可靠性·维修性·保障性技术丛书 12

丛书主编 王自力

RMS

软件验证与确认

Software Verification and Validation

主编 刘斌

国防工业出版社
National Defense Industry Press

可靠性·维修性·保障性技术丛书

软件验证与确认

Software Verification and Validation

主　编　刘　斌
副主编　王轶辰　杨顺昆　殷永峰

国防工业出版社
·北京·

内容简介

本书理论联系实际，由浅入深地对软件验证与确认的相关概念进行了介绍，并结合我国装备软件的研制过程对验证与确认过程进行了详细的阐述，本书对测试、评审和形式化验证等方法进行了介绍，并对当前装备软件研制中的软件测试过程进行了深入的探讨。另外，本书还从实践的角度出发介绍了软件验证与确认活动的自动化辅助工具以及过程文档模板，具有极强的工程参考价值。

本书可供高等院校软件工程、计算机及相关专业的研究生作为学习参考，同时还可作为从事装备软件研发、软件测试以及软件验证与质量保证人员的工作参考书。

图书在版编目(CIP)数据

软件验证与确认/刘斌主编. —北京：国防工业出版社，2011.4

(可靠性·维修性·保障性技术丛书)

ISBN 978-7-118-07306-5

Ⅰ.①软... Ⅱ.①刘... Ⅲ.①武器装备－应用软件－软件可靠性 Ⅳ.①TJ02-39

中国版本图书馆 CIP 数据核字(2011)第 048170 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 710×960 1/16 **印张** 17¼ **字数** 305 千字

2011 年 4 月第 1 版第 1 次印刷 **印数** 1—4000 册 **定价** 45.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)68428422 发行邮购：(010)68414474

发行传真：(010)68411535 发行业务：(010)68472764

Preface 序 RMS

1995 年，国防科技及教育界著名专家杨为民教授组织编辑出版了国内第一套《可靠性·维修性·保障性丛书》，对推动武器装备质量观念的转变，提高武器装备的可靠性、维修性、保障性水平，发挥了重要的推动作用。

15 年后的今天，树立现代质量观，持续提高可靠性、维修性、保障性水平，已成为武器装备建设与国防科技发展中的共识，特别是《武器装备质量管理条例》的颁布实施，表明可靠性、维修性、保障性在现代质量观中具有战略性、全局性和基础性的地位和作用，高可靠、长寿命、好维修、易测试、能保障、保安全已成为武器装备研制、生产和使用中的普遍要求，可靠性、维修性、保障性工程活动已全面进入武器装备寿命周期各阶段，为提高武器装备的效能、降低寿命周期费用发挥了不可替代的作用。

在上述背景下，在武器装备建设与国防科技发展中，无论在技术上还是在管理上，都对可靠性、维修性、保障性提出了更高的要求。为适应这种新形势，我们组织有关专家重新编辑出版了这套《可靠性·维修性·保障性技术丛书》，共 12 册，以满足广大工程技术和管理人员的迫切需求。

本套丛书认真总结了 15 年来国内外武器装备可靠性、维修性、保障性最新实践经验，全面吸收了我国在预先研究和技术基础研究领域中取得的主要研究成果，从装备、系统、设备、元器件等多个产品层次和硬件、软件等不同产品类别，可靠性、维修性、测试性、保障性、安全性等多种质量特性，以及论证、研制、生产和使用与保障等寿命周期各阶段，全方位地论述了相关领域的基本概念、技术方法、实践经验及发展方向，具有系统性、实用性和前瞻性，从而有助于读者全面、系统地了解和掌握该项技术的全貌。本套丛书中阐述的可靠

性、维修性、保障性理论与技术，对武器装备和一般民用工业产品均具有普遍的适用性。

《可靠性·维修性·保障性技术丛书》是一套理论与工程实践并重的著作，它不仅可以为广大工程技术和管理人员提供有用的指导和参考，也可作为有关工程专业本科生、研究生的教学参考书。我们相信，这套丛书的出版，对我国武器装备可靠性、维修性、保障性工程的全面深入发展将起到重要的推动和促进作用。

丛书编辑委员会

2010 年 12 月

Preface 前言

软件工程方法提供了软件质量和可靠性得以确立的基础，而软件验证与确认方法提出并规范了软件质量保证的一系列活动。经过数十年的发展，软件验证与确认已成为暴露软件缺陷、保证软件质量和可靠性的最有效手段之一。

本书旨在从软件质量和可靠性基本概念入手，结合当前我国型号工程领域软件验证与确认的实际经验，全面、深入地讨论适合我国型号工程领域软件验证与确认的方法和手段。

本书第1章将首先介绍软件及软件质量基本概念，并在此基础上阐述软件质量与可靠性管理的发展，最后对软件验证与确认技术进行简介。第2章介绍软件验证与确认涉及的基本概念。第3章主要介绍软件验证与确认活动的过程，以及各个阶段的主要工作。第4章讨论验证与确认方法，主要从软件测试、软件评审及软件形式化验证等方面进行阐述。第5章着重讨论软件测评技术，从软件测试技术及软件测试管理两个方面展开，特别对当前型号软件工程领域常用的软件第三方测评进行了介绍。第6章对自动化的软件验证和确认做了介绍，并对工具进行了探讨。第7章对文档做了介绍，给出了一些工作中常会用到文档的模版。本书的读者对象主要定位于高等院校软件工程、计算机及相关专业的研究生与高年级本科生，还可作为有志于从事软件验证、开发和维护的专业技术人员的参考书。

本书由殷永峰编写了第1、4、5章，王轶辰编写了第2、3章，杨顺昆编写了第6、7章，全书由刘斌统稿，由金惠华教授、宋晓秋研究员主审。在此谨表示诚挚的感谢。

特别感谢阮镰教授在全书组织结构方面给出的良好建议，博士生黄抚群在文字整理及附录准备等方面所做的大量工作。感谢北京航空航天大学011室和中航工业计算机软件北航可靠性管理与测评中心的同事们，本书是他们多年学术耕耘和工程实践的心血和结晶，是他们多年的积累和帮助才使本书能与读者见面。

由于时间和精力的限制，本书在深度与广度方面有一定局限性，不当及谬误之处，恳请读者批评指正，以帮助我们改进并完善本书。

本书编写组

2010年5月26日

Contents 目录 RMS

第1章 绪 论

1.1 软件概念及其特点

新世纪伊始，我们的社会已步入知识经济时代，知识经济的特点在于创造价值的主要源泉已不再是依赖于资源、资本和人的简单劳动，而是依赖于人的智慧和科技的创新。人类文明的发展史已充分证明，科技的更新对生产力的发展起着决定性的作用，对于知识经济时代，此作用则应更加明显。

计算机行业是人类历史上发展最为迅速的行业之一。随着信息产业的迅猛发展，软件产业持续发展，已成为推动信息产业、国民经济发展的战略性产业。尤其在过去20年里，软件已经成为各行业中事务处理不可分割的一部分。事实上，软件及软件工程技术的发展，大大推动了人类信息科技产业的进程，已成为人类进入信息化社会的支柱。软件产业关系到国家经济和文化安全，体现了国家综合实力，是决定21世纪国际竞争地位的战略性产业。如果说微电子是信息社会的“细胞”，网络是信息社会的“神经”，那么软件就是信息社会的“灵魂”。与此同时，计算机软件在计算机系统中所占比例也越来越高。1966年经济合作与发展组织技术级别报告指出，计算机中硬件部分的价值和软件的开发费用比率20世纪60年代初以前为70%对30%，到70年代初是50%对50%，80年代初上升到20%对80%，90年代初进一步上升到10%对90%，表1-1所示为软件在国外战机航电系统中的应用情况。计算机产业结构逐渐从以硬件为核心向以软件为主的方向过渡，现代及未来影响计算机应用领域扩展的主要因素是软件的技术进步。

表1-1 软件在国外战斗机航电系统中的应用

第X代战斗机	机 型	软件所实现的航电系统功能比例
第一代	F-100	约8%
第二代	F-111	约20%
第三代	F-16	约40%
第四代	F-22	80%左右
	F-35	80%以上

目前，工业界和学术界对于软件的普遍解释为："软件是计算机系统中与硬件相互依存的部分，它包括程序、数据及其相关文档的完整集合"，一般由应用程序、系统程序、面向用户的文档、面向开发者的文档四部分构成。

软件的主要特点如下：

（1）软件作为脑力劳动的产物，是一种逻辑实体，而不是具体的物理实体。软件具有抽象性，这个特点使得软件与计算机硬件或其他工程对象有着明显的区别。人们可以把软件记录在纸上，保存在计算机存储器内，也可以存储在其他介质如硬盘、磁带和光盘上，但却无法看到软件本身的形态，必须通过观察、分析、思考、比较、判断等手段，去了解它。

（2）软件的生产与硬件不同，即软件开发过程没有明显的制造过程，因为软件是通过人的智力和脑力活动，把知识与技术转化为信息的一种产品。一旦软件开发成功，就可以很容易地对相同内容进行复制，因此带来软件产品的知识产权保护问题。

（3）软件在运行和使用过程中，不存在像一般硬件的机械磨损、老化的问题。任何机械、电子等硬件设备在使用过程中，其失效率一般都遵循图 1－1 所示的浴盆曲线。因为在硬件设备刚投入使用时，各部件尚未做到配合良好、运转灵活，容易出现故障。经过一段时间磨合运行后，质量可以稳定下来，并经过一段时间的保持。当设备经过较长时间运行，就会出现磨损、老化，从而导致失效率慢慢变高。当失效率达到用户不可接受程度时，设备寿命终止。而软件的情况却不相同，一般它没有浴盆曲线的右半翼，因为它不存在磨损、老化的问题。然而，软件存在退化问题。在软件生存周期中，为了使软件能够不断适应硬件、运行环境及用户不断提出的新需求，往往需要多次修改、升级和维护，而每次修改则会不可避免的引入新的软件缺陷，导致软件失效率升高，软件失效率曲线如图 1－2 所示。

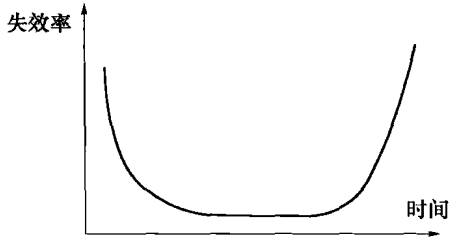

图 1－1　硬件失效率

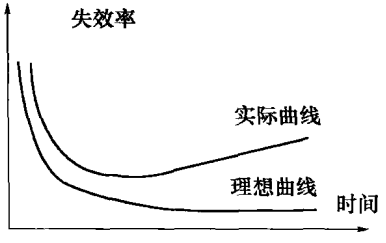

图 1－2　软件失效率

(4) 软件开发和运行往往受到计算机系统的限制,对计算机系统有着不同程度的依赖性。软件不能完全摆脱硬件单独存在并运行,这种依赖性给软件开发提出了软件可移植性问题。

(5) 软件本身的复杂性。软件是人脑智力的产物,决定了其本身固有的复杂性,它要反映自然规律或各类设备的事务处理,软件开发往往涉及相关领域的多种专业知识,使得软件复杂性已成为不可回避的事实。

(6) 软件工作往往与设备因素相关。软件开发和运行则涉及众多机构、体制及管理等方面,甚至人的观念和心理因素也会与之相关。对于这些社会因素如果重视不够,往往会有碍软件工作的开展,甚至影响到软件项目的成败。

1.2 软件质量基本概念

在计算机技术的发展过程中,软件质量问题始终是伴随着软件业发展的一个顽疾,软件质量的低下主要表现为经常出现的软件失效。随着软件规模的不断膨胀,失效已经成为限制软件发展的桎梏。Tassey Gregory 博士在一项由 Triangle 研究所和美国国家标准及技术研究院资助的研究中得出:软件失效导致美国每年 595 亿美元的经济损失,占国家净国有资产的 1%。根据 Gregory 博士的估计,减少当前软件 1/3 的缺陷,就能挽回 222 亿美元的经济损失。在欧洲,奥地利一家名为"软件在线"的网站针对 358 名 IT 业经理的调查显示,由于劣质软件之故,将近 75% 的欧洲企业每年要损失大约 50 万欧元;15% 的拥有超过 5000 名员工的企业甚至因此亏损上百万欧元。据美国国家标准与技术研究所 2002 年公布的一份美国软件工程行业研究报告,软件工程师把平均 70% ~80% 的时间用于软件测试和调试,平均每个软件缺陷花费 17.4h 的修复时间。研究报告估计,美国平均每年花费超过 500 亿美元用于软件测试和调试。尽管如此,软件缺陷的问题依然突出,据美国国防部和 NASA 统计,当今航天和武器系统项目中的软件可靠性比硬件系统大约低一个数量级。可见软件质量和可靠性问题已成为制约软件产业发展的瓶颈,下面就软件质量基本概念进行阐述。

(1) 软件质量定义。软件质量是软件产品满足用户使用要求的程度。

(2) 软件质量管理。软件质量管理是在软件质量方面指挥和控制组织的协调的活动。

(3) 软件质量控制。软件质量控制是对开发可用软件产品的过程的测量与监控。软件质量是软件产品的一组固有特性满足用户使用要求的程度。为了使软件产品质量满足用户使用要求,必须实施软件质量管理。我们从软件质量管

理的角度讨论过程控制，实际上是讨论软件生存期过程特别是软件开发过程的质量控制，只要这些过程在质量方面得到恰当的控制，所开发的软件产品的质量就会使用户满意。

需要说明的是，本书并不涉及质量管理的所有方面。因为，质量管理是在质量方面指挥和控制组织的协调的活动。在质量管理方面的指挥和控制活动，通常包括制定质量方针和质量目标以及质量策划、质量控制、质量保证和质量改进。而本书主要涉及质量控制。质量控制是质量管理的一个重要部分，致力于满足质量要求。

软件质量控制的核心是过程控制。

(4) 软件的质量模型。对于软件的质量特性，必须予以量化与测量。因为对任何事物，如果不能测量它，也就不能控制它。对软件的上述质量特性建立量化的模型是为了更好地控制软件质量。

1.3 软件质量与可靠性管理的发展

在软件出现的初期，是没有软件质量和可靠性管理的，直到20世纪60年代末，在世界范围内爆发了“软件危机”后，人们才认识到，只靠编程语言、编程方法来开发软件，尤其是大规模的复杂软件是不行的。必须有一套工程化、规范化的方法来指导软件的开发和管理。于是，在70年代初，就有了软件生存期的第一个模型——瀑布模型(WFL)和软件工程(SE)。在70年代中期开发出了第三代编程语言(3GL)。在80年代初，则推出了全面质量管理(TQM)。80年代中后期有快速原形技术(PROTO)和计算机辅助软件工程工具(CASE)。在90年代，软件质量管理上了一个新台阶，即从软件产品的质量管理发展为对软件开发过程的过程管理。这一标志是1991年美国推出的CMM(即软件能力成熟度模型)和在90年代中期推行的SPI(软件过程改进)，包括PSP(个体软件过程)和90年代末的TSP(小组软件过程)等。

软件可靠性则是在20世纪70年代中期提出，到80年代中期得到发展，大约在1988年，技术人员开始使用软件可靠性方法。AT&T Bell实验室围绕软件可靠性工程(SRE)的概念进行了一系列的工作，软件可靠性的工作已超出了软件可靠性的建模和测量，扩展到了软件可靠性测试和软件可靠性管理。1990年IEEE的软件可靠性工程分委会成立，而到了90年代中期才发展出了软件可靠性工程，其中当然包括了软件可靠性管理。

图1-3所示为从20世纪70年代直到2000年，软件质量和可靠性管理以及软件工程的发展历程。

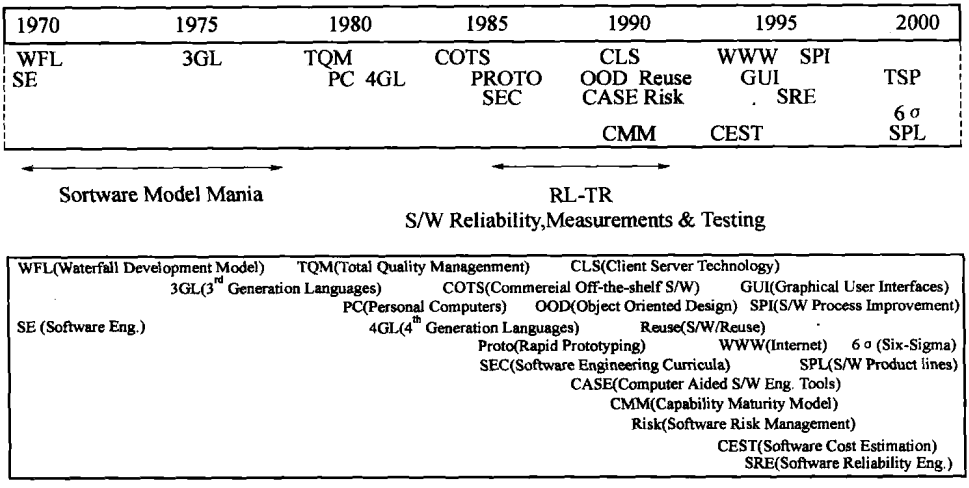

图 1-3 软件质量和可靠性管理的发展历程

1.4 软件验证与确认技术简介

软件验证(Verification)和软件确认(Validation)是软件工程领域的两个基本概念,往往缩写成"V&V","V&V"定义(IEEE Std 1012-2004)如下:

(1) 软件验证是"通过检查和提供客观证据,证实规定的软件需求是否已经得到满足。

(2) 软件确认是"通过检查和提供客观证据,证实特定预期用途的需求是否得到满足。"

通俗地讲,软件验证和确认是软件测试的两种技术。软件验证是在软件开发的各个阶段,从软件技术人员的角度,测试当前的开发成果(文档,代码等)符合设计的规范,保证按照设计流程和要求进行开发,即"正确地做了事"。软件确认是从用户的角度,测试当前的开发成果符合用户的真正需求,即"做了正确的事"。

经过数十年的发展,软件验证与确认技术已成为暴露软件缺陷,保证软件质量的最有效手段之一。

第2章　基本概念和活动

2.1　基本概念

软件验证与确认是软件质量保证的一项重要而且有效的手段。软件验证与确认活动涉及软件质量、软件测试等多个领域的知识，本章首先对涉及的一些基本概念进行讨论，然后概括地说明软件验证与确认的基本活动。

2.1.1　软件质量模型

软件质量是指软件系统或系统中的软件部分的质量，即满足用户需求，包括功能需求和性能需求的程度。

如上所定义，软件质量是软件产品的一组固有特性满足用户使用要求的程度。为了使软件产品质量满足用户使用要求，必须实施软件质量管理。从软件质量管理的角度讨论过程控制，实际上是讨论软件生存期过程特别是软件开发过程的质量控制，只要这些过程在质量方面得到恰当的控制，所开发的软件产品的质量就会使用户满意。软件质量控制的核心是过程控制。

质量模型是一组特性及特性之间的关系，它提供规定质量需求和评价质量的基础。通常利用软件模型来描述影响软件质量的特性。已有多种有关软件质量模型的方案，它们具有共同的特点就是将软件质量属性规定成分层模型，其中最基本的叫做基本质量特性，它可以由一些子质量特性定义和度量，这些子质量特性在必要时又可以由它的一些子质量特性定义和度量。

ISO 的软件质量模型是目前最广为使用和借鉴的质量标准，它包括四部分：

（1）ISO/IEC 9126－1:2001《软件工程产品质量第1部分:质量模型》

（2）ISO/IEC TR 9126－2:2003《软件工程产品质量第2部分:外部度量》

（3）ISO/IEC TR 9126－3:2003《软件工程产品质量第3部分:内部度量》

（4）ISO/IEC DTR 9126－4:2004《软件工程产品质量第4部分:使用质量的度量》

根据这个模型，将软件质量模型分为内部质量模型、外部质量模型和使用质量模型。

外部质量是基于外部视角的软件产品特性的总体，即当软件执行时，在模拟环境中用模拟数据测试时使用外部度量进行典型地测量和评价的质量。在测试