城市轨道交通车辆智能运维系统信息安全技术方案

皮　魏
（株洲中车时代电气股份有限公司，412001，株洲）

摘　要　［目的］随着城市轨道交通规模迅猛增长，车辆运维信息化和智能化应用日趋广泛，城市轨道交通车辆智能运维系统的信息安全问题逐渐凸显和亟待解决。［方法］基于城市轨道交通车辆智能运维系统可能面临的软件漏洞、系统性防护缺失、网络传输安全等诸多信息安全风险和问题，参考多项国家和行业的信息安全标准，体系化地提出了安全分区、边界隔离、纵向认证、集中监管的信息安全防护技术方案。通过软件加固、访问控制、安全审计、入侵防范保护设备主机的安全；通过车载、车地、地面各通信网络之间的安全分区、边界隔离、安全传输、鲁棒网络保护网络传输的安全；通过管控保护业务数据的存储、传输、应用、销毁各环节提高其安全性；通过身份认证、会话管理、访问控制、安全审计、入侵防范保护应用平台的安全；通过分权管理和集中管控实现全系统的安全管理中心。［结果及结论］构筑的信息安全防护技术体系具备系统性、统一性、全面性，避免车辆智能运维系统遭受恶意攻击和非法入侵，保护系统安全性，从而实现安全、高效、可靠的城市轨道交通车辆运维。

关键词　城市轨道交通；车辆；智能运维；信息安全
中图分类号　TP393.08；U231.94
DOI：10.16037/j.1007－869x.2024.06.051

Technical Solution to Information Security of Intelligent Operation and Maintenance System for Urban Rail Transit Vehicles

PI Wei
（Zhuzhou CRRC Times Electric Co., Ltd., 412001, Zhuzhou, China）

Abstract　［Objective］With the rapid growth of urban rail transit scale, the application of information-based intelligent vehicle operation and maintenance system becomes increasingly extensive, and the information security problem of the intelligent vehicle operation and maintenance system for urban rail transit becomes prominent gradually and needs to be solved urgently. ［Method］Based on the information security risks and problems that the intelligent operation and maintenance system for urban rail transit vehicles may face, such as software vulnerabilities, systematic protection missing, network transmission security, etc., and with reference to a number of national and industrial information security standards, the technical solutions to information security protection are systematically proposed, including security zoning, boundary isolation, vertical authentication, and centralized supervision. The device host security is safeguarded by software hardening, access control, security audit and intrusion prevention. The network transmission security is safeguarded by secure partition, boundary isolation, secure transmission and robust network of the communication networks between vehicle-mounted, vehicle-ground and ground communication networks. The business data security is improved by controlling and protecting the processing steps including storage, transmission, application and destruction. The security of application platform is safeguarded by identity authentication, session management, access control, security audit and intrusion prevention. The security of the whole system management center is implemented through decentralized management and centralized control. ［Result & Conclusion］A systematic, unified and comprehensive information security protection technology system is constructed to prevent the vehicle intelligent operation and maintenance system from malicious attacks and illegal intrusions, and protect the system, so as to achieve safe, efficient and reliable vehicle operation and maintenance in urban rail transit.

Key words　urban rail transit; vehicle; intelligent operation and maintenance; information security

近年来，我国城市轨道交通发展迅速，运营规模、客运量、在建线路长度、规划线路长度均屡创历史新高。数以万计的城市轨道交通车辆在线路上载客运输，其繁重的车辆运维工作正逐步向数字化、自动化和智能化方向转型。城市轨道交通车辆智能运维系统（以下简称“车辆智能运维系统”）应运而生。然而在车辆智能运维系统为车辆运维带来高效便捷的同时，信息安全风险和漏洞也随之增多。随着国家、政府及行业各级主管部门以及企业对信息安全问题日趋重视，车辆智能运维系统的信息安全问题亟待解决。

1　车辆智能运维系统概述

车辆智能运维系统主要包含车载监测子系统、

轨旁检测子系统、车辆检修子系统及地面运维子系统，其通过车地传输子系统，汇集从单个车辆设备，到单列列车、单条线路，乃至整个线网的多源车辆数据，采用大网络带宽、多并发接入、高处理性能、大容量存储的大数据存储分析集群，结合云平台、数据挖掘、机器视觉及深度学习等技术，实现车辆全生命周期数字资产管理，最终为运营和检修工作人员提供高质高效的服务。车辆智能运维系统框架如图 1 所示。

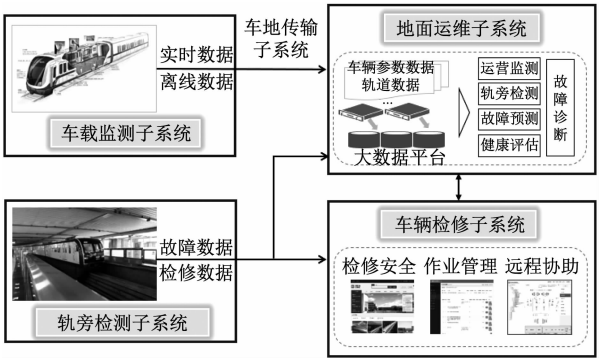

图 1　车辆智能运维系统框架图

Fig. 1　Framework diagram of vehicle intelligent operation and maintenance system

车载监测子系统采集汇总车辆各关键子系统的实时数据与离线文件，实现对车辆数据的融合、处理、存储及分析，并将数据发送给地面运维子系统；轨旁检测子系统通过在轨道旁边部署各类检测设备对回库车辆进行多维度的日常故障检测，提高车辆故障检测效率；车辆检修子系统智能化管理整个检修流程，提高检修作业效率，降低成本；车地传输子系统借助无线通信网络，为车辆智能运维系统提供车辆和地面的网络传输通道；地面运维子系统对各子系统的高频、大并发海量数据进行接收、解析、存储、分析及展示，并承载主要业务流程，为车辆运维提供决策依据，实现车辆高质、高效的运维管理。

2　信息安全面临的风险

随着车辆智能运维系统所涉及的设备和系统越来越多，网络传输压力越来越大，信息集成融合度越来越高，设备、主机、网络、系统及平台已不再是信息孤岛，其对外暴露的设备接口、网络设备、通信链路及数据协议等很多方面都缺少安全防护。攻击者可通过多种攻击手段入侵设备、网络、系统及平台，从而造成不可估量的损失。

2.1　软件漏洞风险

车辆智能运维系统中涉及的嵌入式设备、服务器、应用终端绝大部分采用了操作系统、中间件和应用软件相结合的软件架构。这些软件或多或少地存在着各种各样的信息安全漏洞，尤其是当版本较低，或未及时修复漏洞时，其漏洞已被明确暴露。此外，部分嵌入式设备和服务器因其更新或修复很不方便，长期存在漏洞，更易遭受数据窃取和恶意攻击。攻击者可借助该台设备或服务器入侵整个车辆智能运维系统，甚至入侵到城市轨道交通的其他应用系统和关键基础设施中。

2.2　系统性防护缺失风险

车辆智能运维系统的系统性防护体系缺失，部分防护措施和功能只进行局部防护，各子系统之间，各车载设备、服务器及应用终端之间，以及车载网络、车-地网络及地面网络之间缺乏统一的防护管控机制。比如：缺乏统一的用户登录管理及访问权限控制、数据安全管控及安全审计机制、软件防护管理等。这样各自为战的防护模式可能造成各设备、各子系统、各网络的防护水平不一致，进而造成某单个设备或单个子系统的某单方面的信息安全防护不足，从而影响到整个车辆智能运维系统。

2.3　网络传输安全风险

车辆智能运维系统需要通过网络传输海量数据，部分关键数据还需要借助公共无线网络进行传输，故公共无线网络所面临的信息安全风险也随之而来。此外，目前传输的数据报文大部分采用明文传输，其传输认证也只采用了简单的用户名和密码机制，可见数据报文传输的安全防护薄弱，面临网络攻击的威胁。如此薄弱甚至无防护的网络传输势必容易遭受攻击者对网络数据的窃取、篡改、伪造和破坏，网络传输中存在的信息安全漏洞也将会为攻击者提供通过网络入侵车载系统和地面系统的途径，从而会造成系统级的信息安全风险和威胁。

3　信息安全防护技术方案

针对车辆智能运维系统面临的信息安全风险和问题，依据“安全分区、边界隔离、纵向认证、集中监管”的策略，参考 GB/T 22239—2019《信息安全技术 —网络安全等级保护基本要求》和 T/CAMET 11001.3—2019《智慧城市轨道交通 信息技术架构及网络安全规范 第 3 部分：网络安全》中的相关技

术要求，对车载监测、轨旁检测，车辆检修和地面运维等各子系统的嵌入式设备、工控机、服务器、网络传输、应用平台进行信息安全防护，以保证车辆智能运维系统的安全性。信息安全防护方案主要内容分为设备主机、网络传输、业务数据、应用平台、安全管理中心五部分。车辆智能运维系统信息安全技术方案框架如图 2 所示。

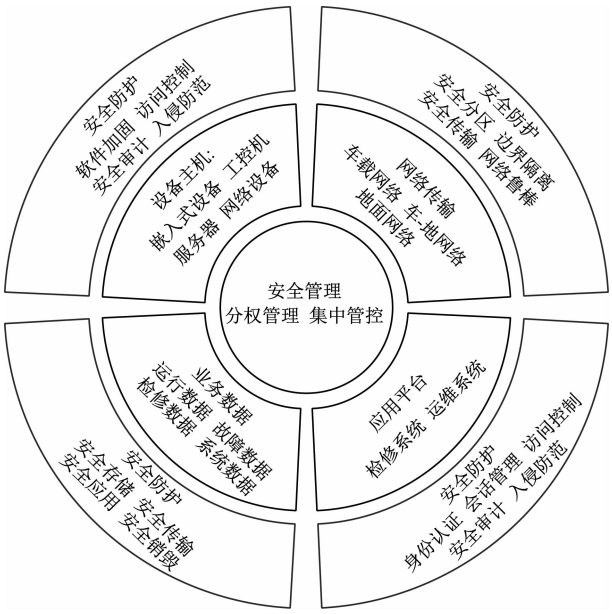

图 2　车辆智能运维系统信息安全技术方案框架图

Fig. 2　Framework diagram of information security technical solution for vehicle intelligent operation and maintenance system

3.1　设备主机的信息安全防护

车辆智能运维系统中的设备主机主要包括各类嵌入式设备、工控机、服务器、网络设备。其防护主要涵盖软件加固、访问控制、安全审计、入侵防范等方面。

1）软件加固。设备主机中的所有软件应安装最新版本或及时更新补丁，建立版本审计机制，确保及时修复漏洞。所有软件安装都遵循最小化原则，仅安装必要组件。设备主机只允许在白名单中的软件运行。

2）访问控制。登录设备主机的用户或软件均需具备唯一性身份标志，并采用密码技术对身份标志进行认证，其密码须满足复杂度要求。管理员等高权限用户须采用两种及两种以上的登录验证方式。须限制登录失败尝试的次数，并在登录超时自动退出。访问权限需遵循最小化原则，仅授予必要权限，限制对资源的访问。及时删除或停用多余和过期账户。建立可信主机机制，只允许用户或软件通过可信主机登录设备主机。

3）安全审计。启动设备主机中的审计功能，如果设备主机无自带的审计功能，则采用具备审计功能的第三方软件。安全审计应覆盖所有用户和程序，对重要用户和程序的行为及重要安全事件进行审计。审计日志包含且不限于用户编号或程序编号、事件时间日期、事件类型、事件来源、事件内容、事件结果，而审计日志中禁止包含敏感和隐私信息。审计记录至少保留半年，并每月定期备份。审计记录只允许审计管理员访问。

4）入侵防范。设备主机关闭不必要的系统服务、默认共享和高危端口。必须对外连接的端口一律设置绑定信息，如芯片串码、MAC（媒体访问控制）地址、IP（互联网协议）地址等。开启防火墙功能，配置白名单策略严格管控对设备主机的访问。安装安全软件，防止攻击入侵和病毒传播。

3.2　网络传输的信息安全防护

车辆智能运维系统网络包括车载网络、车-地网络、地面网络三部分，各网络之间相互隔离，通过受控接口通信。其防护涵盖安全分区、边界隔离、安全传输及网络鲁棒性等方面。

1）车载网络安全。车载网络可划分为车载控制网络和车载维护网络。这两个网络之间通过单向网关进行隔离，数据只能从车载控制网络单向流入车载维护网络。车载维护网络是唯一与外界通信的车载子网。车载维护网络配置百兆带宽和百兆交换机，保证网络服务的可靠运行。

2）车地网络安全。车地网络暴露于外部，是攻击者入侵车载网络和地面网络的主要途径，因此须在车地网络同车载网络及地面网络的边界处分别部署嵌入式硬件防火墙和机架式硬件防火墙，在防火墙上配置白名单，并遵循最小化原则。

3）地面网络安全。地面网络配置千兆带宽、万兆网络交换机，并为关键通信线路和关键交换机配置硬件冗余。通过 VLAN（虚拟局域网）划分应用子网、数据子网和管理子网，实现地面网络分区隔离。应用子网负责接收外部数据，并对外提供应用服务；数据子网负责数据处理所需的网络任务；管理子网负责整个地面系统和平台管理所需的网络任务。部署网络审计设备，对网络边界和关键网络节点进行安全审计。所有网络设备均参考设备主

机的信息安全防护方案进行安全加固。

3.3 业务数据的信息安全防护

车辆智能运维系统业务数据信息安全防护从保护数据机密性、完整性和可用性的角度出发，包含安全存储、安全传输、安全应用、安全销毁等方面，保证从数据生产到数据销毁的全生命周期安全性。

1）安全存储。业务数据的安全存储覆盖车辆智能运维系统的车载子系统和地面子系统。车载监视子系统在采集数据时采用对称加密算法进行加密，以保证数据机密性，并通过散列算法生成散列码来保证数据的完整性。加密业务数据的对称密钥采用非对称加密算法进行加密。在地面应用平台中，借助大数据平台 HDFS（分布式文件系统）的加密区域和密钥管理服务存储数据，并进行三重备份，以确保数据存储的安全性。

2）安全传输。业务数据中的实时数据在由车到地传输过程中，采用安全传输协议 IPSec 或 TLS 构筑加密传输通道。数据文件在传输过程中采用安全传输协议 SFTP。应用平台在对外提供业务服务时所涉及的数据传输采用安全传输协议 HTTPS。这样可以大大提高业务数据在传输环节的安全性。

3）安全应用。业务数据在应用过程中的安全防护可借助服务器和应用系统在身份认证、访问控制、安全审计、入侵防范等方面的防护方案，实现对数据的安全管控。

4）安全销毁。业务数据所在的硬盘存储空间被释放或再分配给其他用户前完全清除。车辆智能运维系统中，数据使用的缓冲存储器及其他动态记录介质在被释放或再分配给其他用户前，须完全清除。车辆智能运维系统内的文件、目录和数据库记录等资源所在的存储空间，在被释放或重新分配给其他用户前，须完全清除。

3.4 应用平台的信息安全防护

车辆智能运维系统的应用平台主要涵盖车辆检修子系统和地面运维子系统。这两个子系统应该采用统一的信息安全管控策略，包括身份认证、会话管理、访问控制、安全审计、入侵防范等方面。

1）身份认证。应用平台给每位用户分配唯一性的用户 ID。用户身份认证采用动态口令和用户密码相结合的方式，其中用户密码须满足复杂度要求并定期更换。须限制用户登录失败的尝试次数；同一用户在同一时间只允许在一个终端上登录。

2）会话管理。若用户登录成功则建立会话，并在用户退出和应用系统退出时销毁会话。建立会话时，生成具有随机性和唯一性的会话令牌，用于后期的交互认证，销毁会话的同时销毁会话令牌。设置会话超时机制，一旦会话超时，则销毁会话，并退出该用户的登录。

3）访问控制。用户访问权限控制采用基于角色的访问控制策略，每个用户和每个角色的权限分配均遵循最小化原则。用户每步操作均进行权限校验。系统管理员在应用系统部署完成后须及时重命名或删除默认账户，并修改默认口令；还须及时删除或停用多余账户和过期的账户。数据库访问账户默认为普通权限，支持表级访问控制。文件数据需支持文件级颗粒度的访问控制。

4）安全审计。应用平台内嵌安全审计功能，覆盖应用平台的每个用户，其安全防护方案可参考设备主机安全审计的防护方案。开启数据库安全审计，对数据库中各类对象的各种操作进行记录。

5）入侵防范。必须对应用平台输入的数据进行检查和过滤，并过滤可能存在安全风险的特殊字符，只有符合规定的数据才能输入平台。对输入文件的类型和元数据进行合规性检查。数据库使用参数化查询来进行过滤处理，自定义统一的错误返回页面，并隐藏服务器信息；拒绝包含意外或缺少内容类型的标头请求，对标头进行合规性检查。

3.5 管理中心的信息安全防护

车辆智能运维系统搭建的安全管理中心便于执行统一的信息安全策略，建立统一的信息安全防护体系。通过安全管理中心，使用者能对车辆智能运维系统整体的安全状态有更加直观、全面和迅速的了解。安全管理中心的信息安全防护主要包括分权管理和集中管控两个方面的内容。

1）分权管理。安全管理中心配置了系统管理、审计管理和安全管理 3 种管理权限。各管理权限各自配置独立且无交互的管理账号、认证机制、访问权限、操作界面。车辆智能运维系统由系统管理员配置、控制和管理系统资源及运行，由审计管理员分析处理审计记录，由安全管理员配置系统安全策略。管理员的所有操作均进行审计。

2）集中管控。安全管理中心对车辆智能运维系统内的嵌入式设备、服务器、工控机、网络设备、应用平台等的运行状况进行集中监测，对这些设备、主机、平台上的所有审计记录进行汇总，对所有

操作系统、中间件和关键应用软件的版本进行集中管理和分析,对已发生的安全事件和可能存在的风险漏洞进行分析、识别、报警。

4 结语

本文主要从技术层面对车辆智能运维系统的信息安全防护方案进行研究,构筑具备系统性、统一性、全面性的信息安全防护技术体系,在多设备主机和多应用层面,实现身份认证、访问控制、数据安全、传输安全、安全审计、入侵防范、分权管理、集中管控等信息安全防护功能,确保全系统安全、可靠、高效地运行。

参考文献

[1] 张彦. 智能铁路时代网络安全问题探讨[J]. 铁路计算机应用, 2019, 28(3): 51.
ZHANG Yan. Discussion on cybersecurity security of intelligent railway[J]. Railway Computer Application, 2019, 28(3): 51.

[2] 刘志宏. 城市轨道交通综合监控系统的信息安全防护研究[J]. 现代信息科技, 2018, 2(8): 149.
LIU Zhihong. Research on information security protection of urban rail transit integrated monitoring system[J]. Modern Information Technology, 2018, 2(8): 149.

[3] 党晓勇. 城市轨道交通综合监控系统信息安全防护方案研究[J]. 电气化铁道, 2020, 31(增刊1): 133.
DANG Xiaoyong. Research on information security protection scheme in integrated supervisory control system[J]. Electric Railway, 2020, 31(S1): 133.

[4] 陶伟. 城市轨道交通信号系统信息安全问题研究[J]. 城市轨道交通研究, 2018, 21(增刊1): 20.
TAO Wei. Research on information security of urban rail transit signal system[J]. Urban Mass Transit, 2018, 21(S1): 20.

[5] 王志, 李波. 中国机车远程监测与诊断系统(CMD 系统)数据安全研究[J]. 中国铁路, 2017(4): 8.
WANG Zhi, LI Bo. On data safety of China locomotive remote monitoring and diagnosis system(CMD system)[J]. China Railway, 2017(4): 8.

· 收稿日期:2021-12-13 修回日期:2022-08-18 出版日期:2024-06-10
Received:2021-12-13 Revised:2022-08-18 Published:2024-06-10

· 作者:皮巍,工程师,pipi_wei2005@hotmail.com

(上接第 280 页)

[7] 赵强, 王涛. 一种三维激光扫描技术隧道整体变形分析方法[J]. 测绘科学, 2021, 46(2): 99.
ZHAO Qiang, WANG Tao. A method for analysis of overall deformation of tunnel based on 3D laser scanning technology[J]. Science of Surveying and Mapping, 2021, 46(2): 99.

[8] ZHANG H, XIA J. Research on convergence analysis method of metro tunnel section: based on mobile 3D laser scanning technology[J]. IOP Conference Series: Earth and Environmental Science, 2021, 669(1): 012008.

[9] 武汉大学测绘学院测量平差学科组. 误差理论与测量平差基础[M]. 武汉: 武汉大学出版社, 2003.
Wuhan University Survey Adjustment Discipline Group of the School of Surveying and Mapping. Error theory and basis of survey adjustment [M]. Wuhan: Wuhan University Press, 2003.

[10] 郭金运, 徐晓飞, 沈毅. 整体最小二乘算法及测量应用研究综述[J]. 山东科技大学学报(自然科学版), 2016, 35(4): 1.
GUO Jinyun, XU Xiaofei, SHEN Yi. Review on total least squares methods and applications in surveying[J]. Journal of Shandong University of Science and Technology (Natural Science), 2016, 35(4): 1.

[11] 黄晓杰, 陈宇磊, 邵跃堂, 等. 基于激光雷达的地铁隧道形变检测方法[J]. 城市轨道交通研究, 2019, 22(11): 47.
HUANG Xiaojie, CHEN Yulei, SHAO Yuetang, et al. Research on metro tunnel deformation detection based on laser radar[J]. Urban Mass Transit, 2019, 22(11): 47.

[12] 董智博. 基于改进欧氏距离的三维点云分割算法分析研究[D]. 北京: 华北电力大学, 2021.
DONG Zhibo. Analysis and research on 3D point cloud segmentation algorithm based on improved euclidean distance[D]. Beijing: North China Electric Power University, 2021.

[13] 成枢, 查天宇, 黄小斌, 等. 移动式三维激光扫描技术在地铁隧道变形监测中的应用[J]. 测绘地理信息, 2021, 46(5): 13.
CHENG Shu, ZHA Tianyu, HUANG Xiaobin, et al. Application of mobile 3D laser scanning technology in deformation monitoring of subway tunnels[J]. Journal of Geomatics, 2021, 46(5): 13.

[14] 陈薪文. 基于地铁隧道点云数据的断面提取及变形分析的研究[D]. 沈阳: 沈阳建筑大学, 2018.
CHEN Xinwen. Research on section extraction and deformation analysis based on point cloud data of subway tunnel [D]. Shenyang: Shenyang Jianzhu University, 2018.

· 收稿日期:2021-12-20 修回日期:2024-01-23 出版日期:2024-06-10
Received:2021-12-20 Revised:2024-01-23 Published:2024-06-10

· 第一作者:谭远鑫,硕士研究生,Tan291217@163.com
通信作者:吴润华,副教授,guorh@tsinghua.edu.cn