军用软件的可靠性管理要求

七〇五 研究所　尹宇光

摘　要：讨论了为提高软件的可靠性而应采用的设计程序、管理措施，并提出了建议采用的设计技术。

关键词：军用软件；可靠性

1.引　言

系统一般可划分为硬件和软件。在硬件领域中，人们在过去几十年里已相当令人满意地建立了一套定量规定、预计和测定系统可靠性的实用程序，并得到了公认；但在软件领域，软件可靠性目前在国际范围内尚处于探索阶段，基本现状是：

1)对基本定义还有分歧；

2)还没有定量规定的方法可供使用；

3)已提出相当多的可靠性模型，但每一种模型都有很大的局限性，很难在实际工程中应用；

4)还没有可用的验证程序。

另外我们国家在这方面距离国际水平也有相当差距。因此，笔者认为，对于软件可靠性的工程应用、度量、预计还为时尚早，应着重于逐步建立起一套较完善的管理体系，使软件能够系统地有条不紊地从抽象逻辑概念发展到具体的物理实现。本文就是讨论这一问题。

2.软件项目的级别

软件项目按其重要性、复杂性等因素的不同可分为3个级别，见表1：

表1

级别	重要性	复杂性	程序规模	使用频度
Ⅰ	普通应用	一般	3000条以下	少数几次
Ⅱ	关键项目	比较复杂	3000～30000条	多次
Ⅲ	产生重大影响	非常复杂	20000条以上	经常

软件项目的级别应由主管总师根据表1所列衡量因素综合考虑确定。

3.软件可靠性设计程序

在软件设计过程中，应严格按照下列程序，以保证软件的可靠性。

1)制订计划

项目开发组应首先根据任务书制订计划，制订的计划包括软件开发阶段的划分，各阶段应完成的文档、各阶段的进度、所需要的硬件和软件资源、所需经费的预算和来源以及开发组织内部的分工及其职责。

制定计划时，应按下表并结合实际情况划分开发阶段：

表2

Ⅲ级软件	Ⅱ级软件	Ⅰ级软件
制订计划	制定计划	制订计划
需求分析	需求分析	
概要设计	软件设计	
详细设计		
编码和单元测试	编码和单元测试	编码和单元测试
综合测试	综合测试	项目开发总结
项目开发总结	项目开发总结	

本阶段结束时应提供项目开发计划作为文档。

2)需求分析

项目组应根据委托单位对项目的要求，参照任务书严格进行项目的需求分析，得出系统的逻辑模型。

需求分析结束后，应产生软件需求说明书。软件需求说明书是整个软件开发工作的基础，也是软件设计、测试、验收和评审的依据，它应该用承办单位和委托单位双方都可理解的语言，清晰、明确地描述所开发软件的功能、性能和硬件、软件环境要求。

软件需求说明必须征得委托单位的认可，对Ⅱ级软件应进行软件需求评审。

3) 概要设计

根据软件需求说明进行软件概要设计(即总体设计)，即确定程序由哪些模块组成以及模块间的关系，它包括程序的基本流程、组织结构、输入输出、接口设计和数据结构设计等。

此阶段结束时，应编写出概要设计说明作为软件详细设计的依据。

4)详细设计

这个阶段的任务还不是编写代码，在这个阶段应对概要设计进行细化，即对模块进行过程描述，程序员可以根据它们写出实际的程序代码。

详细设计结束后应产生详细设计说明书。

对于Ⅱ级软件，概要设计说明和详细设计说明可合并为一个文档，即软件设计说明。对于Ⅰ级软件，可将软件需求说明、软件设计说明合并在项目开发计划中。

5)编码和单元测试

这个阶段的关键任务是写出正确的、容易理解、容易维护的程序模块。

必须对编写的模块进行测试。测试时应确保每条可执行的语句至少执行一次，并满足功能需求。

此阶段结束时应提供出源程序的清单。

6)综合测试

综合测试的目的是确保所开发的软件能够完全满足技术、性能、操作、验收等方面的需求。与软件有关的系统其它组成部分(包括硬件)也参加综合测试，与此相关的每个设计单位必须提供必要的技术支持。

进行综合测试前应编制测试计划。它至少应包括目的、内容、进度、条件、步骤、分析和评价准则等内容。

综合测试结束后，应编写测试分析报告，它至少应包含测试结果、软件功能结论、分析摘要等内容。

对于Ⅱ级软件，可将测试计划和测试报告合并成一个文档，即测试计划与报告。

7)项目开发总结

项目开发总结报告应在综合测试结束后、项目验收前完成。在项目开发总结中说明实际的开发结果(软件及其文档、软件的主要功能和性能、基本流程、预计进度和费用与实际进度和费用的对比)，并对生产效率、技术水平和软件质量等开发工作各个方面进行评价。

对于Ⅰ级软件，可将测试计划与报告、项目开发总结合并为一个文档，即项目技术报告。

4.文档规范

在开发的每个阶段，应以相应文档的完成作为工作的成果和结束的标志。这些文档对提高软件的可靠性有极重要的意义：向管理人员报告软件开发过程的进展情况；记录开发过程中的技术信息，作为以后各开发阶段的依据；提供软件有关运行、维护的信息，以提高维护效率。

1)文档最低要求

对不同级别软件项目规定的文档编制的最低要求见表3：

表3

软件开发阶段	Ⅲ级软件的文档	Ⅱ级软件的文档	Ⅰ级软件的文档
制订计划	项目开发计划	项目开发计划	项目开发计划
需求分析	软件需求说明	软件需求说明	
概要设计	概要设计说明	软件设计说明	
详细设计	详细设计说明		
编码和单元测试	源程序清单	源程序清单	源程序清单
综合测试	测试计划 测试报告	测试计划与报告	项目技术报告
项目开发总结	项目开发总结	项目开发总结	

2)文档签审

软件文档的签审应按编写、校对、审核、标准化审查、批准的顺序进行。文档审核一般由项目负责人承担。对于Ⅰ级软件，应由研制单位负责人批准；对于Ⅱ级软件，应由主管软件的总师批准；对于Ⅲ级软件应由主管整个系统的总师批准。

3)文档保存

软件开发过程中产生的文档(见表3)，都应在所档案部门存档，以查询、借阅、交流，其中源程序清单为打印件。另外，开发单位也应保存这些文档，以供该单位科研工作之用。

5.评　审

对软件开发过程中所必须进行的评审的最低要求见表4：

表4

软件评审	Ⅲ级软件	Ⅱ级软件	Ⅰ级软件
项目需求评审	√	√	
概要设计评审	√		
详细设计评审	√		
验收评审	√	√	√

1)项目需求评审

该评审主要以软件需求说明书为依据，评审的主要内容是：

a)　经分析确定软件需求是否完全满足任务书的要求；

b)　逐项评审全部需求条款的可行性；

c)　外部接口的连接约束是否合理。

应重视进行项目需求评审。据统计，在软件开发后期引入一个变动，比早期引入相同的变动所需付出的代价高2～3个数量级。因此在评审中应认真对此阶段以前的工作和完成的文档从技术和管理两个方面进行检查和评价，找出存在的问题，确保下一阶段的工作有正确而可靠的依据。

2)概要设计评审

该评审以软件概要设计说明书为依据。评审的主要内容是：

a)项目的总体设计是否合理，总体框图是否正确：

b)数据流和控制流设计是否完整、协调；

c)程序的层次结构和模块划分是否合理、正确；

d)分系统的结构设计、输入输出及处理功能设计正确否；

e)接口连接和算法设计的正确性；

f)数据库总体设计的正确性。

3)详细设计评审

该评审以软件详细设计说明书为依据。评审的主要内容是：

a)对每个模块逐渐评审其功能、控制结构、数据结构、输入输出、调用关系的正确性；

b)评审每个数据库的概念模式设计。

4)验收评审

验收评审的主要内容是：

a)文档是否附合1)的规定；

b)文档与需求、文档与文档、文档与程序之间的一致性；

c)程序是否完全附合任务书的要求；

d)功能演示。

6.建议采用的软件可靠性设计技术

在软件开发过程中，应使用各种图形工具：在需求分析阶段使用数据流图；在概要设计阶段使用系统流程图、层次图；在详细设计阶段使用HIPO图；在编码阶段使用程序流程图。

对失效后果特别严重的软件，可采用容错设计方法。容错设计有下列3种途径：

a)加强软件的健壮性。就是把程序设计得能够缓解错误的影响，不致造成诸如死锁或崩溃这样的严重后果。可用在程序中夹有中间测试或在程序中按排周期性检查的办法做到这点，当主要考虑安全时，应使程序在出错时满足安全条件。

b)N版本编程法。即尽可能用不同的算法与程序语言，并让不同的小组编制，以此提高各个软件版本的独立性。这N个软件版本同时在N台计算机上运行，各计算机间能进行高效通信，并作出快速比较，当结果不一致时，按多数表决或者某种预定的策略选择输出。

c)恢复块法。即把程序划分为若干块，给需要作容错处理的块提供备份块(独立设计的相应冗余

备份),附加的错误检测和恢复措施后,把一般块变成了"恢复块"。此法可以在单台计算机上使用。

应对程序进行静态调试,即阅读程序、检查源程序的结构、文法和过程间的接口是否有错。除自己检查自己编写的模块外,项目组成员之间还应互相检查,以提高发现错误的可能性。

在设计中应采用自顶向下的设计方法,即以一个系统功能的最抽象描述开始作为最高层次;以它出发,设计一系列较详细的子系统,由这些子系统来完成最高层次的功能;再以每个子系统为基础,设计出一系列更详细的子系统,等等。如此逐渐向下作功能分解直到最低层次的子系统能够比较方便地用计算机程序设计语言来实现为止。

在设计中应采用结构化的设计方法,即把程序功能要求分解成各个分开的更小的程序或模块化的功能要求。并说清楚是如何于程序中的其它部分接口的。对每一个更小的程序或模块,应能分别编程和测试,使得模块间高度分离。

参考文献(略)

·简 讯·

《舰载雷达通用规范》审查会召开

国家军用标准《舰载雷达通用规范》审查会于1997年10月12日至10月14日在南京召开,会议由601所和雷达军标委共同主持。参加会议的有雷达军标委、海军论证中心系统所、海军第三试验区、海军驻有关厂所军代表室、电子工业部和船舶工业总公司所属有关雷达生产研制的研究所和工厂等共有12个单位的专家代表。

该项标准的修订工作是由主编单位船总第七二四研究所、副主编单位电子工业部第二十研究所、船总601研究所和编制组其他成员单位及各有关方面大力协同,通过2年的努力完成的。与会的专家代表们在听取了编制组的介绍后,对该项标准修订草案送审稿进行了认真细致的审查,并对送审稿的修改提出了一些有益的建议。

修订后的GJB 403A《舰载雷达通用规范》是按《国家军用标准编写暂行规定》第二篇规范的格式编写的,与原GJB 403比较除保留了原来先进性、可操作性等特色外,还有以下特点:

1、适用范围已不包括敌我识别器和询问机;

2、对雷达的主要战术技术性能规定了相应的定性和定量要求;

3、完善并补充了雷达主要战术技术性能试验方法,在对雷达的作用范围的试验方法中提出了威力图的要求,此外特别增加了动目标改善因子和反干扰性能检验方法;

4、在目前可供引用的国家军用标准体系相对比较完善的条件下,简化了一些有关设计、制造的内容。

(林荷香)