文章编号:1671-4598(2021)01-0236-04 DOI:10.16526/j.cnki.11—4762/tp.2021.01.048 中图分类号:V554.3 文献标识码:A

基于代理的航天器自主运行仿真系统设计与验证

范延芳，李瑞军，周晓伶，成宏璟
（北京空间飞行器总体设计部，北京 100094）

摘要：针对目前航天器自主健康管理功能测试过程中，由于故障模拟手段不足造成测试覆盖率低，测试项目不完备，测试效率低等问题，提出一种基于代理的航天器自主健康故障仿真验证系统设计方案；基于该方案实现的故障仿真系统支持根据通用化航天器自主健康故障检测模型，严格按逻辑和时序，无延迟、持续的向全实物或半实物测试系统自动注入故障状态表征参数，模拟航天器整器或任意分系统、单机、软件的故障状态，模拟弥补了长期以来在实物测试环境下，整器故障模式测试覆盖率低，测试用例复用性差的问题；实践证明，此方法能将测试覆盖率提升至95%以上，并将测试时间缩短至传统方式的1/6，有效提升被测航天器产品可靠性。

关键词：自主健康模型；故障仿真；代理模式

Agent—based Spacecraft Autonomous Health Fault Simulation System Design and Verification

Fan Yanfang, Li Ruijun, Zhou Xiaoling, Cheng Hongjing
(Beijing Institute of Spacecraft System Engineering, Beijing 100094, China)

Abstract: Due to insufficient fault simulation methods for the spacecraft autonomous health management system software test, the test coverage rate is not high enough to satisfy the functional test demands, the paper proposed an agent—based spacecraft autonomous health fault simulation strategy. The fault simulation system which was built based on the simulation strategy supports to injects faults data into a whole physical or a semi—physical spacecraft system according to a predetermined logic or timing to simulate any faults status of a spacecraft, subsystem, device or software. For a long time, it was difficult to inject fault to a real spacecraft system without doing damages to the real system, and it was difficult to apply enough fault mode test. However, the fault simulation strategy proposed by the paper can effectively solve the above problem, improve test efficiency and test effectiveness, accordingly improve the reliability of spacecraft products.

Keywords: autonomous health model; fault simulation; proxy mode

0 引言

随着我国航天技术的进步，对航天器的“好用、易用”提出更高要求[1-4]，因此越来越多的航天器支持广泛应用各类传感器采集健康数据并通过综合电子系统对采集数据加以分析处理，实现对航天器在轨飞行健康状态的监测和自主判断，一旦健康状况出现异常，能够根据预先设定的处置方案实施故障排查、预警，必要时还支持自主选择、执行最佳应急处置方案，并将上述情况通过遥测通知地面测控站[5-6]。

然而航天器产品的仿真验证能力并未跟上其设计实现前进的步伐，主要体现在：1）硬件设备的故障模拟手段不足，导致多数自主健康管理策略的验证成为不可测试项，从而导致航天器系统级可靠性、安全性验证不完善；2）在真实硬件设备测试环境下，目前分系统和整星阶段测试多采用内存修改的方式实现故障状态设置，此方法一方面实现起来步骤繁多，需要大量内存地址与数据关系的先验知识，对测试人员能力和知识储备要求高，另一方面，由于测试过程需要对目标设备内存进行反复操作，不但降低测试实时性和测试效率[7]，同时还增加了目标设备内存数据被改写错误的风险。

本文提出一种基于代理的航天器自主健康故障仿真系统设计方案，基于该方案实现的故障仿真系统能够有效解决上述问题，实现根据通用化故障模型动态生成整套自主健康测试用例，支持自动、有序执行，实时判读，同时能针对航天器自主健康管理需求，对其功能实现的正确性和有效性给予评价报告。代理模式方案的另一个主要优势是，无需被迫修改目标机内存，在正样产品测试中不会给被测设备带来负面风险。经实际应用证明，基于该方案实现的测试系统至少能将测试覆盖率提升至95%；同时将测试效率提升60%。

1 基于代理的故障仿真系统设计方案

1.1 基于代理的故障仿真原理

基于代理的故障仿真是指按照航天器系统设计的特定

收稿日期:2020-06-01； **修回日期**:2020-07-06。

作者简介:范延芳(1977-)，女，江苏丹阳人，硕士，高级工程师，主要从事航天器软件开发方向的研究。

引用格式:范延芳，李瑞军，周晓伶，等.基于代理的航天器自主运行仿真系统设计与验证[J].计算机测量与控制，2021，29(1)：236-239.

故障模型，以人为的、有意识的手段，采用代理机制，在确保不改变被测系统健康指标数据采集时序和周期的情况下，将实际采集得到的无故障状况表征信息替换为故障状态表征信息，并通过航天器内部数据总线、I/O 接口等途径，直接或间接的传递给星载中央计算机软件，作为判断航天器运行状态是否符合在轨运行要求的判断依据的过程。

图 1 所示的星/地模块映射结构图给出了故障仿真系统模块与航天器自主健康管理系统模块之间一一对应的关系，从系统组成角度直观描述了基于代理的故障仿真系统原理。

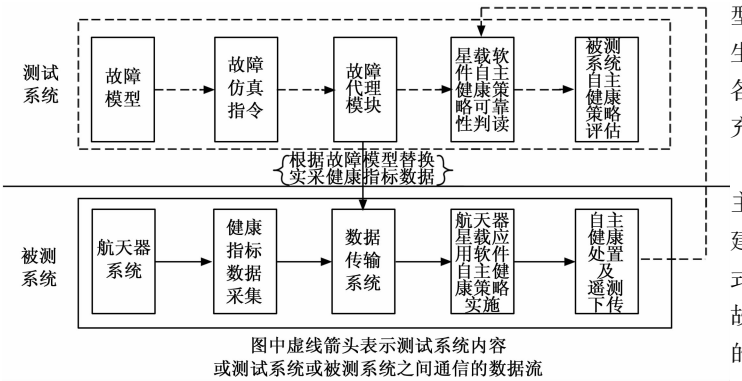

图 1　故障仿真原理图

针对被测试系统的自主健康设计需求开展需求分解活动，采用穷举的方式获取所有待分析健康指标数据，并在此基础上，基于健康指标数据的采集方式（模拟采集还是数字采集）、处理方法、传输协议（采集参数的物理量转化公式、校准方法、传输的数据类型、保留的数据位长及精度等信息）等定义，确定每一类健康指标数据的故障模拟代理策略。

无论采取上述本文 1.3 节中介绍的任何一种故障仿真策略中，均可通过向故障仿真系统发送故障仿真激励指令的方式，命令故障代理模块实施代理动作。仿真激励指令严格按时序发出，故障代理模块在接收到故障仿真激励指令后，能够以微秒级精度完成故障数据的替换及转发；星载计算机自主健康管理模块得到无差别替换健康指标数据后，根据星上软件设计逻辑对采集数据进行分析、处理，并给出针对该组故障数据推导出的星上自主动作序列，包括一组特定的指令链、若干个星上健康表征遥测参数的重新配置及故障描述信息的事件报告下传。

仿真测试系统通过实时监视、获取并解析各个星地接口数据的方式，收集星上计算机软件自主动作的影响域表征数据，并通过对该数据产生时序及解析值含义的判读，为星上故障模式处置策略的有效性和正确性做出客观、准确的定性评价。

1.2　故障模型建立

目前美国的舰船系统、民用车辆等领域广泛采用 ISO13374 和 MIMOSA 标准制定的体系结构——OSA－CBM（open system architecture for condition based maintenance）体系结构，作为飞行器综合健康管理的标准[8]。该体系结构将自主健康管理分成 7 个功能模块，数据采集传输模块，数据处理模块，状态监测模块，健康评估模块，故障预测模块，推理决策模块和人机接口模块。结合我国航天器研制中对自主健康管理功能的设计实现和故障仿真验证系统的运行机制，归纳总结得出下述适合我国航天器产品设计模式的故障仿真模型。

基于代理的自主健康管理故障仿真模型由两部分组成。

首先，自上而下的分解航天器系统自主健康自主安全管理需求，并由需求功能点抽象出通用化故障模型。该模型由两部分组成。一部分通过定量、定性的描述故障发生的前提条件和判读原子，以及判读时间，判读策略、各判读因子之间的逻辑依赖关系等，定义了故障发生的充分必要条件。

判读的对象为星载应用软件采集、处理的航天器自主健康状态表征信号量。这些信号量的定义通过抽象、建模得到的自身属性特征加以描述，包括信号量采集方式分类、处理方法、采集频率、监控时机，等。若某种故障模式的定义比较复杂，需要通过准确定义故障产生的前提条件，持续时间，以及在满足该前提条件的情况下，其他健康状态表征参数之间的逻辑关系。在仿真验证的应用过程中，此部分模型的应用将通过在确定的时刻，通过特定的故障模拟策略，为确定的故障状况表征参数设置满足故障触发条件的采集值，即在仿真序列中，按设计时序发送特定故障参数模拟指令的方式实现。

其次，还需要针对地面遥测参数的判读方式进行建模，包括定义参与判读的健康状态信号量代号，参与状态判断的逻辑、流程、组合权重等。以此模型作为对航天器系统故障处置策略执行结果是否与设计预期一致的自动化评估依据。当满足航天器的健康状况特征参数的采集值满足故障触发的充分必要条件时，根据星载计算机软件自主健康、自主安全管理需求定义，星上应做出相应处置措施。此处置措施就是故障模型必须描述的第二部分，即在轨故障发生后，星载计算机软件应该给出的应对措施的模型描述。此部分模型中应包含以下要素：星载计算机是否需要根据故障的严重程度立刻、自主做出处置动作；如果需要，星载计算机软件给出自主处置动作包含的具体步骤；星载计算机应通知地面星上故障的时机、方法及协议格式。采用基于因果关系的归类方法，对模型要素进行分类，最终通过逻辑公式将上述所有因素加以描述的过程，就是故障模型的第二部分建模的过程。

表 1 定义了航天器自主健康故障模型建模中涉及的主要因子。实际应用中可通过各相关因子的逻辑组合＋时序控制，灵活实现各类航天器在轨故障模式的模拟。经试验统计，采用此方式形成的故障模型涵盖当前航天器设计中至少 95％的自主健康管理故障类型描述。

1.3　基于故障模型的故障代理策略

根据故障模型中健康指标参数采集周期和采集方式的不同，提出了三种故障代理策略。

表 1 基于代理的自主健康故障仿真模型

模型参数	类型					
星载软件功能建模参数	健康指标参数类型	硬通道模拟量	硬通道数字量	软通道数字量	—	—
	健康指标参数处理方法	不带前提条件的直接判读	不带前提条件的 N 取 M	不带前提条件的逻辑与	不带前提条件的逻辑或	—
		带前提条件的直接判读	带前提条件的 N 取 M	带前提条件的逻辑与	带前提条件的逻辑或	—
	状态监测方法	等于/不等于	在上下限之间	在上下限之外	大于/大于等于	小于/小于等于
	健康评估方法	持续不变	持续变化	在特定时间段内连续发生 N 次	在特定时间段内共发生 N 次	连续跳变
地面仿真验证系统建模参数	代理机制	硬通道参数代理	软通道参数代理	附条件代理	—	—
	处置策略判读类型	遥测参数等于/不等于特定数值判读	遥测参数按特定步长递增判读	指令组判读	延时指令判读	遥测包更新判读

1）硬通道 I/O 代理模式：此代理模式适用于周期性采集的硬通道健康指标参数。故障仿真验证系统的代理模块根据故障模型要求，获取当前故障模式下需要代理的健康指标参数及其相关属性信息，例如，航天器建造文档中定义的硬通道采集周期、传输波道、处理方法和正常值范围、判读次数、判读持续时间等，并为每一个硬通道健康指标参数创建对象，一旦在仿真验证过程中收到代理指令，可根据指令要求，按周期，在特定传输通道上实现对该参数采集数据的替换。

软通道参数代理模式：此代理模式适用于突发性的软通道健康指标参数。故障仿真验证系统代理模块根据故障模型要求，获取当前故障模式下需要代理的软通道健康指标参数及其参与故障状态的场景信息，包括参数数据类型、处理方法、正常值范围、和其他参数的关联关系、采集周期、判读次数、判读持续时间，等，并为各参数创建对象。一旦仿真验证过程涉及相应故障模式，则根据故障模型描述，在适当的时机，以特定方式，将该健康指标参数的值改变为故障状态。

2）附条件代理模式：此代理模式适用于需要通过握手确认实现的故障设置方式。被代理数据在传递给代理模块前需要通过消息通知，代理模块将参数注入相应通道后，也需要通过消息通知参数采集方实施采集动作，为了确保星上软件的处理时序正确，需确保上述两个操作严格在一个参数采集周期内完成。

若待仿真健康指标参数对时序性要求特别高，同时具备真实目标机硬件设备的故障仿真测试场景，推荐采用硬通道 I/O 代理模式；若待仿真健康指标参数仅对采集数据的相对时序是否与真实在轨飞行时的采集时序一致做严格要求，而对数据采集绝对时刻不做明确要求，同时又不具备实物目标机，则推荐使用软通道参数代理策略；若待仿真健康指标参数的准确仿真时机依赖与某个事件的发生，则推荐使用附条件的代理模式。基于代理的自主健康故障仿真系统支持触发事件包括：星地遥控指令、特定的突发总线消息或特定的突发遥测源包等。

1.4 基于代理的自主健康故障仿真验证系统架构

基于代理的故障仿真系统架构如图 2 所示。本系统中各模块间通过局域网互联。其中，基于代理的故障仿真模块负责获取、解析故障模拟激励指令；并根据激励指令选取适当的故障模拟策略，将真实采集的健康指标数据替换为故障状态数据按时序要求转送星上数据处理模块的输入端口；测试客户端的测试用例执行模块负责根据自主健康模型生成和自动执行测试序列；测试客户端的故障判读模块负责根据故障模型中定义的处置策略，对星载软件的处置结果进行综合判断，并给出结论性报告。

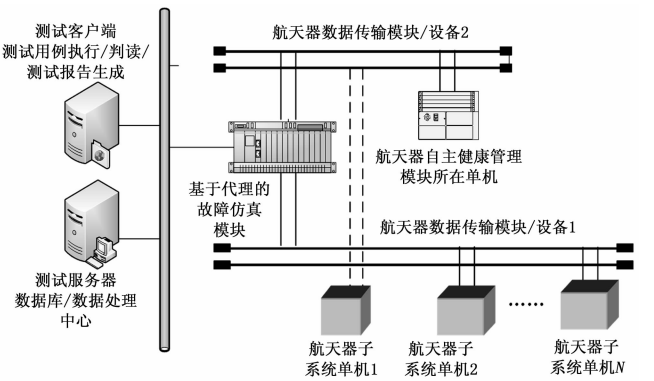

图 2 基于代理的自主管理故障仿真系统架构

基于代理的故障仿真系统实际应用的流程如下：

1）根据对被测航天器自主健康需求分解结果，以及 1.2 节中介绍的自主健康故障建模方法得到的自主健康故障模型，故障仿真系统能够自动生成满足自主健康故障仿真验证覆盖率要求的测试序列。

2）故障仿真系统能够根据测试需要自动加载、解析测试序列脚本，并按照测试时序，逐条发送故障仿真激励指令，为星载软件采集航天器在轨运行故障模式提供依据。

3）仿真验证系统能够实时获取、解析、比较航天器所有星内、星地信息流数据，从中提取用于评估星载软件针对当前故障状态所触发的所有动作表征信息量，包括星上自主发出的遥控指令码、指令间隔、航天器运行状态表征

软遥测、事件报告数据等。

4）仿真验证系统能够充分融合上一步骤获取的所有判读结果，给出被测软件针对当前故障模式是否满足设计要求的综合评估结果。

整个测试流程可由系统自行闭环，无需人工干预。如果一定要针对测试完备性和测试强度做特别评估，可以在测试用例自动生成后，测试用例自动执行前，选取有经验的测试人员对测试用例做人工审查。人工自动审查获得的完善措施，可以在后续仿真验证过程中，通过迭代完善故障模型的方式得以体现和延续。

鉴于航天器星载计算机软件为嵌入式实时操作系统应用软件，其对时序精度要求极为严格，本仿真系统采用了时间同步的通信机制，同时通过实时数据系统共享和多参数并行仿真/判读机制，达到了满足航天器在轨运行故障模式逼真模拟，并实现了对星载软件自主健康处置结果自动、高效判读的功能。

2　实验验证与分析

2.1　基于代理的自主健康故障仿真验证方法及流程

采用基于代理的自主健康故障仿真系统对若干真实在研卫星的自主健康管理功能进行测试。验证方法及流程如图 3 所示，具体步骤如下：

1）搭建基于代理的航天器自主运行仿真验证测试环节；

2）根据型号自主健康管理设计要求和故障建模策略，配置自主健康信号量采集、传输、组织遥测下传的映射关系配置文件；

3）基于自主健康建模策略，利用自主健康测试用例自动生成模块产生故障激励和自主健康执行策略自动判读自动化测试序列；

4）自动化测试序列自动执行和判读；

5）根据自动化测试序列的测试结果给出航天器自主健康管理测试评估报告。

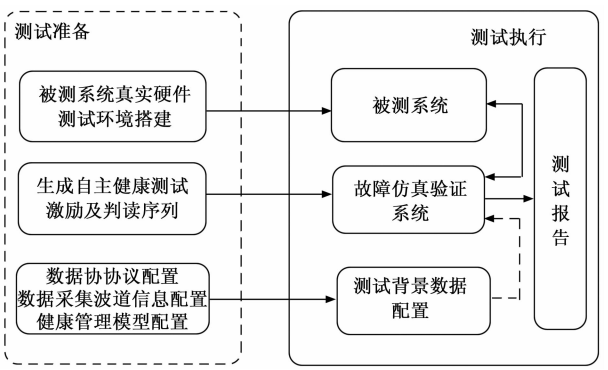

图 3　故障仿真验证流程

从航天器自主健康管理功能分类角度，本仿真验证方法能够覆盖自主安全和自主健康两大类故障模型测试，包括了测控、数管、控制、导航、能源、热控和有效载荷等 7 大分系统近 200 种故障的 1 000 多个测试用例，测试准备用时 5 天，测试执行用时 3 天，测试覆盖率 100%，发现星载软件设计缺陷 10 余项，缺陷类型从文实不符到软件设计缺陷等类型均有涉及，测试回归用时 1 天，测试用例复用率高达 92%。

2.2　实验验证效果

本仿真验证系统在高分 7 号卫星的分系统测试、整星测试中得以应用。实践证明，首先，基于本文 1.2 节故障模型生成的自主健康仿真验证序列能够满足型号 100%测试覆盖率要求；其次，仿真验证系统支持按测试序列时序要求，实时触发代理模式故障仿真激励，其模拟的故障健康指标数据在时序上与真实硬件系统采集、传输的健康指标数据时序完全一致，无延迟；最后，仿真验证系统支持基于故障模型定义实施自动判读，并给出仿真验证评估结果。实验验证评估结论如表 2 所示。

表 2　实验验证评估结论

	基于代理的故障仿真系统	原测试系统
测试覆盖率	100%	60%
测试准备	5 天	15 天
测试实施	3 天	30 天
自动化测试用例复用率（回归测试）	92%	不支持自动执行/判读

3　结束语

本文提出了一种基于代理模式的故障仿真设计方法，并基于该方法实现了一套仿真验证系统。实践验证证明，该方法能够有效解决航天器研制过程中存在的故障模式测试不完备、测试效率低等问题，为在实物硬件测试环境中实现故障模式处置策略的正确性测试提供了一种全新的测试方法，为整器系统级可靠性、安全性提升做出显著贡献。后续若能够基于测试记录数据，开展预测技术与方法的研究，将能够为实现星地联合预测卫星在轨健康状态，有效提升航天器自主管理智能化程度提供创新依据。

参考文献：

[1] 罗荣蒸，孙　波，张　雷，等. 航天器预测与健康管理技术研究 [J]. 航天器工程，2013，22 (4)：95－102.

[2] 潘宇倩，张　弓，白东炜，等. 卫星健康管理故障诊断算法的设计及其实现 [J]. 航天器工程，2011，20 (5)：37－42.

[3] 梁　克，邓凯文，丁　锐，等. 载人航天器在轨自主健康管理系统体系结构及关键技术探讨 [J]. 载人航天，2014，20 (2)：116－121.

[4] 孙　博，康　锐，谢劲松. 故障预测与健康管理系统研究和应用现状综述 [J]. 系统工程与电子技术，2007，29 (10)：1762－1767.

[5] 李　晴，孙国江，李孝同. 基于星务管理系统的小卫星自主健康管理系统 [J]. 航天器环境工程，2012 (5)：574－578.

[6] 王文平，王向晖，徐　浩，等. 高分三号卫星自主健康管理系统设计与实现 [J]. 航天器工程，2017，26 (6)：40－46.

[7] 窦　钠，张红军，范延芳，等. 航天器数据管理系统软件的自动化测试系统设计 [J]. 航天器工程，2018 27 (1)：143－148.

[8] Discenzo F M，Nickerson W，Mitchell C E，et al. Open systems architecture enables health management for next generation system monitoring and maintenance [R]. Development Program White Paper. 2001.