

doi: 10.7690/bgzd.2025.08.022

基于故障注入的航天电气系统流程仿真技术

孙 凯, 魏炳翌

(北京航天自动控制研究所, 北京 100854)

摘要: 针对目前航天电气系统流程设计多依靠其基本规律及专家经验, 尚无数字化设计、仿真工具的问题, 提出基于故障注入的航天电气系统流程仿真技术。采用设计、仿真一体化的技术, 简化复杂流程建模, 加速仿真系统的搭建与仿真分析过程。通过分析电气系统的典型故障模式, 完成系统架构、功能建模、故障溯源和影响分析, 设计基于故障注入(fault injection, FI)的平台体方案; 针对运载火箭发射流程实例, 完成系统电源和通信 2 类典型故障并进行故障注入仿真测试和分析。实践结果表明: 该平台为航天电气系统流程方案验证、可靠性分析、故障分析提供了信息化手段及创新理念, 可适应未来更加复杂的航天系统工程任务。

关键词: 故障注入; 航天电气系统; 流程; 仿真技术

中图分类号: TM74 **文献标志码:** A

Process Simulation Technology of Aerospace Electrical System Based on Fault Injection

Sun Kai, Wei Bingyi

(Beijing Aerospace Automatic Control Research Institute, Beijing 100854, China)

Abstract: Aiming at the problem that the design of aerospace electrical system mostly depends on its basic law and expert experience, and there is no digital design and simulation tool, the aerospace electrical system flow simulation technology based on fault injection is proposed. The technology of integration of design and simulation is used to simplify the complex process modeling and accelerate the process of building simulation system and simulation analysis. By analyzing the typical failure modes of the electrical system, the system architecture, function modeling, fault tracing and impact analysis are completed, and the platform scheme based on fault injection (FI) is designed. Aiming at the launch process example of the launch vehicle, two typical faults of the system power supply and communication are completed, and the fault injection simulation test and analysis are carried out. The practical results show that the platform provides information technology and innovative ideas for the verification of aerospace electrical system process scheme, reliability analysis and fault analysis, and can adapt to more complex aerospace system engineering tasks in the future.

Keywords: fault injection; aerospace electrical system; process; simulation technology

0 引言

航天事业持续多年高速发展, 探月工程、载人空间站、火星探测等国家重大科技专项和重大工程的顺利实施, 标志着我国在重点领域取得的突出成就。随着航天任务日益向高可靠、低成本、时间周期短的方向发展, 传统的科研模式已经无法适应。目前, 航天研制方案设计与仿真验证是串行研制的模式, 设计部门给出硬件、软件需求至生产单位、软件开发人员手中, 需要等待样机及软件生产出来后才能进行仿真验证。随着验证的进行, 硬件软件的更改带来管理上的难点, 同时反复迭代导致工程研制周期时间成倍增加, 容易引发质量问题^[1]。同时, 故障信息与航天各分系统、单机及元器件互相独立, 仅能以人工形式进行检索和关联, 无法实现

故障的自动追溯。

现阶段, 故障分析与故障处理的有效性与正确性需要在系统方案设计完成后, 通过原理样机测试与试验进行验证, 难以进行早期的系统级仿真验证。采用故障注入(FI)的仿真技术^[2], 在确定故障模型的基础上尽可能地模拟真实系统运行时发生的故障, 通过人为手段直接将故障注入至待验证的系统中, 从而验证系统方案设计过程中安全性、兼容性、可靠性。运载火箭等飞行器控制系统设计过程中涉及到箭上计算机与平台、惯性组合、陀螺、伺服机构等敏感器、执行器的通信拓扑方案, 飞行器飞行过程中执行的程序流程^[3]。

基于仿真的故障注入提高了故障注入的时间效率, 解决了基于模拟的故障注入时间长的问题, 但是比较依赖建模的准确性。目前国内航天领域尚无

收稿日期: 2024-09-16; 修回日期: 2024-10-26

第一作者: 孙 凯(1989—), 男, 山西人, 硕士。

电气系统流程设计、仿真工具，对于流程的设计主要是依靠设计师的工程研制经验，迫切地需要复杂系统工程电气系统流程设计、仿真验证、可靠性分析等方面工作的数字化软件工具^[4]。

笔者基于航天电气系统流程的设计仿真平台将系统时序流程分解为硬件拓扑网络、单机设备流程、可故障注入流程步 3 个部分进行建模，将故障信息在具体时序流程步中进行表达。同时，在航天电气系统流程仿真系统的基础上，进一步设计了基于故障注入技术的设计仿真系统。通过模块化的流程搭建，对航天电气系统不同功能架构下的不同故障模式进行可视化建模。将故障模式、系统架构、单机设计与故障信息进行互联，以实现故障影响的动态溯源，大幅提升对电气系统通信拓扑、流程编排的协同设计能力及可持续创新能力。最后，利用系统单机设备流程泳道图的形式直观表达故障过程并进行动态仿真，在系统早期暴露出系统流程设计的不合理性，及时识别故障风险。

1 航天电气系统流程设计仿真平台设计

航天电气系统流程设计与仿真技术的需求为实现不同流程在实际系统中的不同软件、硬件设备在整个飞行器飞行/测试过程中的动作与步骤^[5]，包括硬件通信网络设计、通信协议设计、流程模型的生成、加载、配置、仿真和管理等功能，具备设计与仿真错误提示与纠错能力，并能通过拓扑图的形式可视化呈现，从而在模拟飞行/测试过程中对系统流程设计方案进行评估。图 1 展示构成航天电气系统流程设计与仿真平台的各类要素的逻辑关系。

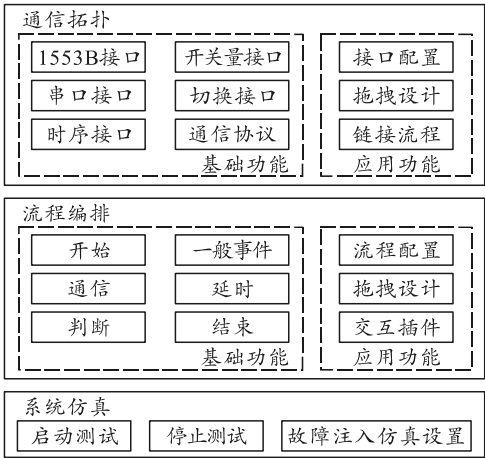


图 1 仿真平台

航天电气系统流程设计与仿真平台主要包含 3 大功能：1) 通信网络拓扑设计功能；2) 流程编排设计功能；3) 系统仿真功能。实现航天电气系统的

硬件搭建，流程编排顺序、各类参数设计及全系统仿真。通信拓扑及流程编排功能描述如表 1 和 2 所示。

表 1 通信拓扑功能描述

分类	内容	功能描述
设备	拓扑大小	用于调整模块界面大小
	接口列表	对接口类型、编号、通道数进行显示
1553B 接口	接口编号 通道号 子网/总线	对接口编号、通道号、子网、总线进行显示
串口接口	连接信息 信号方向	对连接信息、信号方向进行显示
时序/开关量接口	连接信息 信号方向	对连接信息、信号方向进行显示

表 2 流程编排功能描述

分类	内容	功能描述
开始	启动方式 启动开关	实现流程开始功能，设置流程开始启动方式、启动开关
一般事件	表达式	对流程中的数据进行处理
通信	1553B 接口	对 1553B 接口进行配置,包括 BC/RT 状态, RT 地址设置等
	1553B 数据传输	对 1553B 数据进行传输设置,包括 RT 子地址设置, 通信协议选择、数据内容设置等
	时序/开关量传输	对时序/开关量内容进行设置,包括逻辑 0, 逻辑 1, 上升沿, 下降沿等
	时序/开关量状态清除	对时序/开关量现有状态进行清除
	串口接口	对串口进行配置,包括接口形式,波特率、数据位等
延时	串口数据传输	对串口数据进行传输设置,包括通信协议选择、数据内容设置等
	延时时间	对延时时间进行设置
判断	判断模式 判断内容	对判断模式、判断内容进行设置
结束	/	实现流程结束功能

通过采用设计、仿真一体化的技术，简化复杂流程建模，加速仿真系统的搭建与仿真分析过程。将系统设计文件由静态图纸转化为虚拟系统。通过设计与仿真验证一体化的模式能够解决传统的、只能在系统实物交付后再进行验证的低效率问题。

2 基于故障注入的平台方案设计

2.1 故障模式分析

针对笔者所提基于故障注入的航天电气系统流程仿真平台要完成对研制航天电气系统流程进行模拟故障注入，因此平台设计的通用性是设计时要考虑的重点，从而模拟出飞行器在飞行/测试过程中的故障情况。针对飞行器控制系统计算机、平台、惯性组合、导引头、伺服机构、电缆网等设备硬件或软件故障。对各个设备的故障模式进行分析，以飞

行器/火箭系统常见硬件故障为例^[6-9], 如表 3 所示。

表 3 系统典型故障模式分析

故障模式		故障原因	故障影响
计算机	短路	供电电路某点出现短路	部分器件无法稳定工作
	断路	供电电路某点出现断路	整个系统或部分模块无法工作
	纹波故障	在直流电源耦合各种交流成分	部分器件无法稳定工作
	信号叠加	通道切换异常	通信数据失真或通信故障
	信号替换	时钟异常	通信数据失真或通信故障
	速率故障		
	5V/28V/三相电源无输出	二次电源故障	整个系统或部分模块无法工作
	陀螺仪无输出	陀螺仪故障	陀螺仪数据异常
惯性组合	加速度计无输出	加速度计故障	加速度计数据异常
	信号放大器无输出	再平衡放大组合故障	陀螺仪、加速度计数据异常
	A/D 转换故障	A/D 变换电路故障	陀螺仪、加速度计数据异常
	综合放大器故障	电子元件失效或电路故障	整个系统或部分模块无法工作
伺服机构	伺服阀故障	喷嘴、节流孔堵塞	整个系统或部分模块无法工作
	作动器故障	活塞卡死	整个系统或部分模块无法工作
	反馈电位计故障	反馈电位器烧毁	整个系统或部分模块无法工作
电缆网	短路	电缆网某处短路	整个系统或部分模块无法工作
	断路	电缆网某处短路	通信故障或整个系统或部分模块无法工作

根据上述故障模式分析, 需要建立可故障注入的流程步, 包括开始、一般事件、1553B 通信、串口通信、时序开关量、延时判断中加入故障模式。笔者设计故障注入模式主要针对单机设备供电、数据通信及设备失效类型的故障^[10]。

针对系统软件错误按照程序造成的影响可以将软错误影响分为数据流错误和控制流错误 2 大类。数据流错误主要是软错误发生在各设备数据存储位置错误的数据在飞行控制/测试过程中不断传播, 从而对系统运行造成影响; 控制流错误是指程序未按照正常的软件流程分支进行执行, 运行过程中进行了错误跳转, 从而对系统运行造成影响。系统软件错误需要按照故障类型进行针对性设计。

2.2 系统架构与功能建模

根据技术指标和各设备常见故障模式分析, 针对软件和硬件故障, 对航天电气系统流程仿真进行故障注入, 且故障注入具备使能开关, 可设置故障注入时间点, 注入类型包括:

1) 流程步停止故障, 使该流程步无法执行, 模

拟计算机断路/短路、伺服机构综合放大器等故障造成的部分模块无法工作;

2) 链路中断故障, 使该流程无法通信, 模拟电缆网断路、计算机信号叠加等造成的数据通信故障;

3) 数据错误故障, 可以在通信的数据设置校验和错误, 程序在产生数据发送前或收到数据处理前, 修改数据中额校验和字段, 模拟各个设备软件的数据流错误;

4) 设备终止故障, 使该设备对应的所有流程均停止, 模拟惯性组合二次电源故障、计算机断路/短路等故障造成整个系统无法工作。

其余故障均可通过各个流程步及交互按键的组合进而实现, 系统软件的控制流错误, 可以通过按键设置流程执行至判断流程步时跳转另外的分支或直接结束。针对单机设备供电故障, 可以通过按键设置该设备对应的流程直接结束进行模拟。对于系统故障注入仿真时, 故障流程步的故障处理可以选择不处理继续向下执行或者停止流程步。

2.3 故障溯源与影响分析

在完成了故障模式分析、系统架构与功能建模后, 为进一步对故障进行溯源及影响分析, 需要利用系统仿真平台对故障相关元素建立模型间的关联^[11]。

通过航天电气系统流程设计仿真平台设计建立了从系统硬件网络拓扑至单机设备流程及单个流程步间的关系。在系统故障注入仿真完成后, 针对单个系统功能的故障问题, 在每个故障单机的流程泳道图中涉及到的故障流程步均会由灰色变为黑色。在单机设备对应的开始流程步中对应了仿真停止的时间, 通过故障流程步的时间先后, 定位故障位置, 准确快速地确定故障与功能间的溯源关系。

每个潜在的故障均与单机或部组件的失效相关联, 流程仿真与硬件通信拓扑表达了软件部分与硬件功能故障的对应关系, 实现了底层故障信息向更高层功能故障信息的传递。通过系统硬件网络拓扑及流程泳道图中故障单机的数量、对应单机流程的故障流程步数量, 直观地看出该故障影响的功能数量, 确定故障模式影响范围。

相比于传统文档形式的传递, 通过可视化的表达形式更加直观地判断出故障点与影响, 由于流程仿真模型的唯一性, 在此基础上进行方案设计更改, 相关的故障溯源及影响均会在仿真后实时同步, 实现故障的动态追溯与仿真结果生成。

3 系统实例测试与分析

航天电气系统流程设计与仿真平台采用基于 Python 与 QT 相结合的环境进行开发,对运载火箭发射流程的典型模型设计了仿真实例。运载火箭箭上设备包括控制组合 1、控制组合 2、惯性组合、伺服机构 1、伺服机构 2、液氢液氧发动机、分离开关,地面设备包括地面计算机、显控设备、电源 1、电源 2^[12]。

通信网络拓扑设计中包含了 1553B 总线通信接口、422 串口通信接口、时序/开关量接口,1553B 总线通信接口包含箭上 1553B 总线及箭地 1553B 总线。其中,实线框代表设备,虚线框代表 1553B 总线,灰色及线条代表 1553B 板卡及子线,箭上拓扑图如图 2 所示,地面拓扑图如图 3 所示。

针对每个设备设计了对应的流程,如图 4 所示。将运载火箭典型发射流程中各个设备间的信息流、时序流交互进行了流程编排,以泳道图的形式呈现。以箭上控制组合 1 为例,在地面计算机控制打开电源 1 后,控制组合 1 流程开始执行,依次完成对箭上 1553B 接口初始化,循环接收地面计算机发送的点名自检指令,收到后每间隔 1 s 发送上电自检指令到惯性组合、伺服机构 1、伺服机构 2,发送完自检指令后向液氢液氧发动机发送点火时序,

并开始接受各个设备的数据,延时 50 s 后,向分离开关发送分离时序,延时 100 s 后结束控制组合 1 的流程。

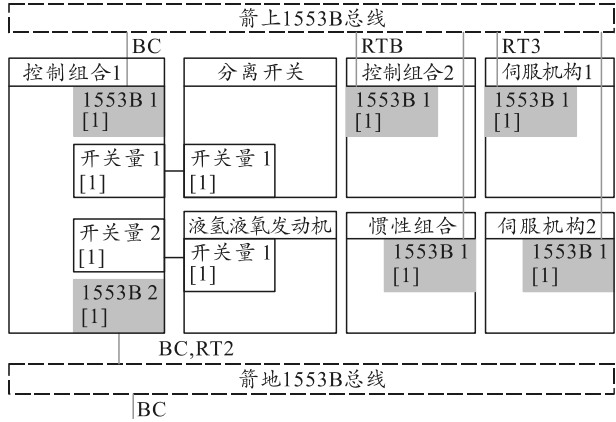


图 2 运载火箭发射流程箭上通信拓扑

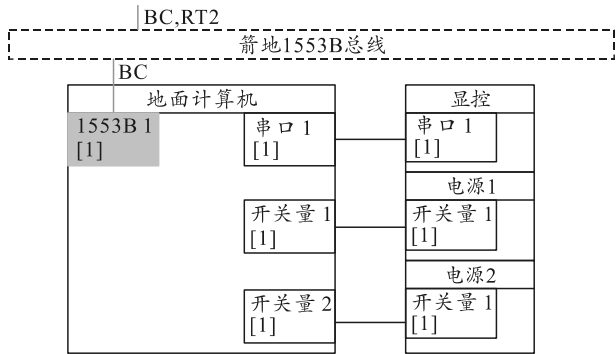


图 3 运载火箭发射流程地面通信拓扑

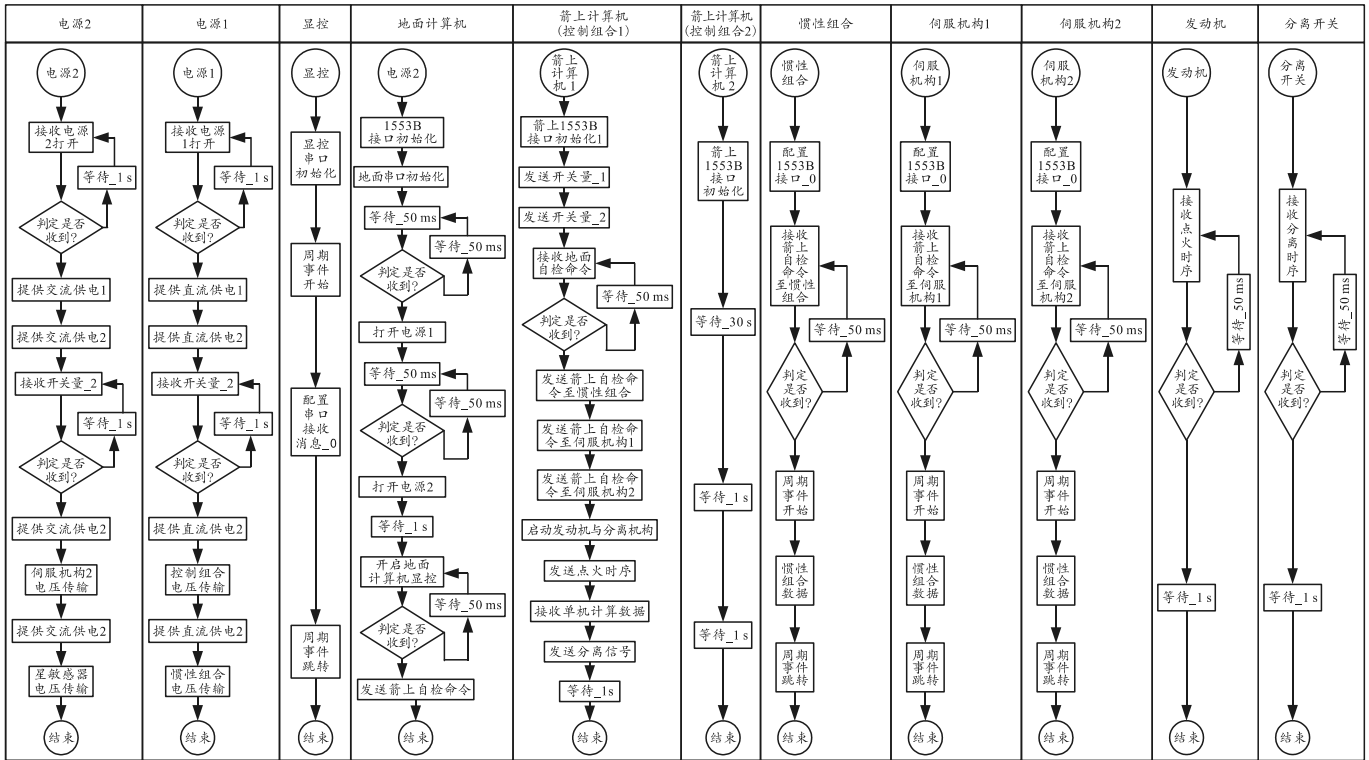


图 4 运载火箭典型发射流程泳道

3.1 电源故障注入测试

系统的电源故障包括计算机断路、惯性组合二次电源故障等。以控制组合 1 出现断路故障为例，在控制组合 1 发送点火指令后出现电源故障进行系统流程仿真如图 5 所示，控制组合 1 流程仿真细节如图 6 所示。

其中流程灰色表示已经正确执行完，黑色表示流程执行错误，从图 5 可以看出：故障发生后控制组合 1、分离开关流程受到影响，其中控制组合 1 的延时流程步报红且无法向下执行，分离开关流程还未开始执行，所以定位故障发生在控制组合 1。从图 6 可以看出：控制组合 1 的时序控制主流程影响的后续流程步包含收单机计算数据、延时、发送分离信号，与控制组合 1 的时序控制主流程相关的收单机计算数据副流程也无法向下执行，从而确定故障发生位置及影响范围。

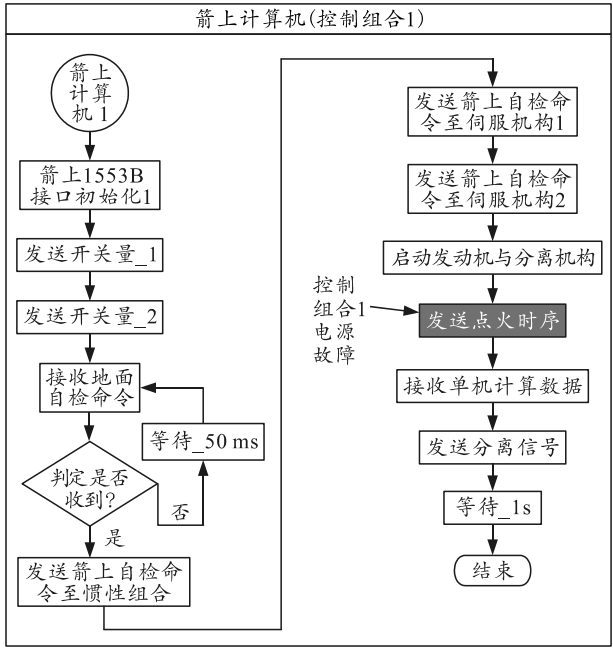


图 5 控制组合 1 电源故障流程仿真(局部)

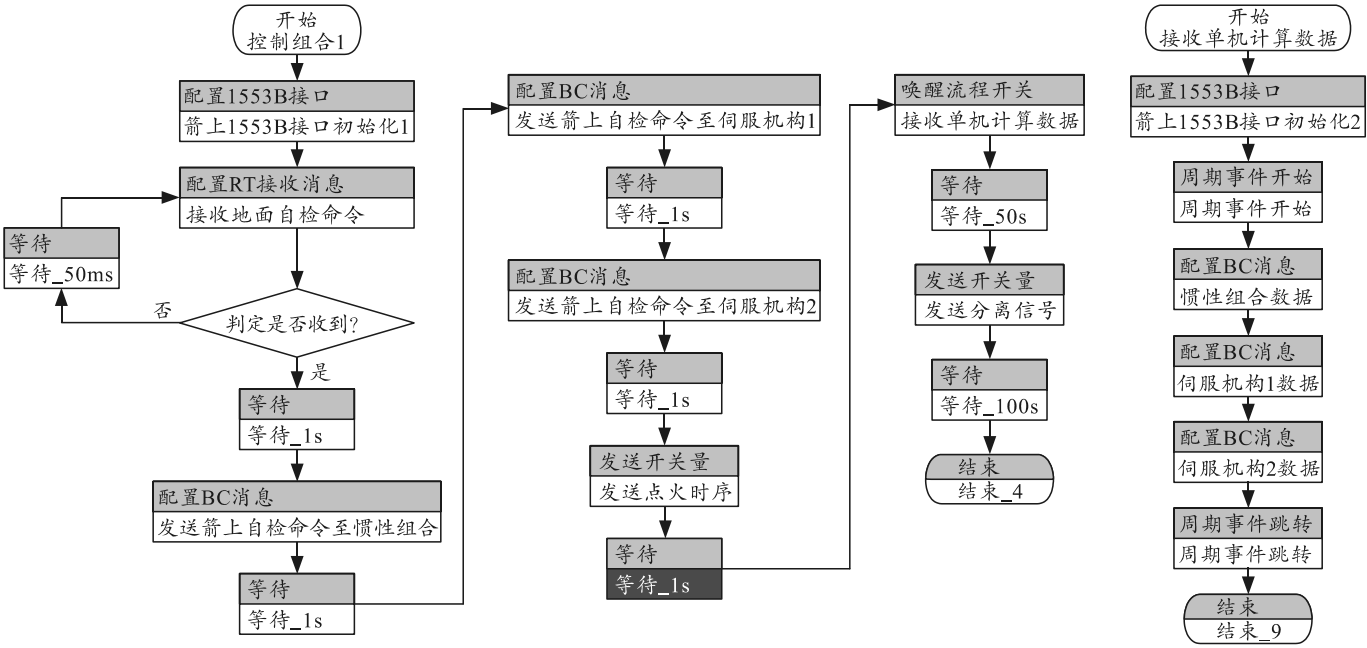


图 6 控制组合 1 流程仿真细节(局部)

表 4 是控制组合 1 单机设备流程仿真测试结果，展示了运载火箭发射流程各个设备相关流程时的开始时间、结束时间、执行时间、执行状态及变量变化。由表 4 可以看出：在在控制组合 1 上电 14.372 s 时发生了故障，控制组合 1 的延时流程执行失败，控制组合 1 流程无法继续向下执行。

3.2 通信故障注入测试

系统的通信故障包括计算机通信故障、伺服机构通信故障、电缆网断路故障等。以伺服机构通信故障为例，在控制组合 1 向伺服机构 2 发送自检命

令时注入通信故障进行系统仿真如图 7 所示，控制组合 1 与伺服机构 2 的总线通信流程出现故障，控制组合 1、伺服机构 2 流程仿真细节如图 8 和图 9 所示。

表 4 控制组合 1 电源故障仿真测试结果

序号	流程	开始时间/ms	结束时间/ms	执行时间/ms	执行状态
316	配置 BC 消息_3	133 62	133 67	5	成功
317	等待_10	133 67	143 67	1 000	成功
318	发送点火时序	143 67	143 72	5	成功
319	等待_11	143 72	143 72	0	失败

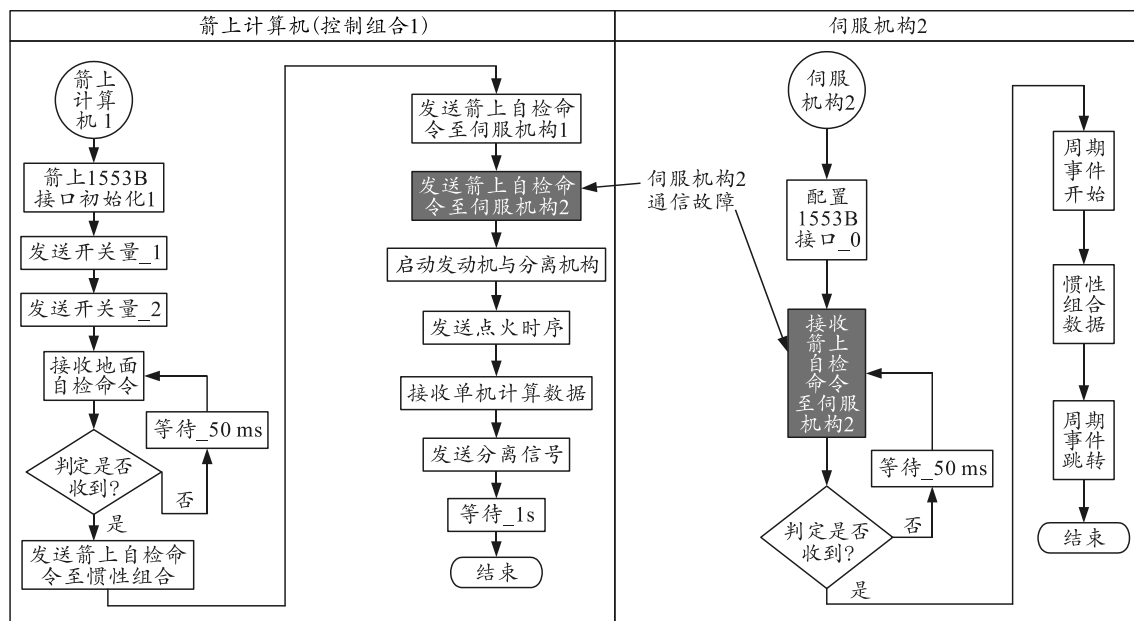


图 7 伺服机构 2 通信故障流程仿真(局部)

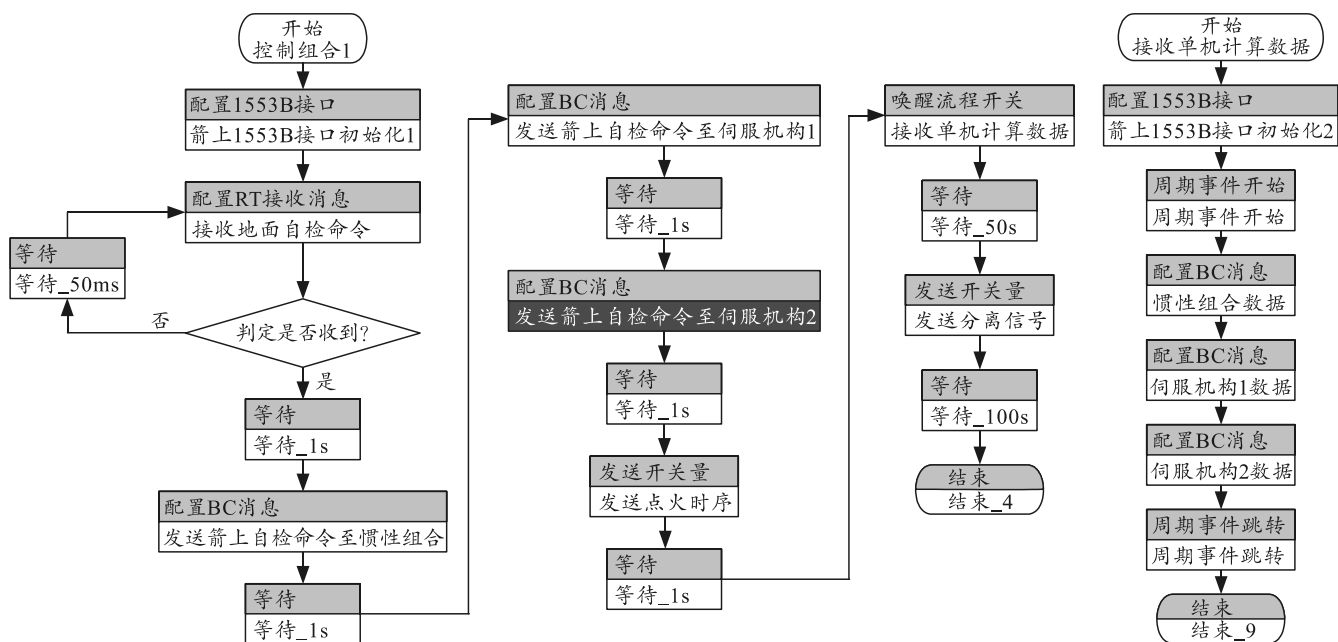


图 8 控制组合 1 流程仿真细节(局部)

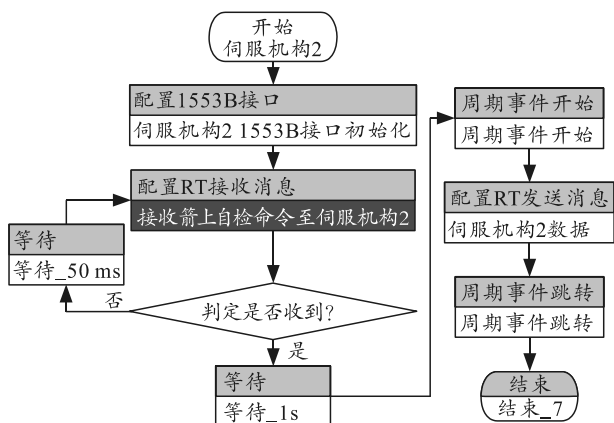


图 9 伺服机构 2 流程仿真细节(局部)

从图 7 可以看出,故障发生后控制组合 1、伺服机构 2、液氢液氧发动机、分离开关流程受到影响,其中控制组合 1 的发送箭上自检命令至伺服机构 2 流程步、伺服机构 2 的收箭上上电自检指令流程步报红且无法向下执行,液氢液氧发动机、分离开关流程还未开始执行,所以定位故障发生在在控制组合 1、伺服机构 2 间的通信。从图 8 和图 9 可以看出:控制组合 1 的时序控制主流程影响的后续流程步包含发点火时序、收单机计算数据、延时、发送分离信号,与控制组合 1 的时序控制主流程相关的收单机计算数据副流程也无法向下执行,伺服

机构 2 流程影响的后续流程步包含延时、发伺服机构计算数据，从而确定故障发生位置及影响范围。

表 5 和 6 是控制组合 1 和伺服机构 2 单机设备流程测试结果。由表 5 和 6 可以看出：在控制组合 1 上电 8.64 s 和伺服机构 2 上电 4.339 s 时，控制组合 1 与伺服机构 2 间的 1553B 通信发生了故障，控制组合 1 的发送箭上自检命令至伺服机构 2 流程与伺服机构 2 的接收箭上上电自检命令流程步执行失败，2 个单机设备流程无法继续向下执行。

表 5 伺服机构 2 通信故障测试结果

序号	流程	开始时间/ms	结束时间/ms	执行时间/ms	执行状态
213	发送箭上自检命令	862 5	863 0	5	成功
214	等待_8	863 0	863 0	0	成功
215	发送箭上自检命令	863 0	863 5	5	成功
216	等待_9	863 5	863 5	0	成功
217	发送箭上自检命令	863 5	864 0	5	失败

表 6 伺服机构 2 通信故障测试结果

序号	流程	开始时间/ms	结束时间/ms	执行时间/ms	执行状态
1	伺服机构 2	10	432 0	431 0	成功
2	伺服机构 2 1553B 接口初始化	432 0	433 9	19	成功
3	接收箭上自检命令至伺服机构 2	433 9	434 4	5	失败

4 结束语

在当前航天任务倍增、周期缩短、资源受限的情况下，航天电气系统采用的串行研制模式已经难以适应航天任务快速研制的需求。对系统流程进行故障注入仿真，能够在软件技术要求提出前验证软件任务书的正确性、流程与接口的匹配性，减少软件方案设计错误更改产生的时间。笔者针对当前电气系统流程方案设计时多依靠相关人员经验及无数化工具的现状，设计了航天电气系统流程仿真平台。同时，对基于故障注入的仿真平台设计及实现进行了介绍，通过分析电气系统的典型故障模式，设计了系统架构、故障建模、故障溯源和影响分析，

完成了平台的总体方案设计。在基于 Python 和 QT 语言开发的软件平台，针对运载火箭发射流程实例，完成系统电源和通信 2 类典型故障进行故障注入仿真测试和分析。试验结果表明，该平台对航天电气系统可靠性仿真测试和故障检测具有重要的研究意义和参考价值。

参考文献：

[1] 赵岩, 李佳, 解世禄, 等. 基于 MIL-STD-1553B 的运载火箭故障诊断与故障注入方法[J]. 计算机测量与控制, 2021, 29(9): 10-16.

[2] 董志腾. 面向复杂环境的软错误故障注入和检测技术研究[D]. 南京: 南京航空航天大学, 2021.

[3] 张宏德, 彭越, 徐利杰, 等. 运载火箭箭上电气系统基础架构研究[J]. 计算机测量与控制, 2022, 30(1): 147-153.

[4] 刘潇翔, 汤亮, 曾海波, 等. 航天控制系统基于数字孪生的智慧设计仿真[J]. 系统仿真学报, 2019, 31(3): 377-384.

[5] 夏云, 卢冀. 雷达数字化设计与仿真的技术体系架构研究[J]. 火控雷达技术, 2019, 48(2): 90-96.

[6] 李强, 吕克洪, 刘冠军, 等. 某型惯性测量组合故障传播机理与建模分析[J]. 测控技术, 2021, 40(2): 6-12.

[7] 陈兴根, 潘骏, 陈文华, 等. 电液伺服机构故障树分析[J]. 机电工程, 2009, 26(4): 25-27, 35.

[8] 张磊, 李伟刚, 陈红涛. 导弹伺服机构中电液伺服系统故障诊断方法研究[J]. 机床与液压, 2011, 39(15): 154-156.

[9] 牛亚峰, 沈怀荣. 航天系统关键设备故障诊断信息源研究[J]. 航天控制, 2007, 25(1): 80-84.

[10] 张博. 星载计算机的模拟故障注入平台研制[D]. 哈尔滨: 哈尔滨工业大学, 2020.

[11] 种靖宜, 周昊澄, 袁文强, 等. 基于 SysML 的通信卫星故障分析方法研究[J]. 计算机仿真, 2022, 39(3): 57-61, 390.

[12] 宋征宇. 高可靠运载火箭控制系统设计[M]. 北京: 中国宇航出版社, 2014: 70-74.