

# 关于提高系统及重大应用软件的 可靠性与安全性的建议<sup>\*</sup>

中国科学院学部

(北京 100864)

**关键词** 系统, 应用软件, 可靠性, 安全性

在现代信息技术的各类载体(计算机硬件、软件、网络与通信设施等)中,软件的可靠性、安全性是最难保证的。我们现在使用的计算机都属于“通用数字计算机”。用通用数字计算机解决一个特定的问题,要靠特定的软件去完成。计算机能解决多少问题,就需要多少软件。现代信息社会对计算机的依赖,主要表现为对软件的依赖。计算机软件已经成为信息基础设施中最薄弱的环节。不可靠、不安全的软件系统对国家安全和社会稳定是不可忽视的隐患。

我国近年来不断发生由软件问题引起的事故。仅 2006 和 2007 两年中见诸主流媒体报道的重大软件事故就达 9 起,涉及机场、银行、医疗等要害部门,严重扰乱了正常的社会秩序。

我国在软件可靠性、安全性领域,既存在管理上的问题,也存在技术上的问题。

我们发现,从未有机构对在社会上造成重大影响的软件事故进行过独立的调查。事实上,没有任何政府部门或机构负责对软件事故进行调查,也没有任何部门、行业组织或专业团体从事软件问题的数据收集和整

理的基础性工作。不仅如此,事故发生的单位、企业,为了保护自身的“形象”,往往采取各种措施严密封锁与事故有关的信息。这样的行业文化使得“前车复辙”不能成为“后车之鉴”,严重妨碍了软件行业可靠安全水准的提高。

目前,我国保证软件可靠安全的主要技术手段是测试。由于软件系统动态行为的高度复杂性,任何可行的测试都只能覆盖所有可能执行路径的极其微小的部分;由于软件行为的非连续性,根据有限的测试结果对软件系统的可靠性和安全性难以做出有说服力的推断。关于测试,软件大师、国际计算机科学基础研究的最高奖 ACM 图灵奖获得者 Dijkstra (狄克斯特拉)的名言至今仍然有效:“测试只能证实错误的存在,而不能证明没有错误”。因此,仅靠测试不可能为通常所要求的软件可靠性和安全性提供充分的证据。

为了提高我国系统及重大应用软件的可靠性与安全性,特提出如下建议。其中,主要政策性建议有两条:

## 1 建立有效的软件事故调查机制

指定专门的机构,其职责为:

(1)组织由主管部门以及各界专家组成的调查组,对重大软件事故进行调查,分析事故的原因,提出改正的建议,并及时将调

<sup>\*</sup> 本文为咨询报告摘要。咨询研究组成员:中国科学院院士林惠民、何积丰、张钹,教授蔡开元、应明生、王戟,研究员张健、叶东升  
收稿日期:2008 年 4 月 15 日

查结果向主管部门、相关企业和研究机构通报。

(2)建立软件事故案例档案,对涉及软件问题的数据进行系统的收集、整理和统计,供相关部门、企业和研究机构分析、研究,为逐步形成软件可靠性和安全性的评价体系提供基础数据。

## 2 加强并提升软件评测中心的作用

在加强软件评测中心业务素质培训的同时,将其功能从单纯“在软件中找错”提升到“帮助把错误尽可能消灭在萌芽状态”。评测中心可以利用所积累的经验 and 案例,发现高安全、高可靠软件开发过程中存在的主要问题和薄弱环节,通过提出解决方案以及制定相应的设计和编程准则等方式,帮助软件厂商降低软件产品的错误率。

其他政策性建议:逐步建立软件可靠安

全性评价体系;加强高可靠安全软件基础研究。

主要技术性建议:

软件生存周期的各个阶段,包括需求分析、规约、设计、编程、测试、维护,都应当为所能达到的可靠安全性提供证据。这些证据应形成相互衔接的、完整的链条,作为文档的独立部分加以保存,以便分析和检查。测试是提供这种证据的重要手段之一,但要清醒地认识到测试的局限性。对于可靠性安全性至关重要的软件系统,应考虑使用更为安全的编程语言、严格的过程管理以及形式化的设计与开发方法。

其他技术性建议:将与可靠安全性密切相关的代码集中到尽可能少的模块;从系统工程的角度考虑软件可靠安全问题。



中国科学院

(接 368 页)

性能。目前在束流能量为 2.5 GeV 时,流强已超过 250 mA、束流寿命 10 小时,同步辐射硬 X 光强度提高了一个数量级以上,实验性能和效率明显提高,并进一步扩展兼用光运行。BEPCII 建造期间仍继续为同步辐射用户提供专用光实验,得到用户的一致好评。目前 BEPCII 已开展了 3 轮同步辐射专用光实验,合计 4 个月。BEPCII 建造过程中,还进行了核物理实验和慢正电子实验等科学研究。

2007 年底,BEPCII 的注入器——直线加速器改造通过了中科院组织的工艺测试,所有指标均达到或超过设计指标,性能达到国际先进水平;2008 年 3 月,BEPCII 的同步辐射专用光模式也通过了中科院组织的工艺测试,能量为 2.5 GeV,流强大于 250 mA,

所有指标均达到设计要求。大型高能物理探测器 BESIII 已安装到位,经过联合调试,各子探测器工作正常,已观测到了宇宙线事例,并已开始与加速器联合调试。

目前,科学家们正发扬连续作战的精神,争取 2008 年底达到 BEPCII 的验收指标,按时完成任务。

BEPCII 建成之后,其亮度是美国康奈尔大学对撞机设计亮度的 3—7 倍,预期每年能获取 80 亿  $J/\psi$  事例,或 20 亿  $\psi(2S)$  事例,为粲物理实验研究提供高统计量的数据和小的系统误差的精确测量,并探索新的物理现象。预计投入运行后 3—5 年内,将获得若干对世界高能物理研究产生重大影响的创新性物理成果。

(相关图片请见封三、封四)