LKJ 车载数据无线换装系统安全设计

闫龙[1]，尹亮[1]，赵志宽[2]

1. 国能新朔铁路有限责任公司机务分公司，内蒙古 鄂尔多斯 010300

2. 河南思维自动化设备股份有限公司，河南 郑州 450001

摘　　要： 按照《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》以及铁路轨道交通等相关标准要求，科学合理评估 LKJ 系统合规差距和安全风险，协助其合理确定安全保护措施，在此基础上科学规划设计一整套完整的安全体系，充分发挥国密安全技术与产品、工业控制系统安全防护产品和服务的优势，为 LKJ 车载数据无线换装系统提供全方位、多层次的深度防护，建设基于 LKJ 车载数据无线换装系统纵深防御的一体化防御体系，全面提升系统的自身免疫能力，确保支撑列车运行安全的信息基础设施和重要设备安全运行的必然要求。

关 键 词： 列车运行监控装置；无线换装；车载数据；系统安全；国密；安全防护

Safety Design of LKJ Vehicle Data Wireless Replacement System

Yan Long[1], Yin Liang[1], Zhao Zhikuan[2]

1.China Energy Xinshuo Railway Co., Ltd. Locomotive Branch, Ordos, Inner Mongolia 010300

2.Henan Thinking Automation Equipment Co., Ltd. Zhengzhou, Henan 450001

Abstract: The safety design of the LKJ onboard data wireless replacement system follows the basic requirements of GB/T 22239-2019 Information Security Technology Network Security Level Protection and relevant standards for railway rail transit. It scientifically and reasonably evaluates the compliance gap and safety risks of the LKJ system, assists it in determining reasonable security protection measures, and based on this, scientifically plans and designs a complete set of security systems, fully leveraging national security technology and products The advantages of industrial control system security protection products and services provide comprehensive and multi-level deep protection for the LKJ onboard data wireless replacement system. Building an integrated defense system based on the LKJ onboard data wireless replacement system's deep defense, comprehensively enhancing the system's self immunity, and ensuring the necessary requirements for the safe operation of information infrastructure and important equipment supporting train operation safety.

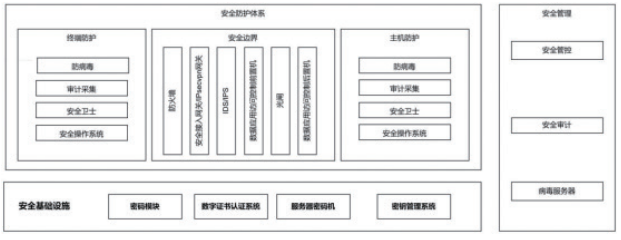
Keywords: LKJ; wireless replacemen; onboard data; system safety; national secrets; safety protection

根据车载 LKJ 车载数据无线换装系统的业务特点、当前任务和未来发展需要，结合国家网络安全等级保护相关要求，制定针对性的系统安全设计方案[1-2]，为 LKJ 车载数据无线换装系统，构建国密安全应用、等级保护的安全监测、态势感知、边界安全防范、等技术手段对 LKJ 车载数据无线换装系统关键信息基础设施安全防护体系，指导完成车载 LKJ 车载数据无线换装系统建设工作。

LKJ 系统整体安全防护技术方案主要包括：国密安全防护体系设计、等级保护安全防护体系设计、安全监控与运维设计、车载操作系统安全加固、安全应急响应设计几部份组成。

一、安全体系统架构

基于目前轨交行业中的现存安全风险及脆弱性，结合车载 LKJ 系统的业务特点，以国密技术为基础，针对车载 LKJ 系统依据政策标准从不同的安全防护点入手，结合“白名单”技术手段，采用主动免疫系统防御机制，提供基于业务模型和关键应用执行程序的可信体系[3]，阻止非授权及不符合预期的网络访问或执行程序运行，实现对车载 LKJ 系统互联边界安全、主机安全、行为操作安全等进行主动安全防御，降低车载 LKJ 系统完整性及可用性被破坏的风险，为车载 LKJ 系统网络打造一套安全闭环纵深防御体系。



> 图1　安全防护体系架构

整体框架分别由安全防护体系、安全管理体系、安全基础设施三部分构成，三套体系分别承担车载 LKJ 系统中的安全防护及安全管理能力。

作者简介：闫龙（1985.11-），男，汉族，内蒙古包头土默特右旗人，本科，工程师，研究方向：铁路机车。

（一）安全防护体系

安全防护体系分别由终端安全防护体系、边界安全防护体系[4]、主机安全防护体系组成，其中终端安全防护体系，针对 LKJ 车载终端存在的安全风险通过安全操作系统、安全管控、安全模组等方式实现终端计算、网络的整体安全防护；边界安全防护由防火墙、安全接入网关、IDS/IPS 入侵检测等产品等构建，实现安全边界的安全防护、授权访问、入侵防范等能力，提升整体网络的安全防御能力；主机防护由安全操作系统、安全管理组件、防病毒软件等构成实现对地面系统主机的计算环境的安全防护。

（二）安全管理体系

安全管理体系由安全管控、安全审计、防病毒等产品构成，为保障 LKJ 车载数据无线换装系统的安全、稳定运行。其中安全管控系统实现对 LKJ 系统的基本管理，涉及本系统内的软硬件资产管理、本系统内的人员管理、人员数字证书发放撤销等日常安全管理工作；安全管控系统通过制定、下发安全策略实现对主机、安全边界的安全管控[4]；实时收集系统内设备的运行日志，实现对系统内设备的运行状态的检测，并对异常状态实时告警；安全审计实时收集系统内各个运行主体的运行日志，对系统的安全事件进行审计，确保系统内的主机、网络等运行主机的运行活动是授权许可的，并对非授权的活动实施告警。

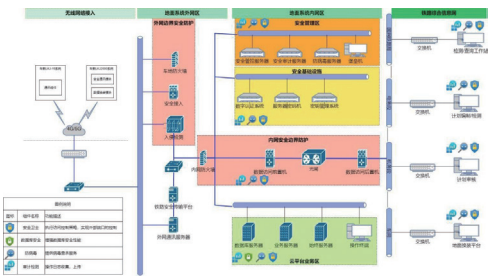
（三）安全基础基础设施

本方案是参照《LKJ 车载数据无线换装系统技术方案》和国标 GB/T22239-2019《信息技术信息系统安 全等级保护基本要求》等相关要求设计，系统整体以身份鉴别构建基于策略的安全访问控制机制，并对访问行为进行入侵检测，实现了对整体系统的安全管控。安全基础设施是为整体系统提供基础安全服务，保障系统的基本安全运行。安全基础设施主要有密码模块、数字认证系统、服务器密码机、密钥管理系统等组成。其中密码模块和数字认证系统为 LKJ 车载终端、地面系统主机、堡垒机等提供双因素认证，保证合法、授权用户访问系统[5]；为 LKJ 车载终端网络传输提供数据加密服务；服务器密码机和密钥管理系统为系统提供商用密码加密基础服务和密钥保存服务，实现地面系统的数据安全传输与存储，为整个系统的安全提供基础保障。

二、安全体系部署

（一）安全架构

针对 LKJ 车载数据无线换装系统的系统架构，结合本方案的安全技术体系架构，形成了 LKJ 车载数据无线换装系统安全体系的部署架构，如图所示：



> 图2　安全架构图

LKJ 车载数据无线换装系统整体可分为无线区域、地面系统区域、内网业务区。针对地面系统，基于安全防护要求[6]，形成了 5 个子分区，分别是外网边界安全防护、内网边界安全防护、安全管理区、安全基础设施、云平台业务区。

（二）外网边界安全防护

主要是针对无线接入的外部网络攻击。其组成由防火墙、安全接入、入侵检测等系统组成。防火墙实现对非授权设备网络访问的阻断，入侵检测实现对网络攻击行为的检测和阻断，防火墙和入侵检测结合是实现了非授权设备和违规行为的阻断。安全接入构建了 LKJ 车载终端与地面系统的安全通讯链路，实现数据的安全传输，防止业务数据泄露。

（三）内网边界安全防护

主要针对内部网络设备对地面系统的网络攻击以及地面系统对内部网络的攻击。为了保障了系统的可靠性，因此采用了负载均衡设计。与外部边界安全防护相似，内网边界防护系统继续采用防火墙和入侵检测系统实现对内网、地面系统相互的网络攻击行为的阻断。针对地面系统与内网平台进行数据交换存在的安全风险，提供数据应用访问控制系统，实现不同网络之间数据传输单向，防止通过隐通道的安全风险，同时数据应用代理实现了协议剥离和协议分析功能，杜绝了网络传输过程中的协议攻击行为，避免了诸如 sql 注入攻击等隐蔽攻击行为，极大的保障了数据传输的安全。

（四）安全管理区

主要实现地面系统的运行体系进行管理，保障高效、安全、可靠、稳定的业务运行环境[7]。安全管理基于三权分立原则设计，通过事前策略规划、事中访问控制、事后安全审计的面向业务的全链条的安全管控。

（五）安全基础设施

主要为系统提供基础的安全防护，包含身份认证、身份鉴别、数据加密、密码保存等安全服务和业务系统，用于为安全防护提供基础的身份鉴别以及安全管理提供基本的认证、加解密服务等。

三、安全平台

安全防护体系分别由边界安全防护、主机安全防护组成，实现对 LKJ 车载数据无线换装系统的整体安全防护。

（一）边界安全防护

边界安全防护分为内网边界防护和外网边界安全防护两部分组成。内网边界防护主要是地面系统连接铁路系统内部业务网络的部分，实现内部业务系统与地面系统之间的数据交互的安全防护；外部边界防护主要为地面系统与 LKJ 车载系统通过无线网络的数据通讯提供安全保障。内部边界防护和外部边界防护都遵守等级保护要求由防火墙、入侵检测、安全接入、数据交换平台等构成，具备边界防护、访问控制、入侵检测、病毒防护等基基本功能，同时边界防护系统纳入统一的安全管理。

（二）主机安全防护

主机安全防护系统主要针对地面运行系统中运行的主机以及

LKJ 车载终端系统存在的 安全风险，通过安全加固和安全管控或者安全卫士实施，保障主机或者终端的运行环境安全、可信、可控。主机安全防护系统主要由安全加固或者安全操作系统、安全管控或者安全卫士、防病毒软件、数据库安全组件等部分组成。

系统安全加固 / 安全操作系统，实现主机的可信度量，防止恶意代码或者非法应用使用。 避免系统受到未知病毒或代码的攻击，保证系统的运行安全。

安全管控 / 安全卫士，通过安全监管平台下发的安全策略实现主机或终端的安全管控。防止非授权的软硬件端口被访问（例如 Usb 口、串口、蓝牙、Wifi 等）。

防病毒软件实时监控系统内运行环境是否存在病毒软件或者类似病毒的攻击行为，确保系统的运行的稳定、安全。

数据库安全组件实现对数据库安全管控，确定授权用户受控访问数据，并对数据库访问行为进行安全审计。

四、安全管理

安全管理区。主要实现地面系统的运行体系进行管理，保障高效、安全、可靠、稳定的业务运行环境。安全管理平台主要由安全管控系统、安全审计审计系统、防病毒系统组成[8]，实现对地面系统所有的设备运行维护和管理。

（一）安全管控系统

安全管控系统实现对系统内运行的设备以及使用者进行监控、管理。安全管理系统基于安全策略规则实现对管控主体的管控，针对不同的业务需求，为不同的网络设备和用户制定不同的安全策略，并下发给终端安全管控组件或者安全卫士，并实时监控策略执行情况。

（二）安全审计系统

安全审计实时收集系统内各个运行主体的运行日志，对系统的安全事件进行审计，确保系统内的主机、网络等运行主机的运行活动是授权许可的，并对非授权的活动实施告警。

（三）防病毒系统

针对本系统中安全计算环境面临病毒及恶意软件攻击的安全风险，由反病毒系统提供了全方位的信息安全保护，可以有效地保护企业系统的安全和稳定运行。

五、安全设施

安全基础设施主要为系统提供基础的安全防护，包含身份认证、身份鉴别、数据加密、密码保存等安全服务和业务系统，用于为安全防护提供基础的身份鉴别以及安全管理提供基本的认证、加解密服务等。

（一）数字认证系统

数字证书认证系统（certificate authority system，简称：CA），是 PKI/CA 应用基础产品，为生命周期内的数字证书进行全过程的管理。通过为业务系统的用户或设备签发数字证书，有效解决网络应用数据传输的安全性问题、数据的完整性问题、身份认证问题和防抵赖问题，为网络应用提供完善的安全保障。产品可广泛应用于电子政务、电子商务、云计算、金融、物联网等对 PKI 技术有强需求的领域。该产品采用我国密码行业标准定义的“双证书 + 双中心”建设机制，双证书指签名证书和加密证书，双中心指密钥管理中心和数字认证中心。其中数字认证中心由数字证书注册系统、数字证书签发系统、在线证书查询系统、证书目录服务系统四个子系统组成。密钥管理中心和数字证书认证中心都需要依赖服务器密码机提供的密码服务。

（二）服务器密码机

密码机能够适用于各类密码安全应用系统进行高速的、多任务并行处理的密码运算，可以满足应用系统数据的签名 / 验证、加密 / 解密的要求，保证传输信息的机密性、完整性和有效性，同时提供安全、完善的密钥管理机制。

密码应用系统通过调用密码机提供的标准 API 函数来使用密码机的服务，密码机 API 与密码机之间的调用过程对上层应用透明，应用开发商能够快速的使用密码机所提供的安全功能。密码机 API 接口符合《密码设备应用接口规范（GM/T0018-2012）》标准接口规范，通用性好，能够平滑接入各种系统平台，满足大多数应用系统的要求，在应用系统安全方面具有广泛的应用前景。

（三）秘钥管理系统

密钥管理系统提供对生命周期内的加密证书密钥对进行全过程管理的功能，包括密钥的生成、分发、存储、更新、归档、撤销、备份、恢复和销毁等，提供基于数字证书的身份认证及完善的安全审计等功能，为用户创建安全便捷的密钥使用环境。

密钥管理系统是国家密码管理局鉴定通过的密码算法和硬件密码加密设备，遵循国家密码管理局发布的 GM-T 0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》等标准规范的要求，与数字证书认证系统共同在 PKI 应用领域提供技术和策略方面的安全保障。

六、安全辅助工具

针对系统实施运维过程中存在的问题，提供两组安全套件，用于升级和运维服务。

（一）产线证书烧写工具

针对 LKJ 车载数据无线换装系统，承载密码服务的载体（安全芯片、安全模组）通常和 LKJ 车载数据无线换装系统办卡继承在一起。传统的针对密码服务载体的发证方式是面向密码服务的载体（例如 Usbkey、TFkey 等）直接插入发证终端，即可完成证书的方法[10]。本系统中密码服务载体集成到 LKJ 车机系统中，原有的密码模块的接口以及那个封装在 LKJ 车机系统内部，除非拆卸，否则无法采用原有的方法发放证书。

根据 LJKJ 车机系统，开发产线证书烧写工具，部署在产线专用 PC 机，通过 LKJ 车机板卡连接车载板卡上的安全芯片，访问发证接口服务为设备申请签发设备证书。为第三方集成，可供 SDK 形态。

（二）国密中间件

针对 LJK 车载数据无线换装系统中存在基于 WEB 形态的网络传输机制，针对 WEB 传输过程中存在的安全风险需要进行基于国密算法的加密改造。通常 WEB 应用的国密改造需要在服务端的算法、证书等改造，客户端浏览器也需要进行算法和证书等改造，有一定的工作量，且可能影响业务的发展。

针对已有、在建的 WEB 应用系统提供一种透明的国密改造。基于 Nginx 反向代理原理，实现对 WEB 应用的透明加密传输改造，数据通道支持国产密码算法，支持国密数字证书的双向认证，支持信创的国密浏览器。通过配置可实现 WEB 应用的安全传输，避免对 WEB 应用的改造。同时该组件支持同时可支持同时多 WEB 应用。

七、结束语

LKJ 车载数据无线换装系统建设不仅要满足网络安全等级保护2.0和《网络安全法》等安全合规性需求，还需要在铁路系统联动趋势加速、信息安全形势日益严峻的今天，充分保障 LKJ 系统业务和数据资产不受威胁[9]。如何在 LKJ 系统建设之初就统筹规划好安全体系建设，使之既能满足等级保护要求，又能充分发挥安全技术体系的有效性，抵御新威胁，切实地解决安全问题，减少事故发生的概率，注定成为 LKJ 业务基础架构的必然要求和重点关注对象。

参考文献

[1] 何之煜，李辉. LKJ 无线换装车地数据传输关键技术研究［J］. 铁道通信信号，2023,59(5):67-71.

HE Zhiyu,LI Hui.Research on Key Technologies of LKJ Remote Reloading Process Between Train and Ground［J］. Railway Signalling & Communication,2023,59(5):67-71.

[2] 姜永富. 把握规律 化解风险 着力提升铁路通信本质安全水平［J］. 铁道通信信号，2023,59(4):1-6.

JIANG Yongfu.Grasp the Rules and Resolve Risks Strive to Improve the Intrinsic Safety Level of Railway Communication［J］. Railway Signalling & Communication,2023,59(4):1-6.

[3] 曹玉. 深化安全基础建设 提升电务本质安全 服务铁路现代化高质量发展——2023年全路电务重点工作［J］. 铁道通信信号，2023,59(2):1-5.

CAO Yu.Deepen the Safety Infrastructure Construction, Improve the Intrinsic Safety of Signaling Service, Serve the High-quality Development of Railway Modernization - the Key Work of Signaling Service of the Whole Railway in 2023［J］. Railway Signalling & Communication,2023,59(2):1-5.

[4] 叶永华. 提升 LKJ 数据管理水平的实践［J］. 铁道通信信号，2023,59(1):90-93.

YE Yonghua.Practice of Improving LKJ Data Management Level［J］. Railway Signalling & Communication,2023,59(1):90-93.

[5] 陈庆华，何镭强，牛勤，等. LKJ 车载数据无线换装功能实现［J］. 铁道通信信号，2020,56(12):6-9，13.

CHEN Qinghua,HE Leiqiang, NIU Qin, et al. Realization of LKJ Onboard Data Replacement via Wireless Transmission［J］. Railway Signalling & Communication, 2020, 56(12):6-9,13.

[6] 郑理华，李一楠，阳亦斌. LKJ 车载数据无线远程换装系统设计［J］. 铁道运输与经济，2018,40(9):51-56.

ZHEN Lihua,LI Yinan, YANG Yibin. A Design of LKJ Onboard Radio Remote Data Reloading System［J］. Railway Transport & Economy, 2018,40(9):51-56.

[7] 朱晓慧. 列车运行监控记录装置软件设计与实现［J］. 信息通信，2015(12):282-283.

[8] 路峻崴，王晓霞. 机车 LKJ 监控装置数据换装卡控管理信息系统［J］. 科技创新与生产力，2014(7):97-99.

LU Junwei,WANG Xiaoxia. LKJ Locomotive Facelift Card Data Monitoring Device Control Management Information System［J］. Sci-tech Innovation and Productivity, 2014(7):97-99.

[9] 迟学力. LKJ 车载基础数据换装方案探讨［J］. 中国铁路，2015(10):51-53.

CHI Xueli.Discussion on Transform Plan of LKJ On-board Basic Data［J］. China Railway, 2015(10):51-53.

[10] 刘晓虎. 基于无线网络技术实现 LKJ 车载数据的换装［J］. 铁路计算机应用，2012,21(7):52-54.

LIU Xiaohu. Implementation of on-board data replacement based on wireless netword technology［J］. Railway Computer Application, 2012,21(7):52-54.