航天科技图书出版基金资助出版

航天型号高可靠软件系统调试原理与技术

蔡铭 程胜 王瑞 著

中国宇航出版社

本书针对复杂航天型号对软件系统的高可靠性要求，在深入分析软件故障特征的基础上，阐述了当前软件调试手段与工具的技术分类体系，介绍了一批最新的、具有代表性的软件调试技术，包括程序规则分析、用户行为分析、虚拟化调试支持、故障重现与逆向调试、统计调试、不变式调试等内容，以提高软件故障诊断与分析的自动化、智能化程度，提高软件调试效率，缩短软件交付周期，提高航天型号软件系统的可靠性。

本书主要读者对象是航天型号软件系统的设计人员、开发人员、测试人员及管理人员，也可作为其他科技人员了解和掌握高可靠软件系统质量保证与调试技术的参考书。

ISBN 978-7-80218-424-4

9 787802 184244 >

定价：65.00元

航天科技图书出版基金资助出版

航天型号高可靠软件系统调试原理与技术

蔡铭 程胜 王瑞 著

中国宇航出版社
·北京·

图书在版编目(CIP)数据

航天型号高可靠软件系统调试原理与技术/蔡铭，程胜，王瑞著.
—北京：中国宇航出版社，2008.8
ISBN 978-7-80218-424-4

Ⅰ.航...　Ⅱ.①蔡...②程...③王...　Ⅲ.航天器—软件可靠性—调试　Ⅳ.V47-39

中国版本图书馆 CIP 数据核字(2008)第 119593 号

责任编辑　张艳艳　**封面设计**　03 工舍　**责任校对**　祝延萍

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 / www.caphbook.com.cn
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　2008 年 8 月第 1 版　　2008 年 8 月第 1 次印刷
规　格　880×1230　　开　本　1/32
印　张　12.25　　字　数　339 千字
书　号　ISBN 978-7-80218-424-4
定　价　65.00 元

序

随着航天型号功能的日趋复杂，软件在型号中的应用越来越多，其规模和复杂度也日趋上升。从近年来对型号问题的统计数据来看，由于软件所导致的问题已占据一定比例。软件已经成为航天型号产品质量和可靠性的关键因素之一。

调试和故障诊断是软件研制过程中的重要环节，其主要的工作是针对故障现象完成故障的分析和定位，是保障和提高软件质量和可靠性的重要手段。目前，在型号软件研制过程中，软件调试工作绝大部分都依靠人工完成，尚未形成理论化、系统化、精确化、自动化的调试手段。

本书作者结合他们在开发高可靠复杂软件方面的实际经验和研究成果，在深入分析软件故障特征的基础上，阐述当前软件调试手段与工具的技术分类体系，并系统地介绍了当前国内外最新的、具有代表性的相关研究成果和技术。通过这些手段的应用，可以提高软件故障诊断与分析的自动化和智能化，快速、准确地定位故障，极大地提高软件调试效率。希望本书的出版能对推动航天型号软件可靠性工作起到积极作用。

总装备部载人航天工程软件专家组组长
中国航天科技集团公司软件专家组组长

前　言

软件系统广泛应用于当前各类航天型号系统中，为了能够适应各种复杂的空间环境和完成繁杂的空间任务，软件系统的应用规模、复杂度、重要性程度以及所承担的功能比重，近年来均呈急剧上升趋势。

软件是设计师塑造的、功能强大的工具，但寄生着各种 bug 的软件，顷刻间又可能转变为破坏力强大的敌人。随着计算机体系结构、程序设计语言的不断丰富，软件规模不断膨胀，任务复杂度不断提高，系统并发性不断加强，型号软件系统中潜在的 bug 已越来越难以捕捉、定位与控制。

不少事实证明，软件故障是导致型号系统失败的重要因素，软件系统的质量与可靠性已经成为型号产品质量与可靠性的关键因素之一，甚至可能直接影响发射任务的成败。

但令人遗憾的是，软件的质量和可靠性仍远不如人意。与硬件系统的可靠性相比，软件的可靠性一般要低一个数量级，在避错技术、防错技术、容错技术，以及故障检测和诊断等方面都明显落后。

软件调试技术是型号软件质量与可靠性保障体系中的重要环节之一，它是一个根据故障现象定位错误本质，并修正软件缺陷的循环迭代过程。与软件工程中的其他环节相比，软件调试技术无论在理论与方法、支撑技术与辅助工具、系统化支持程度，以及调试自动化、智能化方面仍然处于较原始的状态，软件调试过程低效、单调、乏味。

软件调试技术，尤其对于可靠性要求高的复杂型号软件而言，蕴含着非常丰富的实践经验和技巧，但是在当前计算机学科教学体系中（如 IEEE—CC2005），主要注重于软件的设计、开发方面的教学与训练，对于软件可靠性保障的后端技术，如软件测试、验证等则涉及极

少。其中，软件调试技术的教学部分完全为空白，软件调试的相关技术、方法和经验，需要程序员在实践工作中逐步摸索与积累，因而，难以在短期内被完全掌握。

随着型号软件系统越来越复杂化，对软件错误的跟踪、定位、分析与诊断困难重重，急需软件调试支撑技术、辅助工具的同步提升。当前软件调试技术在不断推陈出新，因此及时了解、熟悉与掌握最新的软件调试技术、方法与工具非常必要。

本书将软件调试技术作为一门学科进行研究和分析，以 bug 为中心，围绕软件调试技术这一主题进行组织，提供了大量的代码实例，对 bug 分类及其分布规律，以及各类调试技术原理、实现技术和支持工具等进行细致而深入的阐述，具有较强的可操作性与较广的技术覆盖面。

本书所涉及的工作得到了“十五”总装预研项目、国家“十五”863 重大软件专项、“十一五”总装预研项目、航天科技创新基金、航天支撑技术基金等多个项目的资助，课题组针对当前最新的各种软件调试方法、智能化故障定位技术等进行了全面的跟踪与探索，并与型号单位紧密配合进行了实践，面向高可靠型号软件开发应用的需求，研制了一系列软件调试、测试及验证等支持工具。本书是对上述成果的全面整理与总结。

全书共分为 13 章，从 3 个方面进行介绍：第一部分介绍软件调试技术概述、国内外型号软件中出现的典型 bug，bug 分类及分布规律分析；第二部分针对 bug 类型，详细介绍软件调试中涉及的内存类 bug 调试、静态分析、动态分片、Delta 调试、统计调试、不变式调试、难以重现类调试、体系结构扩展调试，以及数据挖掘调试技术；第三部分介绍对软件调试技术的评价与调试基准测试程序。

本书主要面向的读者群是型号软件系统的设计人员、开发人员、测试人员，以及管理人员。对于非型号软件系统的开发人员而言，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质量保证与调试新技术的可选之书。

总装备部载人航天工程软件专家组组长、中国航天科技集团软件专家组组长汪玲研究员对本书提出了许多宝贵而重要的意见，并在百忙之中为本书作序，在此谨表示诚挚的谢意。

本书由蔡铭、程胜同志负责全书的总体策划、文字修改和最后统稿。参加本书编写工作的还有王瑞、富浩、杨子江、叶珂珂和马超等同志。因时间紧迫、水平有限，错误之处在所难免，敬请读者批评指正。

在本书的出版过程中，感谢航天科技图书出版基金的大力支持。

编 者

2008 年 6 月

目　录

第1章　软件调试技术概述

1.1　软件系统的“双刃剑效应”

软件系统作为计算机系统的神经中枢，已经延伸到现代武器型号设备、装置中的各个角落，为了能够适应各种复杂的空间环境和完成繁杂的空间任务，软件系统的应用规模、复杂度以及重要性程度，近年来均呈急剧上升趋势。例如：

• 一个国际太空站需要上百万行的软件系统，控制各种导航、通信及实验设备；

• 美国航空航天局(NASA)的太空飞船项目中，其船载软件代码量大于50万行，地面控制和处理软件代码量约350万行；

• 我国神舟五号载人飞船中，船载软件模块共60余个，软件指令达70万条，地面支持系统的软件规模则大于140万条指令；在神舟六号飞船的7大系统、13个分系统中，软件模块规模进一步扩大到82个。

在型号设备的功能分布中，由软件系统承担的功能比重不断加大。例如，在美国第二代歼击机F—111中，由软件部分所实现的功能约占20%，到了第四代机F—22，这个比例已上升为80%。与此相类似，在我国新研的军用飞机中，其飞控系统、火控系统及弹射救生系统等，均采用软件系统逐步替代原有的机械、光学设备，实现其控制，某些机种的机载代码量已超过了百万行量级。

由于软件错误直接造成系统失效的比例持续递增，据1986年的统计数据表明，系统失效事件中诱因是软件错误的比例约占25%，而到2000年，该比率已超过40%。软件错误所导致的经济损失也触目惊心，根据美国国家标准技术研究所2002年6月公布的调查表明，由