浅析机载软件测试策略

Analysis on Testing Strategy of Airborne Software

张国升 王保松／江苏金陵机械制造总厂

摘 要：归纳、分析了机载软件所特有的实时性、反应性、嵌入式、高度的可靠性及安全性的特点，并依据其特点提出了机载软件的测试策略。在综合分析讨论的基础上，总结得出了进行机载软件测试的原则和方法，对保证机载软件质量，提高其稳定性、可靠性、安全性具有指导意义。

关键词：机载软件；软件测试；测试策略
Keywords： airborne software；software testing；testing strategy

0 引 言

机载软件是应用于机载设备内部的计算机软件，主要包括机上的信息管理和指令控制系统和系统的依托平台等。随着机载计算机在军用战机控制系统中的广泛使用，机载软件质量问题愈显突出，甚至成为机载计算机软件能否发挥其优越性能的一个制约因素。现代战机大量采用自动化控制系统，机载计算机不仅数量多、品种杂，而且软件程序复杂，为了稳定飞机作战性能、保障战斗力，机载软件的可靠性、安全性测试必不可少。机载软件测试不仅是机载软件生存周期中的一个关键环节，也是保证机载软件质量的重要活动之一，其重要性不亚于软件的开发环节。解决机载软件可靠性、安全性问题的一个重要手段就是对软件进行充分的测试。但由于机载软件本身的复杂性和特殊性，其测试仍然存在许多困难。本文在对机载软件特点总结归纳的基础上，对机载软件的测

拦截地空导弹、直径130纳米的电子纤维“蒲公英”，就源自NEMS技术，每架飞机可以携带数以百万计的“蒲公英”，撒布在空中，使对方雷达显示一片迷茫，导弹将难以找到准确的攻击目标。

3 总结

MEMS技术正在全球产生航空工业的新一轮变革，在我国航空领域的应用始于微惯性传感器，已初步构建高校、企业和科研机构三位一体的研发体系，MEMS的发展经历了理论设计期、样机研制期、正迎来产业化应用的高速发展期。随着技术的培育积累，MEMS技术必将对我国航空工业乃至国民经济等产业提供强有力的技术支撑、带来重大的技术变革，也将哺育出一个新的产业。 AST

参考文献

[1] 毕克允. 微电子技术：信息化武器装备的精灵[M]. 第二版. 北京：国防工业出版社，2008.

[2] 任子西. MEMS技术将会为战术导弹带来一场革命[J].战术导弹技术，2010 (1):1−8.

[3] 周新春, 昂海松. 微型飞行器研究进展与关键技术[J]. 传感器与微系统，2008，27(6)：1−4.

[4] Klaus Schadow，Ayman El−Fatatry. RTO−MP−104：military/aerospace MEMS applications：AVT task group 078[R]. Brussels:The RTO AVT Symposium, 2003.

[5] Jiang Fukang, Xu Yong, Weng Tianxiang, Han Zhigang, etc. Flexible shear stress sensor skin for aerodynamics applications.micro electro techanical systems[C]. Miyazaki, Japan: MEMS 2000.

[6] 刘亚威. 国外航空微系统的研究应用[J]. 国防制造技术，2010,6(3)：36−39.

[7] 彭灏，李业惠，张素梅. 多拦截器：弹道导弹防御的新锐[J]. 现代军事，2006(1)：44−45.

作者简介

陆志东，中航工业导航技术首席专家，西安飞行自动控制研究所总工程师、研究员，长期从事惯性仪表及惯性导航技术重点型号及预先研究等工作。

余才佳，西安飞行自动控制研究所传感器室副主任、高级工程师，长期从事MEMS技术、微惯性仪表的预先研制等工作。

试进行了分析，并提出了测试对策。

1 机载软件的特点

1.1 实时性

实时性是指系统能及时或即时响应外部激励，满足时间约束的特性[1]，多数机载软件均要求具备实时性。对于实时软件，响应的及时性和高度的可靠性、安全性是实时软件质量评估的关键指标。从满足时间约束苛刻程度来说，实时系统可分为硬实时系统和软实时系统。硬实时系统是指若未满足时间约束的处理请求，则会认为系统请求响应失败；而软实时系统是即使不满足时间约束请求，也不会导致系统请求响应失败。换句话说，硬实时系统的时间约束非常关键，就是必须满足时间约束，而软实时系统是是希望满足时间约束，火控系统特别是火控计算机多采用硬实时系统，火控系统的实时性，直接影响飞机的作战效能，因此需要对其时间特性进行单独测试。

1.2 反应性

所谓反应性，是指根据外部时间做出响应的特性[2]。具有反应性的系统称为反应式系统。反应式系统的输出状态与输入的当前状态有关，还与历史状态有关，一般用输入－输出的序列来描述，不能简单用输入－输出的二元组来描述。反应式系统的行为一般是无限的，因而其中的进程通常也都是无终止、不间断地响应环境的激励。反应性使得软件的输入空间更大，更复杂，因而测试难度也更大。

1.3 嵌入式

嵌入式是指将一个计算机系统甲内置于一个更大的系统乙中，则称为甲嵌入于乙[3]。嵌入式系统在更大的系统中提供控制和计算功能，是系统的核心，管理和控制系统中的其他部分。嵌入式软件系统的一个显著特点在于：一般只为软件提供运行环境，而不提供软件的开发环境(宿主环境)。也就说，嵌入式软件的开发环境和运行环境是不一致的。正是这个不一致，给嵌入式软件的测试带来不少麻烦。因为即使在宿主机环境下测试再充分，也不能说明在目标机环境下该软件的运行不出问题。因而，嵌入式软件还面临着目标环境的测试，这不仅增加了测试的代价，而且还带来了嵌入式软件的测试策略问题，即哪些测试分配在宿主环境下进行，哪些测试分配到目标环境下进行。

用于机载设备的绝大部分机载软件为嵌入式软件，主要特点有两点。

一是软硬件紧密结合。嵌入式软件是面向专用控制系统设计的，而不是面向应用开发，对专用控制系统没有要求的功能进行了删除，提高了时序效能，使得软件和硬件有机结合，软件脱离特定硬件往往无法运行，引起软件异常，与硬件故障难以区分。

二是开发运行环境差异。一般情况下，嵌入式机载软件的目标运行环境与开发环境是不同的，给嵌入式机载软件的测试带来了麻烦。在开发环境下进行再充分的测试，也不能保证在目标运行环境下不出问题，因此嵌入式机载软件需进行目标运行环境下的测试。

1.4 高度的可靠性和安全性

大多数机载软件属高度安全关键软件，如果性能不可靠将会带来灾难性的后果，因此对其可靠性、安全性要求很高。为此，在机载软件设计时常采用一些提高可靠性、安全性的先进技术，如容错技术、N版本技术、安全监控和安全隔离技术等。

高可靠性、安全性的要求本身就大大增加了测试的工作量，而为了提高软件的安全性和可靠，采用多种技术后，软件系统的逻辑更加复杂，测试也更加困难。

2 机载软件测试策略

机载软件的特点，要求必须有与其相适应的测试策略。尽管传统的测试已不能完全满足机载软件的新特性要求，但已有的测试方法和技术在其测试中仍然可用。本文从机载软件测试管理的基本要求入手，分别针对实时性、嵌入式和高安全性要求等特点讨论机载软件的测试问题。

2.1 软件测试的基本要求

软件测试是使用人工或者自动手段运行或测试某个系统的过程，其目的在于检验它是否满足规定的需求或弄清预期结果与实际结果之间的差别，帮助识别开发完成的计算机软件正确度的软件过程，其基本要求包含三个方面。

1）开发过程的工程化管理。提高软件产品质量，最基本的要求是软件开发者要有一套完善的软件开发过程管理体系，而且必须在软件开发过程进行工程化管理，将有利于提高软件产品的质量。2）测试的艰难性。通常软件测试所耗费的人力、物力是十分巨大的。当人力、物力等资源紧张时往往是测试最容易被遗漏或者忽略的时候。3）与质量保证的关系。如果说质量保证是确保客户能得到满意软件产品的过程，那么软件测试就是执行这个过程的有效方法。进行软件测试不一定能百分之百确保质量，但不进行测试则根本无法保证质量。

2.2 实时性的测试

实时软件的本质特征在于其时间特性。实时软件的功能和行为的正确性验证仍可采用传统的测试技术，机载软件的实时性测试，对时间特性进行验证，也是实时嵌入式测试的关键内容。

时间特性的测试有两种方法，即静态时间分析和动态实时检测。

1) 静态时间分析

静态时间分析是在不执行被测程序的情况下，通过对程序结构的分析，预估程序、进程或子程序执行时间[4]。静态时间分析中，关键要分析最坏情况下，能否满足时间约束，因此，最大执行时间是计算的关键问题。另外，静态时间分析不仅应计算单个任务的执行时间，而且必须考虑多任务调度问题。

2) 动态实时检测

动态实时检测是通过运行程序测试程序的时间特性。通过仿真器、模拟器和插装工具均可实现动态实时检测。在线仿真器可以监视和测量程序的执行。其优点在于测量无需改变程序，而且测量相当精确，其缺点在于其结果只是测量值。模拟器也可得到程序的运行时间，与在线仿真器有同样的优点和缺点。插装工具则是通过向程序特定位置插入探针从而记录程序的执行时间，缺点在于改变了被测程序，增加了程序的复杂性，减慢了程序执行速度，且记录的时间不准确，甚至程序的执行结果也会受到影响。

目前，国内动态实时检测工具的研究已经相当成熟，如北京航空航天大学的NSM、ADA等检测工具。从理论上讲，只有通过静态分析才能发现程序执行的最大时间，其他方法都是测量，缺少安全性。静态时间分析工具所产生的结果比测量的可靠，所需的时间也较少，且具有预测性。

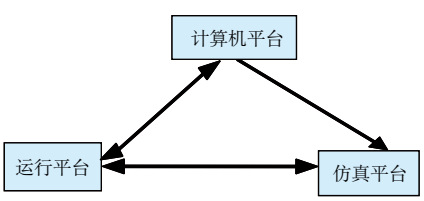

图1 软件仿真测试示意图

2.3 反应性的测试

反应性与实时性在本质上是一致的，主要是两者的侧重点不同，反应性尽管强调时间约束特性，更强调逻辑性，即软件的功能和行为特性，反应性对软件测试有很深地影响，使得软件必须通过输入序列和输出序列的二元组描述。同样的输入数据在不同时刻会产生不同的结果，这就给测试带来了困难。因此，构造测试用例是测试的关键问题。当前处理反应性，即软件行为特性的测试，一般用CASE工具创建应用系统模型，模拟反应式系统的行为，并检查外部事件结果，然后将以上分析活动作为设计所进行的测试用例的基础。反应式软件的测试用例的构造有许多技术可循，可使用类似等价类划分的技术对各种事件(如中断、控制信号、数据)按类进行测试。

反应式软件的特殊需求造成了系统中包含大量的与环境保持同步关系的进程，包括中断、任务或线程。这样，反应式软件已不是顺序软件，它具有并发的特性。软件的并发性所引入的错误是软件功能测试和单元级的测试所难以发现的，因此在系统测试时还必须针对并发性进行测试。

2.4 嵌入特性的测试

嵌入式软件的突出特点在于其运行环境(目标环境) 与开发环境(宿主环境)的不同[5]，这一特点导致嵌入式软件测试可分为宿主机测试和目标机测试。

1) 宿主机测试

一般情况下，宿主机上进行的测试是单元测试，如果被测单元所使用的是C++等高级语言或与目标机相同的汇编语言，则可以直接在宿主机上进行测试，但要求有可以生成宿主机代码的汇编程序或编译器。如果被测单元使用的汇编代码与目标机不同，若要在宿主机上测试则需要指令仿真器。因此，整个软件在宿主机上进行测试通常非常困难，尽管宿主平台上测试存在诸多麻烦，在宿主机上进行软件组装测试和系统测试的研究还是很受欢迎。

2) 目标机测试

无论在宿主机上的测试如何完善，目标机上的测试仍是必须的。因为一些问题只有在目标机上才可能发现和确认。但如果完全在实物环境下测试软件系统，其测试代价会非常昂贵，测试周期也会很长。所以一般在系统联试时，对软件进行全实物环境下的功能测试，而大量测试在全仿真环境下进行。

目标机上常用的测试手段是软件仿真测试，一般由运行平台、仿真平台和计算机平台三个部分组成，其构成关系如图1所示。其中，计算机平台完成测试用例的生成、调度管理、数据分配及测试后的评估工作，运行平台是嵌入式系统的硬件和被测软件，仿真平台是模拟嵌入式系统外部运行环境，并向嵌入式系统提供激励信号，同时接收反馈信号。纯软件仿真测试的主要问题是软件测试依赖于硬件，软件和硬件的故障难以分离。

目标机上的测试侧重于功能测试，也就是通常所说的黑盒测试，但在很多情况下也要使用结构测试，即白盒测试，这就要求在目标机环境下对程序的执行情况进行记录，常用借助于在线仿真器和插装技术两种方法。采用插装技术记录程序的执行情况，会改变源程序，增加程序的复杂性，使程序执行速度减慢。特别是在实时嵌入式系统中，时间和空间(内存)都很紧张，插装往往造成意想不到的后果。

2.5 可靠性安全性的测试

1) 可靠性测试

对于机载计算机的核心组成部分——机载软件，通过常规测试是远远

不够的，还必须进行可靠性测试，评价其可靠性。由于可靠性测试需要进行实物环境模拟测试，对机载软件来说难度很大，其难度在于构建测试环境、产生测试数据和评估测试结果。

a. 构建测试环境

对机载软件进行可靠性测试，其测试环境可以分为三类。一是纯数学环境，即将嵌入式软件的代码剥离出来进行测试；二是真实物理环境，即被测系统直接与实物连接；三是仿真测试环境，即建立仿真平台，模拟系统输入激励和输出响应并与目标机构成一个闭环系统[6]。当系统复杂时，纯数学环境测试难度大，且某些测试结果不能真实地反映软件的使用情况；真实物理环境虽然准确真实，但当系统复杂时，测试费用较大。因此，对于机载软件而言，可靠性测试最适合的测试环境是仿真测试环境。

b. 生成测试数据

机载软件的可靠性测试数据生成，必须解决三方面的问题：一是能反映出用户实际使用软件的统计规律；二是测试数据与嵌入式软件的特性相一致，使测试数据满足嵌入式软件的数据格式、发送源及目标和方式等要求；三是实时性要求，即测试数据需要满足实时软件的实时输入特性。可利用Use−case图、类图和顺序图生成测试数据。具体步骤为分析软件文档、构造Use−case剖面、提取输入输出变量、抽象输入输出类、建立输入顺序图和输入的描述。

c. 评估或判定

软件可靠性评估是指在软件可靠性增长测试中，根据测试失效数据，对软件可靠性状况进行定量估计并对其发展趋势进行预测[7]。软件可靠性验证测试可参照GJB899中的定时结尾或序贯试验方案进行。

软件可靠性增长测试结果的评估根据软件可靠性增长模型进行。目前，已提出上百种软件可靠性模型。但是，由于软件逻辑结构的复杂性、输入空间的复杂性以及失效模式的复杂性，没有一个软件可靠性模型是普遍适用的，而且这些模型也存在精度低、一致性差的问题。

2) 安全性测试

对于软件测试来讲，可靠性测试理论已经较为成熟，出现了很多种软件可靠性测试方法，并有完善的统计理论指导产生测试用例，能够有效地缩短测试持续期，减少测试用例，这些理论完全可以成为机载软件安全性测试的有效借鉴。

机载软件系统主要关注安全性测试，目的是通过测试发现机载软件的运行缺陷，提高其安全性水平，确保并验证其功能是否达到规定的安全性指标要求。机载软件安全性测试的关键在于暴露那些对降低事故风险作用比较大的软件缺陷。因此，在对航空机载软件进行无失效的安全性指标验证测试时，应该遵循以下基本原则：

1) 测试之前应该进行充分的机载软件安全性分析；

2) 测试用例的选择必须重点倾向于高风险的软件运行；

3) 应对可能造成灾难性事故的事件进行最充分的覆盖。

在对机载软件进行安全性测试时，应对软件硬件系统进行综合的失效模式和影响分析，以发现软件系统存在的安全性问题，为安全性测试用例提供依据。

3 结束语

本文首先归纳和分析了机载软件所具有的实时性、反应性、嵌入式、高度的可靠性和安全性的特点，并从软件测试的基本要求出发，针对其特点提出了机载软件的测试策略。在总结分析的基础上，得出5点结论。

1) 静态时间分析是实时性测试的最佳手段；

2) 反应性测试需针对软件的并发性特征进行；

3) 嵌入式软件测试可在宿主机和目标机分别进行；

4) 软件可靠性的测试的困难在于构建测试环境、产生测试数据和评估测试结果便可实现；

5) 指出了软件安全性测试的原则。

总之，本文的讨论与分析对保证机载软件质量，提高其稳定性、可靠性、安全性具有一定的指导意义。 AST

参考文献

[1] 孙昌爱，靳若明，刘超，金茂忠.实时嵌入式软件的测试技术[J].小型微型计算机系统，2000，21(9):920–924.

[2] 万永超，赵宏斌，董云卫.航空机载软件安全性测试技术研究[J].计算机测量与控制，2010，18(5):1017–1021.

[3] 韩峰岩，王昕.机载计算机软件的测试[J].航空计算技术，2004，34(3):65–69.

[4] 邵辉.实时嵌入式软件的仿真测试技术研究及环境的实现[D].北京：北京航天航空大学，1998.

[5] 韩峰岩，王昕.计算机实时控制系统软硬件综合FMEA[J].计算机工程，2003，29(20):50–53.

[6] Broekman E N. Testing embedded software [M]. New Jersey：Pearson Education Inc，2003.

[7] 朱鸿，金凌紫. 软件质量保障与测试[M].北京：科学出版社，1997.

作者简介

张国升， 工程师， 主要研究方向为综合航电技术。