DOI:10.16262/j.cnki.1000-8217.2004.04.004

·学科进展与展望·

关于软件可靠性和软件控制论的若干认识

蔡开元*

(北京航空航天大学自动控制系,北京 100083)

[摘 要] 软件可靠性问题对于安全关键软件而言具有极端重要性。本文论述了软件可靠性工程的三个基本问题以及软件可靠性研究现状和面临的主要问题,进而论述了软件控制论产生的背景。软件控制论探讨软件理论和工程与控制理论和工程的交叉应用,其宗旨之一是将控制理论方法较系统地引入软件工程领域,使得软件过程更加有章可循,进一步保证和提高软件可靠性。本文最后概述了软件控制论的几个研究方向。

[关键词] 软件可靠性,软件控制论,软件测试,控制理论

1 软件可靠性问题的重要性

随着计算机技术的广泛应用,软件系统随处可见。手机芯片和移动通信需要嵌入式软件;民航票务需要大型管理软件系统和数据库;航天飞机、国际空间站、神舟飞船依赖于超高可靠的软件系统;核电站安全保护系统也依赖于超高可靠的软件系统。软件可靠性问题的重要性日益突出,甚至成为软件工程发展的瓶颈之一。这可从以下几个方面加以理解。

(1)现代技术系统和人类社会生活愈来愈依赖于软件技术的广泛应用;

(2)软件系统规模不断扩大,软件系统和软件开发过程极为复杂,其行为愈来愈难以预测和控制;

(3)软件失效的后果可能是灾难性的。一个熟知的例子是,1996年6月4日"阿里亚娜"5型火箭发射升空37秒后爆炸,原因是其惯导软件构件有缺陷;对于载人航天系统而言,一旦软件失效,其后果不堪设想;

(4)至今缺乏行之有效的、成熟的、可重复使用的软件可靠性保障和控制技术。

遗憾的是,实际软件系统无一被证明是正确的,重大的软件失效时有发生。对于飞机飞行控制软件、核电站安全保护系统软件等这类安全关键软件(safety critical software)来说,软件可靠性问题是首要问题。这促使人们投入大量的资源、从多个学科和角度对软件可靠性问题进行研究,为软件控制论的产生提供了强有力的现实背景。

2 软件可靠性工程的基本问题

应该说,自从有了计算机和软件,就有了软件可靠性问题,因为不能保证软件开发人员或软件代码编写人员不犯错误。但软件可靠性研究的真正开展则伴随着20世纪60年代末70年代初软件工程的诞生而开始。在过去的40多年中,软件可靠性工程已取得大量研究成果,积累了丰富的实践经验。这些研究成果和实践经验主要反映了软件可靠性工程领域中三个方面的基本问题[1-3]:

2.1 软件为什么失效

主要内容包括:软件与硬件的本质区别,软件失效机理,软件错误、缺陷、故障、失效分类,软件故障诊断。我们知道,硬件系统开始运行时可以正常工作,但经过一段时间后必将失效,主要原因是物理退化。软件则不存在物理退化问题,如果其正确性能够被证明,则软件永远不会失效。软件失效的主要原因是软件开发过程中存在人的错误,这些错误导致软件设计或代码中存在缺陷,而这些缺陷在一定的软件输入或运行条件下被激活,产生软件故障状

* 1998年度国家杰出青年科学基金获得者.
国家自然科学基金重点项目、"863"计划项目、航空科学基金项目资助.
本文于2004年4月6日收到.

态。如果没有及时检测到软件故障状态和有效的容错措施,必将产生不应容忍的输出结果或状态,也即软件失效。

2.2 如何开发可靠的软件

主要内容包括:软件可靠性度量,软件可靠性过程管理、软件可靠性设计(软件在线自检、软件容错、软件故障树分析、软件失效模式与效应分析、软件复杂性控制、软件潜藏路径分析、软件可靠性分配、软件可靠性早期预测),软件可靠性增长测试。这一问题是软件可靠性工程的核心问题。软件可靠性工程的成败在于是否可以开发可靠的软件。为此,软件可靠性设计应当起着举足轻重的作用,尽管软件可靠性设计这一提法还不普及。

2.3 如何检验软件可靠性

主要内容包括:软件可靠性增长建模,软件可靠性评估测试,软件可靠性综合评估。这一问题对安全关键软件具有特别重要的意义。譬如现代飞机采用电传操纵系统,由计算机控制飞机飞行,在飞机放飞之前必须在地面对机载软件进行充分测试;但测试又不能无休止进行,必须通过软件可靠性综合评估决定何时可以停止测试。

3 软件可靠性研究现状及面临的主要问题

应该说,软件可靠性工程基本成型,已在软件工程领域取得相对独立的地位。这可以以下事实或共识加以说明。

(1)软件可靠性问题的重要性已获充分认识。

(2)软件可靠性问题的要害在于软件的复杂性。在于软件复杂性与人的理解力之间的矛盾,在于软件严格性与人的不严格性之间的矛盾。

(3)软件可靠性工程已基本有章可循。目前进行软件可靠性设计(包括软件容错设计),实施软件可靠性定量评估的软件工程规范(软件过程管理与软件测试)。主要从两个方面采取措施来保证软件可靠性[4,5]:

(1)软件过程管理,如采用软件过程成熟度模型(CMM),ISO 9000 系列标准等。这些模型和标准对软件开发过程中的各种应当进行的活动和应当撰写的文档加以较明确的规定,从而在管理层次上保证软件开发过程的有序进行。

(2)软件测试,包括软件静态测试和软件动态测试。静态测试不执行软件代码,而是直接检查软件设计或代码。动态测试则选择一定的输入或运行条件,执行软件代码,并观测相应的软件输出或响应,以判定软件内部是否存在缺陷。

这两方面的措施使得软件开发基本有章可循,大量的软件缺陷在软件投入使用之前被剔除。但"基本有章可循"与确保软件可靠性存在巨大鸿沟,主要表现在:

(1)软件开发过程仍严重依赖于开发人员的知识和经验,而知识和经验因人而异,缺乏客观统一的标准,人的行为可能不可靠;

(2)软件测试只能证明软件有缺陷,不能证明软件无缺陷,甚至不能保证软件不存在某类特定的缺陷;

(3)缺乏客观标准确定软件测试应何时停止;

(4)缺乏客观有效的方法来综合软件测试及各类软件可靠性相关信息,用于评估软件交付使用前所达到的可靠性水平。

于是不难理解,实际软件系统无一被证明是正确的,软件失效时有发生。与此同时,也难于对软件、尤其是安全关键或超高可靠性要求的软件的可靠性作出准确的评估。所以,软件可靠性研究面临的主要问题有:

(1)如何开发安全关键软件,确保其可靠性;

(2)如何综合各种不同来源的软件可靠性相关信息,有效定量评估软件可靠性;

(3)如何有效刻划软件运行环境,定量描述软件运行环境对软件可靠性的影响;

(4)如何刻划新型软件系统的可靠性,包括网络软件系统、基于构件软件系统等。

4 软件控制论的研究背景

为了进一步保证和提高软件可靠性,有必要分析现有软件开发技术的不足,进一步采取措施以控制软件的复杂性和软件故障行为。这就导致软件控制论思想的产生。而软件系统和软件过程中存在大量的反馈机理,又为控制原理和控制理论提供施展技能的空间。

软件控制论的思想是作者在英国工作期间于 1994 年最先提出[6],并于最近几年得以发展[7-10]。软件控制论探讨软件理论及工程与控制理论和工程的交叉应用,其宗旨之一是将控制原理、理论和方法较系统地引入软件工程领域,以软件过程或软件系统为被控对象,严格刻划、定量分析和优化软件过程和软件系统中的各种反馈机理,达到控制软件(可靠性)行为的目的。

以软件动态测试为例,在测试过程中测试人员

需要选择一定的测试用例(软件输入或运行条件),加载到被测软件中,执行被测软件,观测相应输出,之后要么停止测试,要么选择新的测试用例。这显然是一个闭环反馈过程。如果将被测软件当做被控对象,将软件测试策略当做控制器,那么软件测试用例为相应的控制信号,被测软件与测试策略构成一个闭环控制系统。这样软件测试问题便转化为控制问题。当然,为了设计软件测试策略,必须对被测软件进行建模,明确表达测试目标或控制目标。这显然不是一件容易的事,因为软件与飞机、机器人、工业过程等传统的被控对象有本质的不同。

应当说明,进一步保证和提高软件可靠性只是软件控制论产生的背景之一。软件控制论的产生还有其他背景。譬如,软件系统除了满足可靠性要求外,还应满足功能、性能、服务质量(QoS)等其他方面的要求;这些方面的要求也需要充分利用反馈机理对各种软件行为加以有效控制。另一方面,控制理论的进一步发展也要求面对新的被控对象。

5　软件控制论的若干研究方向

有许多研究课题或研究方向可以在软件控制论的框架下加以讨论,这些研究方向是由不同的研究人员相互独立或合作发展起来的。以下举例说明[10]。

(1)软件过程反馈机理。主要研究软件过程中存在哪些典型形式的反馈机理,如何描述这些反馈机理,这些反馈机理又具有哪些性质等。

(2)可控性与互模拟。可控性是控制理论中的一个基本概念,用于描述系统的行为或状态是否可以被控制;而互模拟是并发软件理论和理论计算机科学中一个基本概念,用于描述不同(软件)进程之间的某种等价关系。研究这两个基本概念之间的可能关系,从而揭示控制理论和软件理论之间的内在联系。事实上,已有研究表明,这两个基本概念之间确实存在内在联系。

(3)自适应软件。研究如何将反馈控制机理引入软件系统,使得软件系统具有在线学习和重构能力。这样的软件系统成为自适应控制系统,控制理论为这类软件行为提供理论基础。

(4)软件设计。如果将软件运行环境当做被控对象,将被设计软件当做控制器,那么软件运行环境与被设计软件构成一个闭环控制系统,于是软件设计问题可转化为控制问题。这一方向研究如何将控制理论用于指导软件设计,从一个侧面保证软件设计的正确性。

(5)软件测试过程反馈控制。研究如何将反馈控制理论用于指导软件测试过程的管理,动态调配测试人员和测试资源,甚至调整测试目标,以保证软件测试可以达到一个合理的目标,在规定的时间内完成。

(6)自适应测试。这一方向将软件测试当作自适应控制问题,在线收集软件测试数据,估计软件的有关参数,改善软件测试策略,以便以最少的代价发现和剔除最多的软件缺陷。

以上研究方向是控制原理、理论和方法在软件工程中的应用。实验初步表明,软件控制论的思想、理论、方法和技术是行之有效的。随着软件控制论的发展,可以相信,软件理论也将在控制工程中找到有效应用,从而发展新的研究方向。

6　结束语

软件可靠性问题对于安全关键软件而言具有极端重要性。目前软件工程主要通过软件过程管理和软件测试来保证和提高软件可靠性,软件开发基本有章可循。但"基本有章可循"与确保软件可靠性存在巨大鸿沟。这就为软件控制论的产生提供强有力的现实背景。软件控制论探讨软件理论和工程与控制理论和工程的交叉应用,其宗旨之一是将控制理论方法较系统地引入软件工程领域,使得软件过程更加有章可循,进一步保证和提高软件可靠性。软件控制论是一个新的、很有希望的研究领域,有大量的研究机会,亟待投资发展。

除本文作者所带领的研究小组外,目前美国、欧洲、澳大利亚等国家均有研究人员从事软件控制论的研究。第一届软件控制论国际研讨会(The First International Workshop on Software Cybernetics; http://rachel.utdallas.edu/compsac)即将于2004年9月在香港召开。

参　考　文　献

[1] 蔡开元.软件可靠性工程基础. 北京:清华大学出版社,1995.

[2] Lyu M R. (editor). Handbook of Software Reliability Engineering. McGraw-Hill, 1996.

[3] Cai K Y. Software Defect and Operational Profile Modeling. Kluwer Academic Publishers, 1998.

[4] Curtis B. The Capability Mathurity Model and Software Process Improvement. McGraw-Hill, 1995.

[5] Binder R V. Testing Object-Oriented Systems: Models, Patterns, and Tools. Addison-Wesley, 2000.

[6] Cai K Y. On the Concepts of Total Systems, Total Dependability and Software Cybernetics. (unpublished manuscript), Centre for Software Reliability, City University, London, Draft version, October 1994; revised version, July 1995.
[7] 蔡开元,李永超,景涛等. 软件测试的控制论方法.航空学报, 2002, 23(5): 448—454.
[8] Cai K Y, Chen T Y, Tse T H. Towards Research on Software Cybernetics. Proc 7th IEEE International Symposium on High Assurance Systems Engineering, 2002, 240—241.
[9] Cai K Y. Optimal Software Testing and Adaptive Software Testing in the Context of Software Cybernetics. Information and Software Technology, 2002, 44: 841—855.
[10] Cai K Y, Cangussu J W, DeCarlo R A, Mathur A P. An Overview of Software Cybernetics. Proc STEP 2003, IEEE Computer Society Press, 2004.

SOME CONSIDERATIONS ON SOFTWARE RELIABILITY AND SOFTWARE CYBERNETICS

Cai Kaiyuan
(*Department of Automatic Control Beijing University of Aeronautics and Astronautics, Beijing* 100083)

Abstract The reliability problem is extremely important for safety critical software. This paper addresses the three basic issues of software reliability engineering and reviews the current status of software reliability research, including the major problems that should be tackled in this area. This paper then describes the motivating backgrounds of software cybernetics, which is aimed to explore the interplay between software and control. One of the major themes in software cybernetics is how to apply existing principles and theories of control engineering to software engineering to make software processes more rigorous and repeatable and thus to achieve the reliability benefits. This paper concludes with identifying a few research directions in the newly emerging area of software cybernetics.

Key words software reliability, software cybernetics, software testing, control theory

·资料·信息·

中国科学院、国家自然科学基金委员会在京签署《柏林宣言》

中国科学院院长路甬祥、国家自然科学基金委员会主任陈宜瑜 2004 年 5 月 24 日在北京分别代表各自机构签署《柏林宣言》,以推动全球科学家共享网络科学资源。

《柏林宣言》由德国马普学会发起,德国、法国、意大利等国的科研机构于 2003 年 10 月 22 日在德国柏林联合签署。宣言全称为《关于自然科学与人文科学资源的开放使用的柏林宣言》,旨在利用互联网整合全人类的科学与文化财产,为各国研究者和网络使用者提供一个免费的、更开放的科研环境。宣言呼吁各国科研机构向网络使用者免费开放更多科学资源,"以促进利用互联网进行的科学交流与出版"。

宣言的主要内容是:鼓励科研人员与学者在"开放使用"的原则下公开他们的研究工作;鼓励文化机构通过在互联网上提供他们所拥有的资源来支持"开放使用";用发展的手段和方法来评估"开放使用"对促进科研的贡献。德国马普学会、弗劳恩霍费尔协会,法国国家科研中心,欧洲科学院等科研机构和一些国家的大学、博物馆等已经签署《柏林宣言》。

(宣传处 供稿)