Science Discovery
2018; 6(1): 52-56
http://www.sciencepublishinggroup.com/j/sd
doi: 10.11648/j.sd.20180601.19
ISSN: 2331-0642 (Print); ISSN: 2331-0650 (Online)

Research on the Quality Assurance Method of Spacecraft Software Based on Software Testing

Zhao Long, Liang Xinjian, Hu Xiaoxi

Beijing Institute of Aerospace Control Devices, Beijing, China

Email address:
15611796238@163.com (Zhao Long), eryazi0425@sina.com (Liang Xinjian), tinasabrina@126.com (Hu Xiaoxi)

To cite this article:
Zhao Long, Liang Xinjian, Hu Xiaoxi. Research on the Quality Assurance Method of Spacecraft Software Based on Software Testing. *Science Discovery*. Vol. 6, No. 1, 2018, pp. 52-56. doi: 10.11648/j.sd.20180601.19

Received: January 16, 2018; **Accepted**: February 11, 2018; **Published**: May 23, 2018

Abstract: Aerospace technology is the most important symbol of the national strength, the national defense and the comprehensive national strength. With the change of times and the development of information technology, the development trend of the Spacecraft is more serialized, more intelligent and more precise. The computer systems are becoming more and more widespread in the spacecraft system. Aerospace engineering is an system which is huge, complicated and high technical difficulty. In this system, the computer and the software play an important role about the system control, process control, data acquisition and processing, data communication and system security and other tasks. The software has become the nerve center of the whole system, and it produces all kinds of information to make the other part of the system perform corresponding actions. The spacecraft software is bigger and bigger, the structure is more and more complex, and the requirement for software quality is higher. This paper investigates and studies the major software quality accidents and its causes. Base on the software test, this paper put forwards the method of software quality assurance and the construction idea of software evaluation Organization. The method proposed in this paper has been applied in several spacecraft, and the results show that the reliability and safety of the software can be effectively improved, and the quality of the spacecraft is guaranteed.

Keywords: Software Testing, Spacecraft Software, Software Quality Assurance, Software Evaluation Organization

基于软件测试的航天型号软件质量保证方法研究

赵龙，梁新建，胡晓曦

北京航天控制仪器研究所，北京，中国

邮箱
15611796238@163.com（赵龙），eryazi0425@sina.com（梁新建），tinasabrina@126.com（胡晓曦）

摘要：航天技术是一个国家科技实力、国防实力和综合国力的重要标志之一，是壮国威、振民心的伟大事业。随着时代变迁和信息技术的发展，航天型号产品系列化、智能化和精确化的发展道路已成为趋势，在航天系统中计算机应用越来越广泛。特别是航天工程是庞大、复杂、技术难度高的系统，在这样的系统中，是嵌入其中的计算机及其软件承担着系统指挥、过程控制、数据采集和处理、数据通信以及系统安全保障等任务，软件已成为整个系统的神经中枢，由它产生各种信息使系统其他部件执行相应动作。因此，航天型号软件规模越来越大，结构也越来越复杂，对软件质量的要求随之更高。本文调查和研究了世界航天重大软件质量事故及其原因，基于软件测试的角度提出了航天型号软件质量保证方法及软件评测机构建设思路。本文提出的方法在多个航天型号中进行了应用，结果表明能够有效提高软件的可靠性和安全性，保证了航天型号的质量。

关键词：软件测试，航天型号软件，软件质量保证，软件评测机构

1．引言

随着型号产品和计算机技术的飞速发展，计算机和软件已成为型号产品的重要组成部分，硬件为基础、软件为核心的特征日益明显，软件的质量和可靠性已成为航天型号产品质量和可靠性的关键因素之一。近年以来，世界航天型号产品质量稳步上升，发射任务连获成功，但是在总装、总测和发射场，以及在轨飞行过程中，仍出现了相当数量的质量问题。随着软件在型号研制中的应用越来越多，软件产品的问题占总质量问题的比例有上升趋势。

软件测试是软件工程中的重要环节，是保证软件质量和可靠性的重要手段。对软件测试的研究结果表明，越早发现软件中存在的问题，开发费用就越低；在编码后修改软件缺陷的成本是编码前的10倍，在产品交付后修改软件缺陷的成本是交付前的10倍。软件质量越高，软件发布后的维护费用越低。

美国航空航天局和美国国防部率先通过第三方机构评审关键项目承制方的软件开发工作，包含软件测试、验证和确认。为克服软件危机，美军采取了三大措施：实行军用计算机标准化计划；统一军用语言；成立软件工程研究所，同时颁布了20余个军用软件方面的有关标准。中国航天软件评测机构，是承担航天型号软件可靠性和安全性保证的重要部门和单位，通过GJB5000A软件质量管理体系的建设在航天型号软件质量保证方面取得了一定成效，通过不断改进软件过程来保证型号软件的质量，但由于各方面条件的限制，仍存在一些问题，特别是在横向型号软件测试项目管理上，缺乏统一、规范、成熟、系统的管理方法。

针对目前软件研制和测试管理过程中存在的问题与不足，本文从世界航天重大软件质量事故及其原因入手，根据软件测试的基本原则和作用提出了航天型号软件质量保证方法和软件评测机构建设思路。

2．世界航天重大软件质量问题及原因分析

软件是设计师塑造的、功能强大的工具，但寄生着各种bug的软件，顷刻间又可能转变为破坏力强大的敌人，随着计算机体系结构、程序设计语言的不断丰富，软件规模不断膨胀，任务复杂度不断提高、系统并发性不断增加，型号软件系统中潜在的bug已越来越难以捕捉、定位与控制，软件往往成为系统可靠性的薄弱环节。系统对软件的依赖性越来越大的同时，软件质量问题给我们带来的危害往往也越来越严重。

在全世界，由于软件质量直接导致飞行失利或运行故障的事件接连发生，具体事故情况见表1。

表1 由软件质量问题导致的航天型号事故统计表。

序号	航天型号事故具体情况			
	航天型号名称	所属国家	事故时间	事故原因及后果
1	金星探测器水手1号	美国	1962.07.22	因宇宙神火箭的软件算法错误而坠毁
2	阿里安5火箭	欧洲	1996.06.04	因惯性导航系统中软件部分的设计错误引起箭体结构断裂
3	火星气候轨道器	美国	1998.12.11	因简单的单位换算错误在火星大气层中烧毁
4	大力神-4B/半人马座上面级运载火箭	美国	1999.04.30	因惯性导航单元的软件文件中一个旋转速度过滤常量的值输错了导致任务失败
5	火星极地着陆器（MPL）	美国	1999.12.03	软件提前（在40m的高度上）向反推发动机发出了关机指令导致坠毁
6	“自主交会技术验证”（DART）卫星	美国	2005.04.15	由软件中所设计的复位措施导致卫星故障
7	火星全球探勘者号	美国	2006.11.02	因一次软件更新导致数据被写入到不正确的存储器地址，造成太阳能电池板被卡住而报废
8	旗舰级天文卫星“瞳”（Hitomi）[1]	日本	2016.04.28	由于错误指令（极性传反）的上传导致了卫星翻滚加剧而解体
9	夏帕瑞丽（Schiaparelli）火星着陆器[2]	欧洲	2016.10.19	因软件缺乏必要的工具和设置来识别错误、恢复数据而撞毁

由于篇幅有限，只罗列了上述几条世界上损失巨大、影响深刻的航天器因软件失效而导致的任务失败的案例，而实际上因软件问题导致任务失败的航天任务数不胜数，针对上述任务失败的问题进行仔细分析，可得出以下原因[3-14]，见表2。

表2 由软件质量问题导致的航天型号事故原因分析表。

序号	航天型号事故原因及代表性型号			
	技术方面原因	代表性型号事故	管理方面原因	代表性型号事故
1	有需求缺陷或者需求质量差	火星极地着陆器、 太阳日光层观测台	责任和权利不清	大力神-4B/半人马座上面级运载火箭、 火星极地着陆器、 阿里安5火箭、 火星气候轨道器
2	不必要的软件复杂度和功能	几乎全部型号事故	沟通渠道不畅及信息流缺乏	火星气候轨道器、 火星极地着陆器、

序号	航天型号事故原因及代表性型号			
	技术方面原因	代表性型号事故	管理方面原因	代表性型号事故
				阿里安5火箭
3	软件重用及变更前的安全性分析不充分	火星气候轨道器、阿里安5火箭		
4	设计中违反基本的安全性原则	阿里安5火箭、“自主交会技术验证”（DART）卫星		
5	质量保证及评审活动不充分	火星极地着陆器、太阳日光层观测台		
6	系统安全性分析严重不足	火星气候轨道器、阿里安5火箭		
7	测试和仿真环境缺陷	大力神-4B/半人马座上面级运载火箭		

3．软件测试的作用及基本原则

血的教训和巨大的损失使人们逐渐认识到，软件质量对整个系统质量具有重要意义，软件测试因此应运而生，成为软件工程中的重要环节，是保证软件质量和可靠性的重要手段[15]。

从用户的角度出发，软件测试的作用就是希望通过软件测试能充分暴露软件中存在的问题和缺陷，从而考虑是否可以接受该产品；从开发者的角度出发，就是希望测试能表明软件产品不存在错误，已经正确地实现了用户的需求，确立人们对软件质量的信心。软件测试的基本原则有以下几条。

3.1．应当尽早地和不断地进行软件测试

软件测试不仅仅是软件开发的一个独立阶段，而是贯穿软件开发的各个阶段的测试过程。广义的软件测试包含在软件开发的各个阶段的技术评审，期望在软件开发过程中尽早地发现和预防错误，把出现的错误克服在早期，杜绝某些发生错误的隐患。

3.2．软件设计师应避免检查自己的程序

软件设计师应尽可能避免测试自己编写的程序，软件开发小组也应尽可能避免测试本小组开发的程序。软件测试不能与程序的调试（debugging）相混淆，调试可能由软件设计师自身来做更为有效，但软件测试不是，所以如果条件允许，最好建立独立的软件测试小组或测试机构作为第三方来进行软件测试工作。

3.3．在设计测试用例时，应当包括合理的输入条件和不合理的输入条件

合理的输入条件是指能验证程序正确的输入条件，不合理的输入条件是指异常的、临界的、可能引起问题异变的输入条件。软件系统处理非法命令的能力必须在测试时受到检验。用不合理的输入条件测试程序时，往往比用合理的输入条件进行测试能发现更多的错误。

3.4．充分注意测试中的群集现象

在被测程序段中，若发现错误数目多，则残存错误数目也比较多。这种错误群集性现象，已为许多程序的测试实践所证实。根据这个规律，应当对错误群集的程序段进行重点测试，以提高测试投资的效益。

3.5．严格执行测试计划，排除测试的随意性

测试之前应仔细考虑测试的项目，对每一项测试做出周密的计划，包括被测程序的功能、输入和输出、测试内容、进度安排、资源要求、测试用例的选择、测试的控制方式和过程等，还要包括系统的组装方式、跟踪规程、调试规程，回归测试的规定，以及评价标准等。对于测试计划，要明确规定，不要随意解释。

3.6．应当对每一个测试结果做全面检查

有些错误的征兆在输出实测结果时已经明显地出现了，但是如果不仔细地全面地检查测试结果，就会使这些错误被遗漏掉。所以必须对预期的输出结果明确定义，对实测的结果仔细分析检查，抓住症候，暴露错误。

4．航天型号软件质量保证方法

目前，中国各个航天机构承担的重大型号任务相关软件已依据GJB5000A要求进行了软件工程化管理，在软件文档编写、评审、版本管理、出入库、开发方测试、第三方测试等方面均能够有效保证软件的质量，在这就不再一一赘述。但是对于民用、横向及系统级软件而言，往往一开始就缺乏统一的规划和顶层设计，只注重功能的实现，对软件工程化要求低，文档编写不规范或者甚至没有文档，软件版本控制主要还是由软件设计师自己负责，改动随意性较大。在交付时，总体若提出软件工程化管理要求，设计师常常采取走过场的方式来满足总体的要求。同时，软件不进行测试，交付后出现软件质量问题的可能性较高。鉴于上述种种存在的问题，需要进一步加大有效措施以保证出厂民品、横向及系统级软件的质量。

4.1．对需求进行充分挖掘、讨论和评审

在项目开始初期，总体对软件的要求往往只停留在功能实现上，对软件设计师交代的任务较为简单甚至模糊，导致在项目进行过程中，新的需求不断展现出来，导致软件设计师大量修改已完成的代码甚至需要修改整个软件架构，这就是前期总体与软件设计师之间缺乏有效沟通、对需求的有效挖掘导致的。在设计师编写代码前需要与总体进行充分的讨论，并将总体要求文档化，并要求总体签字确认作为简单的任务书和需求规格说明书。在软件编写过程中，若涉及需求变更，也需要形成正式的需求变更通知单，做好过程管理和总结。

4.2．顶层设计和软件项目规划

设计师与总体需要在项目初期进行软件的顶层设计和规划。特别是针对软件交付要求要进行充分沟通和协调，包括是否需要文档、是否需要开发方测试、是否需要第三方测试等一系列内容。确定上述内容，对于设计师确定研制时间和研制方确定研制成本有着重要作用。目前已有多个横向项目的总体在最后阶段提出了以上要求，不仅不利于软件研制时间的控制，而且不利于成本管理。

4.3．建立有效的软件版本管理制度

对于软件版本的管理，需要建立一套完整的管理流程和方法。民品、横向及系统级软件的特点在于代码量大、需求变化快、时间短和软件复用程度高，同时对民品、横向及系统级软件管理往往依靠设计师本身，如果超过一定时间，设计师不仅可能出现无法辨别最终软件版本的情况，甚至出现找不到软件代码的情况。若出现人员流动，民品、横向及系统级软件可能直接缺乏传承而导致宝贵软件资产的丢失。需要建立一个统一的管理归口部门，进行横向软件的管理和控制。

4.4．进行软件测试和质量提升工作

软件的质量问题往往是由于不遵循软件编码规则造成，而对于设计师而言，测试和修改自己的代码是一件非常不情愿的事情，这就需要一个强力的第三方质量保障机构，对软件提出有效的改进意见和建议。针对民品、横向及系统级软件采用重大型号软件的测试规范来进行测试是不切实际的，但是对代码进行规则检查和缺陷分析可以解决代码中50%~70%的问题，可以有效地快速提高民品、横向及系统级软件的质量。同时经过软件质量提升后，代码的清晰度和可复用性也进一步加强，有利于项目与项目之间的复用，也有利于设计师之间的传承。

5．航天软件评测机构建设思路

航天软件评测机构是承担软件测试任务，发展软件测试专业的重要部门，对航天型号产品的质量起到了极为重要的保障作用。除了重点航天型号任务的关键软件测试工作外，软件评测机构应在质量保证上再下功夫，从单纯的软件测试机构向软件质量保障与评价机构过渡，发挥更大的软件质量保证作用[16]。

5.1．民品、横向及系统级软件的管理职能

对于民品、横向及系统级软件的管理而言，软件评测机构正好是满足版本控制和软件质量保障双要求的部门。软件评测机构有着重点型号软件工程化管理的经验，这对于民品、横向及系统级软件研制部门和人员而言是缺乏的；软件评测机构拥有成熟的软件评测工具和经验丰富的软件测试人员，作为第三方机构可以提出可靠的软件质量意见和建议，不存在自身设计师不愿意修改代码的弊端；软件评测机构作为所有民品、横向及系统级软件的管理部门，有利于全所软件的统一化归口管理，可以解决部门与部门之间横向软件管理差异性问题。软件评测机构进行有效的版本管理可以有效帮助航天单位完成软件资产的积累工作。

5.2．软件工程化管理支持和过程把控工作

对于航天软件设计师而言，在日常工作中所涉及的软件项目往往只有1~2个，且很多软件设计师为非专职软件人员。而对于测试人员而言，在一年中面临的软件测试项目多达10个，甚至更多，且大部分项目均为重大型号任务，对于软件工程化方面有着丰富的经验，这种经验是随着项目实施过程逐步积累而成。软件评测机构可以作为软件工程化支持方，解决软件设计师在软件工程化和过程把控中的弱项。

5.3．软件测试技术研究，提高软件测试效率和质量

在测试流程及管理方面，软件评测机构可根据CNAS、DILAC、军用实验室资质认可的要求建立一套完整的软件测试管理体系，有效保证软件测试质量。对于软件测试专业而言，测试工具的应用可以有效提高测试的质量、测试的效率。在测试工具的引进、使用和开发方面，软件评测机构要有效地考察和了解软件测试工具，引进并学会测试工具，充分发挥作用，同时，软件评测机构根据经验积累和使用习惯，要能够自主开发效率更高、质量更好的测试工具。在软件测试专业知识工程方面，软件评测机构应进行软件质量案例库建设、软件典型性问题汇编及配合研制单位进行软件模块化建设等。在测试队伍建设方面，需进一步扩充队伍，且有针对性的增加型号相关专业又具有一定计算机基础的人员，同时针对软件测试人员的情况，进行有效的培训和工作安排。

6．结论

软件测试作为软件质量保证的重要手段，在软件工程、特别是在航天系统软件质量保证中有着重要作用。软件评测机构作为软件测试专业的承担部门，在提高软件测试技术和软件测试管理水平等方面有着巨大的作用。进一步加强软件评测机构建设，充分发挥软件评测机构的软件质量保证作用，有效提高航天型号软件质量，为中国建设成为国际一流的航天大国作出贡献。

参考文献

[1] Clark, Stephen. Attitude control failures led to break-up of Japanese astronomy satellite [R], Tokyo: JAXA, 2016

[2] Chan, Sewell. No signal from Mars Lander, but European officials declare mission a success [R], Paris: ESA, 2016

[3] Weiss K A. Leveson N G, Lundqvist K, et al. An analysis of causation in aerospace accidents [C]//Proceedings of the Digital Aviation Systems Conferernce. New York: IEEE, 2001:137-147

[4] Bureau of Air Safety Investigation. Advanced technology aircraft safety survey report [R]. Brisbane: Bureau of Air Safety Invwstingation, 1996

[5] Frola F R, Miller C O. System safety in aircrafta acquisition [R]. Washington: Logistics Management Institute, 1984

[6] Young T, Mars program independent assessment team report [R], washing: NASA, 2000

[7] Leveson N. The role of software in spacecraft accidents [R]. Boston: MIT, 2001

[8] Lion J L. Ariane 501 failure:report by the inquiry board [R]. Pairs: ESA, 1996

[9] Leveson N G. Systemic factors in software-related spacecraft accidents [R]. Boston: MIT, 2000

[10] Weiss K A. An analysis of causation in aerospace accidents [R]. Boston: MIT, 2001

[11] 侯成杰.国外航天软件故障原因分析[J].航天器工程，2012，21(1):89~95

[12] Leveson N G. Evaluating accident models using recent aerospace accidents:part I [R]. Boston: MIT, 2001

[13] Wong W E, Debroy V, Restrepo A. The role of software in recent catastrophic accidents, The IEEE Reliability Society 2009 Annual Technology Report [R]. New York: IEEE, 2009

[14] JPL Special Review Board. Report on the loss of the Mars Polar Lander and Deep Space missions [R], Pasadena, CA: NASA JPL, 2000

[15] 周涛.航天型号软件测试[M].北京：宇航出版社，1999：10~15

[16] 李昱.航天型号软件测试管理研究[D]，北京：中国科学技术信息研究所，2005