

外，有条件的还应配接足够大的散热器，并注意将模块安装在通风良好的部位，必要时还可以采用强制风冷却（增配专用的仪表风扇）方式，控制模块基板温度保持在正常范围以下。

参考文献:

[1] 张聚. 电源模块技术 [M]. 北京: 机械工业出版社, 1989.
[2] 费珈. 直流电源隔离技术与应用 [M]. 北京: 国防工业出版社, 1991.
[3] 武晶明. 电源防护技术与可靠性应用 [M]. 北京: 电子工业出版社, 1992.

作者简介: 张继辉, 1956 年 11 月出生, 大学本科学历, 解放军第二炮兵装备研究第四研究所, 高级工程师, 中国电子学会高级会员; 通信地址: 北京市海淀区清河大楼子 9 号 (邮政编码: 100085), 联系电话: 13601122002; E-mail: bjepkq@163.com

军用软件可靠性问题研究

杨艳妮 彭道勇 张仕念 殷维刚 张国彬

清河大楼子八 100085

摘 要 本文在阐述了软件可靠性定义的基础上, 分别论述了军用软件的可靠性参数和影响可靠性的主要因素, 最后论述了软件可靠性技术中不同的软件容错技术。
关键词 军用软件 可靠性 可靠性参数 容错技术
中图分类号 TN406

The Research on Reliability of the Military Software

Abstract: Based on the definition of the software reliability, this paper introduces the parameters which denote the military software reliability and the main factors that influences the military software reliability, the different tolerant fault methods of software reliability are present in the last.
Keywords: Military Software Reliability Reliability Parameter Tolerant Fault Technology

1 前言

随着计算机技术的飞速发展, 计算机技术在装备中发挥着越来越重要的作用, 随着信息技术在军事领域的广泛应用, 武器装备系统和自动化指挥系统对软件的依赖性越来越强, 军用软件的可靠性已成为确保军事和武器系统质量的关键。软件在军事系统中的比重越来越大, 发挥的作用也越来越大, 近年来的研究表明一个系统发生故障更多的是由于软件的缺陷而造成的。现在软件的复杂性和重复使用的特性不断增长的趋势, 已使软件可靠性成为制约军事系统可靠性的瓶颈。

2 软件可靠性问题的提出及定义

目前,得到广泛认可的软件可靠性定义是 1983 年美国 IEEE 计算机学会对“软件可靠性”一词做出的定义:

- (1) 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;
- (2) 规定的时间周期内,在所述条件下程序执行所要求的功能的能力;

在对于软件可靠性的表述上,最常见的特征量有可靠度、失效率、失效强度、平均失效前时间月均失效间隔时间等。而结合武器装备特点的软件可靠性参数则有:

(1) 可靠度:软件在规定的条件下,规定的时间段内完成预定功能的概率,或者说是软件在规定时间内无失效发生的概率;

(2) 失效率:指在 t 时刻尚未发生失效的条件下,在 t 时刻后单位时间内发生失效的概率。失效率是指不期望行为的发生频率,适用于操作系统、事务处理系统等;

(3) 平均失效前时间 MTTF 和平均失效间隔时间 MTBF。用 MTTF 更为适合。对于稳定使用、具有失效自恢复能力的软件系统,可选用 MTBF 参数;

(4) 成功率:软件的成功率是指在规定的条件下软件完成规定功能的概率。某些一次性使用的系统或设备,如弹射救生系统、防空导弹等系统中的软件,其可靠性参数即可选用成功率。

3 影响军用软件可靠性的主要因素

软件在本质上是一种信息处理器,无论是诸如坦克火控系统的装备控制软件,还是例如指挥自动化系统软件,软件都是接收外界的信息输入,根据一定的规则向外界输出一定的信息。在设计软件的过程中,如果设计人员对用户的需求失察或者误解,忽视了某些军事应用外部环境的规律,在构造技术的使用上出现了偏差,对软件的设计考虑得不够全面,都有可能在软件产品中引入错误。错误引入到军用软件的方式可归纳为三种:程序代码方式,开发过程方式和用户使用方式。

从软件生存周期的各个阶段来分析,软件差错是在软件生存周期的系统分析和设计工作阶段潜藏的人为错误,包括:

(1) 需求分析错误:由于对用户需求的理解有偏差,或用户的需求频繁改动以至于无法有效控制,就会引入这种错误。

(2) 设计错误:这可以分为两个方面,一个是,如果在需求分析错误结果的基础上,对软件系统的体系结构和算法进行描述,那么,即使是高质量的设计也是错误的。另一方面,需求分析是正确的,但设计的方法是错误的,如结构化程度不好,模型有错误等,都会导致软件的错误。

(3) 编码错误:这与系统开发所选用的程式工具 and 编程技术人员的能力经验密切相关。

(4) 测试错误:这个阶段主要包括测试计划不够完善、测试数据不能反映软件使用的真实环境、测试用例过于局限甚至错误,以及测试人员对测试结果的错误分析等错误因素。

(5) 运行和维护过程中的错误:使用手册正确而操作人员误操作、或者操作手册本身就是错误的,这都会在使用时引入错误。

据统计,在软件生存周期的需求分析和软件设计阶段发生错误或故障的比重各占 55% 和 17%,明显高于软件生存周期的其他各个阶段,是影响软件可靠性的关键阶段,所以要尽量把错误消除在开发前期。

4 软件可靠性技术

软件可靠性设计的实质是在常规的软件设计中,应用各种必须的方法和技术,使程序的设计在兼顾用户各种需求的同时,全面满足软件的可靠性要求。软件的可靠性设计和软件的常规设计紧密地结合。目前

软件可靠性设计主要分为以下三类。

(1) 避错技术：利用设计方法学来使得软件尽可能的无错；

(2) 排错技术：主要在软件开发阶段对软件缺陷进行排除包括测试和调试技术；

(3) 容错技术：因为软件的一些缺陷是不可避免的也不容易被检测到容错技术就是使软件在软件缺陷存在的条件下也能正常运行。

大多数的软件缺陷都可以在软件测试阶段和调试阶段被排除。不管怎样开发、测试、调试，软件仍然会含有一些残留的缺陷。也就是说一个软件不可能是无缺陷的，避错技术和排错技术不可能使软件完全无错。因此，软件容错技术成为提高软件可靠性的一种很重要的方法。容错并不是容许错误，而是在错误发生时，软件系统仍然具有正常运行能力的一种设计方法。软件容错的基本思想来源于硬件可靠性的冗余技术容错软件含有众多的冗余单元，增大程序的规模，增加资源的消耗，因此在普通民用领域中不适宜采用容错技术，由于容错技术对软件可靠性的提高有显著的作用，因此在军事系统（例如导弹发射系统、飞机控制系统）适宜采用软件容错技术提高软件的可靠性。

软件的容错技术可以分为三类：

(1) 数据多样性技术：该方法由 Amman 和 Knight 提出。这种技术基于这样的观察：一个软件对某一特定的输入值会发生失效，如果输入数据有一个微小的扰动，那么该失效可能可以避免。数据多样性技术可以很好地处理 Bohrbugs 缺陷，在某种程度上也可以用来处理 Heisenbugs 缺陷；

(2) 设计多样性技术：设计多样性技术主要用来包容由于错误的说明和不正确的编程引起的设计缺陷，它的主要思想是由不同的小组来开发出不同版本的软件来完成一样的功能，这些不同版本的软件以时间或空间冗余的方式来达到容错，主要有 N 版本程序设计、恢复块、N 自检程序设计等方法。设计多样性技术主要来处理 Bohrbugs 缺陷，同时也可以用来处理 Heisenbugs 缺陷，设计多样性技术的缺点是它的高成本；

(3) 环境多样性技术：环境多样性技术是软件容错技术中最新的方法，近年来才认识到它的重要性，基于大多数的软件失效本质上是暂态的，环境多样性技术要求软件在不同的环境下重新执行，可以有效的处理 Heisenbugs 缺陷。一种最有效的屏蔽软件缺陷的方法是重启动系统，环境多样性技术是软件容错技术中一个成本低但非常有效的技术。环境多样性技术的例子有重试操作、重新启动应用程序、重新启动系统。

5 结束语

软件可靠性工程就是保证软件质量问题的有效，本文在软件可靠性定义的基础上，分析了表征军用软件可靠性的参数和影响可靠性的因素，概述了软件可靠性技术的三类方法。

参考文献：

- [1] 刘云, 赵玮. 软件可靠性研究与进展 [J]. 微机发展, 2002, (11): 12
- [2] 黄锡滋. 软件可靠性、安全性与质量保证 [M]. 北京: 电子工业出版社, 2002.
- [3] 蒋乐天, 徐国治. 软件缺陷及软件可靠性技术 [J]. 计算机仿真, 2004, (2): 1443
- [4] 周仲夏, 蒋里强, 宋劲松. 军用软件可靠性工程浅探 [J]. 兵工自动化, 2008, (10): 27
- [5] 唐爱龙, 蒋华, 黄秋勇. 软件可靠性技术的研究 [J]. 柳州师专雪豹, 2006, (6): 21
- [6] 史会增, 缪旭东. 浅析军用软件可靠性 [J]. 舰船电子工程, 2005, (3): 147