国防科技图书出版基金

网络与信息安全前沿技术丛书

嵌入式软件安全保证技术

王崑声 经小川 等编著

Embedded Software Safety Assurance Techniques

国防工业出版社
National Defense Industry Press

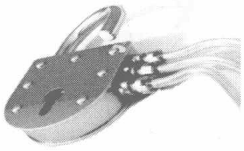
国防科技图书出版基金

网络与信息安全前沿技术丛书

王崑声　经小川　李　宁
张　伟　詹海潭　王潇茵　编著

嵌入式软件安全保证技术

Embedded Software Safety Assurance Techniques



目前，我国工业生产、国防军工等领域大力推进信息化、智能化建设，嵌入式软件作为实现系统智能控制的核心产品，其规模和复杂度不断增长，软件的潜在风险也不断增多。如何保证软件的安全性，避免出现系统故障甚至重大安全事故，是我们急需解决的问题。本书基于航天领域一系列重要型号软件安全性保证的应用经验，总结提炼出一套成体系、可剪裁的安全保证技术，书中所介绍的嵌入式软件安全保证技术体系已在我国国防领域开展应用并得到推广。

国防工业出版社
National Defense Industry Press
·北京·

图书在版编目(CIP)数据

嵌入式软件安全保证技术／王崑声等编著. —北京：国防工业出版社，2015.12
（网络与信息安全前沿技术丛书）
ISBN 978-7-118-10579-7

Ⅰ.①嵌… Ⅱ.①王… Ⅲ.①微型计算机-系统开发-安全技术 Ⅳ.①TP360.21

中国版本图书馆 CIP 数据核字(2015)第 284737 号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号　邮政编码 100048）
北京嘉恒彩色印刷有限责任公司
新华书店经售
*
开本 710×1000　1/16　印张 12　字数 214 千字
2015 年 12 月第 1 版第 1 次印刷　印数 1—3000 册　定价 68.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)88540777　　发行邮购：(010)88540776
发行传真：(010)88540755　　发行业务：(010)88540717

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	潘银喜			
副主任委员	吴有生	傅兴男	杨崇新	
秘书长	杨崇新			
副秘书长	邢海鹰	谢晓阳		
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	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	陆　军
	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		

《网络与信息安全前沿技术丛书》编委会

丛书序

网络的触角正伸向全球各个角落，高速发展的信息技术已渗透到各行各业，不仅推动了产业革命、军事革命，还深刻改变着人们的工作、学习和生活方式。然而，在人们享受信息技术带来巨大利益的同时，一次又一次网络信息安全领域发生的重大事件告诫人们，网络与信息安全已直接关系到国家安全和社会稳定，成为我们面临的新的综合性挑战，没有过硬的技术，没有一支高水平的人才队伍，就不可能在未来国际博弈中赢得主动权。

网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

适逢此时，欣闻由我国网络与信息安全领域著名专家何德全院士任编委会主任，以国家保密通信重点实验室为核心，集聚国内信息安全界知名专家学者，潜心数年编写的“网络与信息安全前沿技术丛书”即将分期出版。丛书有如下特点：一是全面系统。丛书涵盖了密码理论与技术、网络与信息安全基础技术、信息安全防御体系，以及近年来快速发展的大数据、云计算、移动互联网、物联网等方面的安全问题。二是适应面宽。丛书既很好地阐述了相关概念、技术原理等基础性知识，又较全面介绍了相关领域前沿技术的最新发展，特别是凝聚了作者

们多年来在该领域从事科技攻关的实践经验，可适应不同层次读者的需求。三是权威性好。编委会由我国网络和信息安全领域权威专家学者组成，各分册作者又均为我国相关领域的知名学者、学术带头人，理论水平高，并有长期科研攻关的丰富积累。

我认为该丛书是一套难得的系统研究网络信息安全技术及应用的综合性书籍，相信丛书的出版既能为公众了解信息安全知识、提升安全防护意识提供很好的选择，又能为从事网络信息安全人才培养的教师和从事相关领域技术攻关的科技工作者提供重要的参考。

作为特别关注网络信息安全技术发展的一名科技人员，我特别感谢何德全院士等专家学者为撰写本书付出的艰辛劳动和做出的重要贡献，愿意向读者推荐该套丛书，并作序。

前言

先进工业生产、基础通信设备、交通运输、能源控制、智能武器装备等关系到国计民生和国防建设的重要领域都广泛使用嵌入式软件，其安全性对我国工业和国防的现代化、信息化建设，以及国民经济的平稳运行起到了举足轻重的作用。在这些应用领域起到关键作用的嵌入式软件通常也称为安全关键嵌入式软件（简称“嵌入式软件”）。

随着上述领域对智能控制的强烈需求，嵌入式软件已成为实现系统功能的核心产品，其规模和复杂度较以往成倍增长，并逐步取代硬件成为最重要的产品。我国大量先进工业项目的立项对研制自主、可控的工业应用软件有巨大需求。然而，嵌入式系统及软件设计师在面对工期紧、任务重的研制要求时，经常忽略软件的可靠性、安全性等非功能需求，在开发过程中经常出现文档编写与开发并行甚至反序，评审、验证、测试不够充分，软件安全性、可靠性分析薄弱等现象，这些都容易导致软件产品状态受控差、存在潜在风险等问题。

由于软件开发过程属于人的脑力劳动，难以像硬件产品生产那样严格按照开发规范进行生产，所以导致软件产品具有较大的脆弱性和运行时的非预期性。尤其是在实际工业环境中，嵌入式软件在有限的硬件资源、复杂的系统交互、苛刻的运行环境下，更容易引起系统故障，严重时有可能造成任务失败、人员伤亡等重大安全事故。因此，需要结合工程需求，对嵌入式软件的安全性保证技术开展专项研究和应用。

嵌入式软件安全性保证技术涉及风险决策、故障模式影响分析、安全需求提取、安全性形式化验证、安全编程原则、编译器优化原则、软件运行时错误分析等多项技术，这使得该保证技术成为当前学术界和工程界实现高可信嵌入式系统的重要研究内容。

国内外现有的嵌入式软件安全性保证技术主要依靠研发人员的经验，分散在各研制阶段，缺少一套成体系的能够指导嵌入式软件安全保证技术应用的方法及工具。本书以成熟的软件工程化技术为线索，基于在航天领

域一系列重要型号软件安全性保证的应用经验，针对安全关键等级较高的嵌入式软件提出了成体系、可剪裁的安全保证技术体系和关键支撑技术，并提炼和总结出一套工程应用的方法和建议。

本书着重介绍嵌入式软件安全性需求分析、安全性架构设计、安全关键软件实现原则、安全性测试方法等涉及的相关要求、分析技术和方法，共分为7章。

第1章绪论，分析软件安全性的定义、发展现状及现有嵌入式软件安全性保证技术存在的问题。

第2章安全关键嵌入式软件开发过程保证体系，针对当前软件安全性保证技术现状及问题，构建工业软件安全性保证的体系框架。

第3章安全关键嵌入式软件需求分析，从传统的软件需求方法及需求薄弱环节入手，讨论嵌入式软件安全需求工程的方法、技术和支撑工具。

第4章安全关键软件设计分析，讨论软件体系结构安全性设计、安全关键部件/模块/单元的设计，以及软件设计产品的分析验证。

第5章安全关键软件的实现，讨论软件实现的安全编程要求和代码的安全性分析验证。

第6章安全关键嵌入式软件测试，讨论嵌入式软件安全性测试的流程和技术，介绍不同于传统测试技术的安全性测试方法及工具。

第7章技术发展展望，针对嵌入式软件生命周期安全性保证技术的未来发展趋势进行分析和展望。

本书由中国航天科技集团公司第710研究所的型号软件保障技术研究人员编写，主要作者有：王崑声、经小川、李宁、张伟、詹海潭、王潇茵。全书由王崑声研究员、经小川研究员主编，李宁、詹海潭主审。高金梁、郑重、郑平、佟轶、费晰等对本书编写提供了大量资料；著者还参考了大量国内外文献，已在参考文献中列出，在此一并表示感谢。

由于作者水平有限、时间仓促，不足和疏漏之处在所难免，在此衷心希望读者提出意见和建议，不吝赐教。

作者

2015年9月

目　录

Contents