

基于分层验证策略的接口自动化验证平台设计

徐记伟 耿斌*

中国电子科技集团公司第二十八研究所, 中国·江苏 南京 210023

摘要: 为实现跨系统接口自动化验证测试, 对接口交互质量进行体系性评估。设计了由接入解析服务、资源管理服务、接口验证工具集、联试任务调度服务以及量化评估服务组成体系性接口验证平台架构与验证流程, 基于分层验证策略自下而上逐级检验接口交互链路, 通过虚实结合仿真系统模拟真实测试系统数据及运行环境, 驱动自动化接口测试用例生成与多场景测试环境下的测试激励生成, 自动化执行验证用例, 采集接口验证指标及评估接口交互质量, 形成系统间接口标准符合性与运行稳定性的全链路验证评估。

关键词: 系统接口; 分层验证策略; 验证评估

Design of an Automated Interface Verification Platform Based on a Layered Verification Strategy

Xu Jiwei, Geng Bin*

The 28th Research Institute of China Electronics Technology Group Corporation, China Jiangsu Nanjing 210023

Abstract: To achieve automated verification testing of cross-system interfaces and systematically evaluate interface interaction quality, a systematic interface verification platform architecture and verification process are designed, comprising an access parsing service, a resource management service, an interface verification toolset, a joint test task scheduling service, and a quantitative evaluation service. Based on a layered verification strategy, interface interaction links are verified step by step from the bottom up. A virtual-real combined simulation system is used to simulate real test system data and operating environments, driving automated generation of interface test cases and test stimuli in multi-scenario test environments. Verification cases are executed automatically, and interface verification metrics are collected to evaluate interface interaction quality, thereby forming a full-link verification and evaluation of standard compliance and operational stability for inter-system interfaces.

Keywords: System interface; Layered verification strategy; Verification and evaluation

0 引言

随着作战形式的复杂化和多样化, 现代战争形态已从“以平台为中心”向“体系化、信息化、网络化”转变。联合作战指挥控制系统作为信息化作战体系的核心中枢, 承担着战场态势感知信息获取、处理、分析与决策等关键职能, 不仅需要实现单一军兵种内部的高效指挥与控制^[1], 还需具备跨军兵种、跨领域的协同作战能力, 其应用范围也从单一功能模块扩展至涵盖侦察、打击、防御等多维作战任务的综合性体系。体系性集成联试通过一体化集成联试环境对多型未列装的指挥控制系统进行全面联调联试的综合性检验, 在复杂作战场景下, 融合态势感知、指挥决策、火力协同等功能领域, 验证陆、海、空、天等多兵种协同作战能力。接口是各系统间进行信息交互的关键通道, 其质量优劣直接影响到各军种联合作战的可靠性与协同效能。体系性集成联试接口验证在体系集成联试层面通过多阶段、多层次的综合试验, 验证指挥控制系统之间接

口标准的一致性和互操作性^[2], 确保在真实战场环境下各军种、各领域指控系统间实现互联互通和高效协同作战, 提升指挥信息系统单系统内部及多系统之间的兼容性和稳定性。

接口验证在体系集成联试中的重要性已被广泛认可, 但在工程实践中仍面临诸多问题亟待解决。首先, 对遵循同一标准的指挥控制系统接口, 因不同研制厂家对标准的理解不同, 在该标准范围内对接口的实现存在偏差, 从而导致在集成联试阶段调试故障频发。其次, 现有接口验证方法研究已取得一定进展, 大多研究集中于单一技术或特定场景指标参数验证评估, 虽然能有效分析接口及其相关标准的正确性, 但对动态作战环境下接口的适用性支撑有限^[3], 缺乏对体系联合作战指控系统间接口的系统性与综合性验证方法。此外, 接口验证还面临跨系统信息交互、复杂的系统集成方式、标准体系碎片化等问题, 无法有效识别并解决因接口不兼容或标准执行不到位而导致的系统

间通信障碍，难以全面覆盖实际作战需求。

本文基于分层验证策略与虚实结合仿真技术，构建“分层验证策略－自动化测试平台”的综合接口验证架构。通过虚实结合仿真技术的高保真模型代替部分实装设备模拟复杂战场环境与极限处理故障，并采用分层验证策略逐级分解接口信息交互链路，自动化执行验证用例评估检验结果，形成全面、可信的接口质量验证体系。

1 接口指标体系

1.1 标准协议体系

接口的标准协议是确保各系统间能够实现高效、可靠的通信与协同工作的基础。接口相关标准主要分为基于消息传递的接口标准、基于服务架构的接口标准^[4]和基于云计算的接口标准三种类型，每种类型的接口标准都有其独特的特点和适用范围。其中基于消息传递的接口标准，主要用于定义信息系统间的数据交换格式和通信协议；基于服务架构的接口标准，旨在通过松耦合的方式实现不同系统间的功能调用与数据共享；基于云计算的接口标准，适用于分布式部署的军事指控系统，强调弹性扩展和动态资源调度能力。

标准协议规定了信息交换的标准化体系，其内容涵盖了数据格式、传输协议以及交互机制等数据交互多个方面。在数据格式方面，为确保数据在不同系统之间能够准确解析和传递信息，接口标准协议需明确数据的具体组织方式，包括数据结构定义、明确数据关联关系，以及制定统一的信息编码格式及转换规则，从而保证各系统间数据的一致性。传输协议作为接口标准的核心组成部分，旨在规范信息在网络或设备间传输的流程及规则，不仅需要满足高性能要求，还需具备较强的兼容性，以适应多种硬件平台和软件环境，主要包括通信协议的选择、数据分片策略以及重传机制等方面。交互机制进一步细化了系统间的通信流程，明确规定信息的发送方式、传递格式、结果的方式机制以及错误处理规则，使得不同系统间能够进行数据交换和功能调用，如请求－响应模式、发布－订阅模式等，这些机制为复杂任务场景下的信息交互提供了灵活的支持。此外，还需特别关注安全性，接口标准通常集成了加密算法和身份认证机制，以保护敏感信息在传输过程中不被窃取或篡改。通过规范化的标准协议，可以有效降低不同系统之间的互操作难度，提升信息共享的效率和准确性，从而为作战决策提供实时、精确的支持。

1.2 指标体系构建

接口指标体系遵循系统性、层次性与可操作性原则，结合相关标准协议，构建了涵盖功能、性能、可靠性、安

全性四个维度的接口指标体系^[5]，其核心目的是将各系统接口抽象的、定性的质量特征分解为可观测、可度量的量化指标，降低跨系统协同集成联试故障风险，提升业务流转效率。功能指标体系主要检验接口能否按照规范要求正确、完整地实现规定的各项功能，包括接口协议符合性、数据格式准确性、数据格式一致性和业务流程正确性指标；性能指标体系主要检验接口在数据传输和处理方面的效率，包括数据传输正确率、接口响应延时、数据吞吐率和高负载性能稳定性指标；可靠性指标体系是在规定的条件和时间内持续运行的能力，包括连续运转稳定性、故障恢复能力和容错处理机制指标；安全性检验接口在信息传输和交互过程中的数据安全，包括身份认证有效性和数据传输加密指标。接口验证指标体系如下图 1 所示。

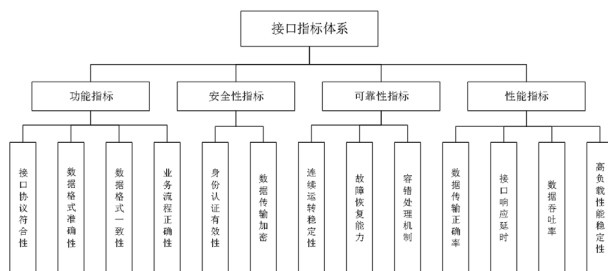


图 1 接口验证指标体系图

2 接口分层验证策略

根据系统集成层次与接口调用关系，将原本复杂的接口验证逐级分解为多个可独立管理、有序推进的验证层级^[6]，每一层聚焦特定范围内的接口质量目标，下层验证通过后方可进入上层，形成“自下而上、逐级收敛”的验证路径。针对各系统间接口的多层次特征，聚焦通信基础、协议规范与业务语义核心关注点，将接口验证按照网络传输层、标准协议层、业务功能层三个抽象层级自下而上逐级开展验证，形成“传输网络可靠、标准协议规范、业务逻辑准确”递进的验证体系。

网络传输层验证接口数据分发以及传输状态，确保数据能够在异构系统之间可靠、有序的传递。该层通过数据传输正确率、接口响应延时、数据吞吐率、高负载性能的稳定性^[7]等指标验证数据传输性能；通过连续运转稳定性、故障恢复能力、容错处理机制指标验证接口在恶劣网络条件下的数据正常传输与恢复能力。网络传输层的充分验证是上层协议与业务能够正常工作的前提，若该层存在缺陷，上层任务语义正确的消息都无法送达。

标准协议层验证接口对各类国家军用标准、工程标准以及行业标准协议的符合程度，确保交互系统的报文格式、交互流程与状态转换严格遵循既定规范。指挥控制

系统接口常涉及多种协议栈,如数据分发服务(如 DDS、KAFKA)^[8]、实时传输协议(RTP)以及基于 XML 的数据编码规范。该层主要验证接口协议符合性指标,验证内容包括:验证协议数据单元(PDU)的字段位置、长度与取值边界等数据格式;验证接口通信协议的选择、数据分片策略以及重传机制(握手、重连)等传输协议;验证接口请求-响应匹配、心跳与保活、幂等性等交互机制;以及验证身份认证有效性和数据传输加密等安全性指标^[9]。标准协议层的合规性验证能够有效避免因协议理解偏差导致的互操作失败。

业务功能层验证面向联合作战场景的实际作战流程,检验接口所承载的业务逻辑的符合性、数据内容的真实性与应用场景的正确性^[10]。业务功能层的验证方法采用场景注入与自动化测试相结合的方式,基于作战任务剖面构建正常、边界及异常的业务流程脚本,通过虚实结合仿真模拟多系统交互^[11],验证接口在完整业务闭环下的行为是否符合预期。该层主要验证数据格式准确性、数据格式一致性和业务流程正确性等功能指标。

基于分层验证策略方法各层次可并行设计用例、独立执行测试,且下层验证的完备性有效减少了上层的重复测试工作量^[12]。

3 体系性接口验证平台架构设计

3.1 接口验证平台总体架构

体系性接口验证平台总体架构主要由接入解析服务、资源管理服务、接口验证工具集、联试任务调度服务以及量化评估服务组成。通过模拟真实测试场景,对各被测系统接口的各项性能指标进行分析评估。体系性接口验证平台架构图如图 2 所示。

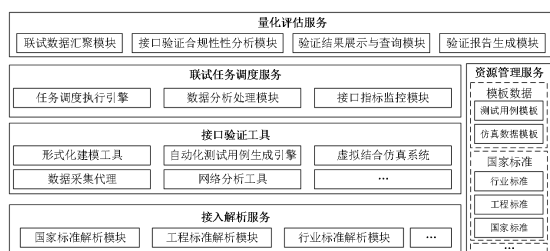


图 2 体系性接口验证平台架构图

接入解析服务负责各参试指控系统的物理接入与协议适配,通过可配置的接口适配器实现不同总线类型、通信协议和数据格式的统一接入转换,支持符合 GJB289A^[13]、GB/T28181、TCP/IP 协议等标准协议的各种指控系统接口接入一体化集成联试环境。

资源管理服务为接口验证提供所需的各类测试资源,

通过关系型、非关系型数据库存储资源数据,包括各类国家标准、工程标准、行业标准、仿真数据格式模板、接口验证及评估模型、指标采集数据、测试用例模板、测试评估结果等验证资源数据。

接口验证工具集提供验证设计的核心方法工具集,通过接口验证工具能够生成接口测试用例、模拟接口测试数据、采集指标数据等,主要工具包括形式化建模工具、自动测试用例生成引擎、虚实结合仿真系统以及各种型号的通用与专用测试软件。

联试任务调度服务负责验证任务的调度执行、测试数据的采集与监控以及异常情况的实时告警,通过分布式同步机制确保跨域接口验证的时间基准一致性和数据一致性。

量化评估服务汇总各系统接口验证结果,形成分层验证报告,基于评估模型输出联试接口的量化评估结论,并生成涵盖用例设计、接口测试、指标评估全过程的接口检验合规性证据链,为系统接口质量验证提供依据。

3.2 自动化接口验证流程设计

自动化接口验证流程通过用测试用例自动构建、测试场景与测试激励生成、实时数据采集与动态评估等主要流程,系统性解决传统手工接口测试与脚本测试中面临的测试规则分散、测试结果难追踪、测试效率低下等问题^[14],支撑各系统快速迭代融合,提升联试覆盖场景与接口验证深度。

测试用例自动构建基于系统接口定义和通信协议的核心描述文件对不同参试系统进行规范性审查,确保格式统一、内容完整、版本受控,在此基础上提取覆盖全部接口功能点的验证目标矩阵,包括命令类型全集验证、数据字段边界验证、异常场景验证和参数范围遍历验证。基于所构建的验证目标矩阵,结合状态机模型和时序图模型,自动生成抽象测试用例,并通过数据字典实现接口字段级和消息级测试参数配置干预,构建标准化的接口报文格式,支持跨系统接口之间的逻辑一致性验证。测试场景与激励生成针对系统接口业务场景特点,基于虚实结合仿真系统,模拟典型业务场景中的数据格式,复现真实接口传递的信息特征、场景条件以及战场环境的各类数据集合,自动生成符合真实作战场景的测试激励与异常激励信息。实时数据采集与动态评估能够在接口调用过程中对通信数据进行实时捕获和解码,并与相关标准规范模型进行动态比对,当测试过程偏离预期时自动给出判定结果;该自动化接口验证流程能够全流程追溯管理测试活动与标准需求、参试装备、测试操作人员等测试要素,形成接口验证结果完整追溯链(见图 3)。

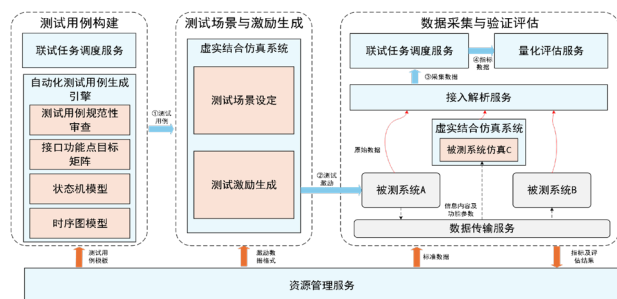


图 3 自动化接口验证流程图

4 跨域协同接口验证案例分析

随着智能化战争的到来，跨域协同联动接口的体系性验证已成为衡量其作战效能的关键环节^[15]。智能化战争强调体系化作战能力的检验与提升，跨域协同智能体系涵盖的系统种类繁多，面临的环境因素复杂，通常难以通过全实装方式有效开展复杂试验，同时较数字化方式下的训练环境与实际应用存在较大差异，导致智能协同联动算法在真实应用环境中部署后性能严重下降，而智能化产品的接口验证尤其重点关注其在作战环境与体系融合中的表现。

面向跨域协同智能联动的接口验证，通过虚实结合仿真系统将模拟实装系统、实装系统以及智能算法模型集成到一体化集成联试环境，采用分层验证策略能够有效满足跨域协同智能体系的多场景、多样本的协同接口验证需求。以某型多军种系统跨域协同智能联动方案接口验证为例，验证依据接口功能实现、测试数据需求、测试前置条件、业务逻辑特点以及遵循的信息格式标准规范等功能点，生成接口验证测试用例，结合设定多场景测试环境、正常与异常激励以及半实物仿真与实装备的有机配合，采集了各系统间在进行协同方案信息交换时的各类指标数据，包括协同方案信息、传输时间、异常状态等指标信息，验证覆盖异构数据传输总线之间的协议转换验证、跨系统数据一致性与准确性验证、数据传输效率以及异常干扰条件下的接口稳定性验证。通过体系性接口验证平台在降低联试成本的同时有效识别了跨域协同接口在协议转换、数据与标准协议符合性以及稳定性方面的多类故障隐患。

5 结语

本文介绍了基于网络传输层、标准协议层、业务功能层三层验证策略方法，设计了一套包含接入解析服务、资源管理服务、接口验证工具集、联试任务调度服务以及量化评估服务组成的体系性接口验证平台架构与自动化验证流程，能够设定多场景验证环境下的测试激励，结合虚实结合仿真系统，对跨军种系统接口交互进行多维度、全链

路验证，有效支撑各系统接口交互中标准协议的符合性以及业务逻辑的稳定性。

参考文献：

- [1] 赵鑫业，王义涛，王超等. 战场信息交换语言统一开发框架[J]. 指挥与控制学报，2021, 7(01): 46-52.
- [2] 徐享忠，汤再江，谭亚新. 作战仿真与指控系统语义互操作技术参考框架研究[J]. 系统仿真学报，2015, 27(08): 1735-1742.
- [3] 张毅，詹武，郭颖辉等. 基于信息流程仿真的作战体系结构设计验证方法[J]. 指挥控制与仿真，2019, 41(01): 131-135.
- [4] 潘昶. 基于多协议字典的通用化通信技术[J]. 兵工自动化，2019, 38(3): 31-34.
- [5] SANTOS E D, CASAS S. A catalog of API gateway metrics and its quantitative evaluation[J]. Dyna, 2025, 92(237): 106-114.
- [6] 刘畅，陈曦. 多协议融合的指控接口一致性分层验证技术研究[J]. 指挥与控制学报，2023, 9(04): 512-517.
- [7] 王欣，姚佩阳，周翔翔等. 指挥信息系统网络信息传输能力评估[J]. 计算机应用，2011, 31(8): 2033-2036.
- [8] 童佳峰. 基于 DDS 的软件接口测试方法研究[J]. 电子测试，2021(09), 113-115.
- [9] 周艳伟，杨博，张文正. 异构指控网络安全交互协议验证技术[J]. 软件学报，2022, 33(05): 1821-1838.
- [10] 王天宇. 基于情境感知的作战指挥界面动态重构模型[J]. 计算机仿真，2024, 41(08): 390-395.
- [11] 何强，刘璐等. 虚实结合仿真环境下指控系统接口全流程验证技术[J]. 计算机工程与设计，2024, 45(07): 2012-2018.
- [12] 李建军，刘浩. 军用信息系统接口分层测试与一致性验证方法[J]. 火力与指挥控制，2023, 48(07): 145-150.
- [13] 中央军委装备发展部. GJB289A-2019 军用计算机通信接口通用规范[S]. 北京：国防工业出版社，2019.
- [14] 陈峰，周凯. 异构指控系统跨平台接口自动化测试框架研究[J]. 舰船电子工程，2024, 44(05): 78-82.
- [15] 王浩然. 智能化联合作战指挥系统人机协同交互范式研究[J]. 国防科技，2024, 45(06): 89-94.

作者简介：徐记伟（1992.01-），男，汉族，河南省郸城县人，硕士研究生，工程师，研究方向：软件开发。

* 通讯作者：耿斌（1990.07-），男，汉族，江苏省南京市人，硕士研究生，工程师，研究方向：UI 设计。