基于故障注入的实时嵌入式软件仿真测试技术研究

苏银科，李艳雷，周 平，常晓航
（北京机电工程研究所，北京 100074）

摘 要：由于强实时性、参与闭环控制、软硬件耦合及可靠性要求高等特点，飞行控制系统嵌入式软件在软件研制、测试及验收阶段往往缺少动态测试环境。本文在仿真测试技术基础上，针对飞行控制系统嵌入式软件的特点与测试需求，进行了基于故障注入技术的仿真测试技术研究，设计了一种实时嵌入式软件仿真测试平台方案。

关键词：实时嵌入式软件；软件测试；故障注入；仿真测试
中图分类号：TP273 **文献标志码：**A **文章编号：**2095-8110（2014）03-0069-05

Research On Technology of the Real-time Embedded Software Simulation Test based on Fault Injection

SU Yin-ke , LI Yan-lei, ZHOU Ping, CHANG Xiao-hang
(Beijing Electromechanical Engineering Institute, Beijing 100074, China)

Abstract: Because of the characteristics of highly real-time , closed loop controlling ,coupling of software with hardware, and the requirements of reliability ,the embedded software of flight-control computer always runs short of dynamic testing system ,especially in the phases of software developing, software testing ,and acceptance testing . In this paper, a method of simulation testing based on fault injection is put forward, after analyzing the testing characteristics and demand, a blue print is designed as well.

Key words: Real-time embedded software ; Software test ; Fault injection ; Simulation test

0 引言

近年来，各种嵌入式计算机系统在飞行控制系统领域得到了广泛的应用。随着嵌入式硬件技术的发展，硬件可靠性得到了较大的提高，与此同时飞行控制系统嵌入式软件的规模及性能却发生了很大的变化。嵌入式系统可靠性的瓶颈正逐渐向软件转移。文献[1]指出目前影响嵌入式系统失效的因素中硬件因素已经从50%降到10%，而软件因素却从3%增长到了62%。因此如何更有效地保证飞行控制系统嵌入式软件的高可靠性面临严峻的考验。

实践证明，软件测试对验证软件的功能和性能、发现软件中的缺陷具有重要的意义。飞行控制系统软件是一类具有容错机制的安全、关键嵌入式软件，具有强实时性、参与闭环控制及硬件接口复杂与专用等特点。对其进行软件测试，尤其是系统测试、验收测试，一直以来缺少有效、可靠的测试环境。本文在飞行控制系统嵌入式软件测试需求分析基础上，提出将故障注入与仿真测试结合，进行测试环境设计。基于故障注入的仿真测试方法是在嵌入式软件仿真测试研究的基础上，结合故障注入过程的特点，将故障分析、故障建模与故障注入技术有效运用于嵌入式软件测试的过程，有效扩展了实时、非侵入式嵌入式软件测试方法的灵活性。

1 飞行控制系统嵌入式软件测试需求分析

飞行控制系统嵌入式软件测试按照测试生命周期可分为单元测试、部件测试、配置项测试及系统测试四个级别，含义如表1[2]所示。

收稿日期：2014－09－21；**修订日期：**2014－10－27。
作者简介：苏银科（1985－），男，硕士，工程师，主要从事系统仿真，仿真测试等方面研究。
E-mail：yinkesu@163.com

表1 飞行控制系统嵌入式软件测试级别释义

Tab. 1 The explication of the embedded software testing

测试级别	含义
单元测试	主要检查软件单元能否正确实现详细设计中的功能、性能、接口和其它设计约束
部件测试	主要对软件单元的集成过程，集成得到的软件部件进行测试，以检验软件单元和软件部件之间的接口关系及软件部件是否符合设计要求
配置项测试	检验软件配置项与软件需求规格说明中的功能描述是否一致，测试内容主要包括功能测试、性能测试、边界测试等
系统测试	检验软件各配置项能否和系统正确连接，软件系统能否满足系统/子系统设计文档和软件研制任务书规定的功能和性能要求

其中软件配置项是指具有完整功能、可独立运行的程序。配置项测试和系统测试与软件开发需求和系统研制需求紧密相关，要求测试必须在真实的目标环境下开展，是一种动态的、实时的、非侵入式的黑盒测试。

飞行控制系统嵌入式软件一般具有强实时性、参与闭环控制、软硬件耦合及可靠性要求高等特点，对其进行配置项测试和系统测试（本文以下合称动态测试），具有较大的工程难度，主要集中在以下方面：

1）飞行控制系统软硬件功能耦合程度高。软件测试时无法将软件与硬件环境剥离，测试激励信号需要通过目标机硬件接口注入；

2）飞行控制系统往往由多个嵌入式设备、机电设备等构成，分系统之间交联关系复杂。实际中因各设备研制进度不一，无法通过真实设备搭建测试环境。因此需要测试工具模拟各外围设备产生激励信号；

3）飞行控制系统具有实时性要求，因此测试环境要求及时产生测试激励；而参与闭环控制的特点要求测试环境不能事先通过离线方式生成测试激励，必须在线根据目标机反馈信号生成测试激励；同时飞行控制系统的高可靠性要求测试环境能够产生反应异常、故障、边界与极限等情况的测试激励。这些对测试激励的生成带来了较大的困难。

上述特点使得目前飞行控制系统嵌入式软件的实时、非侵入式动态测试缺少灵活、通用、可靠的测试环境。一直以来，国内飞行控制系统嵌入式软件动态测试依托于专用测试平台，测试开发难度较大；国外在这一领域目前已拥有一些功能强大，性能良好的测试平台，却因为领域差异、技术保护及价格昂贵，难以在国内得到广泛应用。

2 半实物仿真测试技术原理

近年来工程界针对实时嵌入式软件的特点，提出了多种动态测试平台方案，比较典型的有全数字仿真测试方案、半实物仿真测试方案、全实物仿真测试方案及灰盒测试方案（是一种 processor in the loop的测试方案）等。由于飞行控制系统嵌入式软件的特点，采用半实物仿真测试方案具较高的实用价值。这也是目前国内外公认的、行之有效的、具有广泛应用前景的实时嵌入式软件的黑盒测试方案[3]。

半实物仿真测试也称硬件在回路（hardware in the loop）仿真测试。半实物仿真测试系统通常由目标机、信号调理箱、仿真计算机及测试主控机组成。半实物仿真测试系统的基本原理如图1所示。

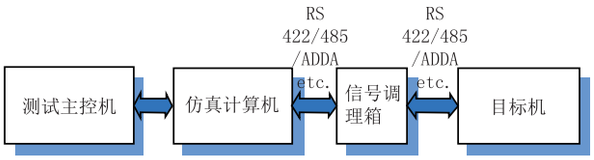

图1 半实物仿真测试系统模型

Fig1. The model of the HIL simulation testing

目标机指硬件实物设备。信号调理箱与专用的目标机进行信号互联，并将各种不同类型的电气信号进行梳理，转发给仿真计算机。仿真计算机中建立了目标机外围环境的仿真模型，与目标机构成虚拟的闭环系统。测试主控机通过一组人机界面为测试人员提供测试开发与过程控制接口。

这种方案能对已固化在硬件中的嵌入式软件进行实时的、非侵入性的闭环测试。实际根据仿真系统的复杂程度，可以将多台仿真计算机联网，构成实时分布式网络，网络中每台计算机都是一个节点，运行仿真模型。实时分布式网络或者单个仿真计算机与目标机之间的通信，可根据目标机的需要进行选择，例如采用AD/DA、RS422、1553B等方式。

半实物仿真测试的核心是利用半实物仿真技

术，在仿真计算机中建立被测目标机交联系统的仿真模型，利用仿真模型代替实物设备产生测试激励。这种方法有效解决了测试激励数据在线生成的问题，也能够保证系统的实时性。但这种方法中交联系统的仿真模型，一般是根据交联系统的功能或原理搭建，是基于正常任务剖面的，难以对飞行控制系统嵌入式软件进行如边界、极限、异常故障情形下的测试。

3　基于故障注入的仿真测试

由于飞行控制系统本身的复杂性及较高的可靠性，飞行控制系统嵌入式软件的动态测试要求进行如边界、强度、极限及异常、故障等特殊情景下的测试。因此有必要研究仿真测试环境下的测试数据控制问题，即如何在仿真测试环境中模拟异常、故障现象，同时研究如何能够使测试人员灵活地修改仿真测试过程数据，增大测试空间，以产生如边界、强度、极限情况下的测试激励。

基于故障注入的仿真测试，借鉴了故障注入技术的思想原理，对仿真环境中的交联系统仿真模型进行动态干预，不仅可以模拟交联系统中发生的各种异常、故障，而且能够按照用户的设定产生各种边界、强度、极限情况下的测试激励。基于故障注入的仿真测试原理如图2所示。其中O_E为系统按照测试规格要求期望的输出，O_T为系统实际的输出。嵌入式软件仿真测试中真实交联环境由交联系统仿真模型E1与通信模型E2替代，故障注入模块通过在仿真测试环境中动态干预仿真模型E1、E2，完成仿真测试。其中F表示故障注入模块产生的故障激励信号。

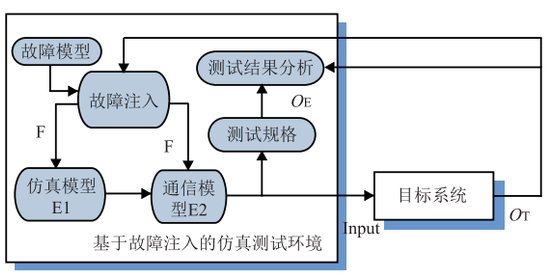

图2　基于故障注入的仿真测试原理

Fig. 2　The principle of simulation testing based on fault injection

基于故障注入的仿真测试与传统故障注入技术的不同在于，不是将故障注入到目标系统中，而是通过采用故障注入的思想，将故障注入到交联系统的仿真环境中，以实时动态地按照用户的设定，产生特定情景下测试激励，是一种故障仿真手段。

通过基于故障注入的仿真测试原理构建测试平台，具有以下优点：

1）不仅能够通过交联系统产生正常任务剖面内的测试激励，还能够干预仿真模型运行，产生各种具体故障情景下的测试激励，可以灵活地更改测试过程中产生的数据，为用户提供更加有效的测试手段；

2）避免了在进行故障、异常测试时直接修改仿真模型的弊端，将系统故障域与正常域分开，保证了测试过程中交联系统状态一致性，提高了结果的可信性；

3）可以将故障模型集中管理，并实现测试资源的重用和简化回归测试；

4）有助于研究故障对目标系统的真实影响及相关失效行为和对目标系统的容错机制进行有效性评估等[5]。

4　基于故障注入的实时嵌入式软件仿真测试平台软件架构设计

4.1　平台架构设计

基于故障注入的仿真测试思想，本文设计了一种嵌入式软件仿真测试平台，如图3所示。软件以共享内存为数据中心，主要由仿真模型解算模块、接口收发模块、通信协议解析模块、测试实时显示模块、实时数据收集与分析模块和测试模块构成。各模块通过共享内存实现数据交互。

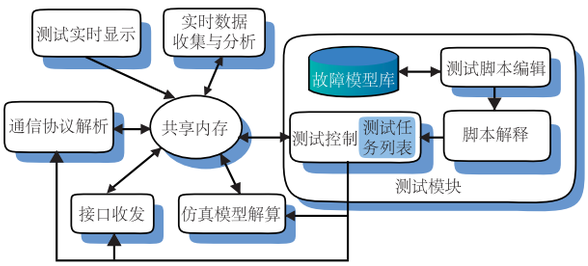

图3　基于故障注入的实时嵌入式软件仿真测试平台软件架构原理

Fig. 3　The architecture of real-time embedded software testing platform based on fault injection

仿真模型解算模块、接口收发模块与通信协议解析模块共同完成目标机交联环境的仿真，合称仿真模块。架构中各模块的功能如下：

1）仿真模型解算模块调用交联系统数学仿真模型进行数学仿真，这些模型只与交联系统的功能或原理相关，与具体硬件特性无关，为系统的内特性模型；

2）接口收发模块对各个硬件接口进行操作，负责对包数据的发送与接收；

3）通信协议解析模块依据接口控制文档（ICD）信息对仿真模型解算模块输出的数据进行组包，或者对接口收发模块采集的数据进行解析；

4）测试模块基于故障注入的仿真测试原理构建，根据测试任务列表中当前测试任务信息，实时地修改共享内存的数据并干预仿真模块的执行结果，完成故障的仿真；

5）测试实时显示模块实时显示测试过程与结果，为用户提供一组直观的测试显示界面；

6）实时数据收集与分析模块实时地进行动态数据转存，并实时判断测试结果，监测平台工作状态。

4.2 测试模块设计

测试模块通过动态地修改共享内存数据及干预各仿真模块的运行，实现对仿真测试过程的干预，执行过程为：

1）用户通过测试脚本编辑环境编写测试脚本（故障模型），可以直接调用保存于故障模型库中的已有故障模型，也可以自定义故障模型；

2）脚本解释模块对测试脚本进行解释，形成一串测试任务序列，保存于测试任务列表；

3）测试控制模块以测试任务列表为依据，实时动态地判断测试干预的条件，判断故障的类型、动作等信息，修改共享内存中产生的各种动态数据、干预仿真模块的运行，从而产生带有故障、极限、边界等特性的测试激励。

4.3 故障仿真模型的建立

依据实际飞行控制系统中故障模型之间的作用关系，对复杂故障进行抽象，将故障模型描述为由基本模式层、模式关系层和仿测特征层三层表示的故障模型。各层之间的关系与含义如图4所示。

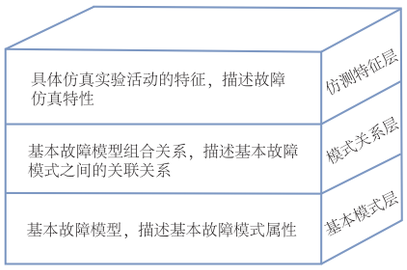

图4 故障仿真模型的三层结构

Fig. 4 The three layer structure of fault model

1）基本模式层由飞行控制系统中底层部件的失效模式仿真模型构成。基本模式层中各基本故障模型是系统表示复杂故障模型的基础,表示了仿真测试试验中故障注入的最小粒度，基本故障模型中包含了故障的基本属性，界定了故障域范围、故障的类型、位置等信息；

2）模式关系层对库中基本故障模型按照特定组合关系进行组合，形成复杂故障仿真模型，对基本故障模型实现了复用；

3）仿测特征层在模式关系层基础上,定义了故障模型与一次测试活动之间的特定关系,目的在于故障仿真试验时确定故障仿真的前提条件和结束条件。

方案中测试脚本编辑环境提供了一套接口，可以对故障模型库中的故障模型进行特定关系组合，并设定一次测试的特征属性，从而完成故障模型的建立。测试控制器依据这些信息，可以完成基于故障注入的仿真测试。

4.4 脚本编辑环境设计

测试人员通过编写具有一定语法格式的测试脚本来描述测试过程以及测试结果的判定条件。仿真测试平台分析并执行测试脚本描述的内容，从而完成整个测试过程。这种将测试脚本作为测试人员与仿真测试平台之间的交互方式方便灵活。

为此平台引入了Python脚本语言，并基于此设计了测试脚本的框架。Python语法类似C和模块化语言的杂合，并具有良好的可扩展性，使得它能很好地适应软件测试的需要。使用Python语言设计的测试脚本即使作了修改，也无需重新编译就可以调用Python解释器直接执行，大大节省了测试

时间。

本文在实现测试脚本编辑模块和框架时，采用了目前主流的C++语言作为主要实现语言。C++与Python的混合编程具有两种方式：扩展与嵌入。扩展是指用C++语言为Python编写扩展模块，以使Python可以使用C++所实现的函数（或类）；嵌入是指C++程序调用Python解释器执行Python编写的模块。为了实现利用Python完成测试过程的控制，对这两种方式进行了有机结合，具体实施了：

1）Python解释器在测试环境中的集成；

2）用C++为Python脚本程序编写扩展模块，使其能够访问和控制共享内存数据交联系统仿真模型；

3）将Python脚本模块嵌入到故障仿真框架中。

5 结论

一本方案以共享内存为数据中心，以测试模块软件为核心，可以完成用户设定的各种测试激励，并将系统故障域与正常域分开，保证了测试过程中交联系统仿真模型状态一致性，提高了软件测试结果的可信性。

参考文献

[1] 王田苗. 嵌入式系统设计与实例开发[M]. 北京:清华大学出版社.

[2] 蔡建平. 嵌入式软件测试实用技术[M]. 北京：清华大学出版社，2010.

[3] 谈琳. 实时计算软件的仿真测试平台的研究与设计[D]. 成都：电子科技大学，2005.

[4] 刘斌，艾俊，阮廉. 模型驱动的实时嵌入式软件测试方法研究[M]. 软件测试学术交流论文集，2005.

[5] 徐应诗，刘斌，阮镰. 基于故障注入的仿真测试方法过程框架[J]. 测控技术，2006,27(10)：50-56.

[6] 叶晓露. 基于故障注入的嵌入式系统测试研究[D]. 浙江：浙江大学，2008 .

[7] 孔文华，苏银科，杨丽霞. 武器装备故障模式仿真建模方法研究[M].中国仿真技术学术交流会会议论文，2012.