文章编号:1671-4598(2019)08-0125-05 DOI:10.16526/j.cnki.11—4762/tp.2019.08.026 中图分类号:TP311.5 文献标识码:A

基于虚拟化技术的卫星控制系统软件构件库运行监控与可信验证技术

沈怡飚[1,2]，张 程[1,2]，何益康[1,2]，林荣峰[1,2]，朱晏庆[1,2]
(1. 上海航天控制技术研究所，上海 201109；2. 上海市空间智能控制技术重点实验室，上海 201109)

摘要：动态系统建模工具可以按照设定的仿真步长对控制器的行为动态模拟，也可以在仿真环境下模拟控制器所在的系统架构和动态数据交互，因此传统的卫星控制系统方案设计时一般采用在同一模型建模体系进行，并进行相应的控制算法设计；但是由于动态系统建模工具其自身的时钟步长和数据流处理逻辑，不能完全模拟目标机的内部 ALU 逻辑和真实外围设备工作行为，可能与真实物理环境要求的系统有一定的出入，造成对承载卫星控制器功能的目标机 CPU 处理系统存在一定程度的失真，影响仿真效果；提出了一种基于虚拟化技术的卫星控制系统软件构件库可信验证技术，使用虚拟化技术实现对真实物理目标机功能的完全模拟，运用软件非干涉运行监控技术，获取可信的开发证据和应用证据，利用协同仿真组件和卫星控制系统方案设计的控制算法模型对各个软件构件进行动态同步仿真验证。

关键词：虚拟目标机；动态系统建模工具；协同仿真；软件非干涉运行监控技术

An Operation Monitoring and Credible Verification Method of Satellite Attitude and Orbit Control Software Components Library Based on Virtualization Technology

Shen Yiwei[1,2], Zhang Cheng[1,2], He Yikang[1,2], Lin Rongfeng[1,2], Zhu Yanqing[1,2]
(1. Shanghai Institute of Space Control Technology, Shanghai 201109, China;
2. Key Laboratory of Space Intelligent Control Technology in Shanghai, Shanghai 201109, China)

Abstract: A dynamic system model—construction tool can be used to simulate the interaction of system framework and dynamic data, and can dynamically simulate the operation of real target machine, so traditional simulation systems generally are based on same systems to scheme satellite attitude and orbit control system, and to design algorithms. But real peripheral equipments of real target machine for the clock step and data flow processing logic units, and there are still discrepancies between the real physical environment and dynamic model systems, because these systems cannot totally simulate inner ALU logic units and which causes a degree of simulation distortion. It is proposed a credible verification method of satellite attitude and orbit control software components library based on virtualization technology, which contains a complete simulation for virtual target machine to real physical ones, an obtainment of credible development evidence and application evidence using software non—interference operation monitoring technology, and a dynamic modeling and simulation with synchronous simulation components and simulink models. In order to verify all software components in the library, and to validate the algorithms of satellite attitude and orbit control software.

Keywords: Virtualization target machine; dynamic system model—construction tool; synchronous simulation; Ssoftware non—interference operation monitoring

0 引言

动态系统建模工具[1]的仿真工具箱被广泛应用于卫星控制系统的方案设计中，为用户提供了非常丰富好用的基础模块，使用户可以根据被控对象的特点从模块库中选用适用的模块，仅修改相应的参数即可建立航天器轨道动力学和姿态动力学模型等，它支持各类连续、离散、线性和非线性等系统的构建，支持对动力学模型进行编译和仿真，可以轻松有效的完成系统的仿真。无论多么复杂的卫星控制系统，都能采用直观的“方框图”[2]，使用面向对象的设计方法，完成控制系统模型的输入和仿真计算，实现对卫星控制系统这一动态系统准确、快速的建模。因此常常被卫星控制系统方案设计师用于卫星控制算法的设计，并利用可视化的仿真工具，对设计的算法进行验证。

然而同时，随着使用的深入，动态系统建模工具技术进行系统仿真也暴露出一些弊端，主要反映在以下几个方面：

a) 集成计算机算法处理到动态系统建模工具模型的设计方法，其内部嵌入式架构算术与逻辑处理单元执行方式，相比传统的基于 CPU 硬件平台的嵌入式软件开发，有比较大的差异，因为 CPU 结构难以完美的被动态系统建模工具

收稿日期:2018-11-04； **修回日期**:2019-01-05。

作者简介:沈怡飚(1986-)，男，江苏省江阴市人，工程师，主要从事软件设计方向的研究。

模型模拟，比如动态系统建模工具模拟的外部中断触发、内部定时机制会严重影响系统任务调度的过程，降低仿真效果，进而影响计算机核心算法处理，这些与实际使用真实微控制器算法的运行结果的差异，会降低关键技术方案设计的可信性；

b）传统的动态系统建模工具模型，往往难以仿真字节或字序颠倒、特殊寄存器的位支持等具体硬件设备的特殊要求，仅对使用通用数据类型的算法处理有着较好的支持（例如 16 位、32 位、64 位整型、浮点数等），因此只能满足基本的计算精度，但是对于卫星控制系统的下位单机软件行为过程的模拟往往不够；

c）卫星控制系统软件运行在真实 CPU 平台上时，是离散型、非线性的状态，因为软件在运行过程中不是动态连续的，会受到中断触发、任务抢占调度等外部影响，而动态系统建模工具模型则往往是动态连续的过程，导致使用动态系统建模工具进行仿真与使用真实 CPU 进行测试的结果存在出入，影响系统的故障模拟、指令注入的测试，甚至全系统的闭环仿真测试；

d）卫星控制系统领域的仿真建模，由于系统的复杂性和实时性，造成使用动态系统建模工具进行算法过程设计时复杂性的提高，随之而来的是执行效率降低，导致实时性的降低影响到系统运行的正确性和精确性；

e）在使用动态系统建模工具搭建卫星控制系统单机模型时，受限于动态系统建模工具自身限制，在面对定制单机的特殊协议，使用面向过程的 Ada、C/C＋＋等高级语言，能够规避资源浪费等问题，灵活性更好。

随着对卫星控制系统软件越来越高的重用化要求，软件研制方基于工程积累的、在轨飞行验证过的成熟软件构件，正在建立可反复利用、可用于后续卫星控制系统软件重用的构件库，以往的开发方式仍以人工手工编码的方式进行软件实现，难以适应当前基于模型的系统工程（MBSE）、以及软件定义卫星等技术的发展，尽管一些动态建模工具已具有一定的自动生成软件代码的功能，以及相应的模型形式化验证功能，但对于生成的软件代码在真实目标环境的运行验证手段不足，也难以实现对任务提出方的需求开展可信验证。

同时，卫星控制系统软件运行监控技术是提供可信证据，驱动协同演化和协同开发过程的关键基础技术。运行监控技术主要应用于软件配置项测试和验证过程中，传统方法中，常使用插桩、植入探针或“打点”的方式进行，这类方式会直接改变软件产品的实体，影响获得结果和证据的准确性及可信性。

基于上述分析，本文通过采用纯软件的实现方法为嵌入式软件开发提供一个可监控的、可信的软件开发和验证平台，提出了一种基于虚拟化技术的卫星控制系统软件构件库可信验证技术，并与任务提出方使用动态系统建模工具实现的控制算法模型进行协同、同步、动态仿真，运用软件非干涉运行监控技术，在不改变卫星控制系统软件实体的情况下，对软件实体的运行状态、动态行为和执行结果进行监控，获取可信的开发证据和应用证据，实现对用户需求的验证与确认。

1 卫星控制系统软件的建模设计

1.1 动态建模工具模型实现卫星控制系统软件功能

软件与硬件设备尚未开始设计的情况下，在卫星控制系统研制的早期，需要验证整个方案设计的可行性，在控制算法模型内部仿真软件算法控制等模型，使用动态建模工具搭建控制算法模型仿真系统，形成一个全数字的闭环仿真系统，与动力学模型之间进行输入输出数据交互，用以验证整个系统方案的可行性，如图 1 所示。

卫星控制系统由控制器、敏感器和执行机构组成。当前卫星使用的敏感器主要包括惯性敏感器、太阳敏感器、恒星敏感器、地球敏感器等，执行机构主要包括反作用飞轮、控制力矩陀螺、推力器等。这些敏感器、执行机构与控制器之间普遍采用 RS422 串口通讯协议、MIL－STD－1553B 总线协议、AD 模拟量输入、PWM 脉冲宽度调制、CAN 总线协议等，因此，在建立动力学模型的输入模块和输出模块也采用这些通讯协议的模拟模块。

动力学模型在接收到卫星控制器发送的执行机构指令后，采用常微分方程组或偏微分方程等的组合，同时考虑卫星的刚体弹性体混合系统及刚体液体混合系统的特性，模拟挠性卫星的姿态动力学和轨道动力学，特别是对卫星受到的主要外力矩进行模拟，比如太阳辐射压力矩、重力梯度力、气动力、地磁场力矩等环境力，以及主要内力矩进行模拟，比如推力器的喷射力矩、反作用飞轮产生的角动量力矩、液体推进剂产生的液体晃动力矩、太阳电池阵产生的扰动力矩。

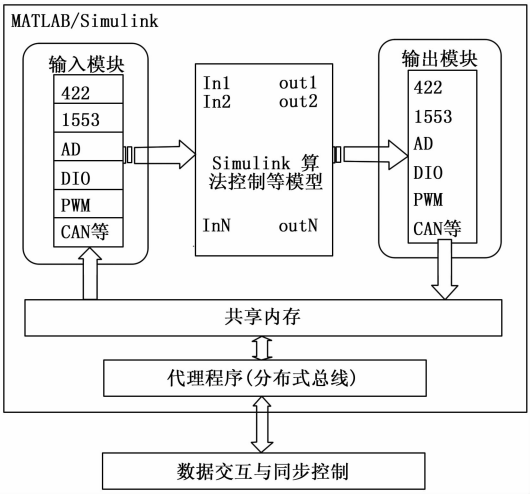

图 1 使用动态建模工具实现控制算法模型仿真系统

为了使得控制算法模型与外部数据可以交互，使用动态建模工具建立姿态动力学模型和轨道动力学模型的外围设备，同时建立控制器模型，从而达到闭环仿真验证卫星控制系统方案的目的。

相对于卫星控制器的控制算法模型来说，控制算法模型的运行控制实现输入模块接口，获取控制算法模型数据是输出模块接口。

输入模块包括 422 模块（模拟 RS422 串口通讯协议）、1553B 模块（模拟 MIL－STD－1553B 总线协议）、AD 模块（模拟模拟量输入功能）、DIO 模块（模拟数字输入输出电路）、PWM 模块（模拟脉冲宽度调制方法）和 CAN 模块（模拟控制器局域网络总线协议）等，他们作为动力学敏感器采集接口的输入。

输出模块包括 422 模块、1553B 模块、AD 模块、DIO 模块、PWM 模块和 CAN 模块等，他们作为动力学执行机构模型的输出。

由于输入模块和输出模块均是使用动态建模工具建立的、模拟真实硬件通讯协议的软件模块，因此，使用共享内存技术可以实现对控制算法模型的控制，使用动态建模工具实现的控制算法模型的仿真数据在内部传递。

1.2　基于虚拟化技术的仿真系统实现卫星控制系统软件功能

在卫星控制系统研制流程中，软件的设计开发往往是在系统方案设计评审通过后，在这个阶段，使用动态建模工具无法对真实计算机算法处理软件进行功能验证与性能测试，因为实现的控制算法模型仿真系统对硬件设备的设计及软件设计无能为力。针对这种情况，使用软件虚拟化技术[3]来仿真真实硬件目标板，仿真出与真实硬件相同的运行效果，在虚拟平台上直接加载卫星控制软件的二进制文件运行，替代早期的动态建模仿真系统中的算法控制单元，提出了全数字超实时仿真系统[4]的需求，并能在系统中进行卫星控制系统软件的运行调试，用以验证软件的功能，如图 2 所示。

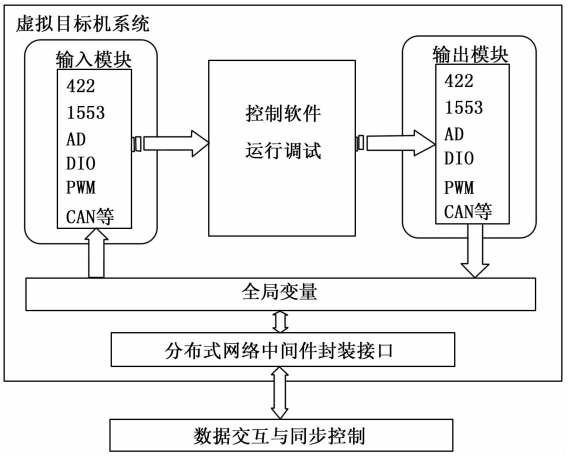

图 2　虚拟目标机分布式仿真系统

输入模块包括 422 模块、1553B 模块、AD 模块、DIO 模块、PWM 模块和 CAN 模块等，他们作为敏感器模型的输出。姿态确定是姿态控制的前提，它的任务是利用星上的姿态敏感器测量所得的卫星姿态信息，经过卫星控制系统软件处理求得卫星本体坐标系相对于空间参考坐标系的姿态角或姿态四元数信息。

输出模块包括 422 模块、1553B 模块、AD 模块、DIO 模块、PWM 模块和 CAN 模块等，他们作为执行机构模型的输入。姿态控制的任务是卫星控制系统软件利用姿态确定求得的姿态角或姿态四元数信息，使用控制算法计算求得相应执行机构的控制脉冲宽度、转速、力矩等指令。

仿真数据在虚拟目标机软件内部传递，输入模块以及输出模块完全模拟真实硬件单机接口，使用全局变量以及分布式总线可以与外部数据交互，将监控探针直接设置在各软件构件上，当卫星控制系统软件在虚拟目标机中运行时，直接由仿真系统负责记录各类运行数据，再由分析工具将运行数据与控制系统软件的目标码或源代码整合，可以获得需要的监控信息，从而达到验证软件功能的目的。

1.3　虚拟目标机分布式仿真系统与动态建模工具控制算法模型仿真的集成

将控制算法模型仿真系统与虚拟目标机分布式仿真系统集成，形成一个全数字闭环仿真系统，在验证软件功能的同时，也可有效帮助卫星控制系统软件任务提出方，即在动态建模工具算法控制等模型与控制软件之间建立数据闭环交互，便于系统方案设计人员验证系统控制算法的正确性，如图 3 所示。

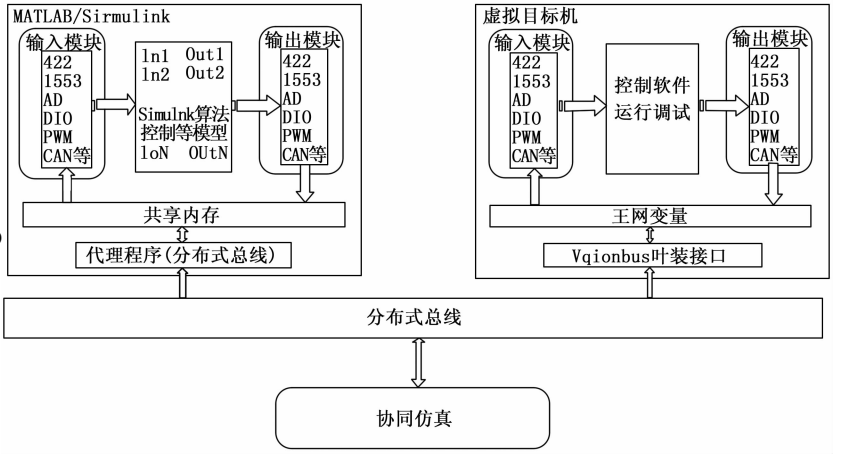

图 3　集成的闭环仿真系统

虚拟目标机分布式仿真系统与动态建模工具控制算法模型之间的数据交互使用分布式总线的协议。

控制算法模型仿真系统通过代理，挂在分布式总线上，动力学模型产生敏感器的输出信号，通过分布式总线，输入到虚拟目标机分布式仿真系统，虚拟目标机分布式仿真系统将会根据控制软件，产生执行器的输出，再次通过分布式总线，输入到控制算法模型仿真系统的动力学中。往返计算，迭代循环，不断验证控制软件的功能和性能。

使用外部的协同仿真工具[5]统一控制二者之间的数据同步，控制仿真速率，确保虚拟目标机分布式仿真系统仿

真周期与动态建模工具控制算法模型仿真步长的同步性，从而达到对整个闭环系统的验证。

2 应用实例

2.1 项目说明

“某型号卫星姿轨控软件”构件库可信验证系统是应用了基于虚拟化技术的卫星控制系统软件构件库的运行监控与可信验证技术的仿真平台，可以实现基于 SPARC V7 架构 CPU、基于 ERC32 的姿轨控计算机 Ada 语言软件的开发调试与测试，用于星载软件进行黑盒的从单元、构件[6]到系统级的验证、开发、测试、维护，和全寿命周期的外部输入输出和软件源代码本身的全过程跟踪、记录等白盒，执行效率更高、系统验证更全面、可信度更高[7]地开展卫星控制系统软件构件库的验证与确认工作，能够对卫星控制策略进行快速仿真验证，对比使用纯动态建模工具建模搭建的仿真系统，动态状态执行控制更逼近真实环境。

2.2 基于虚拟化技术的卫星控制系统软件构件库可信验证技

虚拟目标机[8]和其虚拟外围环境，通过模拟嵌入式软件运行所需要的目标机硬件及外部的信号并让嵌入式软件像在真实目标机上一样运行（计算和处理）[9]，在协同仿真软件的协同调度下，实现基于 Ada/C/C++/汇编等语言的卫星控制系统软件与控制算法仿真模型在基于虚拟化技术的系统仿真与验证平台模式下实时、超实时闭环运行监控与可信验证。

整个系统架构，包含三大部分。第一部分是在轨系统，包括卫星和 GPS 接收机，它们将真实在轨数据反馈到地面；第二部分是地面用户，包括专业用户和基地用户，他们接收在轨数据，放入资源库和数据库中，并通过遥测和三维立体显示进行数据判读；第三部分是实验室验证系统，包括虚拟星载计算机和动力学及单机模型，他们根据地面仿真数据，作为遥控指令的判断，并将指令发送给地面站，进行在轨遥控，同时接收遥测数据，作为仿真数据的比对和性能验证。

在试验室验证系统中，我们采用动态建模工具控制算法模型仿真系统与虚拟目标机分布式仿真系统集成，形成基于虚拟化技术的卫星控制系统闭环仿真系统，其中，使用分布式协同仿真中间件，从面向用户的操作界面软件生成的测试用例，通过遥控转发控制指令给虚拟目标机，再经过中间件的时序调度和仿真控制，将虚拟目标机产生的控制指令转发给封装姿态动力学和轨道动力学模型的模型仿真模块，同时将各节点间的数据传输，包括虚拟目标机产生的遥测数据，以及模型仿真模块产生的过程采集数据，打包转发给数据库服务器和遥测显示软件，一起构建成卫星控制系统软件构件库可信验证系统，从而驱动目标卫星控制系统软件的运行。

虚拟目标机负责解析卫星控制系统软件程序内核[10]，在系统级闭环仿真时可在虚拟目标机上运行目标软件，在虚拟 CPU 中加载基于 ERC32/Ada 语言软件实现的卫星控制系统软件目标码，联合运行动态建模工具搭建的控制算法模型，实施软件非干涉监控技术时，首先设计监控任务定义机制，根据监控需求生成监控任务清单，比如设立影响算法运行的关键的、两个系统相应的观测点，进行同步动态比对，同时在系统中长时间运行并存储监控数据，对所有软件构件运行产生的数据进行过滤、筛选和分析，获得关键的可信证据。

2.3 验证分析

对基于虚拟化技术的卫星控制系统软件构件库可信验证技术进行验证时，取动态建模工具模型仿真步长为 1ms，为做到同步仿真，则虚拟目标机的仿真步长也设定为 1 ms。在模型与卫星控制软件集成之后，为形成一个时序正确的闭环卫星控制系统仿真工具，引入协同仿真工具来实现二者之间的周期同步。

在基于虚拟化技术的卫星控制系统软件构件库可信验证技术中，还可以接入其他必要的外部终端软件，对在卫星控制系统半物理仿真试验中应用的故障模拟软件、遥控注数软件及遥测显示终端，进行无缝接入。

外部终端软件可以对遥测数据进行解码和回放，为验证环境提供判读依据。

故障模拟软件可以进行故障预案的设计，提高系统可靠性。

遥控注数软件可以对遥控指令进行地面仿真验证，实现快速响应的功能。

经过最终的测试比对，以 Matlab/Simulink 为例使用动态建模工具仿真运行的遥测闭环曲线与使用虚拟化技术的卫星控制系统软件构件库可信验证系统仿真的遥测闭环曲线基本相同，选用相同的卫星控制系统模式闭环控制工况，选用影响卫星控制系统算法设计的关键观测点姿态角和姿态角速度进行比对观测，如图 4～图 7 所示，上图为卫星控制系统方案设计方使用动态建模工具仿真获得的姿态角曲线和姿态角速度曲线，下图为用虚拟化技术的卫星控制系统软件构件库可信验证系统仿真的姿态角曲线和姿态角速度曲线，仿真结果可信。

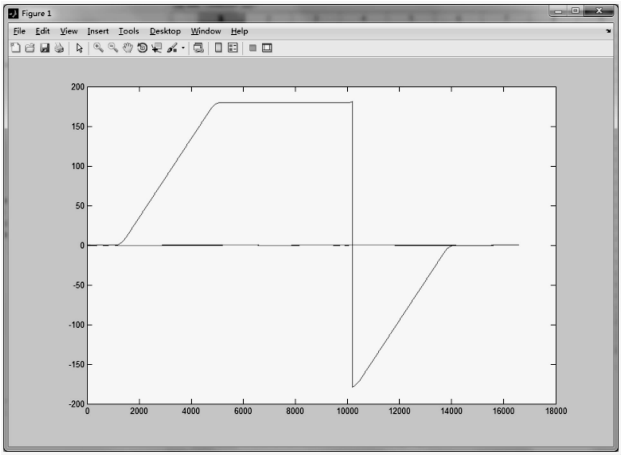

图 4 动态建模工具姿态角仿真曲线图

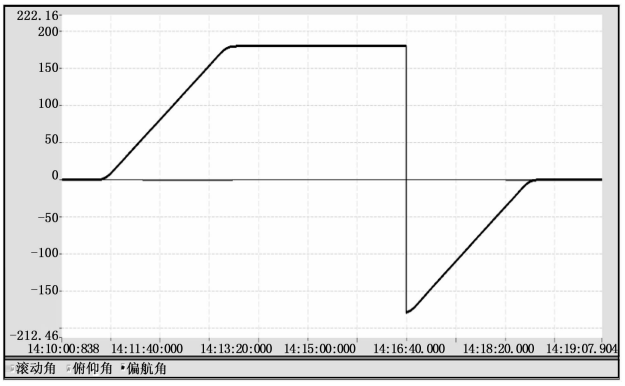

图 5　虚拟目标机分布式仿真系统姿态角仿真曲线图

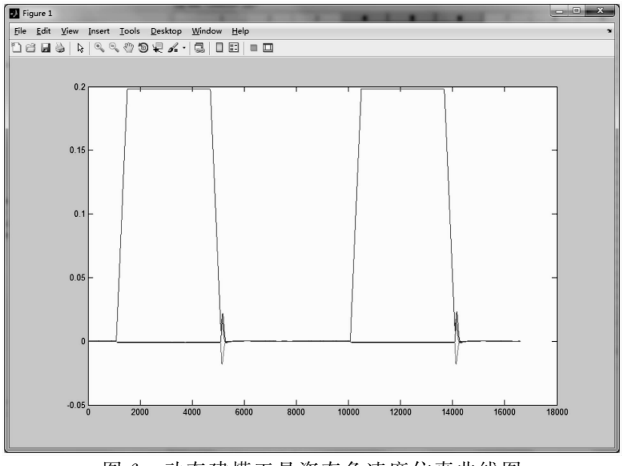

图 6　动态建模工具姿态角速度仿真曲线图

3　结论

本文构建了一套“某型号卫星姿轨控软件”构件库可信验证系统，利用基于虚拟化技术的卫星控制系统软件构件库可信验证技术，实现了两套卫星控制系统的动态同步比对闭环仿真，集成了控制算法模型与真实卫星控制软件，在确保基础功能、算法逻辑正确的前提下，通过软件非干涉运行监控技术获得的可信证据，与纯动态建模工具搭建的仿真系统比对结果表明，该技术全面有效的验证了软件构件库的功能和可信性，对于在真实目标平台上卫星控制系统的模拟仿真，准确性和实时性方面有着更大的优势，

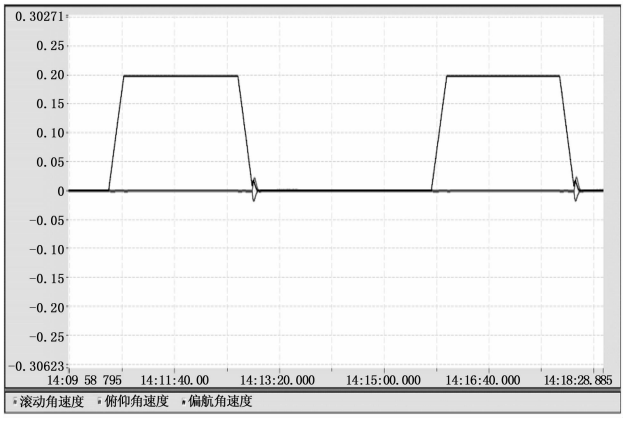

图 7　虚拟目标机分布式仿真系统姿态角速度曲线图

增加了卫星控制软件的可靠性和安全性。

参考文献：

[1] 唐　凯，康凤举，黄永华，等. 一种在分布交互仿真系统中使用 Simulink 模型的方法 [J]. 2007，19 (4)：787 - 789.

[2] 谢海斌，张代兵，沈林成，等. 基于 MATLAB/SIMULINK 与 FLUENT 的协同仿真方法研究 [J]. 2007，19 (8)：1824 - 1827.

[3] 熊光楞. 协同仿真与虚拟样机技术 [M]. 北京：清华大学出版社，2004.

[4] 王江云，王行仁，贾荣珍. 协同仿真环境体系结构 [J]. 系统仿真学报，2001，13 (6)：688 - 710.

[5] 王沫然，Simulink4 建模及动态仿真 [M]. 北京：电子工业出版社，2002.

[6] 郭树行，兰雨晴，金茂忠. 软件构件的可信保证研究 [J]. 重庆：计算机科学，2007，34 (5)：243 - 246.

[7] 金　海，廖小飞. 面向计算系统的虚拟化技术 [J]. 北京：中国基础科学，2008，10 (6)：12 - 18.

[8] 鲁　松，周海兵，刘　阳，赵君. 计算机虚拟化技术及应用 [M]. 北京：机械工业出版社，2008.

[9] 陈立宏. 基于构件的嵌入式实时软件可靠性评估模型的研究与应用 [J]. 成都：电子科技大学，2008.

[10] 蔡　强. 可信嵌入式软件的研究与应用 [J]. 长沙：湖南大学，2012.

(上接第 124 页)

[2] 吕凤军. 基于无线传输机理的轮胎监测系统的研究 [J]. 现代电子技术，2012，35 (9)：161 - 163.

[3] 林桂斌. 基于 CAN 总线的直接单向式 TPMS 的设计 [J]. 机电技术，2015 (1)：108 - 110.

[4] 何德华，陈万培，毛通宝，等. 汽车轮胎温度和压力监测系统设计 [J]. 信息通信，2018 (7)：56 - 57.

[5] 唐　曙，罗武胜，鲁　琴，等. 基于 Android 平台的 USB 通信技术研究 [J]. 计算机测量与控制，2015，23 (12)：4121 - 4123，4127.

[6] 孙　洁，付友涛，孔凡鹏，等. Android 系统下的 USB 设备驱动程序设计 [J]. 计算机测量与控制，2013，21 (5)：1386 - 1388.

[7] 冯生强，张新龙. 基于安卓平台的 USB 接口与串口通信转换的实现 [J]. 中国新通信，2016，18 (18)：84.

[8] 刘　一，任占兵. 基于 USB 接口的远程安卓手机心电测量系统的设计 [J]. 计算机测量与控制，2014，22 (11)：3512 - 3514.

[9] 蔡罗成. Android 后台监听实现机制浅析 [J]. 信息安全与通信保密，2010 (6)：39 - 41.

[10] 李寒江，郭　珂，王月芹. 基于 Android 移动设备的光伏系统监测装置的设计 [J]. 计量与测试技术，2015，42 (6)：5 - 6.