提高武器装备软件可靠性*

徐利明,杨海波,张 笑

(海军潜艇学院,山东 青岛 266071)

摘要:软件是高技术武器装备的大脑,其可靠性已经成为整个武器系统可靠性的瓶颈.针对当前装备软件的开发中存在着设计过程不规范、管理不到位、测试不完整等诸多问题,提出从软件开发过程中的可靠性设计、工程化管理、可靠性测试三个方面提高其可靠性,并把软件作为一种产品加以管理,切实确保其高质量.

关键词:装备软件;可靠性;设计;工程化管理;测试

中图分类号:TP311.5 **文献标识码**:A **文章编号**:1006 - 0707(2009)05 - 0137 - 03

随着计算机技术和信息技术快速发展,越来越多的武器装备采用计算机作为其信息处理的核心,软件成为武器系统的大脑,由于软件故障导致的装备故障率越来越高,软件质量越来越受到军方和工业部门的重视.软件可靠性是当前武器装备重要的战术技术指标之一,加强装备软件的可靠性设计、工程化管理并对其进行严格测试是提高软件可靠性的必由之路.

软件工程涉及软件开发方法、工程规范、软件工具、工程管理等,是保障软件可靠性的基础.软件可靠性工程则是研究提高和保证软件可靠性的设计、预测评估、测试、分析和管理的方法[1-4].有了软件,就有了软件可靠性工程,任何装备软件的设计和程序编码都需要排除错误、缺陷和异常,以确保装备工作的可靠性.

1 装备软件开发过程中存在的主要问题

1) 软件未作为产品列入型号计划和技术配套表.

很多装备生产部门常常将软件作为硬件产品的一个附件来对待,由此引起一系列问题:一是研制合同未把软件作为型号的配套产品单独签订合同,费用与进度往往纳入系统或设备的统一安排,没有考虑软件的特殊性.二是对嵌入式软件更存在一个认识上的误区,认为软件最终是嵌入到目标计算机中的,将嵌入式软件的开发过程与硬件研制混为一谈.三是软件没有单独的可靠性指标,可靠性设计不够完整.

2) 软件设计过程中文档编写不规范.

很多软件开发机构不重视软件设计文档,甚至是在软件实现(编程)完成后才补写,失去了以设计指导实现的作用,而且软件文档的编写也不符合国军标的要求.

3) 软件配置管理不严格、不到位.

有的软件开发机构没有配置管理员,对配置管理概念不清,对软件开发库、受控库和产品库的设置与管理比较混乱,使装备软件基本不受控.

4) 对软件测试不够重视.

足够的测试是软件质量的重要保证,由于开发机构对软件测试认识上的误区、专职测试人员的缺乏及测试环境、工具和手段不够完备,再加上由于种种原因无法进行第三方测试,致使软件测试不能覆盖所有测试需求,难以确保软件质量.

5) 软件开发过程投入不足.

对软件开发人员、设备、资源、工具等投入不足,导致软件开发人员相对缺乏,不能将软件设计、实现、测试三者分开,存在"自编、自导、自演"的情况.

2 提高装备软件可靠性的方法

2.1 加强可靠性设计

加强软件的可靠性设计可以有效避免软件出错机率,可靠性设计需要在设计阶段考虑软件开发环境、设计思想、异常处理与容错技术等.

2.1.1 选用成熟、高效的开发环境

成熟、高效的编程语言是提高软件设计可靠性的第一步,装备软件可以用当前流行的多种编程语言进行开发,但在选择开发环境时,要从标准化、软件的主要功能和用

* **收稿日期**:2009 - 02 - 20

作者简介:徐利明(1975—),男,山西五台人,硕士研究生,讲师,主要从事软件工程和系统仿真研究.

途、软件运行环境等方面综合考虑,一般采用语法严谨、逻辑性强、效率高的高级语言,如 C ++ .

2.1.2 模块化设计

软件在设计时要坚持标准化、通用化、模块化的基本原则,对软件的功能结构进行合理划分. 软件功能的实现尽量采用顺序控制结构、条件控制结构、循环控制结构、分情况控制结构和并行控制结构五种基本结构,尽量避免复杂结构、复杂逻辑和复杂函数的使用,以最简单易行的方式实现软件功能. 应控制每个程序模块的规模,通常可执行语句要控制在 60 行左右,最好不要超过 200 行.

2.1.3 对异常输入的正确反应

载有装备软件的计算机系统工作环境比较复杂,电源故障、电磁感应、静电干扰、系统外部故障等都可能会给计算机系统输入异常信息. 在软件设计是要防止将异常信息当成正常信息进行处理造成系统失控,在对输入输出信息进行加工处理前,应对信息是否正常进行检验,确保计算机做出正确反应. 误操作也是一种常见的不正确输入,软件要对操作员输入的正确性进行判别,对不正确的输入或操作给出音频或视频报警信号. 在重要的系统中还应设置看门狗,对系统的运行状态进行实时监控,当系统出现潜在的不安全状态时,强制将系统转移到规定的安全状态.

2.1.4 采用容错技术

容错技术是提高计算机系统可靠性的有力手段,一般分为两类:

一类是避免故障的防错技术,在软件开发过程中,尽可能避免软件中的缺陷,主要采取的技术有:

1) 软件正确性验证. 使用形式符号及数学归纳潜能等证明算法的正确性.

2) 软件风险分析与故障树分析. 从设计或编码的结构出发,追踪软件开发过程中潜入系统缺陷的原因.

3) 分布接口要求规格说明. 在设计的各阶段使用形式的接口需求规格说明,以验证需求的分布接口实现可能性与完备性.

另一类是采用冗余思想的容错技术,基本思想是使软件潜在的差错对可靠性的影响减小到最低程度,主要技术有:

1) 恢复技术. 当软件运行中检测到系统有错误时,把系统状态恢复到一个一致的状态,然后重新继续系统的运行. 这种恢复技术对一些可预见的错误有较好的效果,但对于设计上的缺陷无能为力.

2) N 文本程序设计. 通过独立设计 N 个功能相同,但内部差异的文本程序和一个表决程序,文本功能为软件功能,N 个文本程序分别在 N 台计算机上同步运行或在一台计算机上依次运行,N 个程序运行结果送到一个表决程序中,按少数服从多数的原则,把 N 文本中多数输出作为正确的输出.

2.2 开发过程工程化管理

软件产品的质量主要由软件开发过程决定,为确保软件质量,在抓好软件工程化开发的同时必须抓好软件的工程化管理,即软件的质量是设计出来的,也是管理出来的[2].

2.2.1 管理的原则

保证软件可靠性是一项十分复杂的质量管理过程,国内软件行业特别是军内已经形成了一套比较完备的软件质量管理体系,在工作中须遵循以下原则:

1) 系统考虑软件的生存周期,制定合适的开发计划,确定后认真实施且不轻易修改.

2) 加强对开发过程与产品的控制,控制阶段明确转移准则,建立产品受控库,进行严格验证与评审.

3) 重视人的因素,配备适当人员,明确权责,制定奖优罚劣政策.

4) 规范开发过程,切忌随意化,不断改进开发过程.

2.2.2 主要管理措施

目前国内软件质量管理采取的主要措施为:审查、会签认可软件开发机构编制的软件质量保证计划等文件;督促开发机构按时生成文档并符合有关标准;督促进行并参加软件开发各阶段的审查或审核,严格控制阶段转移;及时掌握软件开发进度及相关情况,参加软件测试和试运行;严格控制软件技术状态更改,严格进行软件验收[5-8].

1) 制定质量体系程序文件.

2) 编写必要的软件开发文档. 在软件开发过程中要编制软件可靠性保证大纲、软件配置管理计划、软件需求说明、软件概要设计说明、软件详细设计说明、程序流程图、使用维护说明书等文档.

3) 进行软件评审. 一般要进行软件要求分析评审、概要设计评审、详细设计评审.

4) 实行软件配置管理. 软件产品的归档按三级库进行管理:软件开发库,主要设在课题组;软件受控库,设在研究室或总体组,必须有软件归档表和软件登记表;软件产品库,设在档案资料室. 进入产品库的软件,若需修改必须填写设计更改建议书和软件更改报告,经回归测试、审批后才能进行更改.

5) 制定质量文件. 包括《软件受控库管理程序》、《军用计算机及软件采购控制办法》、《计算机软件版本升级控制程序》等程序文件.

6) 严格测试. 严格的测试才是合格软件产品的有力保证.

2.3 加强可靠性测试[9-12]

软件测试技术是目前消灭软件错误的重要措施,其目的是在软件开发各阶段查找出软件残留缺陷并修正它,从而改进软件的可靠性,测试只能说明有错,而不能证明无错,在可能的情况下,尽可能做到比较完备的测试[1]. 测试方法分静态测试和动态测试,静态测试是不执行程序而是检查源程序的结构、文法和过程间的接口是否有错误. 动态测试则是使程序在某种控制环境中运行,在完成所需要的功能的同时,检查是否存在不必要的功能的测试方法,

对要求、数据、结果和内部程序工作状态四部分的对应关系进行准确选择和测定.

1) 人工测试.装备软件在计算机测试前,人工查找错误并及时纠正,可有效降低测试成本,常通过审查会和人工运行两种方式进行,其中软件设计审查用于确认所提出的软件设计方案是否能够满足所规定的功能、设计和工作要求;代码审查能则是设计者与专家一起查错;人工运行是由设计者充当"计算机",针对测试用例沿程序逻辑把测试数据走一遍,实践证明人工测试可有效发现多达 70 %～80 %的错误[13].

2) 测试策略制定.好的测试策略往往能发现软件中的设计缺陷,经典方法是采用黑盒测试法与白盒测试相结合的方法进行,可以为测试人员提供考虑问题的方向,形成新的测试方案.

3) 测试用例的设计.测试过程中有效设计出测试用例十分重要,"黑盒"和"白盒"测试实现起来比较困难,测试用例正是结合两者优点使软件得到合理有效的测试.主要采用等价划分、边值分析、因果图、猜测错误、语句覆盖、判定覆盖、条件覆盖、判定条件覆盖、多重条件覆盖等方法进行测试.

4) 模块测试与高级测试.对于大型系统软件的测试分为两个步骤,即进行模块测试和高级测试.模块测试是对于构成软件的各个模块要对其进行独立测试,对模块间相互作用及接口关系则只能通过综合测试.高级测试则是在其它所有测试工作完毕后进行的最终测试,主要有功能测试、系统测试、验收测试等,高级测试是软件最终成为一个合格产品必经项目.

3 结束语

软件是高技术武器装备的大脑,其可靠性已经成为整个武器系统可靠性的瓶颈,装备软件的可靠性工作涉及范围广,牵扯精力大,提高装备软件可靠性需要开发机构不仅要进行可靠性设计、工程化设计,还要实行工作化管理,装备软件在进入受控库和产品库时还要进行严格测试.只有把装备软件作为一种产品进行设计、加以管理、严格测试,才能确软件质量,才能最终保证装备工作可靠性.

参考文献:

[1] 王少萍.工程可靠性[M].北京:北京航空航天大学出版社,2000.
[2] 熊鹏俊.加强软件工程化管理 提高软件可靠性[J].海军装备,2008,31(8):27 - 29.
[3] 杨为民.可靠性 维修性 保障性总论[M].北京:国防工业出版社,2001.
[4] 刘刚.军用嵌入式软件可靠性及其保证[J].兵工自动化,2008,27(1):1 - 3.
[5] 周新蕾.软件安全性分析技术及应用[J].质量与可靠性,2005,117(3):37 - 40.
[6] 周新蕾.软件测试设计方法与策略[J].质量与可靠性,2008,135(3):47 - 53.
[7] 易红.如何提高军用嵌入式软件的可靠性[J].舰船电子工程,2007,159(3):209 - 212.
[8] 俞敏雯.系统可靠性评估技术发展综述[J].质量与可靠性,2005,116(2):32 - 35.
[9] 张丽珂.软件可靠性预测方法[J].一重技术,2008,121(1):104 - 105.
[10] 贾海滨,刘玉存.武器装备系统可靠性浅析[J].机械管理开发,2006,88(1):51 - 54.
[11] 夏德安,罗金亮.提高武器装备系统可靠性的容错法[J].武器装备自动化,2007,26(9):18 - 19.
[12] 尚珊珊.软件可靠性综述[J].软件导刊,2006(8):3 - 5.
[13] 何国伟.论软件项目管理的质量[J].质量与可靠性,2004,110(2):38 - 41.