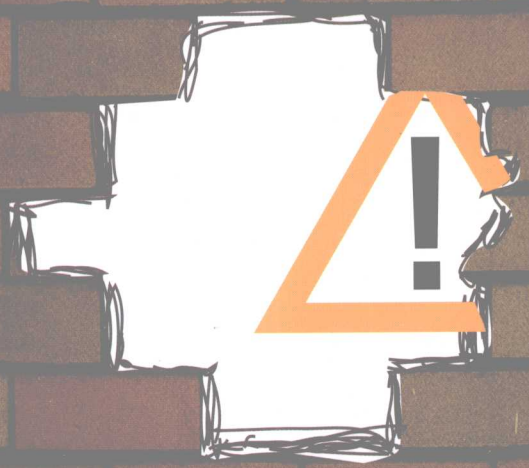
软件可靠性工程



孙志安　裴晓黎　宋　昕　戴忠健　编著

北京航空航天大学出版社

软件可靠性工程

孙志安　裴晓黎　宋　昕　戴忠健　编著

北京航空航天大学出版社

内 容 简 介

本书本着“需求牵引、面向工程、结合实际”的原则，系统地阐述了软件可靠性工程的理论，提出了软件可靠性建模、度量、分配、设计、分析、测试与管理的实践方法。内容包括：软件可靠性工程基础；软件可靠性建模；软件可靠性度量；软件可靠性要求的制定与分配；软件可靠性设计；软件可靠性分析；软件可靠性测试；软件可靠性工程管理等。

本书可供软件开发人员、测试人员、软件工程管理人员、软件质量与可靠性管理人员、其他工程技术人员以及软件工程本科高年级学生、研究生使用和参考。

图书在版编目(CIP)数据

软件可靠性工程/孙志安等编著. —北京：北京航空航天大学出版社，2009.3

ISBN 978-7-81124-419-9

Ⅰ. 软… Ⅱ. 孙… Ⅲ. 软件可靠性—软件工程 Ⅳ. TP311.5

中国版本图书馆 CIP 数据核字(2008)第 159680 号

软件可靠性工程

孙志安 裴晓黎 宋 昕 戴忠健 编著

责任编辑 潘晓丽 张雯佳

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(100191) 发行部电话：010-82317024 传真：010-82328026

http://www.buaapress.com.cn E-mail:emsbook@gmail.com

北京市媛明印刷厂印装 各地书店经销

开本：787 mm×1 092 mm 1/16 印张：22 字数：563 千字

2009 年 3 月第 1 版 2009 年 3 月第 1 次印刷 印数：4 000 册

ISBN 978-7-81124-419-9 定价：39.00 元

序　言

随着计算机科学的高速发展，软件无处不在，成为推进全球经济一体化的驱动器，并且正在成为推进新科技革命、新军事变革及其知识经济飞速发展的引擎。今天，绝大多数产品，尤其是现代武器装备系统等大型复杂系统的绝大多数功能和性能都是由软件所规定和决定的。软件的可靠性对现代武器装备系统作战效能的有效发挥产生着巨大的影响，它已经成为软件业界和可靠性工程界关注的焦点，研究的热点，实践的重点。

经过软件业界和可靠性工程界人士的不懈努力，软件可靠性工程得到了广泛的研究和不断实践，并取得了显著的成效。但是，直到今天，开发足够可靠的软件并测试和验证其可靠性，仍然是非常困难的问题。复杂软件不管是对大型工程系统还是小型工程项目都越来越显示出它是一个薄弱环节，即使是通过完备测试与合格验证的软件，也常常受到错误的困扰。与此同时，一个前所未有日益增长的需求是：软件应具有检定合格的可靠性。例如，武器装备系统、载人航天系统、核安全控制系统等无不对软件可靠性提出了前所未有的高要求。即使是工业和日常生活中一般应用程序的开发与销售，市场对其可靠性要求也越来越高。况且，目前还不能保证软件可靠性水平哪怕是在一段时间的将来是足够的。四十多年前就已波及到全世界范围的软件危机，直到今天依然是我们难以逾越的障碍。

本书编著者本着“需求牵引、面向工程”的原则，对软件可靠性工程的理论进行了系统的研究和深入的探索，针对软件可靠性工程的现状提出了相应的工程实践方法，集中反映了在这一领域的研究成果，使我们看到了解决现行软件可靠性工程问题的希望。

软件可靠性工程是软件工程的重要分支，软件可靠性工程的产生和发展得益于硬件可靠性工程，硬件可靠性工程技术和方法是软件可靠性工程研究和实践的基础。系统研究和解决软件可靠性工程问题，仅有软件可靠性工程专业人员的努力和

热情还远远不够，还需要软件工程界、硬件可靠性工程界以及广大的科技工作者和质量工作者以高度的事业心及责任感，团结协作，相互支持，共同努力，积极探索，努力实践。

海军装备部电子部部长

前　言

软件可靠性工程是为有效地实现软件可靠性目标而采取的系统化技术、方法和管理等活动，它是软件工程的一个重要分支，其研究范畴覆盖了软件可靠性预计、分配、分析、设计、评价、测试、检定以及可维护性设计、安全性设计和可靠性工程管理等方面。

软件可靠性工程研究的目标是如何应用理论知识、科学方法和工程规范来指导可靠软件的开发，以期达到用较少的时间和投入获得高可靠性的软件。它使得软件可靠性的分析、评价、设计和验证以及管理水平迈向了系统化、规范化、全员化的进程。它的诞生标志着软件质量管理跃上了一个新的里程碑。

软件可靠性工程的内容丰富而广泛，它既是软件工程研究与实践的必然结果，也是可靠性工程发展的必然选择。而这两者都离不开知识与技能、方法与技术的灵活运用，更离不开工程实践的驱动。在这一背景下，本书编著者本着“综合分析，建立体系，需求牵引，面向工程”的原则，以提高软件可靠性，以为可靠软件的开发提供指南为目的，对目前软件开发与使用的现状、存在的主要问题及其发展趋势等进行系统分析。在此基础上，跟踪国内外软件可靠性工程研究与实践的成果，提出了软件可靠性工程的体系结构和过程模型；以此为基线，对软件可靠性建模、度量、分配、设计、分析、测试与管理的理论、技术和工程实践方法进行了系统的分析和介绍。

本书共分 9 章。

第 1 章分析总结了软件可靠性工程的基本问题，提出了软件可靠性工程的基本框架和软件可靠性工程过程模型，为全书的展开建立了基线；

第 2 章给出了软件可靠性工程的基本概念，分析了软件可靠性因素、失效机理；

第 3 章按照随机过程类模型和非随机过程类模型叙述了 JM 模型、G－O 模型等主要软件可靠性模型，对模型的比较、选择与合并进行了分析研究；

第 4 章介绍了主要的软件可靠性度量元、度量方法及其在软件可靠性工程中的应用；

第 5 章提出了软件可靠性的定性、定量分析与设计要求，给出了主要的软件可

靠性分配方法及其分配流程；

第 6 章介绍了软件可靠性设计流程与设计过程活动，详细介绍了软件可靠性的避错设计、查错设计、纠错设计和容错设计方法；

第 7 章结合实例介绍了软件故障树分析、失效模式与影响分析、潜藏分析和 Petri 网分析；

第 8 章介绍了软件可靠性测试流程、测试环境、测试条件及其软件可靠性增长测试和验证测试，提出了软件可靠性测试的充分性准则；

第 9 章根据软件工程管理的实际情况，提出了软件可靠性工程管理的准则、要求和方法。

本书可供软件开发、测试、软件工程管理、软件质量与可靠性管理及其他工程技术人员以及软件工程本科高年级学生、研究生使用和参考。但由于编著者水平有限，加之篇目繁多，编著者虽辛勤笔耕，数易其稿，但难免萧兰并撷，珉玉杂陈，不当之处，恳请读者批评指正。同时，作为一门新兴的学科和学术探索，本书只是软件可靠性工程研究和实践的一个新的起点而不是终点。必须看到，以有限的时间和个人认知，探索软件可靠性工程的无限奥妙，路漫漫永难穷尽，还需要业界和同仁的无私支持。

本书编著过程中，北京理工大学戴忠健副教授，北京航空航天大学阮镰教授、陆民燕教授审阅了书稿并提出了很多建设性的意见，作者的妻子刘秀景对有关模型进行了验算，绘制了部分图表，在此一并致以衷心的感谢！海军装备部电子部部长魏刚在百忙中为本书成稿给予指导和关心并作序鼓励，在此致以特别的感谢！

孙志安

2008 年仲夏

目 录

第1章 绪 论

1.1 软件可靠性工程研究和实践的意义

20世纪70年代中后期以来，以软件工程的大力发展为契机，假传统可靠性工程技术和方法，软件可靠性工程得以产生并取得了长足的进展，各种软件可靠性模型相继推出并得到不断改进和优化，模型验证和使用一度成为软件可靠性工程的热点，直到今天也依然是热门话题。软件可靠性设计与测试技术得以开发并逐步应用于工程实践；软件可靠性分析、评估方法不断完善，并在一些特殊的或重点工程项目中得到应用；软件可靠性工程管理技术的开发备受推崇，相应的管理方法被实践所验证，软件业界已充分认识到，绝大多数软件问题是由管理不善所引起的，所以，以过程改进、组织性能改进、管理模式改进、软件开发人员管理为重点的管理体系和管理机制得以产生并日臻成熟；软件可靠性标准化工作得到前所未有的重视，国际电工委员会的TC56技术委员会成立了软件可靠性工作组，一些迫切需要的软件可靠性、维护性标准相继发布，为软件可靠性工程实践奠定了基础。目前，通过软件业界和可靠性工程界的不懈努力，软件可靠性工程得到了广泛的研究并不断实践取得了显著的成绩，但遗憾的是直到今天，开发足够可靠的软件并测试和验证其可靠性，仍然是非常困难的问题。复杂软件不管是对大工程系统还是小工程项目都越来越显示出它是一个薄弱环节，即使是通过完备测试与合格验证的软件也常常受到错误的困扰。与此同时，一个前所未有日益增长的需求是：软件应具有检定合格的可靠性，例如，武器装备系统、载人航天系统、核安全控制系统等无不对软件可靠性提出了前所未有的高要求。即使是在工业和日常生活中一般应用程序的开发与销售，市场对其可靠性要求也越来越高。尽管如此，我们还不能保证软件可靠性水平，哪怕是在一段时间的将来是足够的，四十多年前就已波及到全世界范围的软件危机，直到今天依然是难以逾越的障碍。

软件可靠性问题造成的事故和灾难屡见不鲜，俯拾皆是，触目惊心。

遨游太空，探索宇宙的无穷奥秘，是人类的共同理想。今天，嫦娥奔月，夸父追日已成现实。但这一过程中，人们付出了艰辛的努力，经历了大量的挫折。正是基于此，软件可靠性工程在航空航天领域得到了高度重视，进行了大量的研究和实践，引领软件可靠性工程不断发展。即便如此，在该领域内，人们仍然在不断地饱受软件故障所带来的恶果。比如，耗资3.2亿美元的美国航天局“火星气象卫星”Viking在接近火星表面时失踪，其原因就是弹道计算的量纲不统一，地面控制系统使用磅，卫星使用牛顿，公、英制混淆。又如，2003年5月4日，俄罗斯的TMA1号宇宙飞船从国际空间站返回地面时，由于软件错误导致导航系统故障，自动驾驶仪只能以弹道方式

降落，而在降落过程中，计算机又突然开始搜索国际空间站，并试图与国际空间站对接，使得飞行控制中心在飞船返回过程中与飞船失去联系长达 11 min，最终导致飞船与原定溅落点偏差 460 多公里。再如，1996 年 6 月 4 日，历时 10 年研制的 ARIANE 5 火箭，首次发射升空飞行 40 s 后，由于其攻角大于 20°，引起了极高的气动载荷，导致火箭的助推级与芯级分离，不得不启动自毁装置引爆火箭，造成巨大的损失，直接经济损失达到 5 亿美元，还使耗资 80 亿美元的开发计划推迟了近三年。其原因有两方面：一方面，ARIANE 5 火箭的主惯性参考系统在将 64 位浮点数转换成 16 位有符号整数时，数字转换超界，没有将正确的姿态数据传送给运载火箭的箭载计算机所致；另一方面，ARIANE 5 重用了同样存在这一错误的 ARIAN 4 火箭的飞控软件，但在重用此软件后未进行完备测试，致使错误残存下来。

现代战争不仅是尖端武器的对抗，更是在扩大的空间与缩短的时间、分散的布势与模糊的战线、动态行动的各类军兵种与频繁转换的作战式样基础之上的体系对抗。随着现代武器装备的耦合性越来越高、结构日趋复杂，随着作战指挥体制由树状结构向网状结构的转变，随着新军事变革的不断深化，随着作战理念及作战模式的改变，现代战争对武器装备的可靠性尤其是其核心的装备软件可靠性提出了前所未有的高要求。软件可靠性正在对军事装备战斗力的形成和作战效能的发挥产生巨大的影响，软件可靠性问题已成为军事装备迫切需要解决的重要问题。比如，海湾战争期间，一次“爱国者”防空系统未能成功拦截“飞毛腿”导弹，造成 28 名英军官兵被炸身亡，原因就是其跟踪软件在运行 100 h 后出现了一个 0.36 s 的舍入误差。又如，美海军“约克城”(CG－48)号巡洋舰发生动力系统故障，导致全舰各系统功能几乎瘫痪，使该舰在海上漂流了 2 小时 45 分钟。其主要原因就是软件发生被零除的错误，造成数据溢出，波及到整个网络系统，导致动力系统失灵所致。前车已覆，后车之鉴，在美国国防部军事转型计划的关键项目——网络中心战的研制过程中，为了有效避免软件可靠性问题，国防部不仅采用了软件开发中的最佳成果，而且花费了大量的人力物力来专门研究解决软件的可靠性问题，才有效地确保了进度，控制了成本。

今天，软件可靠性工程的研究和实践已不再只局限于航空航天、军事等特殊领域，而是广泛地应用于包括一般应用软件在内的几乎所有领域。电话必须通，飞机必须飞，货架上的商用软件必须赢得用户的信任，才能为开发商带来利润。事实上，一日千里的商业领域内，无处不在的网络计算机已将软件可靠性关注的焦点推向前台。bug 成堆的操作系统、Web 浏览器以及客户端桌面应用系统，都可能导致严重的漏洞，与此同时，伴随着消费者需求的不断变化和提高，软件可靠性正在成为以网络计算机为手段的政府部门、企业以及个人关注的焦点。

面对软件应用范围日趋广泛、规模迅速扩大、复杂性不断增加、难度日益加大、可靠性要求越来越高的现状；面对软件的工业化、产业化和国际化进程需求空前高涨以及加快开发进度，提高可靠性和降低开发成本此涨彼消的局面；即使是在航空航天、军事、通信等领域都已经过比较深入的研究和实践，但如果有更多的有识之士关注软件可靠性的理论和实践，形成一个能有效激励人们进行创造性工作的领导群体以及富有创造力的开发管理团队，无疑将会引领该领域研究与实践热情的空前高涨。尽管怀疑论正在为新的研究和实践投下阴影，但软件可靠性工程的研究和实践已势不可挡。因此，我们必须对软件的二重性有着清醒的认识，在享受软件所带来的便利以及推进信息技术与信息社会高速发展的喜悦的同时，还必须充分地认识到，软件可靠性问题不仅非常普遍，而且非常突出，软件可靠性问题可能演变成巨大的灾难。所以，加强软件可靠性工程的研究和实践，提高软件可靠性，推进软件工程化和软件产业进步，势在必行。

21世纪是质量的世纪。人们在质量的大堤下生活，企业在质量的波涛中经受考验。质量工作已不再是“单个烟囱”，软件质量正在向着不同的深度和广度发生着深刻的变革。作为软件最重要的质量特征，软件可靠性已经成为开放式技术社会中企业的最后一道防火墙与最重要的市场竞争武器。这一现实强力地推进着软件可靠性工程理论研究与实践的进展。软件可靠性工程的研究和实践具有如下重要意义：

- 推进软件的可靠性设计、测试及其可靠性工程管理能力的改进和提高，确保并不断改进软件可靠性，提高企业诚信，增加顾客满意度，超越顾客期望；
- 指导软件可靠性分析、评估、验证与鉴定，为软件验收(验证)提供依据，增强用户信心；
- 推进软、硬件可靠性工程的均衡发展，提高系统可靠性水平；
- 推进软件工程的不断丰富和发展，促进软件工程管理水平及软件过程能力的改进和提高；
- 转变观念，有效扭转只重视硬件，忽视软件可靠性的现状。

尽管软件可靠性工程尚处于发展期甚至可以说还处于启蒙阶段，尚有大量的问题需要研究解决。但是，如果企业和政府高度重视，积极推进并以市场为导向，以需求为牵引，将软件可靠性当作一种资本而不是成本并将其作为市场竞争的法宝，视推进软件可靠性进展作为业界的义务和责任，软件可靠性工程必将迎来研究和实践的春天。

我们编著此书的目标是在软件业界和可靠性工程界创立一种对话机制与平台，确立一种能引起广泛兴趣的技术基础与高度关注的命题，提出增进软件可靠性的有效方法和实施指南。

1.2 软件可靠性对系统可靠性的影响

软件是绝大多数系统的构成部分，软件可靠性是系统可靠性的构成要素，同时也是系统可靠性的瓶颈，甚至可以说，软件可靠性是系统可靠性最致命的软肋。对于大多数嵌入式系统尤其是一些大型复杂系统，软件可靠性已经成为决定系统成败的关键。以下通过一个实例来说明软件可靠性对系统可靠性的影响。某控制系统是一个分布式系统，由三个分系统SYS1、SYS2、SYS3以及一个网络系统和一套中频电源构成。其中，分系统SYS2由三个子系统SYS21、SYS22、SYS23并联而成。该系统的可靠性框图如图1-1所示。

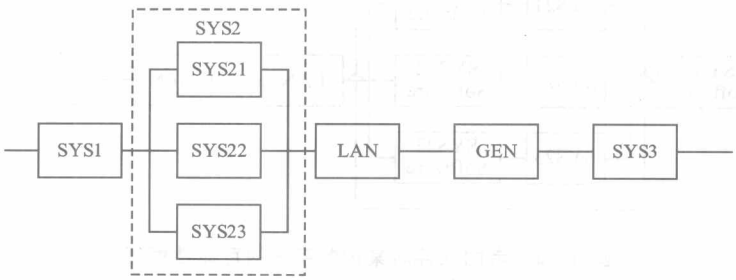


图1-1 某控制系统可靠性框图

该控制系统的各构成部分的可靠性指标分别为：

$MTTF_{SYS1}=280\,h$，$MTTR_{SYS1}=0.53\,h$；

$MTTF_{SYS21}=MTTF_{SYS22}=MTTF_{SYS23}=387\,h$，$MTTR_{SYS21}=MTTR_{SYS22}=MTTR_{SYS23}=0.25\,h$；