

基于国产化的通用指挥控制系统测试平台研究

熊凤阳 夏俊杰 黄和龙

江南机电设计研究所 贵州 贵阳 550009

【摘要】：随着国家信息安全战略的深入推进，指挥控制系统的自主可控已成为国防科领域的重要课题。针对现有测试平台高度依赖进口硬件与国外软件架构、存在供应链安全隐患的问题，本研究设计并实现了一种基于国产化软硬件的通用指挥控制系统测试平台。平台采用“硬件适配+软件定义”的技术路线，底层硬件选用国产高性能处理器与国产化总线，软件层面基于国产实时操作系统与跨平台开发框架构建。通过引入国产中间件技术解决异构组件通信难题，并设计了针对国产化芯片架构的优化算法。实验结果表明，该平台在满足指挥控制系统高实时、高可靠性测试需求的同时，实现了核心技术的自主可控，有效降低了对国外技术的依赖，为国防装备的国产化替代提供了有力的测试验证支撑。

【关键词】：国产化；指挥控制系统；测试平台；自主可控；通用性

DOI:10.12417/3041-0630.26.10.025

引言

在当前复杂多变的国际地缘政治环境下，科技自立自强已成为国家发展的战略支撑。特别是对于国防科技工业而言，实现关键核心技术的自主可控不仅是提升战斗力的需要，更是保障国家安全的底线。指挥控制系统作为现代战争中信息获取、处理、决策与执行的核心，其性能优劣直接决定了作战效能的高低。而在指挥控制系统的全生命周期中，测试与验证环节占据了至关重要的地位，不仅关乎装备能否通过状态鉴定，更直接影响着装备在实战环境下的稳定性与可靠性。

现有的国产化替代研究多集中于单一功能模块的“点对点”替换，缺乏从底层硬件驱动到顶层应用软件的全国产化、通用化设计思路。导致系统内部接口不统一、软硬件兼容性差、生态割裂严重，难以形成规模化应用。因此，研究并构建一种基于国产化软硬件的通用指挥控制系统测试平台，不仅是提升装备测试效率、降低研发成本的迫切需求，更是构建安全、可控、可信国防体系的必由之路。本研究旨在通过系统性的技术攻关，打通国产化测试平台的“最后一公里”，为国防现代化建设提供坚实的技术支撑。

1 国产化测试需求分析与技术挑战

相较于通用的商用测试平台，面向国防应用的国产化测试平台在需求分析阶段必需额外考量生态适配性、供应链安全性以及长期演进能力。

(1) 硬件兼容性问题：在硬件兼容性方面，面临着巨大的挑战。产处理器百花齐放，包括基于 ARM 架构的飞腾、鲲鹏，基于 MIPS 架构的龙芯，以及基于 X86 架构的海光等。这些处理器在指令集、内存管理机制以及外设接口上存在显著差

异。同时，国产化的总线接口种类繁多，驱动程序的开发与维护难度极大。如何解决不同架构处理器与多种总线之间的驱动适配问题，是构建通用平台的首要难题。

(2) 软件生态问题：在软件生态方面，国产实时操作系统虽然近年来取得了长足进步，但其上层应用生产与 Windows 或者主流 Linux 发行版相比仍有较大差距。这要求我们必须对现有的测试算法库、图形用户界面组件进行大规模的移植与重构。特别是在图形渲染效率、多线程并发调度、中断响应延迟等方面，往往存在技术瓶颈，需要针对性地进行底层优化。

(3) 数据安全问题：数据安全性是国产化平台的核心需求。传统的测试平台往往侧重于功能实现，对数据安全关注度不足。而在国产化背景下，平台必须具备内生安全能力。这意味着从硬件固件的可信启动，到操作系统内核的安全加固，再到应用软件的数据加密传输，每一个环节都必须符合国家信息安全等级保护要求。必须采用国密算法（SM2/SM3/SM4）对测试数据进行全生命周期的加密与认证，确保敏感数据在采集、传输、存储、分析过程中不被窃取或篡改。

2 平台架构设计与关键技术实现

为应对上述挑战，本研究提出了“全国产、分层解耦、微服务化”的平台总体架构。

2.1 硬件架构

在硬件架构层面，选用国产高性能加固型工控机作为核心计算节点，搭载国产多核处理器与大容量国产化内存。I/O 接口层采用模块化设计，集成了国产化的高速信息采集、数字 I/O 以及各类军用总线接口。通过设计通用的硬件抽象层，将底层硬件驱动的差异性封装起来，向上层应用提供统一的标准接

口,从而实现了针对不同国产硬件型号的即插即用支持,极大提升了系统的可替换性与可维护性。

2.2 软件架构

在软件架构层面,基于国产实时操作系统与 Qt 国产化分支构建跨平台的应用框架。采用国产消息中间件实现分布式组件间的高效通信,确保数据传输的实时性与可靠性。软件系统在逻辑上划分为四大功能模块:数据采集模块负责多源异构信号的同步采集与预处理;协议解析模块负责对各类军用总线协议进行深度解析与封装;场景仿真模块能够模拟复杂的战场电磁环境与装备交互场景;结果评估模块则依据预设的指标体系对测试数据进行自动化的分析与判读。各模块以微服务的形式独立部署,支持动态加载与热插拔,提高了系统的灵活性与可扩展性。

2.3 关键技术

关键技术突破主要体现以下两个方面:(1)针对国产处理器的指令集特性,对核心测试算法进行了汇编级优化与并行化改造,利用国产化芯片的 SIMD 指令集加速数据处理,显著提升了系统的吞吐量。(2)设计了基于国密算法的双向身份认证与端到端加密传输机制,结合可信计算技术,构建了从物理层到应用层的纵深防御体系,有效防范了数据泄露与非法访问风险。

3 实验验证与性能分析

为验证平台的可行性、稳定性与优越性,本研究选取某型国产化指挥控制系统作为被测对象进行了实测。

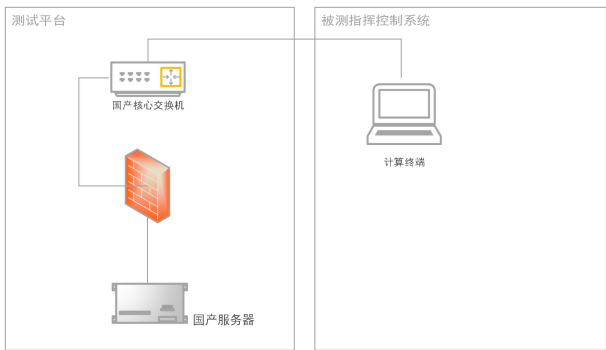


图 1 平台测试环境搭建原理图

参考文献:

[1] 张利彬;张熙;张明;张桢齐.指挥控制系统测试流程设计与功能实现研究[J].计算机测量与控制,2022,30(6):79-83.
[2] 胡婉如;王竹刚;张仁良;胡俊杰;李晓.通用一体化测试平台设计[J].电讯技术,2020,60(11):1368-1372.
[3] 韩小文;赵明;孙进;翼祥.便携式通用发控系统性能测试装置的研究[J].现代防御技术,2018,46(6):135-142.
[4] 周红卫;姜丹丹.云架构多任务指挥控制系统的性能测试方法[J].指挥信息系统与技术,2021,12(1):97-102.

测试环境搭建在全国产化的实验室环境中,包括国产服务器、国产核心交换机、国产防火墙以及被测指挥控制系统,如图 1 所示。测试内容涵盖了功能测试、性能测试以及安全性测试等多个维度。

表 1 测试数据对比表

项目	本平台	传统专用测试平台	提升幅度
功能覆盖	100%	85%	提升 15%
实时性能	1.5ms 以上	0.8ms 以内	—
系统稳定性	无数据丢失或死机	偶发数据丢失或延迟	—

实验数据表明,该平台在功能测试中的覆盖率达到到了 100%,指令传输成功率为 100%,平均响应时间稳定在 0.8ms 以内,满足了毫秒级实时性要求。在并发处理能力测试中,即使在每秒 5000 条指令的高负载下,系统依然保持稳定运行,未出现数据丢失或者死机现象。与传统专用测试平台相比,本平台在测试准备时间上缩短了约 40%,资源利用率提升了 60%。这表明该通用测试平台在保证高可靠性的同时,显著提升了测试效率。

4 结论

本研究成功研制并验证了一种基于国产化的通用指挥控制系统测试平台。通过系统性的架构设计与关键技术攻关,有效解决了测试领域长期存在的“卡脖子”问题,实现了从硬件基础设施到上层应用软件的完全自主可控。实验结果表明,该平台不仅具备高性能、高可靠性的测试能力,还具备良好的通用性、兼容性与安全性,能够满足现代指挥控制系统研发过程中的多样化、复杂化测试需求。本平台的推广应用,将有力地推动我国国防装备国产化进程,降低对国外技术的依赖,提升国防工业的自主创新能力和供应链安全水平。未来工作将重点探索国产化 AI 加速卡在智能测试用例自动生成与故障预测中的应用,进一步提升平台的智能化水平与测试效率。