国防科技工业质量与可靠性专业技术丛书

软件质量管理

石　柱　主编

航空工业出版社

国防科技工业质量与可靠性专业技术丛书

软件质量管理

国防科学技术工业委员会科技与质量司　组织编写

主编　石　柱

编写　遇　今　胡渝彪　王　琪　杨双进

主审　何新贵　宗玮赓

航空工业出版社

内 容 提 要

本书是《国防科技工业质量与可靠性专业技术丛书》之一。

本书共分九章和两个附录，其内容包括：软件质量管理概述和基本概念，软件质量管理基础，软件质量评价、软件开发和维护过程控制，软件验证与确认技术和方法，配置管理和 FRACAS，软件质量管理的相关文档，软件过程改进。两个附录包括软件设计准则和软件设计评审检查单示例。

本书可作为国防工业质量管理专业人员、软件研制人员、软件测试人员、型号研制管理人员对开展质量管理工作提供技术支持和学习参考用书。

图书在版编目（CIP）数据

软件质量管理/石柱主编 .—北京：航空工业出版社，2003.9

ISBN 7-80183-240-X

Ⅰ. 软… Ⅱ. 石… Ⅲ. 软件质量-质量管理及控制

Ⅳ. TP311.5

中国版本图书馆 CIP 数据核字（2003）第 085437 号

航空工业出版社出版发行

（北京市安定门外小关东里 14 号 100029）

利森达印务有限公司印刷　　内 部 发 行

2003 年 9 月第 1 版　　2003 年 9 月第 1 次印刷

开本：787×960 1/16　　印张：14　　字数：284 千字

印数：1—2000　　定价：35.00 元

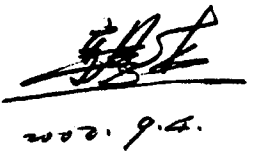
序

随着科学技术的进步和人们对高质量的追求，质量工作越来越显示出它的重要性。三代中央领导同志都十分重视质量工作，多次强调要把质量工作作为关系到国民经济发展的大事来抓，质量工作在全国乃至全世界日益成为人们关注的焦点。质量对于军工产品而言尤其重要，从近代战争的历史看，武器装备的技术水平、质量水平在一定程度上决定了战争的式样和战争的进程。武器装备的质量直接关系到国防事业的发展，关系到未来战争的胜败，关系到战士的生命。国务院领导高度重视军品质量，强调指出“要整顿，要保军”、“保军首先要确保军品质量”。

国防科技工业战线的各级领导干部，长期以来始终坚持“军工产品质量第一”的方针，坚持预防为主，严把质量关，全面完成了党和国家交给的各项光荣任务，取得了一系列的光辉业绩，使国防建设和军工技术迅猛发展。新的国防科工委自成立以来就十分重视质量工作，强调“质量是国防科技工业的生命”，积极推进质量与可靠性基础建设，积极推动武器装备的质量与可靠性工作。但是，近年来，随着武器装备技术和质量要求的提高，随着军工队伍的新老交替，军工科研生产的质量形势依然十分严峻，质量工作面临着前所未有的巨大压力，迫切需要提高质量工作的力度和整体水平，提高全员的质量意识和工作质量，提高工程技术人员、质量与可靠性专业人员的业务素质和技术能力。为此，国防科工委组织编写了《国防科技工业质量与可靠性专业技术丛书》，有针对性的介绍当前质量与可

靠性方面的新要求、新技术、新方法，为全员质量教育培训和质量工作的规范化、科学化提供了强有力的技术支持，以便更加深入地贯彻落实军工质量法规和标准，指导军工科研生产的质量与可靠性工作。

国防科技工业战线的全体员工和广大质量工作者，要加强理论学习，不断增强质量意识和业务能力，以高度的革命热情和事业心、责任感，积极投身到军工科研生产的各项质量工作中去，为国防事业的发展做出更大的贡献。



2002.9.4.

前　言

国防科技工业既是当代高新科技集中应用的重要领域，又是推动高新科技发展的力量源泉。作为时代技术标志的计算机软件技术已广泛地应用于制导、导航、控制、测试、通信、数据处理等关键领域。

在武器装备系统中，计算机软件的规模越来越大，其复杂性程度越来越高，其地位和作用显得越来越重要，关系着系统功能的强弱和成败。在这种背景下，人们对计算机软件的质量和可靠性提出了更高的要求。

为了研制出高质量和高可靠性的计算机软件，应当从技术和管理两个方面入手。在技术方面，应在软件研制过程中采用新的方法和工具，通过避错、查错、排错和容错，减少软件中的潜在缺陷，提高软件的内在质量；在管理方面，应加强对软件研制过程的控制，使软件的研制过程规范化，以过程的高质量来保证产品的质量。

本书总结了近十年来在航天型号软件研制、质量保证、软件评测和质量管理方面的具体实践，吸收了国外在软件质量管理和软件过程改进方面的先进理念，并针对国防科技工业的实际补充了一些切实可行的内容。全书由九章和两个附录构成。

第 1 章主要介绍为什么要进行软件质量管理，并扼要介绍国内外软件质量管理的概况。

第 2 章阐述一些基本概念。包括软件、软件质量、软件质量保证、软件质量管理、软件失效机理、软件危机、软件工程、软件错误分类和软件与硬件的异同。

第 3 章主要介绍软件质量管理的基础。其中包括软件工程的基本原理、软件生存周期模型及选择指南、软件工程标准、软件分级分类管理、外购软件的质量控制、软件工具与环境、文档管理、软件重用、软件容错、软件再工程、净室软件工程法、软件设计准则和软件工程培训。

第 4 章主要介绍有关软件质量评价的内容。其中包括软件的 5 种质量观、软件度量的定义、软件质量特性模型、软件质量度量、软件质量数据采集、软件质量评价过程和评价方法。

第 5 章主要介绍对软件开发和维护过程的控制。包括每个控制节点的开发任务、输入、工作内容、输出和评审内容。

第 6 章主要介绍软件验证与确认技术。其中包括软件评审、软件审查、代码走查、桌面检查、程序正确性证明与形式化方法、软件测试和软件测试工具等内容。

第 7 章主要介绍配置管理、配置管理工具和软件 FRACAS。

第 8 章主要介绍软件质量管理的相关文档，其中包括软件质量保证计划、软件配

置管理计划、软件问题报告和软件更改报告、软件质量记录（软件质量履历书和软件产品证明书）、软件验收申请报告和软件验收评审报告。

第9章主要介绍基于SW－CMM、TSP和PSP的软件过程改进。

附录A给出一个软件设计准则的示例。

附录B分别给出软件需求分析检查单、软件设计检查单和软件实现检查单的示例。

本书可供质量管理专业人员、软件研制人员、软件测试人员、型号研制管理人员、大专院校本科生、研究生、工程技术人员学习及参考。但限于编者的水平，难免存在欠缺和错误，敬请读者批评指正。

本书由石柱主编，何新贵、宗玮赓主审。提供材料及承担部分编写工作的有石柱、遇今、胡渝彪、王琪、杨双进、郭晓慧等人。在本书的编写过程中得到了杨多和、郭瑞霞、卿寿松、赵宇棋、李明华、刘继忠、陈政、夏宇红、孙鹏飞、贾成武、张进明、齐葵、龚庆祥、刘钊等人的关心和支持，在此表示感谢。特别感谢本书的两位主审何新贵院士和宗玮赓同志，他们对本书的形成和完善提出了许多建设性的意见。

编　者

2003年8月

目　录

第1章 绪 论

1.1 引言

随着计算机的应用范围日益广泛，计算机软件变得日益复杂。计算机软件作为一种产品，也与其它产品一样存在着质量问题。在国外，由于软件质量而造成问题的例子俯拾皆是，不胜枚举。例如：

法国气象卫星软件由于质量问题，当计算机应当给一些气象探测气球发出一个“读取数据”指令时，竟错误地发出了一个“紧急自毁”指令，从而毁坏了141个气象气球中的72个，造成了探测任务的失败[1]。

1981年4月10日，美国准备发射一枚空间回收装置，在离发射时间尚有20分钟时，计算机实时控制系统的软件突然发生故障，迫使发射延期进行。事前尽管花了数千小时进行测试和模拟，但仍未测出这个隐患[2]。

一个挂装在F-18战斗机机翼上的导弹在点火之后未能成功地从发射装置中分离，其原因是在导弹发动机产生足够的推力使导弹离开机翼之前，因计算机软件错误而锁住了导弹保持机制，从而使该战斗机严重失控[3]。

1989年9月，苏联载人航天飞船由于软件问题无法启动返回火箭发动机，经修复后推迟两天才返回地面[3]。

Bell实验室曾对一个AT&T运行支持系统进行过统计，发现该系统80%的失效与软件有关[4]。

1979年，新西兰航空公司的一架客机因为计算机控制的自动飞行系统发生故障而撞到阿尔卑斯山上，机上257名乘客遇难[4]。

1983年，美国科罗多河水泛滥，由于计算机对天气形势预测有错，水库未能及时泄洪，以致造成了巨大的损失[4]。

在海湾战争期间，“爱国者”防空系统有一次未能成功地拦截“飞毛腿”导弹，造成军营被炸，28名英军死亡，其原因是其跟踪软件在运行100小时后出现了一个0.36秒的舍入误差[5]。

在过去，由于软件质量造成的灾难触目惊心，屡见不鲜，而在可以预见的未来几年中，这类灾难仍会发生，其主要原因如下[4]：

(1) 软件正成为许多关键系统的核心。由于计算机的使用具有提高效率、能取代人进行某些工作等优点，因此，计算机正日益广泛地应用于监视和控制复杂的、时间

关键的物理过程和机械设备。在这些物理过程和机械设备中，一个错误或失效可能会造成人身伤亡、财产损失或环境危害。而在这些关键的物理过程和机械设备中，软件所起的作用非常关键，它是控制的中枢和灵魂。一旦软件因质量问题出现错误或失效，就会造成系统危险，乃至造成灾难性的后果。

（2）软件是由人开发的，人不可避免地会犯错误。而人所犯的错误会造成软件存在缺陷，这些缺陷一旦在系统运行中暴露，就会导致系统出错或者发生故障。

（3）多数软件是由没有容错能力的机器执行的。计算机从不考虑在其上运行的软件是否存在错误，只是按部就班地执行它的命令，而不管这些命令是不是安全关键的。

（4）在当前的软件开发和维护中，主要考虑的因素是费用和进度，而不是可靠性。美国“阿波罗”宇航员 Gus Grissom 曾经指出[6]：“每当我想到所有的火箭和宇航员舱都是由要价最低的投标者制造的这一事实时，就使我思索再三。”

（5）对软件的测试是有限的，而对于一个复杂的软件系统来说，其路径状态相对来说是无限的，因此，不能保证 100％地剔除软件中的缺陷。

由此可见，软件的质量问题非常重要，应引起我们足够的关注和重视。

1.2 国外软件质量管理概况

1.2.1 美国软件质量管理概况

软件质量管理同软件工程一样，自问题提出以来，始终由需求牵引而不断发展和完善。在美国，这一需求的主要代表是美国军方，它是美国软件质量管理的源动力，推动着工业部门、学校、学术团体以及其它政府机构对有关问题进行研究，对有关成果推广应用，以提高软件的质量。

在 20 世纪 80 年代早期，美国国防部的软件倡议对美国软件技术（包括软件质量管理）的发展有着深远的影响。从 1989 年起，美国国防部每年向国会作一次有关国防关键技术的报告，每次都涉及到了有关软件的内容。例如，1991～1992 年度国防关键技术的第 2 项就是软件工程，提出了要解决软件和系统工程过程与环境、实时和容错软件、重用和重建、用于并行和分布式多机系统的软件，以及高保证软件技术等 5 个方面的问题。美国国防部还针对重大工程，组织研究关键技术，提出有战略意义的项目，并对其进行重点投资，组织研究和开发工作。例如，美国防务分析研究所受战略防御倡议机构（SDIO）之托，考察了行政部门、国防部、工业部门和科研单位，对战略防御倡议机构的软件大纲进行了评估，提出了其独特需求和缺陷，明确了满足战略防御计划（SDI）需求所要研究的关键软件技术领域，并针对可实现性、生产率、可靠性、功能和性能等目标，为战略防御倡议机构（SDIO）所需的软件技术排出了优

先次序。

美国国防部从采办办法方面推动大型软件工程项目的软件质量管理。在DODD5000.2《防务采办管理政策和程序》中关于软件的规定为：要遵守DODD5000.1《防务采办》中的基本政策和程序，加强寿命周期管理，把软件作为整个系统的一个重要组成部分来管理，进行综合系统开发，重视软件测试管理和度量，国防部元器件采办局委派高层执行官员对软件质量负责并监督保障Ada应用及软件工程等。例如，美国军方对“爱国者”系统的软件开发管理通过合同办法委托主承包商负责，并对成本、进度和质量制定具体的管理和控制方法。

美国国防部从能力认证方面推动软件开发单位的软件质量管理。美国国防部委托软件工程研究所（SEI）研究并制定对软件开发单位的能力进行分析评价的办法。在1987年，软件工程研究所提出了称之为“评估承包商软件工程能力的方法”。经过4年的实践，取得了良好的效果，并于1991年提出了经过修订的办法。

美国国防部制定了一系列规范，并通过规范的贯彻实施来保证软件的质量。在这些规范中最主要的规范为DOD－STD－2167A《军用标准——国防系统软件开发》和DOD－STD－2168《军用标准——国防系统软件质量大纲》。前者规定了国防系统软件工程规范的总纲，所有相关的软件规范都要以此为准、与此一致；后者规定了软件质量管理的大纲，所有关键软件都必须按照该规范进行软件质量管理。与上述两个规范配套的规范还有：DOD－STD－7935《自动数据系统文件编制》、MIL－HDBK－286《军用手册——对DOD－STD－2168（国防系统软件质量大纲）的剪裁指南》、MIL－HDBK－287《军用手册——对DOD－STD－2167A（国防系统软件开发）的剪裁指南》、MIL－STD－483A《系统、设备、军需品及计算机程序的配置管理条例》、MIL－STD－490A《规格说明条例》、MIL－STD－973《配置管理》、MIL－STD－1521B《系统、设备及计算机程序的技术评审和审计》、MIL－STD－1083《软件完整性大纲》等数十项规范。

美国的软件质量管理方法主要有下述两种：①对软件开发项目进行管理；②对软件开发单位进行管理。下面将分别介绍这两种方法的主要特点。

对软件开发项目的管理主要有下述几点：

（1）软件开发分阶段进行，各阶段认真进行验证和确认。

（2）重视贯彻军用标准或有关标准，一些大型软件开发单位都有贯彻有关标准的规范。

（3）重视软件测试工作，有独立的软件测试机构。

（4）重视软件质量数据的收集和分析工作，为控制和改进软件开发过程提供依据。

（5）重视先进技术和工具的使用，重视软件重用技术。

（6）重视对市售软件和第三方开发软件的管理，明确承包商对这些软件的质量管理负有全面的责任。

(7) 制定并执行软件质量保证大纲。

对软件开发单位的管理，美国军方主要从下述两个方面进行管理：一方面通过合同体现 DODD 5000.1 和 DODD 5000.2 规定的方针和政策，对承包商提出明确的质量要求，并对成本、进度和质量制定具体的管理和控制办法，以监控承包商遵守军用软件开发规范并建立能保证贯彻有关标准的机构；另一方面，通过对软件开发单位的软件开发能力进行评估，促进并鼓励他们不断提高其整体开发水平。

1.2.2 欧洲软件质量管理概况

欧洲各国的软件质量管理模式与美国的软件质量管理模式相似。例如，①提倡用软件工程来克服软件危机，致力于发展软件工程技术；②从欧洲空间局（ESA）的标准来看，其组织软件开发和进行软件质量管理所采用的基本原理、方式方法和技术工具均与美国军用标准和 IEEE 标准的有关软件工程的规范相似；③美军以 Ada 工程来保证和提高军用软件质量、降低军用软件维护费用的总战略被许多欧洲国家所采纳，并组织开发了集成的程序设计支持环境（IPSE）和可移植的公共工具环境（PCTE）；④从英国 Alvey 理事会委托编著的《软件可靠性手册》中可以看出，其软件项目管理和软件质量管理的原理和方法与美国使用的原理和方法基本相似。

欧洲的软件质量管理方法如下：

(1) 欧洲各主要发达国家都非常重视软件开发技术，欧洲信息技术研究战略计划（ESPRIT）和欧洲研究合作局（EUREKA）每年投资 2 亿美元用于研究软件技术，组织大型软件研究项目，如 EAST（EUREKA 先进软件技术）、ESF（欧洲软件工厂）和 PCTE + 等关键项目。

(2) 欧洲在某些技术领域处于世界领先地位并推出了一些先进的实用工具。例如，著名的维也纳开发方法（VDM）和 Petri 网技术都是诞生于欧洲并得到全世界公认的形式化技术，且得到了广泛的应用。在软件开发工具方面，著名的软件测试工具 LogiScope 就产生于法国。

(3) 欧洲各国在质量管理方面强调质量体系，在 1994 年发布的 ISO 9000 - 3《质量管理与质量保证标准——第 3 部分：ISO 9001 在软件开发、供应和维护中的使用指南》[7]就是以英国标准 BS 5750 为蓝本制定的。该标准把 ISO 9000 标准的一般要求与软件的特点相结合，规定了软件产品研制或生产单位的质量体系，是对这类单位质量保证能力进行认证的依据。

1.2.3 日本软件质量管理概况

日本是在 20 世纪 80 年代初才开始大规模地开展软件质量管理活动的。1981 年日本科技联盟软件生产管理委员会举办了第一次全国软件质量管理研讨会，会议就如何推动软件质量管理提出了下列 5 点建议。