

军队“2110工程”经费资助

软件保障概论

(第二版)

RUANJIANBAOZHANGGAILUN

朱小冬 王毅刚 叶飞 等◎编著

The background of the lower half of the cover features a faint, high-angle photograph of a printed circuit board (PCB) with several integrated circuits (chips) mounted on it. The image is rendered in a dark red, monochromatic style that blends with the overall color scheme of the book cover.

中国原子能出版社

军队“2110工程”经费资助

软件保障概论

(第二版)

朱小冬 王毅刚 叶飞 等 编著

中国原子能出版社

图书在版编目 (CIP) 数据

软件保障概论 / 朱小冬等编著. —2 版. —北京:
中国原子能出版社, 2017.5
ISBN 978-7-5022-8053-6

I. ①软… II. ①朱… III. ①军用计算机—软件工程
IV. ①E919

中国版本图书馆CIP数据核字 (2017) 第 103891 号

软件保障概论

出版发行 中国原子能出版社 (北京市海淀区阜成路 43 号 100048)

责任编辑 胡晓彤

印 刷 虎彩印艺股份有限公司

经 销 全国新华书店

开 本 787mm × 1092mm 1/16

印 张 14.25 字 数 338 千字

版 次 2017 年 7 月第 1 版 2017 年 7 月第 1 次印刷

书 号 ISBN 978-7-5022-8053-6 定价: 42.00 元

网址: <http://www.aep.com.cn> 版权所有 侵权必究

此为试读, 需要完整PDF请访问: www.ertongbook.com

第一版 前 言

随着计算机技术的迅速发展,软件在武器装备中的应用越来越广泛,软件保障已成为装备保障的重要组成部分,软件保障是确保运行和配置软件全面地连续保障装备的作战任务进行的所有活动的总和,包括部署前软件保障和部署后软件保障,是高技术装备形成、保持和恢复作战能力的重要因素。但是目前我军对软件的维护保障问题还没有足够的重视,相关的研究还基本处于空白,为了适应我军武器装备的发展与建设,我们将几年来的研究成果进行总结,完成此书。

本书是一本全面介绍软件保障的书籍,重点介绍了软件保障基本概念、组织实施以及相关的方法和技术。

全书分为10章,第1章为绪论,介绍了软件保障的概念以及主要的研究内容;第2章对软件保障的相关属性进行分析;第3章介绍了软件保障性系统级和要素级的分析方法;第4章从移交前、移交、移交后三个阶段对软件保障模型进行了介绍;第5章介绍了软件维护规划的相关内容;第6章介绍了软件保障机构组成、保障方的职能以及保障机构组织管理的相关内容;第7章介绍了软件供应保障,主要分析了软件供应保障的组织、过程、主要技术,并给出了战时供应保障的实施;第8章介绍了软件保障度量的确定与分析方法;第9章介绍了软件保障工具使用及CASE环境的构成;第10章对近几年才出现的新技术对于软件保障的影响进行分析,主要介绍了面向对象技术以及网络技术对软件保障的影响。最后,在结束语部分,编著者根据近几年的研究以及武器装备发展的任务,分析了软件保障的前景。

本书由朱小冬、杜晓明等人编著,朱小冬编写了第1章,叶飞编写了第2章、第7章,冯静编写了第3章、第8章,刘彦斌编写了第4章、第6章,杜晓明编写了第5章,王毅刚编写了第9章、第10章,马长捷编写了第9章软件测试的部分。全书由朱小冬负责统稿,甘茂治教授负责对全书内容进行了审定工作。全书在编著过程中得到了于永利教授、郝建平副教授等维修工程实验中心同仁的大力支持,在此一并表示感谢!

本书既可作为研究生相关专业的教科书,也可作为相关技术人员的参考用书。

由于编著者的水平有限,书中不妥及错误之处在所难免,恳请读者批评指正。

作 者

2007年1月于石家庄军械工程学院

修订说明

随着计算机软件技术的飞速发展和我军信息化建设的快速推进，软件和软件密集型装备大量装备部队，在装备中所占比重越来越大、发挥作用越来越关键。计算机软件已经成为基于信息系统体系作战的神经中枢，软件保障也成为影响基于信息系统体系作战能力形成的重要因素。为了适应我军软件保障实践需要和软件保障理论与技术的发展，有必要对本书的内容进行及时的更新与调整。为此，在第2版中，增加了部分新的内容，并删除了第1版中部分不再适应的章节。与第1版相比最主要的变化是：

（1）增加了第一章软件保障不同分类的概念与主要活动。在第1版中软件保障分类并没有给出明确的定义，影响了对软件保障的理解。因此，第2版中明确了软件保障三个类别的概念，并对各自的主要活动进行了解释和说明。

（2）更新了第二章软件维护性和软件保障性两节内容。完善了软件维护性相关内容，将软件保障性中的软件保障方案的内容进行了规范描述，并将其从第二章移到第五章，将第五章改为软件保障规划，完善了保障规划的内容。

（3）第三章更新并添加了软件保障性分析相关方法。重新规划了软件保障性分析相关方法一节，系统规划了软件保障性分析的相关方法。

（4）第五章软件维护规划调整为软件保障规划。将原来第二章的软件保障方案进行规范描述后，移入本章。

（5）第八章增加了软件维护性度量。将本团队在软件维护性度量方面的最新研究成果纳入到第八章软件保障度量。

本书第一章、第三章、第五章的修订由王毅刚执笔，第二章、第八章的修订由叶飞执笔。全书由朱小冬、王毅刚负责统稿。

尽管编著者对第2版做了共同的努力，书中不妥及错误之处在所难免，恳请读者批评指正。

作者

2015年10月于石家庄军械工程学院

目 录

第一章 绪论	1
1.1 概述	1
1.2 软件保障相关概念	4
1.3 软件保障与软件工程、软件开发技术	11
1.4 软件保障主要内容	12
第二章 与软件保障相关的属性	13
2.1 软件可靠性	13
2.2 软件维护性	26
2.3 软件保障性	46
2.4 软件测试性	50
2.5 软件安全性	58
2.6 其他	63
2.7 本章小结	64
第三章 软件保障性分析方法与过程	65
3.1 软件保障性分析概述	65
3.2 软件保障需求分析	68
3.3 软件保障性分析相关方法和技术	83
第四章 软件保障模型	101
4.1 概述	101
4.2 软件保障静态结构	102
4.3 移交前的软件保障	105
4.4 软件移交	111
4.5 移交后的软件保障	122

4.6	ISO/IEC 12207 中的软件维护过程	123
4.7	软件保障模型的发展	125
第五章	软件保障规划	126
5.1	概述	126
5.2	软件保障方案	126
5.3	软件维护规划	136
第六章	软件保障机构	146
6.1	概述	146
6.2	软件保障机构的职责	146
6.3	软件保障机构的职能	147
6.4	保障机构的组织与管理	150
6.5	本章小结	153
第七章	软件供应保障	154
7.1	概述	154
7.2	软件供应保障系统分析	159
7.3	软件供应保障系统模型	166
7.4	软件供应保障技术研究	176
7.5	战时软件供应保障初探	184
7.6	本章小结	185
第八章	软件保障度量	186
8.1	概述	186
8.2	软件保障度量的确定和分析	192
8.3	软件维护性度量	198
结束语	216
参考文献	217

第一章 绪 论

1.1 概 述

随着科学技术的发展，计算机技术已经全面深入到了社会的各个领域，快速发展、更新的武器装备更是受到了计算机技术的极大影响，典型的大型装备系统如舰船、飞机、导弹、坦克、自行火炮等肯定会应用大量的计算机技术，甚至连单兵轻武器中都使用了计算机技术，可以说，当今军事装备几乎都采用了计算机技术，并且成为衡量武器装备性能水平的因素之一。

众所周知，计算机技术的核心之一就是计算机软件。实际上，计算机软件正是计算机系统的关键，如相同的硬件平台，搭载不同的软件，就可以成为功能不同、性能各异的系统。再加上计算机软件设计与更改的灵活性，使得软件在计算机系统所占的比重越来越大，据国外统计，从20世纪60年代起，软件在飞机控制系统中实现的功能已经从20%上升至80%。

软件虽然是一种特殊的产品，但它仍然是一种产品，其他产品所具有的属性，在软件产品上依然存在。如产品的可靠性、维护性、保障性等属性。同样，其他产品所需要的服务，亦同样体现在软件产品上，如软件维护、软件保障。

从20世纪60年代，美军在装备系统中已大量使用计算机软件，尽管软件规模较小，但软件问题时有发生，如60年代中期美国首次进行的金星探测计划就是因为软件错误而惨遭失败。“软件危机”这一概念逐渐为人们所接受。20世纪70年代，软件问题更加严重，如美空军投资6亿美元用于阿波罗计划的软件开发，但计划实施中几乎所有严重故障都是由软件问题引起的。国外因为软件质量问题造成的事故还有很多。例如，美军一枚挂装在F-18战斗机机翼上的导弹，在点火后由于未能成功地从发射装置中分离出去，使该战斗机严重失控。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，造成分离失败。

软件的可靠性问题很早就引起了美国军方密切关注，也采取了很多的管理与工程措施。如大量开展软件工程、规范软件开发过程、对承担军用软件的开发的承包商开展软件开发能力评估（CMM）。通过这些措施，仍不能完全避免软件质量问题，据美国军方统计，软件可靠性比同期的硬件可靠性要低一个数量级。再加上软件需求变化，也无法完全对所开发的软件状态进行固化，造成软件经常处于修改状态，软件维护与保障成为软件不可避免的问题。20世纪80年代，美军已开始意识到软件保障问题的重要性，因为美国国防部及工业界的大量研究表明，典型的维护软件产品的费用在其全寿命费用中

的比重已从 60% 上升到 80%，并由此开始了软件保障（维护）的研究与实践。但当时的研究基本上局限于部署后阶段，即在出现软件问题后才从事保障活动，成效甚微，没有从根本上解决软件保障问题。但美国国防部从众多软件密集系统的惨痛教训中，积累了一些经验。同时，鉴于软件保障的高复杂性、高技术性，美军将软件保障称为软件保障的“冰山”。

20 世纪 90 年代后，软件保障费用在美军软件密集型装备保障费用中占着突出地位。1997 年国防部软件维护费用高达 200 亿美元，并呈逐年增长。因此美军十分重视软件保障工作，从软件密集型装备采办、保障体制、保障技术与方法等多方面着手全面系统地开展了软件密集型装备的保障研究，并取得了较有成效的进展。但研究成果尚未全面推广，许多问题有待进一步解决。

2000 年以后，美国陆军软件保障的负责人 Joseph 预计，在任何一个时刻美国陆军都会有 40 或更多战场系统的软件处于维修（更改）状态中。可见软件保障工作量将是十分巨大的。美军对软件保障的理论与应用研究的投入会进一步增大，也将更加深入。

我军在新型装备中也包含了大量的计算机软件，同样出现过大量的软件质量问题。

例如，1998 年，在某空军机场进行无人机夜航试验。无人机起飞后，在飞行高度 200 m 处，无线电综合测控系统主站上的计算机突然死机，技术人员无法通过计算机对无人机进行控制，飞行数据也无法收集，只能将控制状态转到外控，由外控手对无人机进行控制。此时，无线电测控系统机动站各设备工作正常。待技术人员重新启动计算机后，一切恢复了正常。此次飞行虽然最终较好地完成了考核任务，但显然对正常使用有着很大的隐患。最终故障原因是：无人机上的摄像头工作范围是方位正负 110° 、高低正负 60° 之间，应用软件中也按此角度规定了相应范围；但由于起飞过程中的剧烈颠簸，导致角度超出了规定范围，从而产生数据溢出，应用软件无法正常执行，以致导致死机。

某指挥自动化系统在试验时，经常出现指挥过程中受指挥部分单元自行离开系统，无法完成指挥，开始以为是网络接口失效，经更换网络接口后，系统恢复正常。但由于此现象发生频率高，维修中很快将备用网络接口全部用完，而故障依旧频繁发生，而更换下来的接口板没有测出故障，重新换上后又可正常工作，最后分析结果是由于软件缺陷，使软件运行过程中令牌系统丢失令牌，造成接口无效的现象，经修改软件后才正常。

某雷达控制系统，承担着目标侦察、锁定，火炮自动瞄准、控制的任务，但在某部两次演习过程中，装定的参数被自动清零，使火炮炮口归位，处于非受控状态。经部队反复检查系统，排除了硬件部件故障的可能性，但由于软件属非维修单元，再加上由于该故障现象的偶发性，在进行系统检查时无法准确地进行故障再现，使得该系统故障一直得不到妥善解决，部队只好决定该系统以后不再参加演示汇报，以防发生不测。

由此可见，我军装备中软件问题实际上已经大量存在，不仅出现在装备研制过程中，也出现在装备使用过程中。

软件保障已经成为我军装备保障必须面对的课题。近年来，随着我军装备建设的发展，高新技术装备越来越多，越来越多的装备中含有计算机软件，使计算机技术从原来主要在从高、精、尖装备上的使用，到当今应用到各种武器平台，乃至在单兵装备也大量使用；进而，计算机软件从原来的辅从地位，到现在成为装备中的控制核心、指挥中枢，从原来在装备中所占比例很少，到当前在装备中实现大部分功能，如图 1-1 所示，

显示了美军不同时期三代战机中软件实现功能所占的比例。我军在某些型号的装备中，软件实现功能所占比例亦高达 80% 以上。可见，软件已经大规模存在于我军的装备中，再加上当前的软件可靠性水平比硬件低一个数量级，如此大规模的软件应用，肯定会出现相当数量的软件故障需要排除，再加上软件的升级、完善、数据的修改、补充等工作，更需要有组织地进行，因此，软件保障必须在装备保障加以重点考虑。

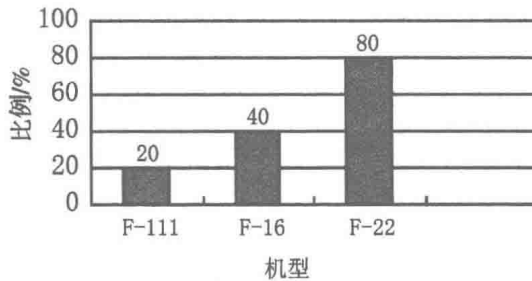


图 1-1 美军不同飞机中软件实现功能所占比例

软件保障涉及的不仅仅是对软件的修修改改，而是一个维修保障的系统工程。软件维护保障涉及的保障的体制、过程、技术与方法，而不仅仅是组织几个软件开发人员对有问题的软件进行修修补补。众所周知，软件开发必须工程化，即实施软件工程，以确保软件开发的质量，但由于软件质量涉及的因素很多，即使是实施了软件工程，也很难确保软件不存在质量问题。据国外统计，当前软件可靠性水平较硬件要低一个数量级。我国多次可靠性试验数据亦表明，软件原因造成的故障约占故障总数的 70%。此外，软件维护数据表明，软件维护的原因不仅仅只是因为软件缺陷，更多的原因是因为存在许多对软件进行扩充的需求，要求对软件进行更改。因此，软件保障是软件使用过程必须开展的一项有组织的工程活动，即便是遵循软件工程过程开发出的高质量软件，在使用过程中同样需要开展大量的保障活动。因此，软件保障应该是整个装备保障的有机组成部分，软件保障甚至比对硬件保障的要求更高、更复杂，如美军将其惊呼为软件保障冰山，如图 1-2 所示，从一个侧面反映出软件保障所面对的不仅仅软件本身，还有许许多多更深刻的内容需要解决。同样，软件保障的冰山也已经呈现在我军面前了。

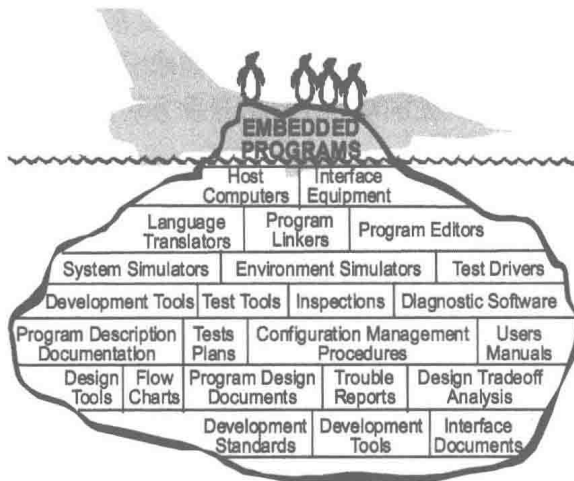


图 1-2 美国空军 F-16 飞机的嵌入式软件冰山

软件保障比硬件系统的保障更为复杂。软件是一种特殊的产品，是人类逻辑思维的生产物，其运行过程往往是不可见的。如果说硬件系统还可以通过模仿来进行保障的话，在软件保障中如果仅仅对可执行程序进行模仿显然是毫无疑问，甚至由于人个体的差异，同一段源代码不同的人会有不同的理解，因此，也就不难理解为什么会出现软件维护人员宁可重新编写系统而不愿对原系统进行维护的现象。但是，软件发展的经验告诉我们，不能进行维护的软件是“短寿”的软件，如果习惯用于新软件代替旧软件、习惯于重新编制软件而不维护软件，则这样的新软件则极有可能仍然是低质量的“短寿”软件。因此，对软件实施保障，更加需要在研制过程中进行规划、设计，以便在使用保障过程中进行组织、实施。当然，对软件工程化程度开展不太理想的软件，也可以通过先针对软件维护性开发改进性维护，再实施全面的保障活动。例如，美国海军安全司令部的软件保障中心成立之初，所保障的软件就属于文档不全、结构不良的软件，在经过半年多的软件维护性改进后，成功地完成了交给的软件维护保障任务。因此，软件保障虽然需要比硬件更加困难的工作，但仍是可以通过系统规划、加强组织来实施的工作。

1.2 软件保障相关概念

1.2.1 相关概念

为了方便描述，先对以下相关概念进行约定或定义。

软件：计算机程序、数据及文档的总称。本书所述的软件是指计算机软件，可以是系统软件、应用软件系统、嵌入式软件或软件模块。

客户：需要软件产品的个人或群体，通常（但不是必须）由他们确定其需求。如装备部门、信息部门等。

用户：直接使用系统与直接与系统打交道的个人或群体。用户通常向客户、供应商或维护方阐述需求。如操作人员、指挥人员等。

供应方：与客户为所供应的软件产品在合同条款下签署合同的组织或机构。供应方与开发方是同义语。如装备研制部门、生产部门等。

开发方：在软件生命过程中从事开发活动（包括需求分析、设计、验收测试等）的组织或机构。本书中将供应方与开发方等同看待，开发方可以是装备研制部门或研制部门的组成部分。

维护方：承担软件维护活动的组织或机构。无论维护工作是由内部机构完成还是外部机构承担，都可将维护方与维护机构等同看待。

保障方：承担软件维护、供应及其管理的组织或机构。

1.2.2 软件维护

软件维护：软件产品在交付使用后，为纠正错误、改善性能和其他属性，或使产品适应改变了的环境所进行的修改活动。软件维护根据其维护目的不同，可划分为纠错性维护、适应性维护和完善性维护。

纠错性维护：纠正在开发阶段产生而在测试和验收过程没有发现的错误所进行的软

件修改活动。软件错误包括设计错误、程序错误、数据错误、文档错误等。错性维护就是排除程序中存在的错误，程序错误导致系统无法完成规定的功能、造成任务中断，往往用户无法容忍，因为系统并没有如其设计和宣称的那样工作。因此，纠错性维护首先要查找的是初始技术规范，以便确定系统原设计是否达到了技术规范，并使之实现规定的技术规范。

适应性维护：为适应软件运行环境改变所进行的软件修改活动。运行环境改变包括系统规则变化、硬件变化、数据格式改变、软件环境改变等。例如，可能升级了操作系统，必须进行必要的修改以适应新的操作系统；自动预警系统中由于战场上敌方装备的变化，必须及时修改系统中的敌方装备数据库，以使预警系统能正确地完成任务。不幸的是，经常发生的是维护人员不得不花费大量的资源完成修改，而用户在使用系统时则并没有发现什么直接的改动，使得适应性维护往往成为一项默默无闻的工作。如美国“爱国者”导弹在海湾战争中，有一次未能成功拦截“飞毛腿”导弹，造成军营被炸，死伤 28 人。其原因是因为该系统设计时跟踪软件存在系统时间误差，但其误差要求满足原来冷战时期导弹系统每 24 小时转移一次、重新开机的战术要求。而在海湾战争期间，没有要求系统每 24 小时进行转移、重新开机，系统连续运行 100 小时后，出现 0.36 秒的累积误差，超出了允许的误差范围，结果造成拦截失败。这就是一起典型的软件适应性维护不到位的事例。

完善性维护：为扩充和增强性能而进行的软件修改活动。如扩充功能、改善性能、改善维护性等。完善性维护是指为满足用户新的需求而进行的所有修改，简言之，如果某些技术要求在原设计或技术要求是没有的，但用户希望在系统中增加这些内容，就属于完善性修改。所有新的用户需求都属于这一类，如果系统功能与技术规范所要求的功能相一致，而用户希望增强其功能，这就是属于完善性维护。

通常，在工作中将适应性与完善性两类合并到一起，称其为扩充性维护。

为什么要区分不同的维护类型？区分不同的维护类型，有利于理解软件维护与保障工作的难度、有利于理解软件保障为什么是一项“昂贵”的活动。

虽然尚没有关于年度经费的准确说法，但已有足够的证据表明维护消耗了软件生命期的大部分费用，是一项“昂贵”的工作。奥索在 1988 年研究软件维护状况时指出，许多软件的生命周期费用中仅仅 1/4 ~ 1/3 用于开发工作，也就是说，大约寿命周期费中的 67% 被用于使用与维护阶段。表 1-1 给出了由不同的人员或机构反馈的有关寿命周期费用中维护所占比例的数据示例。

表 1-1 奥索 1988 年调研的维护费用在整个寿命周期费用中所占的百分比

调查者	年度	维护费用 /%
Canning	1972	60
Boehm	1973	40 ~ 80
DeRose/Nyman	1976	60 ~ 70
Mills	1976	75
Zelkowitz	1979	67
Cashman and Holt	1979	60 ~ 80

这些数据来自 20 世纪 70 年代后期，即出自所有声称可降低整个费用的技术之前，如软件工程创新、方法、技术等。那么，现在的费用又是如何呢？

许多文献指出，由于软件维护费用的增长，维护行业如日中天。一家从事市场研究的高特纳集团公司预测了美国公司单独花费在软件维护上的年度费用达 300 亿美元，在 20 世纪 90 年代，寿命周期费用的 95% 将用于维护，如图 1-3 所示，很明显地可以看出，软件维护是昂贵的，且其费用仍在增长，可以说，所有从 20 世纪 70 年代到 80 年代的软件工程并没有减少寿命周期费用，更没能降低软件维护费用。这是为什么？

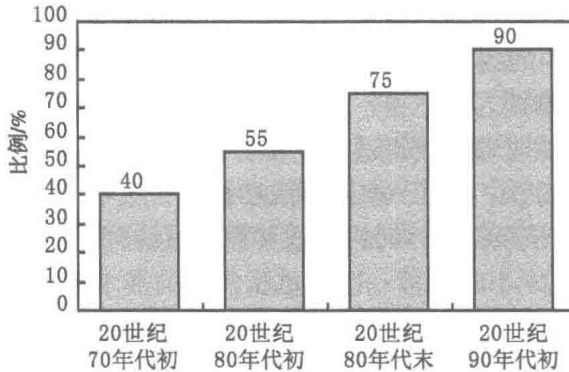


图 1-3 软件寿命周期费用中维护费用比例

导致软件维护费用居高不下的原因并不在于软件缺陷太多，而是因为扩充性维护。雷蒙早在 1980 年就提出软件变化的两个定律，他的第一定律是不断变化定律，该定律指出系统需要不断地变化以便可以继续使用；第二定律是不断复杂定律，该定律指出程序的结构将随着它的变化会变得越来越恶化。随着时间的推移，其代码的结构变得越来越糟糕，直到维护的费效比越来越差，还不如重新编写程序为止。

雷蒙定律指出了软件使用中会出现的事情，即不断地维护，因为软件自己是不会发生什么变化的。软件维护的原因有如下：

- (1) 纠正错误；
- (2) 纠正设计流程；
- (3) 与其他系统的接口发生变化；
- (4) 需要对功能或性能进行扩充；
- (5) 需要对系统进行必要的修改；
- (6) 需要对文件和数据库进行修改；
- (7) 用户要求改进设计。

更改软件以便在不同的软件、硬件环境中应用。

可见，纠正错误只占软件维护原因的一小部分。更多的软件维护统计数据亦支持这一说法，有关软件维护最全面和最权威的研究是 1980 年由 B.P. 李兹和 E.B. 史万森开展的。他们研究了 487 个软件机构，给出了软件生命期中与使用和维护期有关的最佳数据，在他们的研究期间，确定了每一类维护的时间分布，如图 1-4 所示是他们描述的按维护类别划分的时间比例分布。很显然，纠错性维护（即指改正问题和程序调试）只是占整个维护费用的一小部分，来自其他的资料也支持同样的结论：维护费用中的 80% 以上用于扩充性的。

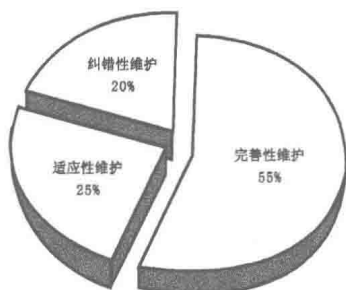


图 1-4 维护类别的分布情况

由此看出，软件维护费用居高不下的真正原因则是用户。他们不知道他们的系统想要干什么，造成在使用和维护阶段不断更改需求来缠住维护方，其中绝大部分是去扩充系统，所以说用户是问题的起因！他们是造成维护昂贵的原因之一。

典型的情况是，用户使用系统，当发现错误或确认扩充时，他们促使管理人员采取行动，管理机构则通过后面将讨论的软件配置管理程序让维护方进行纠错或扩充。所有的工作费用大多数情况都是直接由用户支付的，维护方作为服务机构，其“客户”就是用户。

用户是决定维护做什么事情的因素之一。过去的经验表明，80%的工作是扩充性维护，而软件扩充要比改正错误贵得多。因为是由用户要求的扩充，费用很高。

当然，这也不都是用户的失误，存在诸多原因造成 80% 的费用用于软件改进。我们知道，软件与硬件不同，软件设计完成后是可以更改的，因为其设计与开发都是在头脑中变化的，同时也预计了这种变化。上面的雷曼定律就指出了系统必须更改以便可以使用。例如美军的爱国者导弹系统原设计是用于反导弹的防御系统，在海湾战争期间，便对控制该系统的软件进行了成功的修改，使其具备了攻击能力。

上述数据说明，区分不同的维护类型对理解维护的意义具有很重要的作用，同样也阐明了，即使对于高质量的软件，即使是极为可靠的软件，其软件维护也是不可避免的一项繁重的工作。甚至可以这么理解，如果一个软件是不需要维护的，则其要么是“短寿”的软件，要么是“不重要”的软件。

1.2.3 软件保障

1.2.3.1 概念

软件保障是为保证投入使用的软件能持续完全地保障产品执行任务所进行的全部活动。

这里所指的“产品”可以是软件产品，也可以是包含软件的系统。对一个非独立的软件而言，是与硬件系统相配合以完成其规定功能的。实际上，还没有真正意义的纯软件，所有的软件都是与硬件相配合来共同完成一定功能的。

上述定义中的“任务”不仅仅是指系统设计时规定的任务或规格说明，还包括使用阶段中重新规定或扩充的新的任务需求。这是与硬件产品相差较多之处，硬件系统保障通常中保证其发挥规定的产品职能，而软件系统则还需保障其后续职能。

定义中所指的“全部活动”包括管理活动、技术活动。首先需要指出的是，软件保障活动不仅仅包括对软件的维护，还包括对软件的供应保障、安装保障、培训保障、使

用保障等一系列的保障活动；其次，软件保障不仅仅是保障的技术活动，还包括对软件保障的规划、管理活动，如软件保障性分析、保障方案制订、软件保障体制、保障机构选择或建立、保障资源预计与规划等一系列规划与管理活动。

1.2.3.2 软件保障要素

装备综合保障（ILS）要素通常归纳为 10 个。软件保障同样应考虑这些要素，而且从长远看其重要性、技术难度和所需资源都不亚于硬件。对软件密集系统应当特别重视有关软件和软件硬件接口保障的要素。

1. 维修规划

硬件维修是相对简单的，只将损坏的部件用好部件替换即可。而软件维护就必须重新设计软件以排除类似故障或缺陷，还必须检查系统剩余部分以确保已找到并排除的失效不会将其他错误或潜在故障引入系统。例如，当系统发生故障后，硬件和软件维修有着不同的修复过程和方法。显然软件维修有更高的技术要求。在部队只能进行简单的重新启动、软件复制、安装之类的工作；软件修改则要由基地级（研制单位或高层次的“软件编程中心”）来进行。所以，软件维修通常只需设两个维修级别。

2. 人员与人力

软件维护，不论是纠正活动还是增强性能，通常都是同创造一个新的计算机软件配置项目（CSCI）一样。与软件保障有关的计算机程序员要求编程技巧接近于那些开始开发软件的人员。软件开发往往有相对长的时间和系统的组织指导；而软件维护则可能在较为困难的条件下。从这个意义上说，软件保障可能比软件开发具有更高的技术水平要求。

3. 训练与训练保障

显然软件维护人员需要经过充分的高层次培训。软件的供应人员也需要专门培训。

4. 供应保障

由于软件维护是重新设计，改变了软件配置，故传统意义上的备件对软件维修没有意义。但软件更改后，使用在同样条件下的同型软件都要更新，所以软件仍存在供应问题。同时，软件因媒体损伤或敌对威胁造成破坏时，也有恢复软件配置的问题，这时需要的是类似硬件更换的重新复制，需要再供应。软件供应或再供应与硬件供应有很大不同。软件可以通过卫星传送、有线传送、战术系统传送、快递和战区机动的复制与分发系统等多种方式快速分发。此外，还有软件版本的识别和分发问题，这一问题给管理战场上的软件版本带来沉重负担。

5. 技术资料

对软件维护和保障说来，技术资料的重要性比硬件更突出。对于军用装备中的软件保障，除各种软件文档外，还要有软件综合保障（ILS）计划、投入使用或部署计划、保障转移计划和战场系统用户手册（BSUM）等。

6. 保障设备与设施

软件保障需要的大都是通用设备，如：可编程只读存储器（PROM）和 PCB 程序设计器，光盘存储器（CD-ROM）、磁带、软盘复制器。为提供软件野战再供应能力，需要战区机动的复制和分配系统。它由安装接收卫星、无线电和其他传输设备的车辆与（存放新发布或再补给软件在适当媒体上所需要的）复制设备一起组成。

7. 设计接口

对软件也同硬件一样，应当建立其保障性设计准则。应特别关注可靠性与可维护性。软件开发时不注意维修问题，最后会是一个很差的设计，以至于维修原始编码比全面再开发还花钱。

1.2.3.3 生命周期中的软件保障

软件保障是一项软件保障的系统工程，是软件生命期内的的重要组成部分。因此，在《ISO/IEC 12207 软件生命期过程——信息技术指南》中，将软件保障作为整个生命期内的的重要组成部分。如图 1-5 所示，它包含了以下几个过程。

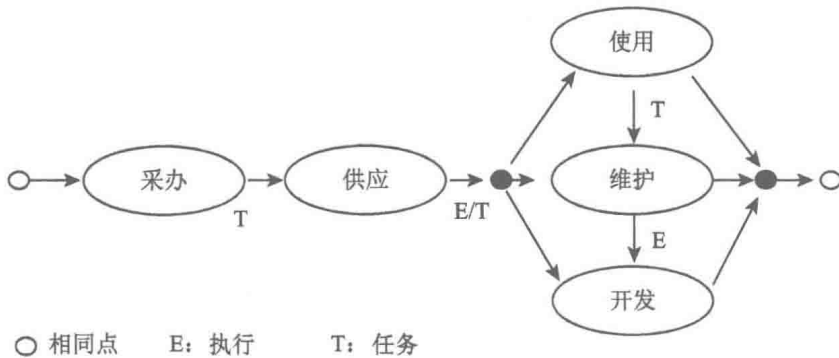


图 1-5 ISO/IEC12207 中的系统生命期

1. 采办过程

采办过程为软件采办方提供指导，它详细说明了为采办一个系统，采办人员和机构所开展的各项活动。它始于对采办软件的需求，然后是提出需求建议、供应方选择、工程采办管理、供应方监督与接口。该过程结束于产品验收及服务。

2. 供应过程

供应过程是为开发产品、维护服务与使用服务的提供方提供指导，它详细说明了供应方的各项活动。它始于一份建议及协议，然后是项目管理，结束于产品的交付与服务。该过程延伸到了训练及帮助采办方。

3. 开发过程

开发过程为软件开发方提供指导。它详细说明了开发方的各项活动，该机构定义和开发软件产品。其始于需求分析，然后是设计、编码、测试及集成，该过程结束于产品完成与安装。

4. 使用过程

使用过程为使用软件提供指导。它详细说明了使用方的各项活动，该机构为用户使用计算机系统服务提供服务。该过程包括对用户的使用保障，并与更改维护过程有关。

5. 维护过程

维护过程为软件维护提供指导，它详细说明了维护方的各项活动，该机构为对软件产品的提供服务。其被用于规划维护，以及由于需要纠错性活动、扩充性或预防性活动的软件更改。该过程还包括软件的移植与退役。

维护过程是 ISO/IEC 12207 的五个基本过程之一（见图 1-5），并指导维护方的活动

与作业。该过程提供维护规划和代码及相关文档的修改，维护过程的活动是维护过程的详细描述，但该过程可以使用或引用其他过程，如ISO/IEC 12207的开发过程。

上述定义中，将软件维护与保障合并在一起作为一个阶段的名称。因为军方通常将产品在使用期间开展的许多工作称之为保障；而在民间，许多工作则称之为技术服务或售后服务，实际也正是我们所说的保障工作。目前许多公司的技术服务工作与软件维护工作是分开的两个部门，因此，ISO/IEC 12207中将软件维护与软件保障（或称之为产品技术服务）并列在一起。本书中将民间的软件技术服务也称之为软件保障工作，以方便内容的叙述，同时，也按照军方的习惯，将软件维护纳入软件保障中，将其作为软件保障的一个组成部分。

软件维护是软件保障的核心。其实，无论从技术难度、资源消耗、影响程度来看，软件维护是软件保障的主体，其他的保障工作，一是确保能获得当前的软件并能被正确、合适地被使用，二是确保新的软件版本能在正确替代旧的软件版本，确保因软件版本不同而造成其他问题。而软件维护保障相对而言却需要耗费更多的资源。因此，在许多部门，并不将软件维护与软件保障加以区别，美军在1997年调研软件保障问题时，专门指出其现在使用的软件维护与软件保障这两个术语是混淆的，并建议以后可不加区别地使用。因为软件维护部门从事的工作往往不限于软件维护（即软件更改），而且包括了大量的其他保障活动。这也从一个侧面反映出软件维护是软件保障的主体。但这里需要指出的是，软件维护实际上并不等于软件保障，而应该仅仅是软件保障的一个子集。

1.2.3.4 软件保障分类

软件应该说是一种无损耗、不变化的特殊产品，同一软件的不同拷贝之间完全不存在个体之间的差异，为什么这样的产品还需要进行保障呢？

我们前面讲软件维护的时候已经阐述了需要开展软件保障的原因之一，即软件是需要维护更改的，软件维护本身就是软件保障的一部分，也就是软件的维护保障。但这就是唯一原因吗？

软件保障的目的是“持续完全地保障产品执行任务”，而导致软件不能执行任务或无法按规格说明进行工作的原因很多。除了上面所述的软件维护保障外，还有如下原因：

一是软件使用过程中需要技术服务。软件在使用过程中，由于其功能复杂、运行环境千差万别，往往会造成用户无法正确使用软件，无法使软件正常发挥其应有的功能，用户在使用过程中，常常需要专门的技术服务部门进行指导、培训，如正确的使用、安装方法指导；使用过程中问题的处理；甚至还包括软件故障出现又必须在缺陷修正前马上使用软件系统，指导用户如何回避这些特殊的软件缺陷等等，以确保软件产品完成规定的任务，也就是说软件在使用过程中的软件使用保障。

二是软件使用维护过程中需要供应服务。软件使用过程中，载体可能损坏，造成软件不能使用，此时就需要供应新的软件，系统中的软件和数据可能需要重新安装；此外，软件维护和硬件维修不一样，硬件维修往往是针对单个系统，通过更换故障单元，可以使故障系统得到恢复，一旦故障的系统恢复正常了，维修过程就结束了，其供应的内容主要是备件、耗材等。而软件一旦被更改，就需要对所有安装该软件的系统进行全面的升级，以确保软件版本的一致。因此，在软件维护完成之后，就需要将更改过的新版软