DOI:10.16080/j.issn1671-833x.2009.08.004

故障注入在航电系统测试过程中的应用

Application of Fault Injection in Avionic System Testing

北京航空工程技术研究中心　虞健飞

特殊的工作条件使得航空器必须具有很高的运行稳定性、健壮性和可维修性。故障注入通过模拟航电设备及其接口可能发生的异常(包括物理连接失败、性能参数下降、功能失效、时序错误等),可对航电系统进行更全面的测试和验证。

虞健飞

高级工程师,博士后,毕业于空军工程大学工程学院,现在北京航空工程技术研究中心工作,主要研究方向为航空装备测试技术。

特殊的工作条件使得航空器必须具有很高的运行稳定性、健壮性和可维修性。因此在航电系统的设计、研发和测试过程中充分考虑各种异常状态可能带来的影响,是航电系统设计的重要内容。

故障注入通过模拟航电设备及其接口可能发生的异常(包括物理连接失败、性能参数下降、功能失效、时序错误等),可对航电系统进行更全面的测试和验证。

航电系统研制不同阶段对故障注入的需求分析

在航电系统研制的整个周期,有效的故障模拟都可以发挥重要作用。

1 系统设计阶段

系统设计阶段一般采用半实物方式建立系统的运行模型,对航电系统信号传输、数据流通信、控制流程和处理算法等进行仿真。这种方法可在系统设计阶段对航电系统的整体方案和关键环节进行验证,从而有效地规避设计风险,提高设计效率。

在当前技术条件下,半实物仿真可以完成一般状态下的系统方案验证,但却无法覆盖到更多异常状态下的逆向测试(例如,对通信协议的测试不仅要考虑总线通信的正常状态,还要考虑总线的物理连接故障、电气特性变化、以及传输噪声可能带来的影响等),这就需要在系统半实物仿真阶段通过各种手段模拟系统运行可能出现的异常状态。

2 产品研制和单元测试阶段

航电设备的研制内容主要包括硬件、软件和结构 3 部分。

(1) 在电子设备的硬件设计中,很大一部分电路用于特殊情况下的故障诊断、异常处理、设计冗余和电气保护,这部分电路的测试在正常情况状态下无法工作,因此需要通过故障注入创造相应电路工作所需要的特殊条件。例如,对于一个模拟量输

入接口，要设计瞬间高压保护电路，那么在单元测试时就需要产生对应的信号以确认该电路是否工作，从而评估其保护能力。

（2）航电设备大部分重要软件运行在嵌入式环境下，其中有很多代码是和硬件电路高度耦合的，而这其中又有很大一部分代码用于处理硬件接口电路可能发生的异常，具有很强的硬件相关性和时序特殊性，很难通过纯软件方法发现其中的问题。因此通过故障注入创建这部分代码运行所需的条件，在最接近真实的状态下对异常处理代码进行测试就显得非常必要了。如在UART（异步串行接口）驱动设计中，测试不同类型中断的响应处理，只有在设备实时工作情况下才能实现，这就需要对起始位错误、校验位错误、BREAK唤醒、通信过载等多种异常情况进行模拟。

（3）在航电设备设计中，保证总线、信号等外部接口在各种工作状态下的安全性和稳定性是非常重要的，这种测试需要模拟总线、信号接口的各种极限状态，以测试设备处理各种异常的能力，如在外部电源波动情况下检测设备的工作状态，以评估设备对电源的容错能力。

3 系统验证测试阶段

在航电系统的验证测试阶段，需要更全面的故障注入来保证验证测试的完整性。

（1）系统冗余性能测试：对于航电系统中进行了冗余设计的总线和信号，要模拟实际运行过程中可能发生的故障，以确认备份通道或功能的切换特性。

（2）电气性能分析：对于航电系统供电、总线、信号等各类接口的电气参数，要通过故障模拟分析系统稳定工作的有效值域、不稳定值域和故障值域来确定，同时要获取实际系统的工作值以评估系统的安全性及电气参数的冗余度等。

（3）可维修性测试：航电设备的BIT（Build-in-Test）功能是保证系统良好运行、在故障状态能够快速修复的重要手段。在系统验证测试过程中，要充分模拟实际运行时可能发生的各种故障，对系统BIT功能进行全面测试。

故障注入的实现手段

故障注入的实现过程涉及航电系统的多个环节，与设计的耦合紧密，跨专业领域较多，是一个非常复杂的过程，需要采用多种技术手段，从不同角度实现不同类型的故障模拟。

1 在仿真和测试环境的设计中实现故障模拟

在系统仿真和测试环境的设计中，可以对数据、信息流和控制时序的变化进行故障注入，即设计算法时不仅要考虑系统正常的状态，还需要考虑各种异常状态，包括传感器和执行机构异常、通信接口异常、信号传递异常、控制时序异常等。

有些通用仿真测试平台（如德国TechSAT公司的ADS-2，国内的FireBlade等系统）的软件具备故障注入功能，可以很方便地实现算法的故障设计。

不管是通用的仿真测试平台还是专门设计的系统，一般都采用COTS（Commercial-Off-the-Shelf）功能模块，这样就只能模拟硬件无关类型的故障，更多体现在处理算法方面，而对于具体的物理层和电气层的故障模拟还需要采用其他手段。

2 手动模拟部分简单故障

在仿真、调试、测试过程中，最方便、直观的故障注入手段是手动地加入一些故障（如电缆物理连接异常、部分控制信息时序异常、接口信号幅度异常等），这也是目前实际应用中广泛使用的方法。但手动操作故障注入的缺点是：能够实现的故障类型比较少；故障注入的实时性无法保证；对操作人员的技术要求比较高。

3 利用仪器仪表和COTS产品的功能

很多仪器仪表（如信号发生器、电阻箱、程控电源、逻辑分析仪、高端的ICE等）可以作为故障注入的辅助工具，通过手动调整和仪器仪表相结合进行故障注入，也是目前常用的手段。

有些针对航电系统的COTS板卡也提供故障模拟功能，如美国GE Fanuc和Alta公司的1553B/ARINC429接口板卡都提供电气层和协议层的故障注入功能。

4 在设备研制过程进行故障模拟设计

对于高稳定性的关键部件，可在嵌入式系统的软硬件设计中实现部分故障状态的模拟，如内存错误模拟、接口IO信号替代、时序延迟等。

采用这种方式实现的故障模拟与系统的耦合度高，可用性好，使用方便，但会提高设备设计的复杂度，带来很多额外的开销，甚至会产生新的设计问题，所以除非特别必要，不推荐使用。

5 采用专业的故障注入设备

目前专业性的故障注入设备还比较少，德国TechSAT公司提供的ADS2-FIBO可模拟航电系统连接电缆上可能发生的连接故障（包括短路、断路、阻抗等）。

北京旋极信息技术股份有限公司吸取国外相关系统的设计经验，结合国内的需求，设计了IceBlade故障注入系统。针对各种航电接口，该系统可在物理层、电气层、协议层和应用层实现故障注入功能，而它特有的探针故障注入功能可以在PCB层面实现故障注入。

IceBlade故障注入系统介绍

IceBlade故障注入系统用于高稳定、高可靠性电子设备的调试、测

试和验证过程。通过模拟电子系统在运行过程中可能出现的异常来实现设备的容错性测试、故障模拟、故障定位和故障分析。

系统可以模拟通信总线和接口信号在物理层、电气层、协议层的性能变化，在不对被测系统进行任何改动的条件下实现故障注入功能。

系统提供电源故障注入和探针故障注入功能，用以模拟电源质量变化情况和线路板上芯片级故障。

IceBlade 故障注入系统在实现故障模拟的同时，还具有对目标信号进行观察、记录和分析的能力，提供最详细的信号，便于调试、测试人员发现任何潜在的威胁。

系统采用积木式结构，可根据需要灵活裁减。

1 系统的设备结构

IceBlade 故障注入系统硬件由故障控制计算机、各通信接口控制单元、各信号接口控制单元、电源故障注入单元和探针故障注入单元组成。其功能有：

（1）故障控制计算机控制故障注入过程。

（2）通信接口控制单元包括：

•IceBlade-1553 故障注入单元。实现对 STD-1553B 总线的故障注入和电气特性分析；

• IceBlade-A429 故障注入单元。实现对 ARINC-429 总线的故障注入和电气特性分析；

• IceBlade-RS × × ×（IceBlade-RS232、IceBlade-RS422、IceBlade-RS485）故障注入单元。实现对 RS × × × 异步串行通信总线的故障注入和电气特性分析。

（3）信号接口控制单元包括：

• IceBlade-ADDA(V/I) 故障注入单元。实现对模拟信号量（电压／电流）的故障注入和电气特性分析；

•IceBlade-TTL 故障注入单元。实现对标准 3V／5V 的 I／O 信号的故障注入和电气特性分析；

• IceBlade-DISCRETE 故障注入单元。实现对离散 I／O 信号的故障注入和电气特性分析。

（4）电源故障注入单元（IceBlade-PWRDC）。实现直流电源信号的故障注入和电气性能分析。

（5）探针故障注入单元（IceBlade-PROBE）。实现探针方式对线路板硬件的故障注入和电气性能分析。

2 系统的软件结构

故障注入单元的软件包括 IceBlade API、各故障注入单元的控制面板和故障注入主控软件。其中 IceBlade API 提供进行二次开发的接口，支持在 Windows 环境下对各故障注入单元的控制；故障注入面板提供设置和控制系统硬件的界面接口。系统支持自动运行和可编程的故障注入方案，可根据需要进行设置后实现无人值守运行，并对感兴趣的节点进行录取。故障注入主控界面显示所有故障注入单元的运行状态信息，并可以综合不同类型故障注入单元的设计，实现集成化的故障测试控制。

3 功能特点

IceBlade 故障注入系统可对航电系统的不同层面实施故障注入，包括：

（1）提供对各个总线类型和接口信号以及总线和接口的电气层信号的观察和录取功能。

（2）IceBlade-Probe 探针故障注入单元可以对 PCB 板上的逻辑电路实现故障注入，模拟存储器和接口电路逻辑故障。

（3）可以模拟直流电源系统的故障，包括电压幅度、负载能力、纹波变化等异常现象。

（4）对于各种接口信号，提供物理层的故障注入能力，可模拟信号电缆可能发生的断路、阻抗变化和信号噪声等传输问题。

（5）针对 MIL-STD-1553B、AINC429、RS232、RS422 等通信总线，实现电气层、协议层和应用层的故障注入。

（6）可对模拟量信号、数字 TTL/LVTTL 信号、隔离 I/O 信号实现电气层和应用层的故障注入。

IceBlade 提供多种控制模式，以实现故障注入操作的灵活性。控制模式包括：

（1）支持仪表工作方式，可以使用设备上的键盘和显示屏进行操作。

（2）支持手动和自动 2 种故障注入模式，提供外部触发功能。

（3）提供系统级故障控制软件，用于实现不同接口类型故障的统一调度和控制。

（4）提供 FireBlade 仿真测试平台的软硬件接口，可以实现与被测系统及其调试环境的互动。

（5）提供 API 接口（应用程序编程接口），支持二次开发。

（6）各故障注入单元可以协同工作，也可以独立运行。

结束语

目前，在航空器的设计中，健壮性和可维修性越来越多地受到人们的重视，故障检测、故障定位等功能需要更全面的故障注入手段进行测试保障。这一方面对技术手段提出了更高的要求，另一方面也需要研发和测试人员不断积累知识，在实践过程中总结更多的经验，进一步建立和完善相关的技术规程。

（责编 小颖）