

一种卫星机构驱动控制类软件测试方法

王诗雯¹, 彭炳锋¹, 梁 宽¹, 王宗盛¹, 陶 艳¹, 徐 昕²

(1. 上海航天电子技术研究所, 上海 201109;

2. 中国航天科技集团商业火箭有限公司, 上海 201109)

摘要: 随着航天技术迅猛发展, 卫星系统设计正朝着智能化、复杂化的方向加速演进; 卫星机构驱动控制软件作为卫星在轨任务执行的核心部件, 主要负责包括太阳帆板、天线在内的机构驱动控制, 控制精度直接影响卫星能源供给、通信链路及科学探测任务的执行; 因卫星在轨发生故障时极难进行现场修复, 故此类软件必须具有极高的可靠性、安全性及稳定性; 针对软件的功能架构进行系统分析, 基于其复杂运动控制、多重安全保护的特点, 提出了一种通用综合测试方法: 既覆盖软件常规测试维度, 又针对航天环境设计故障注入、边界条件、安全性测试用例; 测试结果充分验证了该方法可切实提高测试的充分性与有效性, 为卫星长期在轨运行提供有力技术支撑。

关键词: 卫星机构; 驱动控制; 嵌入式软件; 软件测试; 故障注入; 场景分析

Testing Method for Satellite Mechanism Drive and Control Software

WANG Shiwen¹, PENG Bingfeng¹, LIANG Kuan¹, WANG Zongsheng¹, TAO Yan¹, XU Xin²

(1. Shanghai Institute of Aerospace Electronics Technology, Shanghai 201109, China;

2. China Aerospace Science and Technology Corporation Commercial Rocket Co., Ltd., Shanghai 201109, China)

Abstract: With the rapid development of aerospace technologies, a design for satellite systems is accelerating towards intelligence and complexity. As the core component for on-orbit mission execution of satellites, the drive and control software of satellite mechanisms is primarily responsible for driving and controlling mechanisms such as solar arrays and antennas. Its control accuracy directly impacts the satellite's power supply, communication links, and the execution of scientific exploration missions. Due to the extreme difficulty of on-site repairs in the event of on-orbit failures, this type of software must possess exceptionally high reliability, safety, and stability. The software's functional architecture is systematically analyzed, and a universal comprehensive testing method based on its characteristics of complex motion control and multiple safety protections is proposed, which not only covers conventional software testing dimensions but also specifically designs fault injection, boundary condition, and safety test cases for aerospace environments. Test results fully demonstrate that this method can effectively enhance the sufficiency and effectiveness of testing, providing a strong technical support for the long-term on-orbit operation of satellites.

Keywords: satellite mechanisms; drive control; embedded software; software testing; fault injection; scenario analysis

0 引言

全球太空资源竞争日趋激烈, 卫星作为应用范围最广的航天器类型, 对国民经济发展、国防安全建设、科学研究具有极其重要的支撑作用。而太阳帆板驱动机构(SADA, solar array drive assembly)是卫星在轨获取太阳能、进行动力输出的最基本、最关键的装置, 其驱动控制软件实际作为卫星中枢控制太阳帆板、天线的桥梁, 为卫星实现获取能源、实现通信等核心功能提供具

体实现方法^[1-2]。由于目前卫星机构驱动控制软件一般不支持在轨重构, 且卫星发射入轨之后出现故障时极难进行现场修复, 软件中任何微小的设计缺陷、运行漏洞或发生位翻转^[3]都极有可能引起机构位置超限、运动机构卡死, 甚至直接导致星载硬件设备永久损坏^[4-5]等严重在轨事故。因此, 在卫星地面研制阶段对机构驱动控制软件进行全面严格的验证测试, 是保证在轨任务成功的必要措施。

在测试研究及应用方面, 以美国国家航空航天局

收稿日期:2026-03-28; 修回日期:2026-05-11。

作者简介:王诗雯(1998-),女,硕士研究生,助理工程师。

通讯作者:梁 宽(1998-),男,硕士研究生,工程师。

引用格式:王诗雯,彭炳锋,梁 宽,等.一种卫星机构驱动控制类软件测试方法[J].计算机测量与控制,2026,34(7):68-74.

(NASA, national aeronautics and space administration) 和欧洲空间局 (ESA, european space agency) 为代表的航天强国在软件测试方面处于领先地位。NASA 制定了一系列严格的标准规范，对航天软件的生命周期、测试流程及验证确认提出了详尽的要求，强调测试的可追溯性与完备性。ESA 则建立了基于欧洲空间标准组织 (ECSS, european cooperation for space standardization) 标准的质量保证体系，注重软件的独立验证与确认 (IV&V, independent verification and validation)，通过第三方审查来降低软件风险。国内科研人员对航空航天软件的建模测试方法及自动化测试工具的开发已有十分系统的研究成果^[6-7]，GJB 系列军用标准的推广实施，为我国航天软件的工程化管理奠定了坚实基础。载人航天、探月工程等重大专项的顺利实施，体现了航天软件测试技术取得了长足进步。

当前各国星座组网建设大大加快，空间频谱资源竞争日趋激烈，卫星研制正面临交付周期急剧缩短的现实约束，传统的测试用例设计时间被大幅压缩。由于以上各类标准均只从顶层描述测试方法设计要求，用例往往需要根据目标软件进行针对性的现场设计，时间及人力成本较高，故如何在紧迫的研制周期与严苛的在轨可靠性双重约束下，既保证测试完备性又提升测试效率，已成为航天软件测试领域亟待解决的关键问题。

1 现有方法缺陷分析

现有测试方法通常为符合 GJB 标准的通用的软件测试方法，适用于卫星、运载、飞船上的各类嵌入式软件，普适性强，但并未形成针对机构驱动控制软件的系统性测试方法，对捕获/跟踪/增量过程中角度及速度控制、特殊角度跨越、软限位边界、零位信号异常、通信中断、单粒子翻转模拟等故障处理用例设计时间较长或不够详细。例如在用例设计时间方面，机构驱动控制软件行数普遍在 5 000~10 000 行，用例个数在 200~400 个，人工用例设计需要一周左右，时间较长；在测试覆盖性方面，对于具有主备双零位信号的归零工况，缺少系统化的、根据零位信号到达时间及脉冲宽度的组合工况校验用例，缺少零位修正情况下的旋变故障校验等，未覆盖驱动控制类软件航天特有工况。

为此，针对卫星机构驱动控制软件的特殊性，深入研究并提出了一套系统化测试方法。方法不仅涵盖了传统功能逻辑、接口协议、性能校验等基础测试，更将测试的深度延伸至航天特有的复杂场景，能够在有限的研制窗口内实现软件健壮性的高效验证，同时显著降低测试用例设计时间成本，提升航天软件测评效率。

2 通用功能解析

卫星机构驱动控制软件通常作为 RT 接收并解析来

自星载综合控制软件或姿态轨道控制软件的驱动指令，将解析后的角度、速度等控制信息写入驱动 FPGA 寄存器，实现对太阳帆板驱动机构、天线展开机构等机构的运动控制。同时从驱动 FPGA 采集遥测反馈给星载综合控制软件或姿态轨道控制软件实现控制闭环^[8]。

卫星机构驱动控制软件实现主要有 3 个方面，为总线通信、机构控制、自检及故障处理^[9]。

1) 总线通信主要包括与星载综合控制软件或姿态轨道控制软件之间的通信，软件完成遥控指令解析、数据合法性校验及机构闭环控制。

2) 机构控制可总结模式定义及需求综述如表 1 所示。

表 1 机构驱动控制软件控制功能定义综述

机构类型	工作模式及类型		执行动作
帆板驱动	断电停转		帆板驱动电机不加电停转
	加电停转保持		帆板驱动电机加电停转，电机绕组电流为指令保持电流
	正/反向捕获		一般应用在太阳捕获状态，帆板驱动电机以捕获速度进行转动，捕获速度大于跟踪速度，规定速度档位较少
	正/反向跟踪		一般应用在太阳捕获后跟踪太阳阶段 ^[11] ，帆板驱动电机以跟踪速度进行转动，跟踪速度通常小于捕获速度，速度档位依据姿态轨道控制软件帆板闭环跟踪需求确定
	增量	增量指定角度	帆板驱动电机按指定速度转动至目标角度，目标角度为当前角度与指令规定角度和值
		增量至指定角度（位置指定）	帆板驱动电机按指定速度转动至目标角度，目标角度为指令规定角度
	归零	硬件反馈零位信息	帆板驱动电机按指定速度转动，收到硬件反馈的零位信号时将角度置为 0°，软件输出 0°归零到位信号
		硬件不反馈零位信息	帆板驱动电机按指定速度转动至 0°，软件输出 0°归零到位信号
	零位修正		根据地面上注角度修正值对当前角度进行修正，一般软件根据实际情况进行修正范围限定，将当前角度遥测值与零位修正角度值进行相加或者相减得到新的角度值
	变频控制		转动电机在模式切换时以指定加速度进行减速及加速，避免急停造成机构故障
	堵转		当电机控制采用旋变模式与步进模式两种模式进行控制时，地面上注堵转指令可以指定速度转动指定时间后修正当前步数为特定值，恢复控制精度

续表 1

机构类型	工作模式及类型		执行动作
天线驱动	停转		天线转动电机不加电停转
	展开		天线展开电机按指定速度完成展开,可设置接收到硬件传递展开到位信号时到位停转或展开指定时间后自动转为到位停转状态
	正向/反向转动	按指定速度转动	天线转动电机按指定速度转动
		转动至指定角度	天线转动电机按指定速度转动至目标角度,目标角度为指令规定角度
		转动指定角度	天线转动电机按指定速度转动至目标角度,目标角度为当前角度与指令规定角度和值

3) 自检及故障处理主要用以规避地面或星上可能遇到的危害^[10], 通常情况下的故障注入根据以下要求进行设计, 常见要求如表 2 所示。

表 2 常见自检及故障处理要求

功能要求/安全性需求	复位类型	处理
机构位置超出软限位范围	无复位	控制对应机构停转, 遥测报错错误类型
接收模式切换指令目标模式与当前模式冲突	无复位	保持当前模式, 丢弃新接收指令, 遥测报模式冲突类型
识别非法输入, 丢弃非法指令	无复位	程序数据输入接口函数进行非法判断, 包括包头、包长、包识别、校验和等常规判断以及数据内容有效性判断
连续规定时间无通信	复位通信接口	复位串口通信或 1553 通信
周期性输出喂狗信号, 规定时间内未喂狗则触发咬狗复位	复位	程序中置看门狗寄存器并定时喂狗, 咬狗复位时程序指针指向程序入口
“空白区”设置陷阱, 纠正软件运行错误	复位	使用工具在编译程序时设置将所有未使用的 EEPROM 或 FLASH 空间填充陷阱字符序列, 运行至陷阱时触发看门狗复位, 复位时程序指针指向程序入口
检测单粒子翻转, 纠一检二	两位错时复位	如硬件自带单粒子翻转检测功能, 可直接通过设置寄存器打开, 其他工况可通过三取二避免单粒子翻转

3 测试方法

由于研究对象本质上是一种高可靠的嵌入式实时软件, 因此通用的嵌入式软件测试技术是其测试工作的

基础。

根据软件测试生命周期 (STLC, software testing life cycle) 原理, 可设计测试思路为“需求—场景—用例”。首先, 通过分析总体方任务书、设计方需求规格说明/设计说明等依据文档, 识别主要业务目标与接口, 确定测试场景; 其次, 引入场景法模拟卫星在轨运行期间可能遭遇的各种真实情境, 将孤立的功能点串联为完整的任务流, 对软件的动态行为进行全方位验证, 确定测试项类型, 为正常场景设计工况, 覆盖依据文档中规定的所有正常功能; 最后, 引入故障注入测试, 通过人为地向系统中引入硬件故障 (如单粒子翻转) 或软件故障 (如参数、指令异常), 观察软件的故障检测、隔离和恢复机制是否有效^[12-14], 覆盖每个测试项中的异常工况, 最终实现需求的全覆盖。具体如下。

1) 对于总线通信, 主要测试软件处理总线数据、指令的正确性, 与其他软件间接口实现是否正确, 重点验证数据帧格式解析及数据有效性校验逻辑。

2) 在机构控制方面:

①对于断电停转、加电停转保持模式, 测试可通过外接示波器的方式查看软件输出占空比、电压及电流值是否符合需求要求, 在停转状态及转动状态切换时是否存在尖峰毛刺, 避免降低电机运行效率、损伤定子绕组绝缘或损坏电机轴承, 导致运行不稳定^[15]。

②对于捕获、跟踪、增量、天线正向/反向转动工作模式, 测试主要从以下 4 个切入点进行用例设计。A) 限位处理, 当软件设计有转动限位值时, 能否识别并抛弃可能使转动位置超越限位范围的指令, 解除限位时能否正确超越范围转动; B) 转动过程中角度控制范围边界、特殊点及正常值的处理, 可采用五点法或七点法对边界值处理进行考核, 特殊点应根据不同硬件采集角度方式进行选取; C) 转动过程中速度的控制, 是否能以规定的加速度进行加速或者减速, 转动或模式切换过程中占空比、电压及电流的输出是否满足要求; D) 不同模式间的切换, 是否规定有模式切换冲突。

设计用例过程中, 首先关注软件定义机构有效角度范围为 0°~360°抑或 -180°~180°, 需要根据硬件通信协议约定进行测试角度设计^[16]; 设计测试角度值时, 同样应当注意控制码字与角度的对应关系, 通常关系为

$$\delta = \frac{360^\circ}{65\,536} = 0.005\,493\,164\,062\,5^\circ$$

其中: δ 代表角度控制指令中二进制数 1, 即一码字, 对应角度 0.005 493 164 062 5°, 需要注意的是此角度不能进行保留有效数字, 当码字数特别大时, 保留有效数字后的计算会扩大计算误差。

限位角度范围或控制范围边界取值时, 由于 0.005 493 164 062 5°不一定能够被整数角度值除尽,

当不能够除尽时，使用五点法进行用例设计，能够除尽时，使用七点法对边界取值进行用例设计，均需取边界值左右的最小单位，即一码字，可保证对边界处理的校验有效性。同时可根据硬件设计^[17]或星上具体实施需求对范围内的特殊点增加测试用例。设计取点如图 1、图 2 所示。

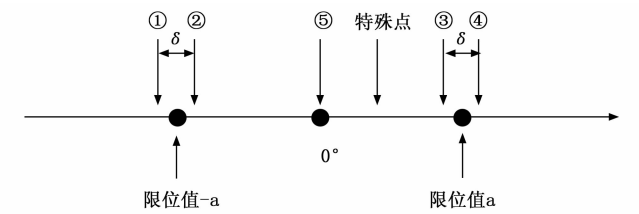


图 1 五点法取值示意图

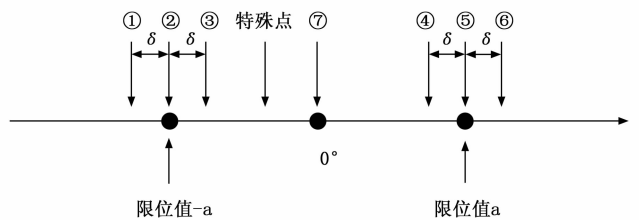


图 2 七点法取值示意图

③由于帆板、天线驱动均有变频控制要求，对于变频控制功能的测试需覆盖所有工作模式，检查模式切换时是否能够依据需求抛弃冲突的切换指令、能否在遥测界面正确显示冲突类型。故可用变频控制测试将转动模式切换校验串联，为软件设计状态机，将断电停转至堵转模式依次标识为 S0~S8，由于软件大部分状态间可进行互相转换，为全连通或接近全连通的状态机，故使用表格表达状态转换关系，如图 3 所示。并在切换过程中对响应捕获、跟踪、增量指令中速度、角度控制范围边界、特殊点及正常值处理进行校验，如电机采用旋变模式与步进模式两种模式进行控制，需对控制模式的切换及不同模式下旋变角度与步进角度的判断及赋值进行测试。

④对于归零模式

测试应当针对不同的归零到位信号进行设计，如果硬件不反馈零位信息，仅需测试模拟发送归零指令后，A) 机构转动归零过程中电压、电流、加速度及速度变化是否正确；B) 遥测显示归零到位时角度与 0°差值，即归零到位精度；C) 归零过程中接收工作模式切换指令是否正确响应。

如硬件反馈零位信息且接收零位信号为脉冲，无非零位、预零位、真零位区别，则测试点与硬件不反馈零位信息工况相同。

如硬件反馈零位信息仅有单零位信号，且接收零位信号需判断上升沿、下降沿，根据零位信号脉宽判断信号有效性区分非零位、预零位、真零位，则需要测试有效脉宽边界处理是否正确，假设判断脉宽范围为 $[t_s, t_e]$ ，脉宽大于 t_s 、小于 t_e 时为零位信号有效，小于 t_s 时标记为窄故障，大于 t_e 时标记为恒高故障，脉冲判断示意图如图 4 所示，设置故障注入模式如表 3 所示。

表 3 单零位归零故障注入参数设定

故障参数	期望结果
主零位信号窄	不归零
主零位信号恒高	不归零
备零位信号窄	不归零
备零位信号恒高	不归零

如硬件反馈零位信息为双零位信号（主零位/备零位），根据零位信号脉宽判断是否归零到位，则需进一步测试主备零位上升沿、下降沿到达顺序及零位信号脉宽有效性关系，覆盖全部工况，主备零位信号均正常情况下脉冲判断示意图如图 5 所示，具体归零结果根据实际需求进行测试。设置故障注入模式如表 4 所示，故障情况下的信号到达顺序判断方法与均正常情况同理。

对具有零位信息判断的软件，测试还应模拟发送归零指令后软件长时间没有接收到归零到位信号工况，考核软件是否进行异常工况处理，是否自行转为默认或上一时刻模式或遥测反馈错误信息等待地面处理，防止工

目标状态	断电停转S0	加电停转保持S1	正向捕获S2	反向捕获S3	正向跟踪S4	反向跟踪S5	增量S6	归零S7	堵转S8
当前状态	断电停转S0	加电停转保持S1	正向捕获S2	反向捕获S3	正向跟踪S4	反向跟踪S5	增量S6	归零S7	堵转S8
断电停转S0	/	加电停转保持指令	正向捕获+速度指令	反向捕获+速度指令	正向跟踪+速度指令	反向跟踪+速度指令	增量+目标角度指令	归零指令+归零到位信号	堵转指令
加电停转保持S1	断电停转指令	/	正向捕获+速度指令	反向捕获+速度指令	正向跟踪+速度指令	反向跟踪+速度指令	增量+目标角度指令	归零指令+归零到位信号	堵转指令
正向捕获S2	断电停转指令	加电停转保持指令	速度指令	反向捕获+速度指令	正向跟踪+速度指令	反向跟踪+速度指令	增量+目标角度指令	归零指令+归零到位信号	堵转指令
反向捕获S3	断电停转指令	加电停转保持指令	正向捕获+速度指令	速度指令	正向跟踪+速度指令	反向跟踪+速度指令	增量+目标角度指令	归零指令+归零到位信号	堵转指令
正向跟踪S4	断电停转指令	加电停转保持指令	正向捕获+速度指令	反向捕获+速度指令	速度指令	反向跟踪+速度指令	增量+目标角度指令	归零指令+归零到位信号	堵转指令
反向跟踪S5	断电停转指令	加电停转保持指令	正向捕获+速度指令	反向捕获+速度指令	正向跟踪+速度指令	速度指令	增量+目标角度指令	归零指令+归零到位信号	堵转指令
增量S6	断电停转指令	加电停转保持指令	正向捕获+速度指令	反向捕获+速度指令	正向跟踪+速度指令	反向跟踪+速度指令	增量+目标角度指令	归零指令+归零到位信号	堵转指令
归零S7	断电停转指令	加电停转保持指令	正向捕获+速度指令	反向捕获+速度指令	正向跟踪+速度指令	反向跟踪+速度指令	增量+目标角度指令	归零指令+归零到位信号	堵转指令
堵转S8	断电停转指令	加电停转保持指令	正向捕获+速度指令	反向捕获+速度指令	正向跟踪+速度指令	反向跟踪+速度指令	增量+目标角度指令	归零指令+归零到位信号	堵转指令

若目标速度与当前速度相差大则可能规定切换失败 通常认为冲突禁止切换 根据型号要求可能认为冲突禁止切换

图 3 变频控制状态转换表/用例表

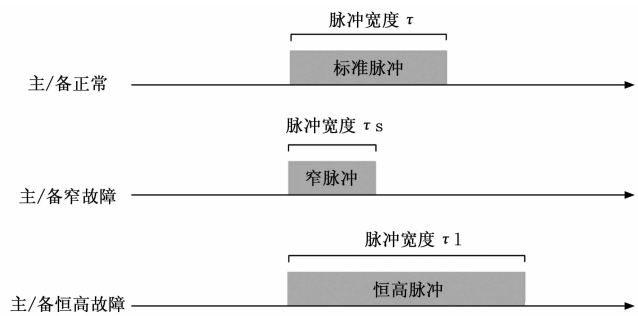


图 4 单零位归零脉冲判断

作模式异常。

表 4 双零位归零故障注入参数设定

故障参数	期望结果
主正常备窄	以主信号为准归零
主正常备恒高	以主信号为准归零
主窄备正常	以备信号为准归零
主窄备窄	均无效,不归零
主窄备恒高	均无效,不归零
主恒高备正常	以备信号为准归零
主恒高备窄	均无效,不归零
主恒高备恒高	均无效,不归零

⑤对于天线展开模式

测试根据不同的展开到位信号判断进行设计,如果硬件不反馈展开到位信号,展开至指定角度后转为到位

停转状态,则考核发送天线展开指令后,A)展开过程中电压、电流、加速度及速度变化是否正确;B)遥测显示展开到位后角度与目标角度间差值;C)展开过程中接收工作模式切换指令是否正确响应。

如果展开到位判据为接收到硬件反馈的展开到位信号,则需另外考核展开到位信号到达后天线机构停转电压、电流、加速度及速度控制是否正确,展开过程中及展开到位后遥测显示工作模式状态切换是否正确。

⑥对于零位修正模式

零位修正模式角度或步数计算方法与硬件安装方式及机构获得当前角度方法有关,如机构驱动仅设计有旋变模式,即对零位修正模式的测试除正常给出允许的零位修正值范围内的修正工况外,应重点对 A) 零位修正值范围边界值注数处理正确性校验;B) 验证通过地测软件修正后角度是否还在有效范围内;C) 机构转动修正值是否始终有效、是否会异常清除;D) 修正值是否作为重要数据进行三取二存储,单机热启动(如有)是否恢复。如机构设计同时有旋变模式与步数模式,则需注意地测软件注数零位修正指令时旋变角度与步数角度的变化是否会造成旋变故障判断为真,导致异常旋变故障处理、报异常遥测。

⑦对于堵转模式

设计堵转模式的初衷主要是解决机构长时间运行或火工品爆炸等因素影响当前角度有效性问题,进行堵转后可恢复控制精度,主要测试点为 A) 接收、处理堵转

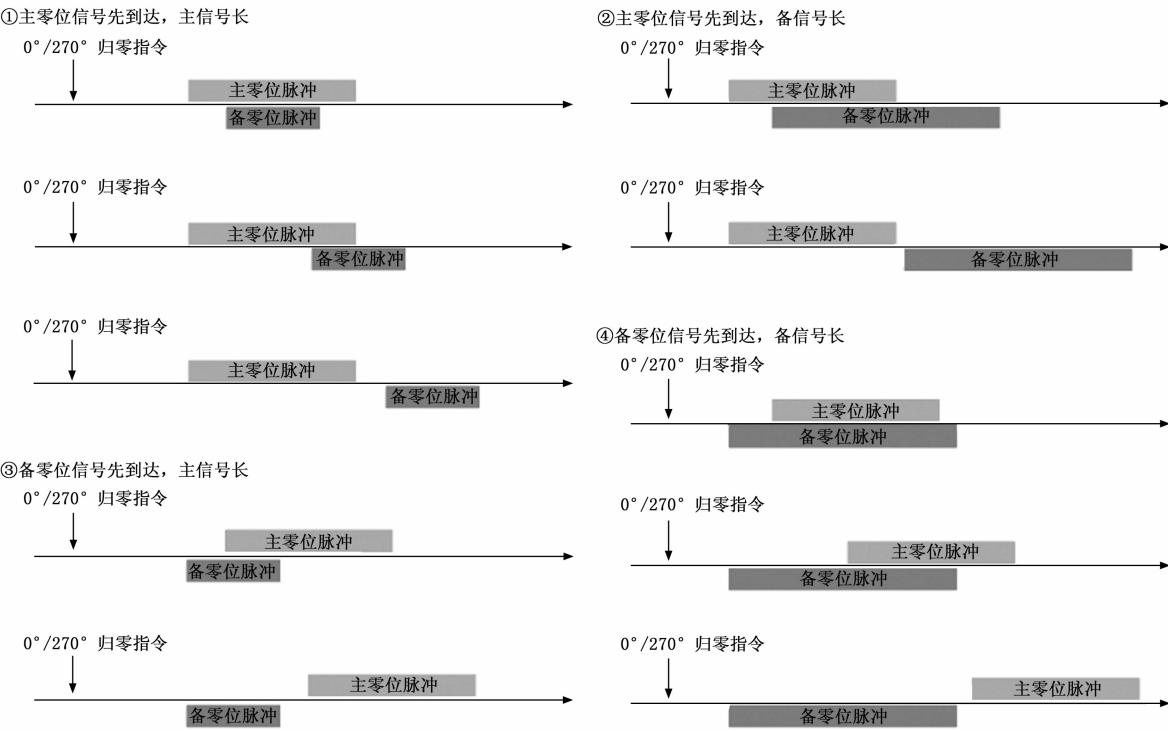


图 5 双零位归零脉冲判断

表 5 自检及故障处理故障注入参数设定

功能要求/安全性需求	故障参数	评估标准
机构位置超出软限位范围	动态测试时上注超限位范围指令	遥测报指令错误信息,抛弃错误指令
接收模式切换指令目标模式与当前模式冲突	动态测试时上注初始模式设置指令,再上注冲突指令进行切换	遥测报指令错误信息,抛弃冲突指令
识别非法输入,丢弃非法指令	动态测试时上注格式非法指令	遥测报指令错误信息,抛弃非法指令
连续规定时间无通信	正常运行后不通过通信仿真软件发送指令或关闭通信仿真软件	复位通信
周期性输出喂狗信号,规定时间内未喂狗则触发咬狗复位	运行前插桩注释喂狗信号输出语句,编译运行后查看咬狗时间	咬狗复位,PC 指针指向初始地址开始运行
“空白区”设置陷阱,纠正软件运行错误	连接仿真器,使用 KEIL 的调试模式赋值程序指针指向空白区	恢复程序运行初态,PC 指针指向初始地址开始运行
检测单粒子翻转,纠一检二 ^[20]	使用 KEIL 插桩设置硬件造错寄存器	一位错时自动检错纠错,两位错时复位
重要数据三取二	连接仿真器,使用 KEIL 的调试模式改错三取二部分变量	三取二一份错时输出未出错的两份数据中的一份;按字节三取二三份错时启动应急软件或提交地面处理;按位三取二三份错时软件应通过按位取值输出计算后结果

指令正确性校验；B) 堵转时长及堵转过程中电压、电流、速度控制正确性；C) 堵转过程中接收工作模式切换指令处理正确性。

3) 自检及故障处理是星上安全性检测的必要手段^[18-19]，可引入故障注入参数如表 5 所示。

4 测试验证

由于每颗卫星的研制目标与在轨任务需求存在差异，各星载驱动控制软件的功能设计与接口设计也各不相同^[20-22]，现阶段常用 Windows 系统为基础运行平台，采用 KEIL 或 Eclipse 作为集成开发环境，同时使用与星上实际运行一致的交叉编译器，保障测试环境与在轨运行环境的一致性。在软件静态分析环节，采用 Test-bed 或 Klocwork 专业工具进行分析；在仿真测试环节，主要依托研制方自主研发的 UI 界面作为仿真工具，完成软件的仿真测试验证。

为验证方法的有效性 & 充分性，在某通信卫星、某导航卫星、某探测卫星的三个驱动控制软件测试项目实践中考核了近十五年的典型案例及举一反三问题的故障检出率，覆盖率可达到 100%，部分案例如表 6 所示。

同时通过 Logiscope 等覆盖率工具在动态测试时进行分析，结果显示语句及分支覆盖率可达 99% 以上（未覆盖部分通过代码审查补充测试）。通过统计测评人员用例数及设计时间可见时间可缩短 60% 以上，对比见表 7 所示。

5 结束语

基于复杂空间环境下卫星机构驱动控制软件高可靠性运行的要求，提出了基于场景法及故障注入的通用综合测试方法，将传统测试方法及航天领域中常用的场景

表 6 近十五年的典型案例及举一反三问题覆盖（部分）

典型案例及举一反三问题	对应模式
未合理设置遥测握手导致遥测存储帧重复或缺失	遥测
多字节接口数据读取顺序错误导致数据异常	遥测
中断屏蔽时间过长导致串口漏帧	遥测
读写未加锁导致读取脏数据	遥测
未正确判断零位修正指令导致触发故障遥测	遥测
全局变量冲突导致指令执行不及时	遥控
宏定义错误赋值全局变量导致指令判断失效	加电保持及其禁止
浮点数运算产生截断误差导致无法调整机构角速度	捕获跟踪
未及时清空异常速度指令导致错误速度值生效	捕获跟踪
模式转换中共用变量状态切换时处理错误	模式切换

表 7 人工用例数及设计用时对比

型号名	案例	通信卫星	导航卫星	探测卫星
有效行数	8 006	8 059	8 312	7 767
用例数	235	237	254	229
用时(人/月)	0.375	0.2	0.225	0.2
千行代码缺陷率	1.124	1.365	1.564	1.287

分析有机地结合起来，并梳理了太阳帆板、天线等典型星载机构的通用控制逻辑，系统化设计用例，解决了定制化卫星软件测试效率低、覆盖不全的问题。

基于“零缺陷”基本要求，对软件边界条件及异常条件进行了系统、严谨的测试验证：强化边界条件测试，包括 0°/360°角度跨越、软限位边界等典型边界场景；着重异常工况测试，包括零位信号异常、通信中断、单粒子翻转模拟等故障处理。在卫星归零模式、变频控制模式的测试中引入故障注入方法，直接、可靠地验证软件在恶劣空间环境下的容错及故障恢复能力。

测试结果表明,该方法不仅能有效检出常规逻辑错误,还能挖掘出潜在的软件缺陷,显著提升了软件测试的充分性,为保障航天器在轨长期稳定运行提供了有效技术支撑。

后续可从三方面研究:1)智能化测试技术应用,引入大模型优化用例设计与缺陷检出;2)构建基于数字孪生的全数字化仿真测试环境,高保真还原在轨场景,降低测试成本;3)面向在轨重构软件的动态测试与验证,保障在轨更新与重构的安全性及连续性。

参考文献:

- [1] ZHU X, et al. Data-driven approaches for satellite SADA system health monitoring with limited data [C] //2024 IEEE 20th International Conference on Automation Science and Engineering (CASE), Bari, Italy: IEEE, 2024: 3225 - 3230.
- [2] 于国庆,刘艳敏,张 猛,等. 航天器太阳能电池阵驱动装置技术与展望 [J]. 空间控制技术与应用, 2024, 50 (5): 17 - 25.
- [3] 李丽娇,石 然,严 丹,等. 一种适用于星载太阳翼的驱动控制器设计 [J]. 空间控制技术与应用, 2018, 44 (6): 22 - 31.
- [4] PETTIT R, PETTIT A. Detecting single event upsets in embedded software [C] //2018 IEEE 21st International Symposium on Real-Time Distributed Computing (IS-ORC), Singapore: IEEE, 2018: 142 - 145.
- [5] KONG C, LIU H, LIN B, et al. Energy adaptability analysis based on the stall fault of solar array drive assembly for medium earth orbit satellite [J]. Energies, 2025, 18 (9): 2315.
- [6] 田 宇,赵昶宇. 浅析嵌入式软件失效模式与影响分析 [J]. 科技与创新, 2024 (10): 125 - 127.
- [7] XU Y, HE S. Avionics equipment cable fault injection design and simulation testing validation [C] //2023 Global Reliability and Prognostics and Health Management Conference (PHM-Hangzhou), Hangzhou, China: IEEE, 2023: 1 - 5.
- [8] 吕 楠,郭建新,肖 帅,等. 东方红系列通信卫星控制技术发展综述 [J]. 空间控制技术与应用, 2024, 50 (5): 1 - 16.
- [9] ZHAO Z, CHEN G, WANG B. Test method for SADA's servo control system of china space station [C] //2019 IEEE 10th International Conference on Mechanical and Aerospace Engineering (ICMAE), Brussels, Belgium: IEEE, 2019: 297 - 301.
- [10] KARA C, ASLAN A B, CANBERI M H. Test software for national satellite on-board computer [C] //2020 Turkish National Software Engineering Symposium (UYMS), Istanbul, Turkey: IEEE, 2020: 1 - 4.
- [11] 黄逍遥,葛 悦,李 宇,等. 太阳帆板驱动控制器的力学仿真与试验 [J]. 机械制造与自动化, 2021, 50 (5): 106 - 109.
- [12] 王 华,高 扬,吴 强,等. 基于故障注入的嵌入式测绘导航软件测试技术研究 [J]. 测试技术学报, 2018, 32 (1): 31 - 35.
- [13] 刘 鹤,张晓明,张 月. 基于总线故障注入的卫星热控自主管理软件测试方案 [J]. 航天器工程, 2024, 33 (3): 135 - 140.
- [14] GEORGE A, LATHIKA T T, KAVYA S. A novel technique for software fault injection testing through FP-GA code instrumentation for verification and validation of software on-board launch vehicles and spacecraft [C] //2025 6th International Conference on Control, Communication and Computing (ICCC), Thiruvananthapuram, India: IEEE, 2025: 1 - 4.
- [15] TONG L, GUO C, LIANG J, et al. A study on the influence of stepper motor drive current on SADA rate stability [C] //2023 IEEE 18th Conference on Industrial Electronics and Applications (ICIEA), Ningbo, China: IEEE, 2023: 458 - 463.
- [16] 黄 智,章 玄,张子亮,等. 低轨星座太阳翼在轨管理策略研究 [J]. 电源技术, 2025, 49 (3): 2069 - 2074.
- [17] 熊一帆,龙 澄,刘明利,等. 卫星天线扫描驱动机构的一体化设计及力学仿真 [J]. 航天制造技术, 2021 (6): 16 - 21.
- [18] 赵昶宇. 嵌入式软件安全性测试技术研究 [J]. 科技与创新, 2023 (21): 81 - 83.
- [19] SAVITHA A, PUSHPAVATHI T P, et al. Risk assessment approach for safety and reliable mission critical software for spacecraft operation [C] //2025 IEEE World Forum on Public Safety Technology (WF-PST), Orlando, FL, USA: IEEE, 2025: 42 - 47.
- [20] ESQUER S, SIERAWSKI B D, WITULSKI A F, et al. Single event functional interrupt (SEFI) sensitivities of a multicore microprocessor [C] //2024 IEEE Aerospace Conference, Big Sky, MT, USA: IEEE, 2024: 1 - 11.
- [21] 邵洪森,何 旭,袁钾光,等. 一种基于半实物仿真平台的卫星故障注入测试研究 [J]. 中国设备工程, 2023 (1): 266 - 268.
- [22] SCHIRMEIER H, HOFFMANN M, DIETRICH C, et al. FAIL*: an open and versatile fault-injection framework for the assessment of software-implemented hardware fault tolerance [C] //2015 11th European Dependable Computing Conference (EDCC), Paris, France: IEEE, 2015: 245 - 255.