可下载教学资料

http://www.tup.tsinghua.edu.cn

高等学校教材

软件工程

软件可靠性工程

徐仁佐 编著

清华大学出版社

高等学校教材

软件工程

软件可靠性工程

徐仁佐 编著

清华大学出版社
北京

内 容 简 介

本书以软件可靠性工程的一些常见问题为出发点，以编者多年来所参与的工程实践为依托，帮助读者对软件质量指标体系中的最重要的质量指标之一——软件可靠性有一个全面的理解，并具有一定的实践能力。

全书共12章，各章均附有习题，一部分是为了复习、巩固本章所学的知识，另一部分是为引导学生进行创新型思维。本书最后提供了包括最新领域发展的参考文献，供有兴趣的读者进一步阅读和学习。

本书语言流畅，结构合理，内容丰富，实例众多，着重理论与实践相结合，学以致用，适合作为高等院校软件工程、计算机及相关专业的本科生和研究生教材，也可以作为软件从业人员及一般读者的参考书。

图书在版编目(CIP)数据

软件可靠性工程/徐仁佐编著. —北京：清华大学出版社，2007.5
(高等学校教材·软件工程)
ISBN 978-7-302-14293-5

Ⅰ.软…　Ⅱ.徐…　Ⅲ.软件可靠性—软件工程—高等学校—教材　Ⅳ.TP311.5

中国版本图书馆CIP数据核字(2006)第152712号

责任编辑：付弘宇　徐跃进
责任校对：李建庄
责任印制：孟凡玉
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 装 者：三河市春园印刷有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：21.75　**字　数**：541千字
版　　次：2007年5月第1版　　**印　次**：2007年5月第1次印刷
印　　数：1~3000
定　　价：29.00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177转3103　　产品编号：016476-01

出版说明

改革开放以来，特别是党的十五大以来，我国教育事业取得了举世瞩目的辉煌成就，高等教育实现了历史性的跨越，已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上，高等教育规模取得如此快速的发展，创造了世界教育发展史上的奇迹。当前，教育工作既面临着千载难逢的良好机遇，同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾，是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月，教育部下发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》，提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月，教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件，指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分，精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间（2003—2007 年）建设 1500 门国家级精品课程，利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放，以实现优质教学资源共享，提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展、顺应并符合新世纪教学发展的规律、代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1) 高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 高等学校教材·电子信息——高等学校电子信息相关专业的教材。

(4) 高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5) 高等学校教材·信息管理与信息系统。

(6) 高等学校教材·财经管理与计算机应用。

清华大学出版社经过20多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

E-mail: dingl@tup.tsinghua.edu.cn

前言

自从美国 AT&T Bell 实验室的 J. D. Musa 于 1991 年在美国得克萨斯州的奥斯汀市召开的第十三届国际软件工程会议(The 13th International Conference on Software Engineering)上正式提出软件可靠性工程(software reliability engineering)的概念,至今已过了十多年的时间。

当时,Musa 先生将软件可靠性工程仅限于"预计、测量、管理以软件为基础的系统的可靠性,以最大限度地满足用户需要的应用科学"的范畴。随着近十几年的软件可靠性工程的实践与发展,随着软件工程的进步,软件可靠性工程的范畴也在逐步地拓宽。软件可靠性工程发展到今天,伴随着软件开发的全过程,在软件生命周期的各个阶段,都发展出了一系列的技术和管理方法。纵观当今软件可靠性工程的实践,可以说,软件可靠性工程是与软件开发过程各阶段同步并行的,用于设计、保证、计量、管理软件可靠性目标的应用科学。由香港中文大学的吕容聪(Michael R. Lyu)教授编辑、IEEE Computer Society Press 出版的《The Handbook of Software Reliability Engineering》一书,收入了一系列早期有关软件可靠性工程的文献,对推动软件可靠性工程的发展起到了一定的作用。但此书中远未包括软件可靠性工程研究的全部,特别是近年来开发的方法和技术。

软件可靠性工程属于软件工程范畴,正如软件需求工程、软件再工程、软件复用工程、软件测试工程等一样,是软件工程的一个子领域。软件可靠性工程的发展要从属于软件工程发展的需要,反之,软件可靠性工程的发展又可以促进软件工程的发展,软件可靠性工程的方法和技术可以补充软件工程的方法和技术,使之更加丰富多彩。

软件可靠性工程是围绕软件质量指标体系中最重要的质量指标之一的软件可靠性来展开研究的,软件可靠性指标的高低,决定了软件是否能稳定、可靠地工作。软件中的错误是在软件的开发过程中,因为人的错误而引入到软件中的。开发软件的人也是社会的人,他们在开发软件的过程中,必然要受到其教育背景、工作经历、开发软件的经验的影响,同时也会受到其生活环境、周围的人们的影响,而且还会受到当时社会上各种思潮的影响。所以,尽快开展软件工程中的人的因素的分析研究工作,对于改善软件的质量有着十分重要的作用。软件可靠性工程中大量的管理工作,实际上一个重要方面就是如何做好人的工作。人的因素是根本的问题,因为从积极的方面来看,世界上所有推动人类社会进步与发展的事情都是由人做出来的。

综合以上原因，有理由认为本书讨论的软件可靠性工程问题已经远远超出了当年Musa先生提出的软件可靠性工程的概念。所以，从这个意义上来说，本书是一本讨论广义软件可靠性工程的著作。

本书是在软件可靠性工程研究课题组全体成员的长期努力下共同创造的成果。笔者的一届又一届的研究生们为此做出了持续不断的努力。如今，他们有的早已走上了工作岗位，有的还在国外继续深造，书中的许多章节就是他们的研究成果。笔者的主要工作就是将他们的这些成果用软件可靠性工程的一根主线贯穿起来，奉献给广大的读者。

在笔者普及、推广软件可靠性工程的工作过程及从事软件可靠性工程的教学过程中，经常会遇到各种各样的问题，其中最重要的问题也就是软件可靠性工程中的核心问题，即“软件可靠性工程与软件工程是一种什么样的关系?”、“应该怎样设计一个软件系统的软件可靠性指标?”、“怎样将软件系统的指标分配到各个软部件、甚至分配到各个模块上去?”、“什么样的技术可以保证软件可靠性指标的实现?”、“怎样反映和控制软件测试的进度与成本?”、“怎样控制将开发的软件产品在正确而适当的时候投放市场?”等。

上述这些问题有着深刻的工程背景，同时又涉及多方面的理论问题，要想清楚地回答这些问题是很不容易的。本书试图部分地回答若干问题，但真正的目的是以这些问题为出发点，将感兴趣的读者引入对这些问题的探讨中来，从而在国内普及软件可靠性工程的基本知识和应用，推动软件可靠性工程在我国的发展，为我国软件产业的发展壮大和国家的现代化做一点力所能及的工作。

本书第1章讨论软件可靠性工程在软件工程中的地位和作用，第2章讨论软件可靠性的基础理论，第3章讨论软件可靠性的分配问题，第4章研究软件测试的基本问题。自第5章开始，分别讨论软件的各种测试方法，最后给出有关部分的参考文献。因为本书是作为教材出版，受篇幅所限，与本书初稿相比较，将参考文献删掉了大半，主要是将那些较早的文献删除。如果书中引用的内容在书后的参考文献中未能找到，则笔者向这些作者致歉！

本书第2、3章介绍的软件可靠性基础理论、可靠性指标分配的优化问题以及第8～12章中有研究性质的内容，笔者建议作为研究生教学的内容和本科教学中的选学内容。

感谢国家自然科学基金委员会的系列资助，使我们这个研究小组得以在软件可靠性工程领域进行长期而稳定的研究工作。

参加本书编写工作的有谢旻、郑人杰等，感谢他们的辛勤劳动。感谢我的研究生周瑞、杨晓清、肖英柏、向剑文、张良平、陈波、张大帅、王果、陈斌、马若锋、郑红军、高俊鹏、刘丽娜、刘彦伸、徐剑宏、韩轶凡、黄灿、戴璐、周乙、鲜军、杨宏、任杰、张学斌、伍雁鹏、汪超、黄巍、齐大鹏、刘文、张霆、龚蓉、魏毅、伍永豪、朱州、晁冰、朱小冬。没有他们卓有成效的研究工作，本书不可能顺利完成。同样，我要感谢软件工程国家重点实验室的其他教授和他们的研究生，本书也包括了他们的许多研究成果。特别要感谢康立三教授和李元香教授领导的演化计算研究小组及他们的研究生，他们对演化计算和面向对象软件测试的研究成果是本书中重要的一部分内容，而演化计算的方法在本书讨论的许多方法中有着大量的应用。

借此机会，我要向我的妻子王旭莹表示衷心的感谢。正是由于她的鼓励和鞭策，本书才得以完成。

我还要感谢所有对我们的研究工作给予过大力指导和帮助的专家学者、组织机构、合作者和朋友们。感谢清华大学出版社的编辑、工作人员对本书的出版所做的大量工作和努力。

受编者水平的限制，书中会有不少的问题和错误。这些问题和错误一律由编者负责。请广大读者提出宝贵的批评和意见。如果在本书的使用中遇到任何问题，请与责任编辑联系：fuhy@tup.tsinghua.edu.cn。

徐仁佐

于武汉 香格里·嘉园

2007年2月

目 录

第1章

软件可靠性工程与软件工程

随着计算机的应用日益广泛，人们对软件质量的要求也越来越高，作为软件质量最重要的一项内容——软件可靠性，自然也受到人们的重视。在这几十年的研究过程中，人们也日益认识到，要保证软件的质量，特别是软件的高可靠性，必须要求软件行业全体人员的积极自主的工作和广泛的协作。于是，在1990年前后，终于形成了软件可靠性工程(SRE)的概念。现在，已发展成每年举行一次国际软件可靠性工程学术会议，以交流本领域的发展与成就。

在软件工程中应用软件可靠性工程方法可以做到：

- 分析、管理和提高软件产品的可靠性；
- 在用户对竞争价格、时效及可靠产品的要求之间求得平衡；
- 确定软件质量何时达到发行要求，将发行软件存在严重问题的风险降至最低；
- 避免因过度测试而来不及开拓市场的悲剧。

上述几项具体的收益，也同样是对最近兴起的软件工程经济学的贡献。

概括起来讲，软件可靠性工程主要包括三个方面的工作：

生命周期阶段	开发步骤	SRE的活动
可行性和需求分析	可行性分析 需求分析　开发设计	确定功能概图 对失效进行定义和分类 确定用户的可靠性要求 进行平衡关系研究 建立可靠性指标
设计和实现	设计 实现	在组间分配可靠性指标 按可靠性指标进行设计 根据功能概图集中配置资源 控制错误的引入和传播 度量现成软件的可靠性
系统测试和现场试运行	系统测试 现场试运行	确定操作概图 进行可靠性增强测试 跟踪测试进展 规定必要的额外测试 证明可靠性指标得到满足
交付和维护	运行　维护	规划发行后的人员需求 监视现场可靠性是否达到指标 跟踪调查用户的满意程度 通过监视可靠性安排新功能的引入时间 用可靠性度量指导产品及工程过程的改进

图1.1　软件产品生命周期中的可靠性工程活动

① 对软件可靠性的设计、分配和定量量测；

② 管理软件可靠性工作；

③ 软件可靠性的保证技术的选择与使用。

图 1.1 说明了围绕软件产品生命周期所进行的可靠性工程活动。该过程的各个阶段不必遵循严格的顺序，可靠性工程的各种活动也是如此，其中有很多交叉和重复。应该将每个可靠性工程活动只放在要求工作量最多的阶段完成。

1.1 软件的问题

软件是人的大脑逻辑活动的产物，因为人的教育程度、工作经验、思维习惯、认识能力、工作、敬业精神等多方面的差异，致使软件出错在所难免。

软件出错的事例报道有很多。20 世纪，美国范登堡空军基地导弹试射的失败的原因就是计算导弹飞行轨道的公式中一常数丢失小数点；欧洲阿里亚娜火箭的失事等的教训，使得人类认识到软件如同硬件一样，有着可靠性的问题，而且，其中的问题，比硬件可靠性还要严重得多。

目前，我国的软件形势严峻：透明度差，用户对软件不信任，软件危机日益严重。目前，我国的许多软件企业还没有认识到软件的质量对企业发展的重要性，还没有认识到软件的可靠性对国民经济发展的重要性。

解决之道在于软件生产的工业化——软件工程水平的普及与提高，软件可靠性工程的实施与进步。

软件工程的目的就在于提高软件生产率，改进软件质量。

1.2 与软件质量有关的基本概念

1. 概念

(1) 特性(characteristic)

帮助识别和区分各类实体的一种属性，包括物理、化学、外观功能或其他可识别的性能。

(2) 质量(quality)

反映实体满足规定和潜在需要能力的特性之总和。

(3) 需求(requirement)

需求应明确规定以下内容：

① 性能。

② 实用性(usability)。

③ 广义可靠性(ISO 文件称为可信性，即 dependability)，用于表示可用性、可靠性、安全性、机密性、完整性、维修性等的综合概念。

2. 质量

下面的基本概念从各个不同的方面用以表示软件的质量。