电子科技大学学报社科版　2002 年(第Ⅳ卷)　第 3 期　技术管理研究
Journal of UESTC (social sciences edition) Sept.2002,vol.4,No.3

软件可靠性学科发展现状及展望**

□陈光宇　黄锡滋　[电子科技大学　成都　610054]

[摘　要]　软件可靠性工程的发展主要是在信息技术、可靠性工程、用户需求等综合因素的作用下形成和发展起来的。本文简要回顾软件可靠性学科的三个阶段的发展,侧重阐述软件可靠性工程的形成及特征,并提出软件可靠性工程发展中需解决的问题。

[关键词]　软件可靠性;　软件可靠性工程;　可靠性工程;　软件工程;　软件危机
[中图分类号]N945.17　[文献标识码]A　[文章编号]1008-8105(2002)03-0099-(04)

计算机软件经过了 50 多年的发展,已经成为现代信息社会中的关键。社会的日常运行对这种系统失效的容许能力却越来越小。软件工程帮助在预定费用内按期交付符合功能性要求的软件产品,还帮助满足一定的质量标准。从用户的角度来说,软件的质量标准中最直观和最直感的就是软件可靠性。

一、软件可靠性学科发展回顾

软件可靠性是软件工程学与可靠性工程学结合产生的前沿学科。它的兴起和发展源于三个方面的因素。首先,需求的拉动力:持续了二三十年的软件危机与上世纪九十年代软件故障引发的许多重大事故大大损害了客户满意度;其次,技术的推动力:信息技术(硬件技术、软件技术)的迅猛发展有力推动软件可靠性发展;最后,可靠性工程的理论和方法对软件可靠性的支撑力。见下图 1。

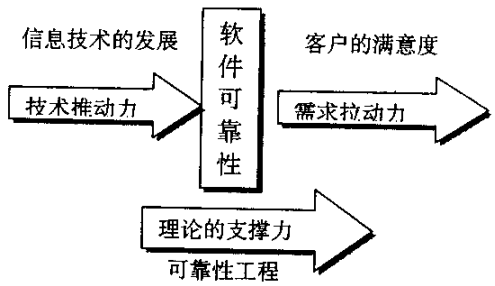

图　1

软件可靠性的发展伴随着信息技术和可靠性工程的发展而成长。软件可靠性发展至今可分为下列三个阶段:

第一阶段:(1950—1967 年),软件可靠性学科萌芽时期

在 1950—1958 年间。在软件发展过程的这个原始阶段中,完全没有软件可靠性的概念。那时没有专职的程序员,程序是由应用计算机的科学家和工程师自行编制的,没有公认的规则可供遵循。1957 年,美国国防部电子设备可靠性顾问团(AGREE)的报告是公认的可靠性工程的奠基性文件,但是,完全没有提及软件和软件可靠性的问题.可靠性(Reliability)的定义是:产品在规定的条件下和规定的时间内完成规定功能的概率。

在 1959—1967 年间。在计算机硬件技术和软件技术飞快发展的同时,软件可靠性问题仍然被人冷落,软件危机由此产生。1965 年国际电工委员会(IEC)可靠性专业委员会的成立,标志着可靠性工程成为了一门国际化的技术。可靠性工程(Reliability Engineering)的定义是:为获得可靠性而进行的一系列设计、研制和生产活动。

第二阶段:(1968—1987 年),软件可靠性学科的形成时期

在 1968—1978 年间。以集成电路为主体的小型机逐渐得到了广泛的应用,在硬件技术迅速发展的推动下,以及在软件危机带来的用户对软件可靠性需求的紧迫性的拉动下,软件可靠性学科和软件工程学科得以建立和发展。软件工程学的理论和技术为可靠软件的设计、测试和管理提供了指南和工具。但是,它没有能力解决在系统开发中,用户要求对软件可靠性的定量评价的问题。于是,许多著名的软件工程专家开始致力于利用和改造硬件可靠性工程学的成果,使之移植到软件领域。由于他们的努力,迎来了软件可靠性学科的开创

* [收稿日期]　2002-05-08
** [作者简介]　陈光宇(1969—)男,四川省雅安市人,电子科技大学管理学院,博士生,讲师;黄锡滋(1934—)男,重庆市人,电子科技大学管理学院,教授.

时期。这个时期的特点是:以软件可靠性为主题的国际学术会议频频召开,吸引了各界人士的关注。软件可靠性的数学模型尤如雨后春笋般地大量涌现。著名的 JELINSKI—MORANDA 模型、SHOOMAN 模型、NELSEN 模型、MILLS—BASIN 模型都是在这个阶段推出的。此外,软件失效数据的积累和分析工作也有了初步发展。

在 1978—1987 年间。由于大规模集成电路的出现,对软件技术的发展产生了深刻的影响。这个时期的特点:各种验证和试用的软件可靠性模型相继推出;软件可靠性管理技术的开发已列入日程;软件可靠性标准化工作开始起步。国际电工委员会(IEC)的 TC56 技术委员会在 1985 年成立了软件可靠性工作组,并制定了软件可靠性和维修性管理规范(草案)。在 80 年代中期,软件安全性问题受到了特别的重视,硬件可靠性和安全性分析中所采用的故障树分析法(FTA)、故障模式效应分析法(FMEA)和潜藏回路分析法(SCA),已在软件安全性分析中使用,并取得了令人鼓舞的成果。

软件可靠性(Software Reliability)的定义:在规定的条件下,在规定的时间内,软件不引起系统失效的概率,该概率是系统输入和系统使用的函数,也是软件中存在的错误的函数。系统输入将确定是否会遇到已存在的错误(如果错误存在的话)。

第三阶段:(1988 年至今)软件可靠性向工程应用过渡的时期

超大规模集成电路的出现,将人类带向信息社会。软件逐渐成为全球经济的中枢。但是,由软件引发的、震惊科技界的故障持续不断,在某些类型的设备中软件故障甚至远远超过了硬件,成为系统的主要故障源。

下面我们仅列举几起人们印象深刻的事件。

·在医疗设备方面,九十年代中期,美国 Therac 25 型放射治疗仪 2# 治疗模式(x 射线模式)发生的 54# 故障,多次产生超计量辐射,造成了两人死亡和多人受伤的重大医疗事故。Therac 25 是 Therac 6 的改进型,使用软件安全互锁装置,旧式的 Therac 6 使用机械安全互锁装置,却从来没有发生过类似故障。

·在航天技术方面,1996 年欧洲航天局首次发射阿丽亚纳 5 号火箭失败,直接损失 5 亿美元,还使耗资已达 80 亿美元的开发计划推迟了近三年,事故的原因是火箭控制系统的软件故障。

·90 年代后半期,‘千年虫’问题震惊世界,各国投入了大量的人力和物力,耗资数千亿美元,虫害才基本上得到控制。‘千年虫’实际上就是一种特殊的软件故障。

软件可靠性的重要性从它的反方向更加清楚地呈现出来,在警钟齐鸣之中,沉痛的教训使客户空前地重视软件的可靠性。客户对软件可靠性的强烈需求有力地拉动了软件可靠性工程的发展。1988 年,软件可靠性工程一词从此登上了学术讲台,并为学术界广泛认同,标志着软件可靠性从纯粹的理论研究向工程应用转化。到目前为止,软件可靠性学科范围已经扩展到软件可靠性、软件维护性、软件安全性和软件保障性。

二、软件可靠性工程的形成及特征

(一)软件可靠性工程的内涵

软件可靠性工程(Software Reliability Engineering)一词的最早出现是在 1988 年,AT&T 贝尔试验室为它的一个内部软件可靠性系列教程,标以软件可靠性工程教程之名,软件可靠性工程一词从此登上了学术讲台。贝尔试验室在解释这个词汇时,明确说明,它不仅包括了软件可靠性模型及软件的可靠性度量,还包括应用模型和度量实现软件项目可靠性管理。1992 年,AT&T 贝尔试验室对软件可靠性工程的内涵作出定义,认为重要软件项目的开发应该制定一个软件可靠性大纲,一个好的软件可靠性大纲应包括以下四个系列 20 个工作项目:可行性和需求(确定功能剖面;失效定义和分类;识别需方的可靠性需求;进行权衡分析;设置可靠性目标);设计和实施(在部件中分配可靠性;适应可靠性目标的工程措施;基于功能剖面的重点资源;对故障的引入和传播的管理;外供软件的可靠性测量);系统测试和现场试验(确定运行剖面;进行可靠性增长测试;跟踪测试进展;项目必须的附加测试;认可可靠性目标);售后和维护(建立必须的售后服务机构;监视现场可靠性是否满足可靠性目标;跟踪需方对可靠性的满意程度;拟定软件的改进和提高进度;产品和开发过程改进指南)。AT&T 贝尔试验室的工作,为软件可靠性工程的实施指出了明确的方向,对软件可靠性工程的建立和发展,功不可没。

J.D.Musa 认为软件可靠性工程是‘一门以减少基于软件的系统在运行中不满足用户要求的可能性为目标的应用科学’,同时说明软件可靠性工程研究的内容包括:

1. 软件可靠性的分析:确定指标、设计开发过程、进行预计、分析失效严重性等。

2. 软件可靠性的测量:用失效数据和软件可靠性模型估计(或测量)软件运行的可靠性。

3. 软件可靠性的管理:利用可靠性测量和其它信息来控制和改进开发过程,并对采购或重用的软件进行管理。

4. 开发过程的改进:确定影响软件可靠性的因素,改进费用效益关系。

(二)软件可靠性工程的定义

1992 年,美国航空与航天学会(AIAA)在其发布的标准“ANSI/AIAA R-01 3—1992 推荐的软件可靠性实践”中定义软件可靠性工程是‘应用统计技术处理在系统开发和运行期间所采集的数据,以便详细说明、预计、估计和评价基于软件的系统可靠性。”这个定义的两个特点:一是应用统计技术来处理有关故障数据;二是把软件可靠性工程的目的仅限于‘详细说明、预计、估计和评价基于软件的系统可靠性’,以此区分软件可靠性工程和软件工程界限。

我们认为软件可靠性工程不仅仅是用数理统计的方法来

电子科技大学学报社科版　2002 年(第Ⅳ卷)　第 3 期　技术管理研究

Journal of UESTC (social sciences edition) Sept.2002,vol.4,No.3

详细说明、预计、估计和评价基于软件的系统可靠性,还应该包括软件可靠性的需求、分析、设计、实施、售后及维护、工程管理活动。因此,我们认为美国航空与航天学会(AIAA)发布的软件可靠性工程的定义是片面的,而软件可靠性工程的正确定义应该是:为获得软件可靠性而进行的一系列开发、维护软件产品的活动。这些活动包容了 AT&T 贝尔试验室提出的软件可靠性大纲的 20 个工作目录和 J.D.Musa 提出的软件可靠性的研究内容。这些活动的相关技术包括:软件可靠性的分析(可靠性的需求分析、指标分配、故障树分析、故障模式及效应分析、特性分析等);软件可靠性的设计和实施(防错设计、容错设计、检错设计、纠错设计、故障恢复设计、软件可靠性增长等);软件可靠性的测量(用失效数据和软件可靠性模型进行软件可靠性的测试、预计、估计及验证);软件可靠性工程管理(利用可靠性测量和其它信息来控制和改进开发过程,并对采购或重用的软件进行管理,确定影响软件可靠性的因素,改进费用效益关系)。我们将这些活动用下图 2 描述出来:

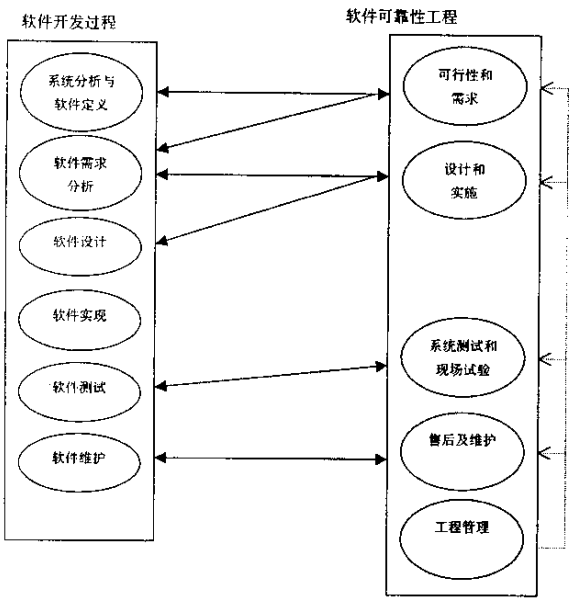

图　2

(三)软件可靠性标准化的进展

一个工程应用学科的发展,必然伴随着标准化的进程,同时,标准化的程度,也是该应用学科发展成熟度的重要因素。

软件可靠性的标准化,早在 80 年代中期就已起步了。从事这项工作的,既有国际标准化组织,也有兼具标准化职能的学术机构。它们的努力在九十年代结出了成果。在学术机构方面,1992 年,美国标准化研究所/美国航空航天学会发布"软件可靠性"标准号:ANSI/AIAA R—013—1992;1995 年,美国电机电子工程师学会发布"IEEE 软件异常分类指南"标准号:1004.1—1995;1998 年,美国汽车工程学会发布"软件可靠性程序标准"标准号:SAE JA 1002 和"软件保障性程序标准"标准号:SAE JA 1004。在国际标准化机构方面,国际标准化组织(ISO)和国际电工委员会(IEC),有明确的分工,IEC 负责有关电子工程、电气工程领域的国际标准化工作,其它领域则由 ISO 负责。所以,ISO 没有直接制定软件可靠性的标准,但是在著名的 ISO-9000"质量管理和质量保证"系列标准中,明确指出可靠性是产品的重要质量属性,在 ISO 9000—3"ISO 9001 在软件开发,供应和维护中的使用指南"局部地涉及了软件可靠性问题。因此,软件可靠性国际标准的制定,是由国际电工委员会(IEC)负责进行,经过长期的努力,现在有三个标准:

1. 标准号:IEC 60300—3-6

名称:可信性管理体制—第三部分:应用指南—第六章:软件的可信性问题(dependability management-Part 3:Application guide-Section 6:Software aspects of dependability)

发布时间:1997 年

2. 标准号:IEC 61704

名称:软件可信性评估的测试方法指南(Guide to test methods for dependability assessment of software):

发布时间:待定

3. 标准号:IEC 61713

名称:软件生存期全过程的可信性应用指南(Software dependability through the software life-cycle processes Application guide.)

发布时间:2000 年

(四)软件可靠性工程的国际会议(ISSRE)

在软件可靠性工程国际会议(ISSRE)方面,1990 年电子领域的学术权威组织 IEEE 计算机学会成立了"软件可靠性分技术委员会",在它成立的第一年就发起召开了第一届软件可靠性工程国际会议,科技界的反映十分积极。此后每年召开一次软件可靠性工程国际会议成为定制,沿袭至今。会议的影响也日益扩大,1998 年,IEEE 可靠性学会正式署名作为会议的联合发起单位之一,使其在软件可靠性领域的学术权威性进一步得到确认。这个软件可靠性工程国际会议,以倡导理论和实际应用相结合为宗旨,对软件企业产生了强大的吸引力。九十年代为软件可靠性发展作出贡献的学术会议,并非仅一家。比较有影响的还有"软件维护性国际会议(ISSM)和软件保证、确认国际会议(ISACC).

(五)软件可靠性方法工具化的进展

软件可靠性理论应用的最大障碍是复杂的数学公式、浩繁计算和难于掌握的分析方法。从 80 年代中期开始,软件可靠性应用工具的开发逐渐受到关注,到 90 年代在以下几个方面取得了稳步的进展。

1.AT&T 软件可靠性测量工具:

是一种应用软件工具,由 AT&T 开发,最初是供内部使用。

2.SMEFS (Statistical Modeling and Estimation of 1iability Function for Software)

由美国海军水面作战中心于 80 年代中期开发,90 年代仍

在继续使用。既适用于 TBF 模型也适用于 FC 模型,模型包括 Schneidewind 模型、Yamada S-Shaped 模型、BrookS&Motely 模型、MuSa/Okumoto 模型和 Littlewood-Verfall 模型。

3.SRMP (Software Reliability Modeling program)

由 Reliability and Statistical Consultants 公司 90 年代初开发,特点:采用似然函数、u 图和 y 图对九种模型进行比较,优选出适用的模型。

4.SoRe 工具

由美国国家科学研究中心 LAAS 试验室开发,它的特点是在选择模型前,先对数据进行趋势分析,借以判定软件是处于可靠性增长阶段、可靠性衰减阶段或无明显趋势阶段,然后再确定适用的模型。这个工具软件是在 Macintosh 操作系统下运行。

5.CASRE (Computer Aided Software Reliability Estimation)

CASRE 是在 SMETFS 的基础上,将各个模型的计算结果进行线性组合处理,从而提高了模型预测的精度。CASRE 可在 Windows3.1, Windows 95,Windows 98 和 Windows NT 下运行。

三、软件可靠性工程发展中需解决的问题

自从 1992 年以来,我国在软件可靠性方面的研究从以前的分散的零星研究转化为团队和规模研究,形成了一定规模的骨干队伍。到目前为止,我们的基础理论研究与国外十分接近,在工程应用方面,却有相当的差距。我们认为有以下若干问题需要继续研究和解决:

(一)结合实际项目,运用标准化的方法,逐步形成完整的实施软件可靠性工程的方法

在软件开发周期中,运用 PDCA 循环持续不断地改进软件可靠性的分析、设计和实现、测量评估、工程管理等的方法。

(二)对软件系统模块失效数据的研究

由有条件的项目开始,研究失效数据的收集处理系统及其机制。可以将硬件的失效数据规范的方法应用到软件的失效数据的研究中,为软件可靠性的快速预计、设计提供理论依据和实际分析手段。

(三)继续开展理论方法的研究

1. 数学模型的有效性和适用范围

2. 软件可靠性测试和验收方法的研究

3. 软件可靠性快速预计技术的研究

4. 软件安全性设计和分析方法的研究 (包括 SFTA, SFMEA, SSCA 和软件的 Petri 网分析方法)

5. 软件复杂性度量和软件可靠性的关系的研究

6. 大规模分布式软件系统的可靠性分析方法

7. 硬软件复合系统的可靠性综合分析方法

在我国的 IT 管理方面,已经注意到软件质量的重要性,也采取了一些管理和技术措施,但是这些措施基本上只限于实施软件工程的层面,远没有达到软件可靠性工程的深度。这种状况的出现,又主要源于对软件可靠性缺乏认识。从历史的角度,在我国高级技术和管理人员中,了解和懂得软件可靠性技术的寥寥无几。因此,我们必须跟踪国外软件可靠性技术的发展、继续开展和支持软件可靠性研究,同时还应加强宣传教育和推广应用的力度,使更多的技术管理高层人士认识软件可靠性,使更多的软件设计和管理人员能够掌握基本的软件可靠性方法。对重点工程的关键部分,应明确提出软件可靠性要求。此外应该对国际标准 IEC61704 和 IEC61713 的发布和实施予以关注,建议尽快地将其转化为我国的标准,并参照其内容,结合我国 IT 管理的需求,制定出国家质量标准。只要措施得力,我们完全有能力跟上国际发展的步伐。

参考文献

[1]黄锡滋.二十世纪九十年代软件可靠性进展回顾[J].装备质量,2000(9).

[2]黄锡滋.软件的可靠性与安全性[M].北京:科学出版社,1993.

[3]黄锡滋.系统可靠性设计理论与方法[M].北京:科学出版社,1983.

[4]王纬.软件可靠性工程发展现状[J].装备质量,2000.

Actuality and Prospect of Development of Software Reliablity Subject

Chen Guangyu　Huang Xizi

(UESTC　Chengdu　610054)

Abstract　Development of Software Reliability Engineering (SRE) mainly depends on three impulses including IT, Reliability Engineering, customer demand. Three stages of development of SRE are introduced, focusing on establishment and characteristic of SRE and putting forward problems that are necessary to solve in the development of SRE.

Key Words　Software Reliability; Software Reliability Engineering; Reliability Engineering; Software Reliability; Software crisis

软件可靠性学科发展现状及展望

作者： 陈光宇， 黄锡滋
作者单位： 电子科技大学,成都,610054
刊名： 电子科技大学学报(社会科学版)
英文刊名： JOURNAL OF UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA (SOCIAL SCIENCES EDITION)
年，卷(期)： 2002,4(3)
被引用次数： 14次

参考文献(4条)

1. 黄锡滋 二十世纪九十年代软件可靠性进展回顾 2000(09)

2. 黄锡滋 软件的可靠性与安全性 1993

3. 黄锡滋 系统可靠性设计理论与方法 1983

4. 王纬 软件可靠性工程发展现状 2000

本文读者也读过(8条)

1. 李峰.方旭升 浅谈软件可靠性工程的应用[期刊论文]-中小企业管理与科技2008(2)

2. 孙志安.Sun Zhi'an 软件可靠性工程进展[期刊论文]-舰船电子工程2008,28(6)

3. 党涛立.潘新祥.赵海涛.DANG Tao-li.PAN Xin-xiang.ZHAO Hai-tao 软件可靠性工程综述[期刊论文]-鱼雷技术2005,13(2)

4. 崔玉宝.曲凤娟.CUI Yu-bao.QU Feng-juan 软件可靠性工程研究[期刊论文]-科技情报开发与经济2006,16(6)

5. 盛志森.SHENG Zhi-sen 可靠性工程简史[期刊论文]-电子产品可靠性与环境试验2008,26(6)

6. 黄昭毅.HUANG Zhao-yi 可靠性工程理论是设备维修重要的科学发展观[期刊论文]-中国设备工程2005(11)

7. 杨玉丽.YANG Yu-li 软件可靠性研究现状与展望[期刊论文]-电脑知识与技术2010,6(1)

8. 李祥臣.彭道勇.齐俊臣.朱三可.张德才 浅论可靠性工程发展的若干方向[期刊论文]-电子产品可靠性与环境试验2009,27(z1)

引证文献(14条)

1. 刘明真 软件黑匣子在软件故障诊断中的应用研究[期刊论文]-莆田学院学报 2013(2)

2. 黎忠文.姚绍文 软件安全核的可信性问题[期刊论文]-计算机科学 2006(1)

3. 张大强 一种基于.Net的软件体系结构的设计与开发方法[学位论文]硕士 2006

4. 程跃华.崔艳 组合模型在软件可靠性预测中的建模与仿真[期刊论文]-计算机仿真 2011(6)

5. 俞华锋 神经网络在软件可靠性预测中的应用研究[期刊论文]-计算机仿真 2011(4)

6. 杨玉丽 软件可靠性研究现状与展望[期刊论文]-电脑知识与技术 2010(1)

7. 李江敏.陆力 商业软件项目可靠性管理初探[期刊论文]-福建电脑 2006(2)

8. 陈吉灵 以软件可靠性增长测试推动软件可靠性工程的实施[期刊论文]-福建电脑 2009(6)

9. 刘明真.许克静 软件可靠性工程对软件业发展影响的研究[期刊论文]-科技和产业 2008(9)

10. 杜波.王智平 软件可靠性分析评估方法及故障分类管理优化设计[期刊论文]-江西科学 2011(5)

11. 刘明真.黄文兰 软件可靠性在软件战略中的地位研究[期刊论文]-计算机安全 2009(8)

12. 郑艳艳.郭伟.徐仁佐 软件可靠性工程学综述[期刊论文]-计算机科学 2009(2)

13. 胡海宏.沈元隆 基于用户要求并考虑软件失效的费用模型[期刊论文]-计算机技术与发展 2011(7)

14. 陈光宇.黄锡滋.唐小我 多阶段系统可靠性的混合式分析[期刊论文]-系统工程理论与实践 2005(2)