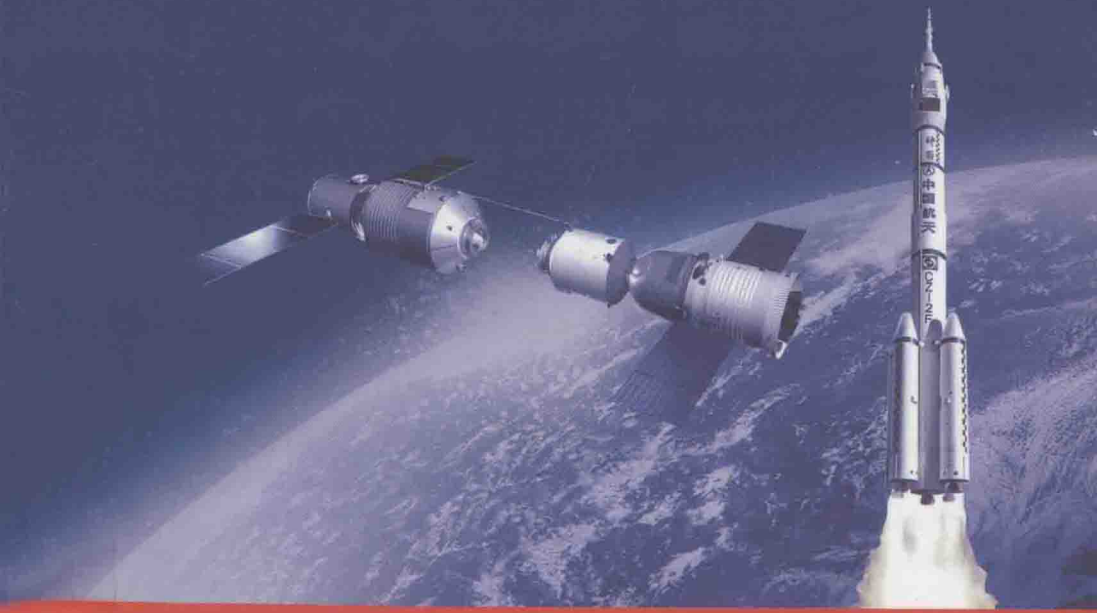
航天科技图书出版基金资助出版

航天高可靠嵌入式实时操作系统原理与技术

程胜　蔡铭　著



中国宇航出版社

航天科技图书出版基金资助出版

航天高可靠嵌入式实时操作系统原理与技术

程 胜 蔡 铭 著

中国宇航出版社
·北 京·

图书在版编目（CIP）数据

航天高可靠嵌入式实时操作系统原理与技术/程胜，蔡铭著. --北京：中国宇航出版社，2012.7

ISBN 978-7-5159-0254-8

Ⅰ.①航… Ⅱ.①程… ②蔡… Ⅲ.①航天器—实时操作系统 Ⅳ.①V446

中国版本图书馆 CIP 数据核字（2012）第 159867 号

责任编辑 赵宏颖 **责任校对** 祝延萍 **封面设计** 文道思

出　版
发　行　中国宇航出版社

社　址　北京市阜成路 8 号　　**邮　编**　100830
（010）68768548

网　址　www.caphbook.com

经　销　新华书店

发行部　（010）68371900　　（010）88530478（传真）
（010）68768541　　（010）68767294（传真）

零售店　读者服务部　　北京宇航文苑
（010）68371105　　（010）62529336

承　印　北京画中画印刷有限公司

版　次　2012 年 8 月第 1 版　　2012 年 8 月第 1 次印刷

规　格　880×1230　　**开　本**　1/32

印　张　12.375　　**字　数**　353 千字

书　号　ISBN 978-7-5159-0254-8

定　价　88.00 元

航天科技图书出版基金简介

航天科技图书出版基金是由中国航天科技集团公司于2007年设立的，旨在鼓励航天科技人员著书立说，不断积累和传承航天科技知识，为航天事业提供知识储备和技术支持，繁荣航天科技图书出版工作，促进航天事业又好又快地发展。基金资助项目由航天科技图书出版基金评审委员会审定，由中国宇航出版社出版。

申请出版基金资助的项目包括航天基础理论著作，航天工程技术著作，航天科技工具书，航天型号管理经验与管理思想集萃，世界航天各学科前沿技术发展译著以及有代表性的科研生产、经营管理译著，向社会公众普及航天知识、宣传航天文化的优秀读物等。出版基金每年评审1～2次，资助10～20项。

欢迎广大作者积极申请航天科技图书出版基金。可以登录中国宇航出版社网站，点击“出版基金”专栏查询详情并下载基金申请表；也可以通过电话、信函索取申报指南和基金申请表。

网址：http://www.caphbook.com

电话：(010) 68767205，68768904

前　言

近年来，随着航天技术的快速发展，航天型号软件的规模、复杂度、重要程度，以及在型号中所承担的功能比重均呈急剧上升的趋势。

美欧航天发达国家的航天型号研制经验表明，采用嵌入式实时操作系统对于提高复杂型号软件的开发效率，以及软件的可靠性、安全性、继承性都具有重要意义。实时操作系统（简称 RTOS）是指能在确定的时间内响应外部事件的一类操作系统。从国外的应用历程及规律分析可知，目前我国航天嵌入式 RTOS 正处于“磨合期”，一旦技术上有所突破，将会出现大量应用的局面。

航天型号对 RTOS 的可靠性、安全性等要求苛刻，虽然 RTOS 的代码规模不大，但是其操作系统内部状态组合所带来的高度复杂性，导致对其进行分析、测试及验证工作的技术难度高、工作量大，需要非常丰富的实践经验和技巧。

当前 RTOS 技术在不断推陈出新，及时了解、熟悉与掌握最新的原理、技术与方法，对于 RTOS 的技术选型、自主研发，以及升级现有的基础软件平台都非常必要。

本书以阐述嵌入式 RTOS 构成原理、方法与技术为主线，围绕高可靠、高安全这一技术要素进行内容组织，对 RTOS 设计模型、实现技术、测试方法、支持工具等进行细致而深入的阐述，并提供了大量的系统实例，具有较强的可操作性与较广的技术覆盖面。

本书内容来源于笔者承担国家重大科技专项、国防基础科研、总装预研、航天科技重点创新基金、航天支撑技术基金等课题的研

究成果。笔者针对高可靠 RTOS 架构、设计、测试与验证方法等进行了长期跟踪与研究，并在航天型号研制中进行了实践。本书是对上述成果的整理与总结。

全书共分为 8 章，从 3 个方面进行介绍：第 1 章～第 4 章介绍 RTOS 现状及概述、高可靠软件标准及规范、RTOS 基本概念及原理以及国外航天应用的 RTOS 产品；第 5 章～第 7 章针对 RTOS 的设计、实现技术展开，详细介绍 RTOS 设计原理、设计模型、系统实例、容错实时调度、内存空间保护、资源竞争防护、设备驱动加固、容错恢复以及健康监控技术；第 8 章介绍 RTOS 的测试技术与方法。

本书主要面向航天型号系统软件的设计、开发、测试以及管理人员，对于其他嵌入式软件研发人员而言，本书也不失为一本有助于拓宽视野、了解和掌握高可靠软件设计、开发与测试新技术的可选之书。

本书的编写工作得到了很多同志的帮助，特别感谢潘丽、仲顺洪、黄建晓、迟明帅等同志。感谢航天科技图书出版基金的资助和中国宇航出版社的大力支持。

因笔者水平有限，时间紧迫，书中缺点和不当之处在所难免，敬请读者批评指正。

程　胜

2011 年 9 月

目　录

第 1 章　高可靠实时操作系统

1.1　高可靠实时操作系统概述

进入 21 世纪以来，世界航天活动呈现蓬勃发展的新态势：运载器向大吨位、高可靠、快速响应、高环保、低成本及强适应性发展，卫星系统向高可靠、长寿命、高空间与时间分辨率、大容量及高速率发展，并逐步突破地球轨道载人航天技术，向载人深空探测发展。

为了适应更为复杂的空间环境并完成繁杂的空间任务，航天领域的嵌入式软件系统无论其应用规模、复杂度，还是重要性程度，近年来均呈急剧上升趋势。原有依靠人工进行资源管理及调度的方式，难以解决资源冲突、中断阻塞、自主管理等问题，因此需要利用实时操作系统在机制上予以保障，保证系统的稳定性、可靠性与高质量，并提高软件的开发效率。

实时操作系统（Real Time Operating System，RTOS）是指能在确定的时间内对外部事件做出响应并执行功能的一类操作系统。

20 世纪 70 年代起，美国就着手研制 RTOS 产品，1981 年 Ready System 公司发布了世界上首个实时操作系统产品 VRTX32。从 80 年代开始，RTOS 在美国的军事和航天领域中逐步得到应用，并取得了显著成效：

1）1997 年，美国国家航空航天局（NASA）喷气推进实验室（JPL）研制的火星探路者号探测器，搭载了美国 Wind River 公司的 VxWorks 实时操作系统登上火星，并在空间试验中成功实现了远程系统重构，纠正了优先级逆转问题，使得 VxWorks 成为第一个登上火星的商业 RTOS，进而在后续的火星探测计划中得以应用，包括：

2004 年的机遇号、勇气号，2008 年的凤凰号，都相继选用了 VxWorks 实时操作系统作为火星探测器的基础软件，并获得成功。

2）2000 年，美国 Green Hills 公司的 Integrity 实时操作系统中标洛克希德·马丁公司研制的联合战斗机，成为其控制系统的核心软件。

3）2005 年，美国 Express Logic 公司的 ThreadX 实时操作系统，为 NASA 深度撞击号探测器提供了高分辨率摄像头的精确与实时控制，成功完成了对坦普尔 1 号彗星的撞击任务，并收集了撞击产生的彗核碎片物质。

4）2009 年，美国 Wind River 公司宣布，NASA 将采用 VxWorks653 安全实时操作系统产品，作为新一代运载火箭战神 1 号和战神 5 号飞行控制计算机的实时操作系统。

欧洲、日本、加拿大、澳大利亚等国家和地区在航天型号中也已大量应用实时操作系统产品。事实证明，选用 RTOS 作为航天领域基础软件，这一举措是非常成功的，在弹、箭、星、船等强实时、高可靠应用中发挥了极为重要的支撑作用。

欧美国家将 RTOS 的选型作为一项重要的战略性决策对待。例如，2003 年，加拿大航天局研究员 Philip Melanson 在空间数据系统会议（Data Systems in Aerospace，DASIA 2003）上发表了题为“A Selection Methodology for the RTOS Market”的论文，阐述了加拿大航天局对 RTOS 产品的选型思路及方法，包括粗选和精选两个步骤。在粗选阶段，主要根据技术服务能力、产品持续发展能力等进行筛选；在精选阶段，提出了一个包含 8 个大项、43 个子项的技术评分表，涉及内核架构、编程模型、实时性能、编程接口等方面，对 RTOS 产品进行细化分析与比较权衡，从而形成应用 RTOS 产品的推荐排序。

我国航天领域也已部分应用了 RTOS，如：实践五号、探索一号使用了 pSOS 实时操作系统。随着我国航天嵌入式软件的系统规模及功能复杂度持续递增，自研或选用高可靠 RTOS 产品作为嵌入式软件支撑平台将成为必然趋势。

1.2　高可靠 RTOS 发展现状及趋势

与微软公司的 Windows 操作系统在桌面应用中“一枝独秀”截然不同，RTOS 商用产品及开源系统数量极为丰富。据统计，总量达上百种，如 VxWorks、Integrity、QNX、RTEMS、ThreadX、LynxOS、uC/OS 等都有广泛的应用，并涌现了 Wind River、Green Hills、QSSL、Express Logic、Gaisler 等著名公司。

可将现有的 RTOS 产品及系统按照图 1－1 所示的方式进行分类。

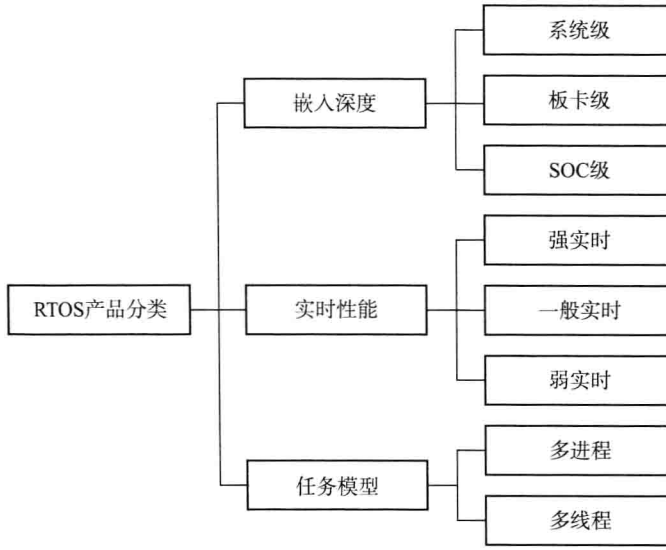


图 1－1　RTOS 产品技术分类示意图

（1）嵌入深度

嵌入深度代表了不同 RTOS 的资源规模及服务对象，主要可分为系统级、板卡级、SOC 级三个级别，其中：

1）系统级的 RTOS 内核规模相对较大，一般为 1Mbyte 以上，

具有网络、图形等丰富的功能，主要运行在资源充足的嵌入式实时系统中，如 RT－Linux、WinCE 等；

2）板卡级的 RTOS 内核规模一般为几百 Kbyte，运行于各类嵌入式板卡中，如 VxWorks、Integrity、QNX、RTEMS 等；

3）SOC 级的 RTOS 内核规模仅为几 Kbyte，运行于各类深度嵌入的场合，如 ThreadX、uC/OS 等。

（2）实时性能

实时性能代表了 RTOS 对外部事件的响应能力和水平，主要可分为三个级别：强实时、一般实时、弱实时，其中：

1）强实时的 RTOS 中断及任务响应时间为微秒级；

2）一般实时的 RTOS 中断及任务响应时间为毫秒级；

3）弱实时的 RTOS 中断及任务响应时间为秒级。

（3）任务模型

任务是 RTOS 运行的基本单元，不同的任务模型造就了不同的编程模型及资源调度策略。RTOS 的任务模型主要可分为两种类型：

1）多进程型，如 VxWorks 6.x、VxWorks653、Integrity、QNX 等；

2）多线程型，如 VxWorks 5.4、ThreadX、uC/OS、pSOS 等。

研制高可靠、高可用、强实时的 RTOS，一直是嵌入式系统工业界多年以来锲而不舍的追求目标，出现了如下的平台化、标准化、系列化发展特点。

（1）嵌入式基础软件的平台化发展

RTOS 是嵌入式软件系统的核心，与编译器、调试器关系密切。各类主流的 RTOS 供应商，如 Wind River 公司、Green Hills 公司等，均自主维护了由操作系统、编译器、调试器等一系列基础软件在内的完整平台，使得技术支持与服务能力雄厚，发展游刃有余。

（2）面向安全关键应用的标准化发展

面向航天型号等安全关键（Safety Critical）应用的 RTOS，越来越强调其符合标准化、规范化程度。各 RTOS 厂商，相继推出了符合军

用标准的安全RTOS产品，如Wind River公司的VxWorks653、LynuxWorks公司的LynxOS－178B符合ARINC 653和DO－178B标准，Wind River公司的VxWorks MILS 2、Green Hills公司的Integrity－178B实现了多重独立安全等级（Multiple Independent Levels Of Security，MILS）架构，并通过了EAL6＋认证。

（3）贴近行业应用特点的系列化发展

面向各类行业应用特点，提供贴近应用需求的实时内核、编程模型及开发工具，是当前实时操作系统发展的重要趋势。例如，Wind River公司面向航空航天、汽车电子、网络设备、工业控制、医疗电子等，分别推出了相应的一体化解决方案及应用平台；Green Hills公司共提供了3个系列5个内核，以有效支持各类应用需求；QSSL公司也提供了4个内核，以适应不同应用需求。

进入21世纪以来，国外对RTOS的系统架构、编程模型、冗余容错、健康监控、安全验证等可靠性保障技术研究的关注度明显加大。近年来，在操作系统设计、嵌入式系统、系统体系结构、软件工程等领域的国际顶级会议，如SOSP、OSDI、ASPLOS、RTSS、RTAS、MICRO、ICSE等，陆续发表了一些研究成果，研制了一批新型的实时操作原型系统，并呈现如下的技术发展趋势。

1）可配置、可重构、组件化技术，提高RTOS快速扩展能力。

通过二代微内核、超微内核、可重构、构件化等技术，有效分离RTOS内核功能服务与应用功能服务，降低实时操作系统内核耦合度与复杂度，提高RTOS面向应用需求驱动的快速定制、扩展、细粒度配置与裁剪能力。

2）高可靠、高可信支持，提高RTOS内核容错、安全验证与防护能力。

面向安全关键应用，避免单点失效崩溃与安全漏洞，采用避错、防错、消错、容错、健康监控、故障诊断，以及内核形式化验证等技术，提高RTOS的可靠性与安全性支持。

3）面向新型嵌入式应用，提高RTOS适应性。

面向 SOC/SIP 等深度、亚深度嵌入应用需求，以及相变存储器（Phase Change Material，PCM）等新型非易失性存储介质出现，研制更为精简的实时内核、有效的能量优化技术，以及新型存储技术已成趋势。

4）基于软硬件协同的新型内核设计，提升 RTOS 实时性能。

结合硬件芯片特性，采用资源优化配置、新增处理器指令、工具链扩展等软硬件协同技术手段，开展面向硬件体系结构的深度优化，全面提升 RTOS 实时性能。

5）新型体系结构与编程模型设计，提高 RTOS 易用性。

随着多核、众核、网格计算、云计算等新型计算模式出现，需要 RTOS 提供有力的并行处理、流式处理等新型编程模型及配套功能、性能优化技术支持手段。

1.3 航天对高可靠 RTOS 的需求

根据 2011 年发布的《中国的航天》白皮书介绍，我国将启动并继续实施载人航天、月球探测、高分辨率对地观测系统、新一代运载火箭等重大航天工程，部署和发展航天领域的前沿技术，加快航天科技的进步和创新。

在新一代航天型号装备的研制过程中，出现了新的发展趋势，对嵌入式实时操作系统提出了如下需求。

（1）新型复杂冗余设备支持

随着载荷水平不断提高，航天器寿命不断延长，以及深空探测计划的逐步实施，对系统整体的可靠性提出了更高的要求，满足长寿命、高可靠要求的 4 机、甚至 5 机冗余方案将得到应用，在系统运行控制模式、设备状态管理、备份交替策略等方面的复杂度将显著提升。此外，各类部件级冗余也进一步丰富，如 CPU 冗余、输出驱动冗余、数据冗余缓冲，以及各种混合冗余结构。迫切需要 RTOS 提供对复杂冗余设备、冗余部件进行有效管理的支持。