文章编号：1005-8451（2015）02-0055-04

铁路客票安全系统联调联试技术的研究

周泽岩，史　宏，张　彦
（中国铁道科学研究院　电子计算技术研究所，北京　100081）

摘　要：随着国家对信息安全的重视不断提高，高速铁路客运服务系统联调联试亟需增加对客票安全系统的测试。本文从保护客票系统业务安全的角度出发，提出了一套信息安全联调联试方案，阐述了测试场景、测试内容、测试流程和测试方法等，并创新性的提出采用配置核查工具，开发基于正则表达式的测试脚本，实现对安全策略的配置核查功能。

关键词：联调联试；信息安全；客票安全系统
中图分类号：U29-39　　**文献标识码：**A

Technologies of Test on Completion for Railway Ticketing and Reservation Security System

ZHOU Zeyan, SHI Hong, ZHANG Yan
(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing　100081, China)

Abstract: With the increasing of national attention to information security, Test on Completion(TOC) for high speed railway was needed to the Railway Ticketing and Reservation System. Starting from the protection of service security point of view for the System, this paper put forward a set of test plan, including test scenarios, test content, test process and test methods. The configuration verification tool was used to develop the test script based on regular expression, implement the configuration verification function to the security policy.

Key words: Test on Completion(TOC); information security; Railway Ticketing and Reservation Security System

在新建高速铁路开通运营前，为确保高速铁路工程达到建设目标，满足系统整体性功能验证需求，将所有系统及接口匹配关系进行测试、检验、调试，以优化各系统的状态和整体系统性能，从而提高中国铁路工程建造技术水平，为高速铁路顺利开通提供科学依据[1]，这一系列的过程称为“高速铁路联调联试”。

铁路客票安全系统，实现了信息系统安全的结构化保护，杜绝未经授权的访问和蓄意攻击，为铁路客票系统提供了信息安全保障。面对各种源于内外的安全威胁与风险，铁路客票安全系统在投入运营生产之前，应与其他信息系统一样，需要通过联调联试技术手段，验证铁路客票安全系统的各项保障功能是否能正常生效。

1　铁路客票安全系统

铁路客票安全系统的安全方案，是按照 GB17859-1999《信息安全技术—计算机信息系统安全保护等级划分准则》和 GB/T25070-2010《信息安全技术—信息系统等级保护安全设计技术要求》等标准和规范的要求，建立的一个明确定义的形式化安全策略模型，将自主和强制访问控制扩展到所有的主体与客体，辅以其它方面的信息安全技术，将客票系统的安全保护环境实现结构化，达到信息安全等级保护四级要求，确保客票信息系统安全。

根据网络层次结构，将铁路客票安全系统划分为三级：铁路总公司中心、地区中心和车站。铁路总公司中心的安全职能是监控客票系统的整体安全运行状况，行使身份认证中心（CA 系统信任根节点）的功能，并保障铁路客票系统自身的信息系统安全，达到等级保护四级要求；地区中心的安全职能是监控本区域的客票系统的安全运行状况，本区域身份认证中心（CA 系统信任子节点），采用网络管控器、CA 认证服务器、安全通信系统、配置管理系统和安全审计系统等技术手段，保障地区中心客票系统的信息系统安全，要求达到信息安全等级保护四级要求；

收稿日期：2014-10-08
作者简介：周泽岩，工程师；史　宏，研究员。

车站的安全职能是保护客票系统终端安全，包括对客票终端、交换机、路由器等设备的实时监控，并采用网络管控器、安全通信系统和配置管理器等技术手段，保障车站客票系统的信息系统安全，采用安全隔离与信息交换系统（网闸）进行安全隔离，保障与旅客服务系统的数据安全交互，要求达到保护等级 3 级要求。铁路客票安全系统部署示意图如图 1 所示。

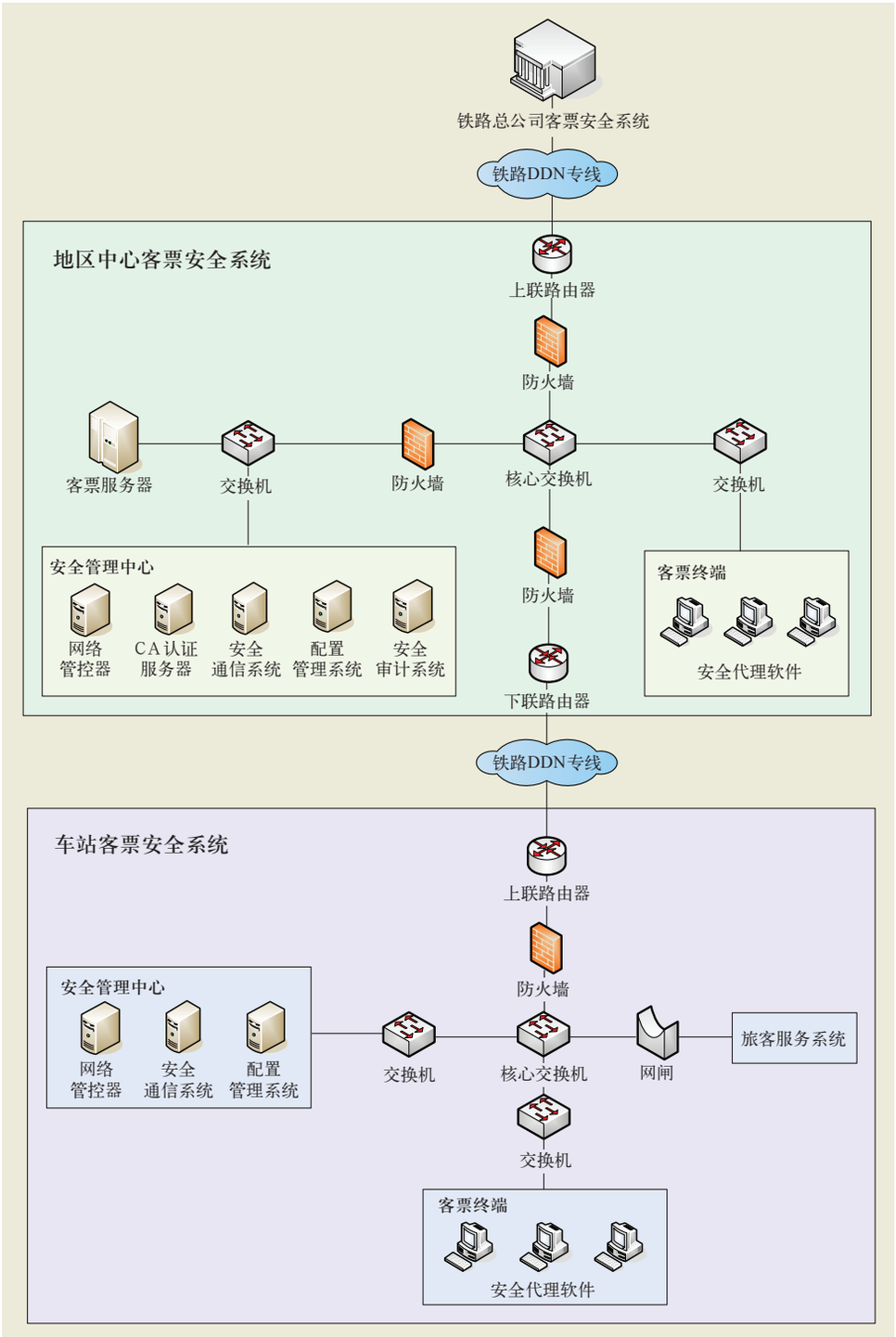

图1 铁路客票安全系统部署示意图

2 场景设计

由于高速铁路联调联试的实施范围都是在车站层面，故本文只对车站客票安全系统的联调联试方案展开探讨。针对车站铁路客票安全系统的网络部署结构，和所采用的安全设备，从对客票系统业务防护的角度，设计 7 个测试场景，详细的测试场景内容如下。

2.1 测试环境检查

在开展联调联试工作前，需要在现场对系统的准备情况进行全面检查，检查的重点是安全系统的硬件安装情况，软件调试情况和运行数据的配置情况，包括：硬件是否部署并调试完成，软件是否完成安装并初始化，网络是否畅通等测试环境检查。

2.2 安全配置核查

采用配置核查工具，设计基于正则表达式设计配置核查脚本，对各项安全设备的安全策略实施配置核查。

2.3 身份鉴别场景

将车站客票安全系统提炼出 3 个核心的身份鉴别过程，即对安全代理登录过程、安全设备登录过程、安全管理系统登录过程进行身份鉴别测试。

2.4 访问控制场景

将车站客票安全系统提炼出两个重要的访问控制层面，即对窗口售票终端访问客票服务器、网络

边界设备进行访问控制测试。

2.5 安全管理场景

从保护车站客票系统业务的角度，设计出安全管理层面的测试内容，即对节点管理、用户管理、USB-Key 管理进行安全管理测试。

2.6 集中监控场景

依据安全监控的层面，提出集中监控的测试内容，即对网络设备、主机设备、安全代理、安全设备进行集中监控测试。

2.7 安全审计场景

从系统日志、安全事件两个层面对安全设备展开审计测试。

3 测试内容

3.1 测试环境检查

3.1.1 硬件测试环境检查

网络管控器、安全通信系统、防火墙、安全隔离与信息交换系统（网闸）等安全设备、配置管理系统服务器等是否部署和调试完成。

3.1.2 软件测试环境检查

配置管理系统和安全代理系统等是否安装并初始化完成。

3.1.3 网络环境检查

客票广域网、车站客票局域网、车站旅客服务系统局域网是否畅通。

3.1.4 相关系统环境检查

窗口售票系统、旅客服务系统、客票系统与旅客服务系统的接口服务器是否安装并调试完成。

3.2 安全配置核查

3.2.1 系统配置核查

检查安全设备的相关系统配置是否正确配置完成，保障设备的正常运转，内容包括：配置管理系统、安全代理系统、安全通信系统、防火墙、网络管控器、安全隔离与信息交换系统等安全设备等。

3.2.2 安全策略核查

检查安全设备的相关安全策略是否正确配置完成，保障设备的安全功能正常配置，内容包括：配置管理系统、安全代理系统、网络管控器、防火墙、安全隔离与信息交换系统等安全设备等。

3.3 身份鉴别场景

检查各项安全系统或安全设备的用户登录身份鉴别功能是否正常生效，内容包括：安全代理系统、配置管理系统、防火墙、安全隔离与信息交换系统等。

3.4 访问控制场景

3.4.1 售票终端访问控制测试

售票终端主要依靠安全代理系统实现对客票服务器的访问控制，主要测试安全代理系统正常登录及异常登录的各种情况，以及不同的用户登录后，具有不同的访问控制权限等。

3.4.2 网络边界访问控制测试

负责网络边界的访问控制，主要是依靠两个安全设备：防火墙和安全隔离与信息交换系统，主要测试防火墙的包过滤功能和其他静态规则是否正常生效，测试安全隔离与信息交换系统的安全策略是否正常生效。

3.5 安全管理场景

配置管理系统可以实现对网络设备、安全设备、安全策略等内容的管理功能，验证安全管理功能是否正常生效，测试内容包括：节点管理、USB-Key 管理、用户管理和安全策略管理等。

3.6 集中监控场景

配置管理系统可以对网络设备和安全设备等实现集中监控的功能，验证集中监控功能是否正常生效，测试内容包括：对路由器、交换机、售票终端、防火墙、网闸、网络管控器、安全隔离与信息交换系统等设备的安全监控功能。

3.7 安全审计场景

当出现系统入侵等安全事件时，安全审计是进行事件追踪的重要依据，本场景主要测试各项安全设备的安全审计功能是否正常生效，检查内容包括系统日志和安全事件，被测设备包括：配置管理系统、防火墙、安全隔离与信息交换系统等。

4 测试流程

铁路车站客票安全系统的联调联试工作大致分 6 个过程，如图 2 所示。

（1）根据高速铁路工程需要，成立信息安全联调联试项目小组，明确分工，落实职责；

（2）根据高速铁路工程实际情况，编制联调联试大纲，提交铁路总公司、铁路局、客专公司审查，明确测试目的、范围和内容；

（3）与集成商交流系统概况和功能，编制测试用例，明确工作内容；

（4）开展现场联调联试工作；

（5）整理测试结果，认真分析试验数据，准备编制检测报告的编写；

（6）完成动态检测、联调联试等报告的编制和修改工作。

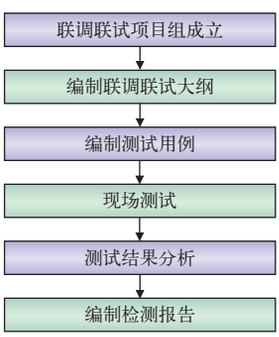

图2 铁路客票安全系统联调联试测试流程

5 测试方法

铁路客票安全系统保障功能的联调联试，依据铁路行业标准、铁路客票安全系统的设计方案、国家信息安全相关测评标准，采用专业的安全测评工具，运用科学的方法和手段，验证信息安全保障的各项功能是否能正常生效。

5.1 检查

通过直接访问配置管理系统、网络设备、安全设备等，检查安全保障策略是否合理，是否配置完成。

5.2 手工检测

使用专业的测试方法，直接操作 SOC 管理系统、网络设备、安全设备等，执行有效的操作指令，根据测试结果分析安全保障功能是否正常生效。

5.3 工具检测

借助配置核查等安全检测工具，对被测设备发送相关指令，根据正则表达式筛选返回结果，与期望结果值进行对比，检测测试结果是否与期望值一致。

部分检测项不能在图形界面上操作，不能获取测试结果，需要借助专业的测试工具进行检测。本方案采用配置核查设备，通过自主开发测试脚本，实现对网络管控器、网闸、安全通信平台和主机管控器的配置核查操作。配置核查设备工作原理：通过配置核查设备，将操作指令发送给安全设备，设备返回结果数据信息，测试脚本利用正则表达式对结果进行筛选，提取出需要的数据，与预先设定的期望返回值进行对比，检测测试结果是否与期望值一致。

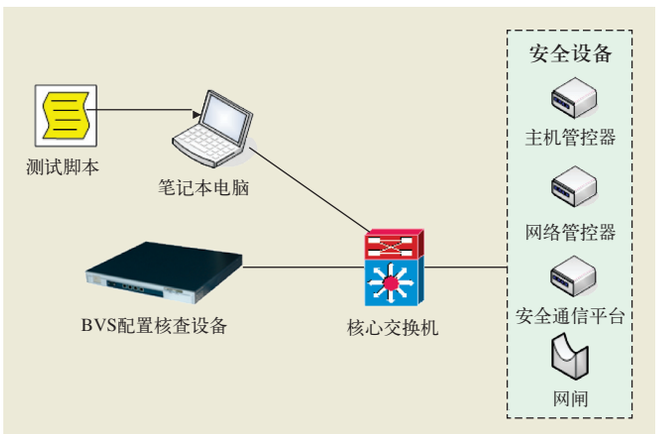

图3 配置核查工作原理示意图

6 结束语

本文针对铁路客票安全系统的保障功能提出了测试方案，从保护客票系统业务安全的角度，提出 7 个测试场景，内容包括环境检查、配置核查、身份鉴别、访问控制、安全管理、集中监控和安全审计。针对部分安全设备的安全策略不易在图形界面上进行检测，提出采用配置核查工具，设计了基于正则表达式的测试脚本，实现对安全策略的配置核查功能，且能够正确输出测试结果。本方案还有不完善之处，在未来的联调联试工作实践中不断修正和改进。

参考文献：

[1] 康 熊 . 高速铁路联调联试技术 [J]. 中国铁路，2010（12）.

[2] 崔德山，张 彦，刘育欣 . 高速铁路客运服务系统联调联试技术研究 [J]. 铁路计算应用，2010，9（11）.

[3] 朱建生，单杏花，周亮瑾，刘春煌，刘 强 . 中国铁路客票发售和预定系统 5.0 版的研究与实现 [J]. 中国铁道科学，2006（11）.

责任编辑 徐侃春