

综合通信导航识别系统的故障注入方法研究

王 涛, 朱会柱, 吴 敏, 刘 龔

(中国航空无线电电子研究所, 上海 200241)

[摘 要] 针对综合通信导航识别系统的综合化、模块化特点, 在综合分析系统故障检测诊断机制、构建系统故障信息库的基础上, 设计了一种面向综合通信导航识别系统的软件故障注入方案, 可提高综合通信导航识别系统故障诊断软件的效能。通过利用此方案进行故障注入试验, 验证了综合通信导航识别系统故障诊断软件的功能和性能。

[关键词] 综合通信导航识别系统; 故障诊断系统; 故障注入

[中图分类号] TP277.3 [文献标识码] A [DOI 编码] 10.12175/j.issn.1006-141X.2020.01.08

[文章编号] 1006-141X(2020)01-0045-05

Research of Fault Injection in Integrated Communication Navigation and Identification System

WANG Tao, ZHU Hui-zhu, WU Min, LIU Yan

(China National Aeronautical Radio Electronics Research Institute, Shanghai 200241, China)

Abstract: Aiming at the integration and modularization character of the integrated communication navigation and identification system, based on the analysis of the fault detection and diagnosis mechanism, with building the fault information database of the integrated communication navigation and identification system, a scheme of software fault injection geared to integrated communication navigation and identification system is designed. The scheme will enhance the performance of the system diagnosis software in integrated communication navigation and identification system. By applying the scheme to fault injection test, the functionality and performance of diagnosis system in integrated communication navigation and identification system are verified.

Key words: integrated communication navigation and identification system; diagnosis system; fault injection

0 引言

通信导航识别(CNI: Communication Navigation and Identification)系统是机载航电系统的重要组成部分。随着软件无线电技术的发展和航电系统架构的演进, 联合式架构已发展为高度综合化架构。系统综合性越来越强, 复杂度越来越高。与传统的分

立式、联合式设备硬件资源相比, 综合 CNI 系统通过采用综合化、模块化、数字化技术, 具备多任务、多功能、多状态, 不同功能所需的硬件资源集成到一个模块中, 一个模块可能同时支持几个功能运行, 这种变化带给系统更多的故障模式, 增加了故障诊断的复杂性。

故障诊断技术发展至今主要分三类: 基于信号

处理的方法、基于解析模型的方法和基于知识的诊断方法。前两种方法需要建立精确复杂的数学模型,定量分析故障状态特征参数,在工程实践中较难实现。随着计算机技术的发展和人工智能技术的兴起,基于知识的诊断方法引起广泛的研究和关注,继而发展出专家系统故障诊断方法、模糊故障诊断方法、故障树故障诊断方法、神经网络故障诊断方法和信息融合故障诊断方法等故障诊断方法理论。目前机载领域的故障诊断技术发展趋势是将机载各系统的机内自测试(BIT: Build-in-Test)信息与系统状态数据信息相结合,实现系统实时故障诊断与维护的综合化、智能化和网络化。

综合 CNI 系统进行了 BIT 设计,它分为模块级自检和系统级故障诊断两部分,以提高系统自身故障检测和故障隔离能力。模块级自检检测模块内部故障;系统级故障诊断由故障诊断系统软件完成,进行故障识别、故障定位、故障隔离,使得系统具备进一步故障处理(如重构、启用备份、降级管理、记录、上报)能力,可大大提高综合 CNI 系统的可靠性,缩短维护时间,提高维护效率。

系统级故障诊断是综合 CNI 系统测试设计中的重要组成部分,故障检测、诊断能力直接影响系统的可靠性,有必要通过人为故障注入的方式对其进行功能性能的验证。

故障注入技术是验证综合通信导航识别系统测试性设计的重要测试手段,传统的硬件故障注入有其优点和局限性。硬件故障注入方式通过直接短路或断开元器件管脚、改变电路板焊接点、外接开关电路、更换元器件等引入额外的硬件方式实现故障注入,这种方式的优点是注入的故障接近实际情况,能够较好地模拟实际的硬件故障,试验过程中无需专门开发故障注入模型,但其不足在于试验装置复杂、费用高,并且难以精确控制故障注入的时间和位置,对目标系统硬件容易造成损伤等。另外,这种方式无法模拟所有的故障特别是由于软件引起的故障。

软件故障注入是根据一定的故障模型,通过修改目标系统的总线数据或内存来模拟系统硬件或软件故障的发生。此方法灵活方便,易于实现,应

用成本低,对目标系统的硬件环境没有损坏。缺点是不能够将故障注入到软件不可访问的位置。

美国、法国、德国、英国等国家有不少高校和研究部门从事故障注入的研究工作,取得了较多的成果,处于国际领先地位。如在源代码中加入故障注入程序,通过外部请求响应方式产生故障的 FIAT 故障注入器;采用软件陷阱,通过在适当位置捕获被注入程序,从而产生故障和错误的 FERRAY 故障注入方法;采用定时中断和陷阱触发故障,及修改代码注入故障的 DOCTOR 方法;利用超大规模集成电路的测试扫描链的测试访问入口注入故障的 FIMBUL 方法;基于文本模型而实现的 FTT-1 故障注入工具等。

本文设计了一种面向综合 CNI 系统的系统故障诊断的软件故障注入方案,用于对系统故障诊断软件的功能性能进行验证。

1 综合 CNI 系统及其故障诊断机制

1.1 综合 CNI 系统简介

综合 CNI 系统按照 IMA 硬件体系架构,以标准化的模块实现各个功能单元,将功能相近或者相同的资源模块进行功能分区,划分为孔径综合、射频综合、数字综合三个分区,如图 1 所示。

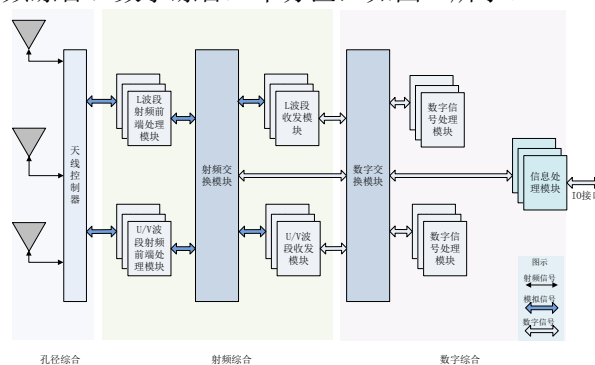


图 1 综合 CNI 系统示意图

其中,孔径综合分区完成射频接收和发射功能,采用宽带天线设计,多个波形可共用一个天线,可以有效减少天线数量。

射频综合分区可提供多个射频收发通道,以满足不同波段或同一波段的多个波形的射频信号处理需求。主要完成模拟信号与中频数字信号之间的转换功能:接收时,将来自宽带天线的信号经过

射频前端的预处理、下变频、A/D 采样、数字预处理后, 将中频数字信号发送到通用数字信号处理资源进行处理; 发射时, 将来自通用数字信号处理资源的数字化中频调制信号经过 D/A 转换、上变频、射频前端预处理后由天线发射。

数字综合分区由通过 RapidIO 数字交换网络连接的数字信号处理模块和信息处理模块组成: 其中数字信号处理模块由高性能的现场可编程门阵列 (FPGA: Field Programmable Gate Array) 和数字信号处理器 (DSP: Digital Signal Processor) 构成数字信号处理通道, 能通过加载代理实现波形组件在数字信号处理资源上的动态重构; 信息处理资源由高性能 CPU 组成, 负责完成所有波形与外部系统的数据交互、波形信息解析、封装以及完成波形组件在信号处理资源上的分配、部署, 控制波形组件的运行, 通过数字交换网络收集系统内部各模块的健康状态信息, 完成对系统的故障诊断、故障处理等功能。

1.2 故障诊断机制设计

综合 CNI 系统参照 ASAAC (Allied Standard Avionics Architecture Council) 规范, 将系统划分为综合区域级 (IA : Integration Area) 和资源级 (RE: Resource Element), 如图 2 所示。IA 级模块驻留模块健康管理软件和系统故障诊断软件, 除了负责本模块的健康状态监控和故障处理也负责整个系统的健康状态监控和故障处理, RE 级模块驻留模块健康管理软件, 仅负责本模块的健康状态监控和故障处理。

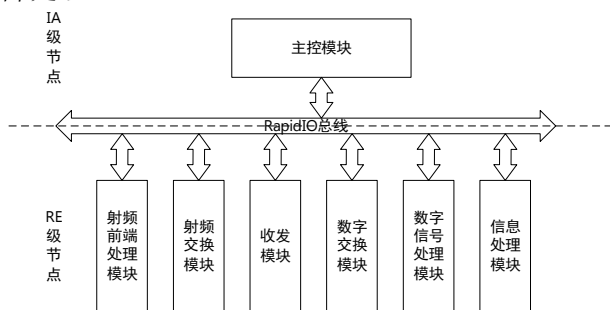


图 2 故障诊断网络示意图

系统运行过程中的故障诊断机制由模块级故障检测和系统级故障诊断两部分组成, 如图 3 所示。

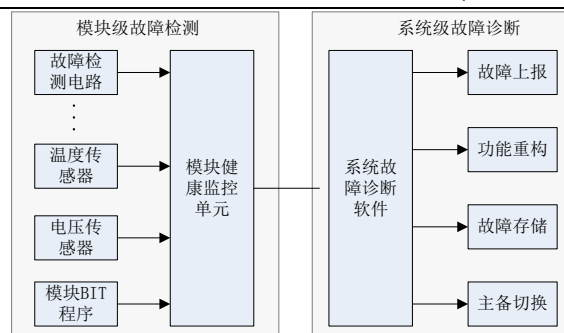


图 3 故障诊断机制示意图

其中模块级故障检测由射频前端处理模块、射频交换模块、收发模块、数字交换模块、数字信号处理模块和信息处理模块的 BIT 自检功能实现, 通过自检电路 (通常不超过模块电路规模的 20%) 或者利用运行于模块内部数字器件的 BIT 程序, 在系统运行过程中能够实现对模块内部核心元器件、通信链路、软件运行状态的监控, 故障信息与状态信息由模块内部的健康监控单元统一收集并上报, 每个模块均应支持上电 BIT、周期 BIT 和维护 BIT。故障诊断由运行于信息处理模块的系统故障诊断软件完成, 实现故障过滤、故障定位和故障隔离, 并进行故障处理。

综合 CNI 系统的故障诊断流程如图 4 所示。各模块在系统上电启动后, 开始进行上电 BIT 检测, 然后转入正常运行过程中的周期 BIT 检测, 检测到故障信息后, 通过数字交换网络主动发送给信息处理模块的系统故障诊断软件。系统故障诊断软件接收到各模块的故障信息后, 经分析处理后, 将故障定位和隔离到某一个或某几个模块, 将故障信息和对应的告警信息实时上报给航电系统, 并将故障信息以日志的方式存储在信息处理模块的存储器内, 在维护时由维护人员从存储器读取, 方便排故使用。如果故障信息满足主备切换的条件, 进入主备切换的流程, 将故障的模块切换到备用的模块。如果故障信息满足自动重构的条件, 进入自动重构的流程, 将故障模块上运行的波形重新加载到正常的模块上, 恢复波形功能。

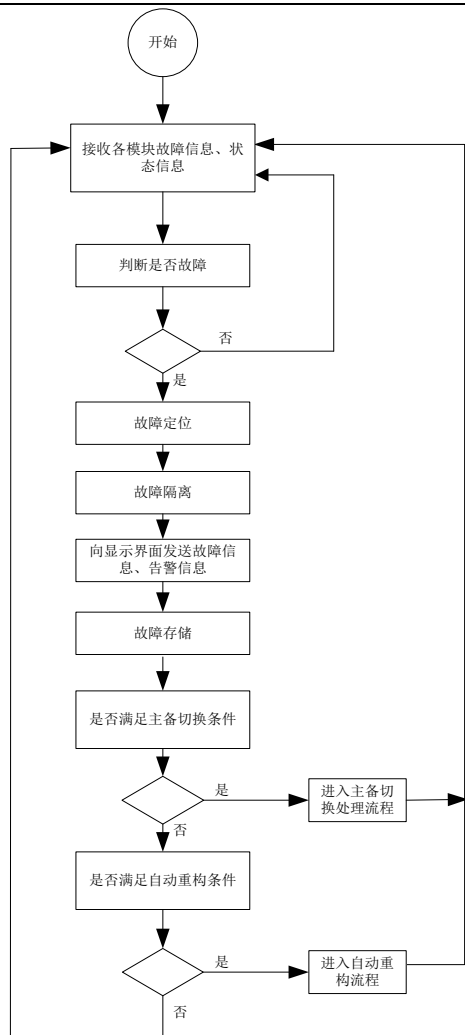


图 4 故障诊断流程图

2 故障注入方案设计

2.1 系统故障信息库设计

对于图 1 所示的综合 CNI 系统，在设计阶段采用故障树分析（FTA: Fault Tree Analysis）和故障模式及影响分析（FMEA: Failure Mode and Effect Analysis）可靠性工程的理论和方法，综合分析导致设备出现故障的各种因素及可能发生的故障模式对系统产生的影响。对系统各模块可能发生的故障信息进行分析与统计，在模块验收测试时进行模块 BIT 设计的验证，以确保故障信息的完整性、准确性与可验证性。将统计与验证后的故障信息纳入系统故障信息库，作为系统测试性试验的样本故障注入。故障信息库内容包含模块上报的故障信息内

容及其故障代码，故障诊断系统软件上报给显示界面的故障信息内容及代码，后一种上报显示的信息应与模块内部上报的故障信息对应。故障信息库的内容如表 1 所示。

表 1 故障信息库内容示例				
模块	模块上报故障信息及故障代码		故障诊断系统软件上报故障信息及代码	
信息处理模块	CPU 故障	0x0101	信息处理模块故障	a1
	FC 子卡故障	0x0102		
	DDR 故障	0x0103		
	...	...		
数字信号处理模块	FPGA 故障	0x0201	信号处理模块故障	b1
	SRIO 链路故障	0x0202		
	DSP 故障	0x0203		
	...	...		

2.2 故障注入点分析

图 3 所示的综合 CNI 系统的系统故障诊断软件通过数字交换网络接收各个模块自检检测上报的故障信息及状态信息，对系统的健康状态进行在线监测，依据故障信息库将故障信息上报用户显示界面，为用户提供故障分析和诊断结果。因此可在交换网络总线采用软件故障注入的方法，人为注入故障信息库各模块内部可能发生的故障信息对应的故障代码，发送给信息处理模块，以此观察故障诊断系统软件是否能够按照系统测试性设计准确进行故障诊断和处理，如图 5 所示。

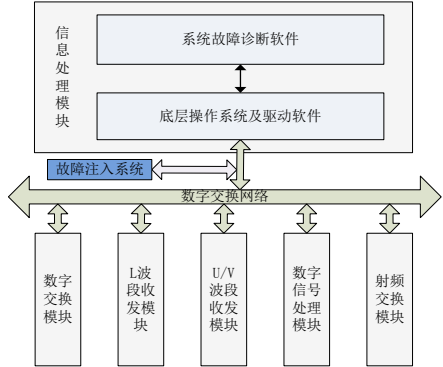


图 5 故障注入点示意图

2.3 故障注入系统设计

本方案的故障注入系统由用户操作界面和驻留于信息处理模块的故障注入软件两部分组成，用户操作界面和故障注入软件通过以太网通信，如图 6 所示。其中用户操作界面提供根据故障信息库定

义的故障模式选项,通过选择不同的故障模式,将模拟的故障信息发送给故障注入软件,然后由故障注入软件通过数字交换网络总线发送给系统故障诊断软件。故障诊断软件接收到故障信息后,进行相应的处理,通过以太网接口反馈给用户操作界面。用户操作界面根据故障信息库对比故障注入信息和反馈的结果,做出评估。

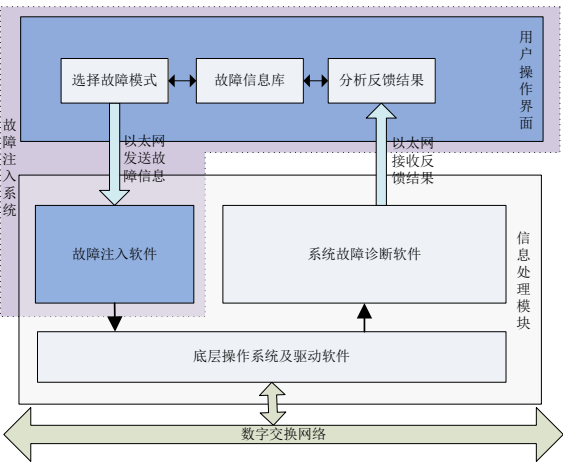


图 6 故障注入系统示意图

3 故障注入方案验证

本文通过软件注入,观察综合 CNI 系统系统故障诊断软件的功能(包括故障定位、故障隔离)和性能(包括故障检测率、故障覆盖率)两个方面的指标,从而实现对软件注入方案的验证。

根据第 2 章节提出的软件故障注入方案,将故障注入系统的用户操作界面运行于工控机,启动目标待测系统,运行故障注入软件和系统故障诊断软

件,将待测系统总共 26 个模块的 282 个故障信息进行了故障注入,覆盖率 100%。在用户操作界面观察系统故障诊断软件的故障定位和隔离的反馈结果,并进行统计分析,故障检测率能达到 100%。

表 2 示出的是采用软件故障注入方案与传统的硬件注入方法的指标对比。由表 2 可见,传统的硬件注入方式在覆盖率和检测率方面存在明显的不足,主要是软件故障无法模拟,部分模块的 BIT 检测达不到预期分析指标。

表 2 软件故障注入与硬件故障注入对比

故障注入方法	样本总数	可模拟总数	可检测数量	覆盖率	检测率
软件故障注入	282	282	282	100%	100%
硬件故障注入	282	256	218	90.7%	85.2%

4 结束语

本文针对综合 CNI 系统,设计了一种软件故障注入方案,对系统故障诊断软件的功能性能进行验证,保证了系统级故障诊断的可靠性和稳定性,从而提高系统的可靠性与维护性。经过实验验证,此方案是有效的,达到了预期效果。

随着软件无线电技术的发展与应用,在综合 CNI 系统中软件扮演的角色越来越重要,软件的测试性和可测试性设计也是这种复杂系统装备测试性应纳入考量的范围。今后的系统测试性设计应从软硬件综合设计的角度出发,使软硬件测试手段相辅相成,才能对系统全面的测试。

参 考 文 献

[1] 李佳亮. 故障注入技术与展望[J]. 机械工程师, 2016, 8:83-85.
[2] 吴敏, 常坤, 李裕. 基于功能分区的综合通信导航识别系统设计[J]. 航空电子技术, 2013, 44(2):4-9.
[3] 李志宇, 黄考利, 连光耀. 基于测试性设计的软件故障注入研究综述[J]. 计算机测量与控制, 2013, 21(5): 1112-1114.
[4] 刘少伟, 郑文荣. BIT 技术发展与应用研究[J]. 理论与方法, 2011, 30(5): 23-25.
[5] GJB8895-2017 装备测试性试验与评价[S]. 2017.
[6] 佟向鹏, 王文凤. 基于故障注入的系统测试方法及应用[C]. 2013 年首届中国航空科学技术大会论文集, 2013.

[收稿日期] 2019-11-29