障模型	64	3.1 Fault Model	64
3.1.1 按时间分类的故障模型	65	3.1.1 Fault model classified by time	65
3.1.2 按空间分类的故障模型	65	3.1.2 Fault model classified by space	65
3.2 故障检测技术	68	3.2 Fault Detection Techniques	68
3.2.1 概述	68	3.2.1 Introduction	68
3.2.2 CPU 的故障检测方法	69	3.2.2 Fault detection methods of CPUs	69
3.2.3 存储器的故障检测方法	75	3.2.3 Fault detection methods of memories	75
3.2.4 I/O 的故障检测方法	83	3.2.4 Fault detection methods of I/Os	83
第4章 总线技术	85	4 Bus Techniques	85
4.1 星载总线技术的概述	85	4.1 Introduction to Space-borne Bus	85
4.1.1 基本概念	85	4.1.1 Fundamental concept	85
4.1.2 基本术语	86	4.1.2 Fundamental terminology	86
4.2 MIL-STD-1553B 总线	87	4.2 MIL-STD-1553B Bus	87
4.2.1 总线系统故障模型	88	4.2.1 Fault model of the bus system	88
4.2.2 总线冗余容错机制	92	4.2.2 Redundancy fault tolerance mechanism of the bus system	92
4.3 CAN 总线	101	4.3 Can Bus	101
4.3.1 总线协议标准	103	4.3.1 Bus protocol	103
4.3.2 物理层协议及容错性	103	4.3.2 Physical layer protocol and fault tolerance	103
4.3.3 数据链路层协议及容错性	105	4.3.3 Data-link layer protocol and fault tolerance	105
4.4 SpaceWire 总线	109	4.4 Spacewire Bus	109
4.4.1 物理层及容错性	110	4.4.1 Physical layer protocol and fault tolerance	110
4.4.2 链路层及容错性	114	4.4.2 Physical layer protocol and fault tolerance	114
4.4.3 网络及路由	121	4.4.3 Networking and Routing	121
4.4.4 容错机制	124	4.4.4 Fault tolerance mechanism	124
4.5 其他总线	126	4.5 Other Buses	126
4.5.1 IEEE 1394 总线	126	4.5.1 IEEE 1394 bus	126
4.5.2 以太网	130	4.5.2 Ethernet	130
4.5.3 I ² C 总线	132	4.5.3 I ² C Bus	132

第 5 章 软件容错技术	134	5 Software Fault Tolerance Techniques	134
5.1 软件容错的基本概念和原理	134	5.1 Fundamental Concept and Principle of Software Fault Tolerance	134
5.1.1 软件故障	134	5.1.1 Software fault	134
5.1.2 软件容错	135	5.1.2 Software fault tolerance	135
5.1.3 软件故障发现和表决	135	5.1.3 Detection and Voting of software fault	135
5.1.4 软件故障隔离	137	5.1.4 Isolation of software fault	137
5.1.5 软件故障恢复	137	5.1.5 Recovery of software fault	137
5.1.6 软件容错的技术体系	139	5.1.6 Taxonomy of software fault tolerance	139
5.2 单版本软件容错	140	5.2 Single-Version Software Fault Tolerance	140
5.2.1 回卷恢复	140	5.2.1 Rollback recovery	140
5.2.2 基于编译器的软件容错技术	142	5.2.2 Software fault tolerance based on hardening the control flow	142
5.2.3 软件陷阱	145	5.2.3 Software trap	145
5.3 多版本软件容错	146	5.3 Multi-Version Software Fault Tolerance	146
5.3.1 恢复块	146	5.3.1 Recovery Block (RB)	146
5.3.2 多版本编程	147	5.3.2 N-Version Programing (NVP)	147
5.3.3 分布式恢复块	148	5.3.3 Distributed Recovery Block (DRB)	148
5.3.4 N 自检软件	149	5.3.4 N Self-Checking Programming (NSCP)	149
5.3.5 一致性恢复块	151	5.3.5 Consensus Recovery Block (CRB)	151
5.3.6 接收表决	151	5.3.6 Acceptance Voting	151
5.3.7 多版本的优缺点	152	5.3.7 Pro and Con of multi-version software fault tolerance	152
5.4 基于数据多样性的软件容错	152	5.4 Software Fault Tolerance Based on Data Diversity	152
5.4.1 数据重表达	153	5.4.1 Data Re-expression Algorithm (DRA)	153
5.4.2 重试块	153	5.4.2 Retry Blocks	153
5.4.3 N 复制编程	154	5.4.3 N-Copy programming	154
5.4.4 两次仲裁	154	5.4.4 Two-pass adjudicators	154
第 6 章 FPGA 容错技术	156	6 Fault Tolerant Techniques of FPGA	156
6.1 空间环境对 FPGA 的影响	157	6.1 Space Environment Effect on FPGA	157
6.2 SRAM 型 FPGA 的故障模式	160	6.2 Fault Modes of SRAM-Based FPGA	160
6.2.1 SRAM 型 FPGA 的结构	160	6.2.1 Structure of SRAM-based FPGA	160
6.2.2 SRAM 型 FPGA 的故障分类及故障模式分析	163	6.2.2 Types of Fault Mode and Related Analysis	163
6.3 SRAM 型 FPGA 容错技术	167	6.3 Fault Tolerant Techniques of SRAM-Based FPGA	167

6.3.1	SRAM 型 FPGA 的设计 缓解技术	167	6.3.1	Mitigation Techniques of SRAM-based FPGA	167
6.3.2	SRAM 型 FPGA 重配置 技术	176	6.3.2	Reconfiguration Techiques of SRAM-based FPGA	176
6.4	典型的 SRAM 型 FPGA 容错 设计方案	195	6.4	Typical Fault Tolerance Design of SRAM-Based FPGA	195
6.5	反熔丝型 FPGA 的容错技术	203	6.5	Fault Tolerant Techniques of Anti-Fuse FPGA	203
第 7 章 故障注入技术			7 Fault Injection Techniques		
7.1	故障注入的基本概念	206	7.1	Fundamental Concept of Fault Injection	206
7.1.1	实验者	207	7.1.1	Experimenter	207
7.1.2	建立故障模型	207	7.1.2	Building fault model	207
7.1.3	执行故障注入	207	7.1.3	Executing fault injection	207
7.1.4	故障注入的目标系统	208	7.1.4	Objective system of fault injection	208
7.1.5	系统行为观察	208	7.1.5	Observation of system behavior	208
7.1.6	实验结果分析	208	7.1.6	Analysis on experiment results	208
7.2	故障注入技术分类	208	7.2	Taxonomy of Fault Injection	208
7.2.1	仿真实现的故障注入	209	7.2.1	Simulation-based fault injection	209
7.2.2	硬件实现的故障注入	211	7.2.2	Hardware direct fault injection	211
7.2.3	软件实现的故障注入	212	7.2.3	Software indirect fault injection	212
7.2.4	物理的故障注入	214	7.2.4	Physical-based fault injection	214
7.2.5	混合的故障注入	216	7.2.5	Hybrid fault injection	216
7.3	故障注入系统的评价及应用	217	7.3	Evaluation and Application of Fault Injection System	217
7.3.1	注入的可控性	217	7.3.1	Controllability of fault injection	217
7.3.2	注入的可观性	218	7.3.2	Observability of fault injection	218
7.3.3	注入的有效性	218	7.3.3	Effectivity of fault injection	218
7.3.4	故障注入的应用	219	7.3.4	Application of fault injection	219
7.4	故障注入平台及工具	220	7.4	Platform and Tools of Fault Injection	220
7.4.1	EDA 环境下的故障注入 平台	222	7.4.1	Fault injection platform in EDA environmnet	222
7.4.2	基于计算机总线的故障 注入平台	223	7.4.2	Fault injection platform based on computer bus	223
7.4.3	基于串行加速器的故障 注入实例	226	7.4.3	Example of fault injection through particle accelerator	226
7.4.4	故障注入技术研究的发展 方向	228	7.4.4	Techniques trends	228

第 8 章 智能容错技术	229	8 Intelligence Fault Tolerance Techniques	229
8.1 可进化硬件容错	229	8.1 Evolvable Hardware Fault Tolerance	229
8.1.1 基本概念和原理	229	8.1.1 Fundamental concept and principle	229
8.1.2 进化算法	233	8.1.2 Evolutionary algorithm	233
8.1.3 可编程器件	243	8.1.3 Programmable device	243
8.1.4 可进化硬件容错的实现方法	250	8.1.4 Implementation methods of Evolvable Hardware fault tolerance	250
8.2 人工免疫硬件容错	265	8.2 Artificial Immune Hardware Fault Tolerance	265
8.2.1 基本概念和原理	265	8.2.1 Fundamental concept and principle	265
8.2.2 人工免疫容错方法	276	8.2.2 Fault tolerance methods with artificial immune system	276
8.2.3 人工免疫容错的实现	288	8.2.3 Implementation of artificial immune fault tolerance	288
附录 术语	294	Appendix Glossary	294
参考文献	297	References	297