

轨道交通车辆通信网络系统的安全纵深防御策略

马法运 徐东超 徐燕芬

(中车青岛四方车辆研究所有限公司, 266001, 青岛)

摘要 [目的] 车辆通信网络系统具有种类繁多、数量庞大的内外网通信接口,使得车辆信息安全风险持续攀升。传统的物理隔离已不能满足高等级的车辆通信网络安全要求,应采用多层次防护的设计方法,以提升车辆通信网络的安全防护等级。[方法] 分析了车辆通信网络外部和内部的安全风险。提出建立轨道交通车辆通信网络系统的安全纵深防御策略,并在安全准则、安全要求规范、安全设计、安全实施、安全认证和确认测试 5 个方面,建立了该策略的“安全技术+安全管理措施”防护体系。[结果及结论] 该策略可实现车辆通信网络系统从安全需求到系统设计、从安全产品开发到运营维护全生命周期的管理,可全面提升车辆通信网络系统的安全防护能力,满足信息安全要求。

关键词 轨道交通车辆; 车辆通信网络; 纵深防御策略; 信息安全

中图分类号 U283.2

DOI:10.16037/j.1007-869x.2024.09.038

In-depth Security Defense Strategy for Rail Transit Vehicle Communication Network System

MA Fayun, XU Dongchao, XU Yanfen

(CRRC Qingdao Sifang Rolling Stock Research Institute Co., Ltd., 266001, Tsingtao, China)

Abstract [Objective] The vehicle communication network contains a wide variety and a large quantity of internal and external network communication interfaces, resulting in continuous rising of the vehicle information security risks. As the traditional physical isolation can't meet the high-level security requirements of the vehicle communication network, a multi-level protection design method should be adopted to upgrade the security protection level of this network. [Method] The external and internal security risks in the vehicle communication network are analyzed. Establishing an in-depth security defense strategy for the communication network system of the rail transit vehicle is proposed. A security protection system of the strategy based on security technology and security management measures is established from five aspects, i. e. security criteria, security requirement specification, security design, security implementation, security certification, and confirmation tes-

ting. [Result & Conclusion] The proposed strategy can achieve the whole life cycle management of the vehicle communication network system from security requirements to system design, from secure product development to operation and maintenance. It can comprehensively enhance the security protection capability of the vehicle communication network system, meeting the information security requirements.

Key words rail transit vehicle; vehicle communication network; in-depth security defense strategy; information security

近年来轨道交通行业网络安全事件频发:波兰的城市铁路系统遭受网络攻击,导致列车脱轨;黑客团伙攻破了美国旧金山市的轻轨系统,导致其售票系统整体瘫痪;深圳地铁因乘客携带的 Wi-Fi 信号意外侵入列车控制网络,导致车地通信中断;上海轨道交通信息发布系统和运行调度系统也因无线网络受到攻击,影响了地铁运营秩序。

目前轨道交通的网络安全控制主要集中在信号系统领域^[1-5]。随着计算机和网络技术的发展,基于工业以太网的车辆通信网络在复兴号动车组、北京/深圳等多地的城市轨道交通车辆中得以全面应用。特别是轨道交通行业运维信息化与车辆通信网络的深度融合,使车辆通信网络同 CCTV(闭路电视)、PIS(乘客信息系统)、车地无线等外部网络相连,车辆通信网络不再是一个完全封闭的网络。车辆通信网络内既有车载通信,也有车地通信。信息化在提升了列车运行效率和自动化水平的同时,病毒、木马等威胁也通过外部接口扩散到车辆通信网络中,导致车辆通信网络安全问题日益突出。

车辆通信网络作为列车的大脑和神经系统,是保障列车安全运行的核心。对车辆通信网络信息安全的研究主要集中在安全设备开发和使用上,而对车辆通信网络的多层级防护研究较少。本文建立了车辆通信网络系统的纵深防御策略,以期保障轨道交通列车安全、高效运行。

1 车辆通信网络安全风险分析

轨道交通信息化建设已处于多个系统间互联互通、信息共享,并向集成化、智能化方向发展的阶段。增加了无线通信、车地通信、运维管理等新功能后,车辆通信网络不再是相对封闭和安全的“孤岛”,存在着来自车辆外部、内部两个方面的网络安全攻击风险。

1.1 车辆外部的网络安全攻击风险

无线通信是车地信息交互的主要方式,通过4G/5G、LTE(长期演进)、WLAN(无线局域网)等形式将车辆信息持续发送至地面平台及PIS、信号系统。无线通信处于开放空间内,不可避免会受到车辆外部无意或恶意的干扰,导致数据泄漏:

- 1) WLAN、4G、5G、LTE等商用网络通信数据被拦截或截取;
- 2) 通过车地无线通信网络通道攻击或劫持车辆运行控制信息。

1.2 车辆内部的网络安全攻击风险

由于轨道交通信息网络规模大,从业者多,且车辆上操作维护的工作量巨大,误用内网终端和滥用外网终端均会导致接入车辆网络安全风险的概率大幅增加。车内通信的主要安全风险在于:

- 1) 部分车载系统(PIS、信号等)有自身的一套内网,系统内网出现故障,会导致车辆通信网络同步故障,进而影响列车控制信息传输;
- 2) 当车载设备出现故障时,会异常发包,抢占网络带宽,同时可能导致其他设备通信负荷较大而宕机,进而影响列车控制信息传输;
- 3) 终端通过网线非法接入车辆通信网络;
- 4) 非法远程登录、访问车辆网络设备。

2 车辆通信网络安全管理的纵深防御策略

依据国际电工委员会发布的IEC 61375-2-3:2015《TCN 通信规约》(TCN为列车通信网络)、IEC 62443:2010《工业通信网络-网络和系统安全》及我国发布的GB/T 22239—2019《信息安全技术—网络安全等级保护基本要求》等标准,本文从保密性、完整性、可用性等方面进行安全需求分析,提出适用于轨道交通车辆通信网络的安全技术方案。

图1为轨道交通车辆通信网络安全管理的纵深防御策略。

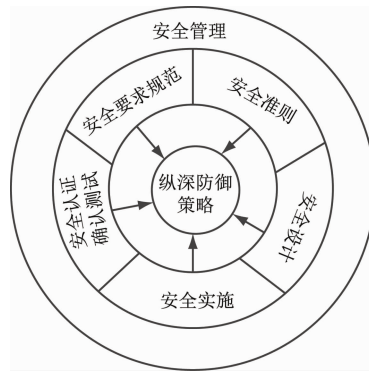


图1 轨道交通车辆通信网络安全管理的纵深防御策略
Fig. 1 In-depth security defense strategy for the communication network security management system of rail transit vehicle

2.1 安全准则

安全准则的内容包括:建立安全策略、组织和意识;成立正式组织,为安全管理提供方向指导和监督;采用合适的安全对策,确保人员和物理环境的安全;根据需求将网络划分为不同的安全等级区域,制定访问控制策略,进行账户、认证及授权管理。

应基于安全准则实现轨道交通车辆通信网络的安全管理:

- 1) 周期性审查安全管理的实施情况,并不断改进安全管理体系。
- 2) 细化安全管理措施:①对所有用户及其标志符进行有效管理;对于采用密码方式登录的人员和设备,应具有密码强度和周期管理、登录鉴别反馈管理等措施。②对于允许无线访问的网络设备,应具备识别和认证接入用户的能力。③根据用户分类和角色进行使用控制,不同的用户拥有不同的操作权限。
- 3) 根据安全标准划分区域等级,严格约束不同等级区域的信息交互;实现终端设备间信息交互的连续监控和审计,对异常信息进行追踪、溯源、记录,必要时发出告警。

2.2 安全要求规范

安全要求规范是安全设计的依据,也是实施安全管理的重要准则。轨道交通车辆行业不仅需要完善相应的网络安全法律规定,用以指导合法的安全防护,严惩网络安全侵害行为,还应通过新型安全监测/监控软件加大对网络的监控力度,做到“早发现、早处理”。在实际的列车运行管理中,运营方应制定内部的安全管理制度及流程,不断完善内部网络管理措施,约束内部工作人员的不合理操作,

提升车辆通信网络的整体安全性和信息传播的稳定性^[6]。

基于安全要求规范,需要进一步健全的内部管理办法主要包括:

1) 网络安全策略管理办法。该办法应提供各安全级别操作人员必须遵守的规则,包括明确网络安全策略的责任人和实施者等。

2) 安全组织管理办法。应在管理层领导下成立相应的安全管理组织/机构,明确组织/机构的职责,为系统安全提供方向指导和监督。

3) 人员安全管理办法。应制定人员安全策略,阐明人员安全职责,明确网络安全条款及条件。

4) 物理和环境安全管理办法。应建立1个或多个物理安全边界,以保护资产不被未授权者访问,保护资产免受环境破坏,制定监控和告警规程,制定资产添加、移除和处理规程等。

5) 访问控制管理办法。应针对系统账户管理要求,制定授权策略,记录访问账户,检查账户权

限、审核账户信息;应制定对系统设备访问的适当逻辑和物理许可方法,为关键系统提供多种授权方式。

6) 安全管理监视和改进管理办法。应执行各项安全管理措施,对安全管理措施及效果进行定期评估,对存在的问题采取纠正措施,对可能的风险实施预防措施,并评估安全管理办法对缓解安全风险的适用性。

2.3 安全设计

2.3.1 安全系统的架构设计

按照 IEC 61375:2015,车辆通信网络组网时采用点对点接入,实现实时以太网通信。图2为车辆通信网络拓扑截图。如图2所示,车辆通信网络系统设计了2套独立的通信网络,1套是控制网,仅用于传输列车控制信息;另1套是融合网,用于传输列车控制信息和维护信息。这2套网络采用了物理隔离的设计方式,相互独立,冗余设置。

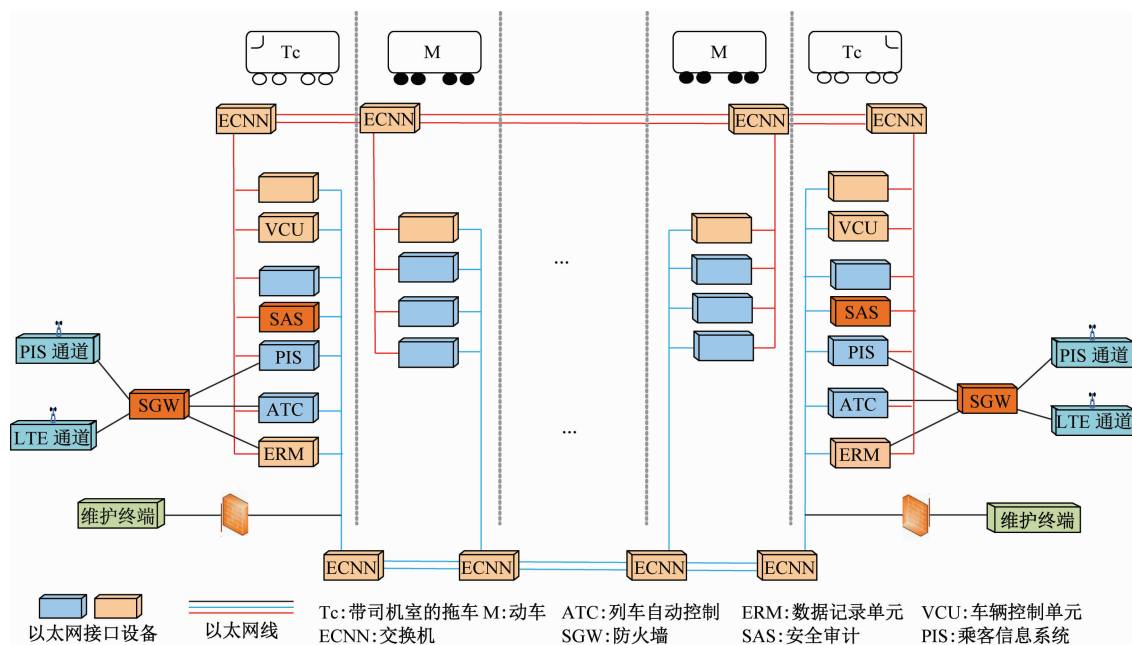


图2 车辆通信网络拓扑截图

Fig. 2 Screenshot of the vehicle communication network topology

2.3.2 安全系统的功能设计

从系统平台开发、梯度防御、数据传输等方面进行安全系统的功能设计。基于层次化和梯度防御要求,提出安全防护方案和设备配置,可以实现边界防护及访问控制、入侵及恶意代码防范、流量审计等功能。车辆通信网络系统的安全防护措施及其功能如表1所示。

车辆通信网络安全防护采用冗余配置,在列车的头车及尾车各配置了1套“安全网关+安全审计+专用防火墙”。安全网关设在车地无线通信车载终端与车辆内部网络交换机之间,可实现边界防护及访问控制功能,保证车地通信时车辆和地面网络的隔离。列车维护和控制信息由安全审计设备进行审计,运维时须经过专用防火墙进行控制验证。

表 1 车辆通信网络系统的安全防护措施及功能

Tab.1 Security protection measures and functions for the vehicle communication network system

措施	功能
网络隔离	所有车载系统设备设有内外网口物理隔离措施(即设置了独立网卡),为车辆通信网络划定安全边界
端口限速	异常发包时会有流量限制,不会导致网络堵塞
标准接口	按照 IEC 61375:2015,采用以太网通信接口,并应用成熟可靠的接口通信规范,丢弃异常数据包
接入认证	设备放置在专用电气柜内,采用固定 IP(互联网协议)分配机制,并采用 802.1x 接入认证技术
入侵检测	具有查询分析客户端登录、访问和用户权限功能,可根据通信行为或资源使用状况是否正常来判断是否存在异常入侵,并发出告警
流量审计	监视网络中关键节点的数据流量和协议类型;通过与基线数据的对比,审计出异常通信流量,并发出告警
主机加固及恶意代码防护	根据系统漏洞定期更新和加固主机系统安全;发现恶意代码攻击时,及时阻断并进行防护
单向通信	将 ERM 车地通信设为单向通信,避免外部网络访问
专用维护	只能通过专用维护接口对车载设备进行维护,且维护数据经过防火墙模块进行控制及验证

图 3 为车辆通信网络信息安全的一体化管控策略。

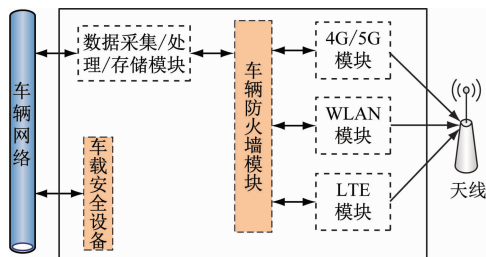


图 3 车辆通信网络信息安全的一体化管控策略

Fig.3 Integrated control strategy for the vehicle communication network information security

1) 采取区域划分方式。根据对外接口分界将车辆通信网络划分为可信网和非可信网,同时根据车载系统业务功能进行虚拟局域网划分和端口限速,以隔离不相关业务。

2) 采用对外隔离方式。将车辆通信网络与外部网络进行隔离,采用白名单的形式实现流量限制与访问控制,减少外网访问干扰,防范已知的或未知的网络攻击。对常见的拒绝服务攻击(如欺骗、泛洪等)进行防护^[7-8]。

3) 采用对内认证技术。对接入车辆通信网络内部的设备 IP、MAC(媒体接入控制)进行绑定及身份、口令认证,不同的身份认证具有不同的操作权限,避免非法设备异常接入。

4) 采用基于通信的审计技术。审计通信流量基线,审查用户的登录、配置等操作行为,并联动报警^[9]。

2.3.3 安全系统的技术方案

根据车辆通信网络系统与其他系统的数据流交互情况、车辆通信网络系统内部各子系统和模块之间的数据流交互情况,设计车辆通信网络的全防护技术方案。具体包括:

1) 关键设备冗余部署,如 VCU 等关键设备均在头尾车冗余部署。

2) 关键设备双归属接入。例如,VCU、HMI(人机接口)等关键设备通过 2 个网络接口接入车辆通信网络,且实现报文的冗余备份。

3) 车辆通信网络采用双网拓扑。任一个网络若发生单点故障,并不影响另一个网络的正常通信。

2.4 安全实施

2.4.1 平台与开发安全

车辆通信网络系统平台应通过不低于 SIL2(安全完整性等级二级)的安全认证。依据 EN 50128:2011《铁路应用—通信、信号和处理系统》、EN 50129:2018《通信、信号和过程控制系统—信号的安全相关电子系统》中 SIL2 的相关要求,以及 EN 50126:2017《铁路应用—可靠性、可用性、可维护性和安全性(RAMS)的规范和证明》中可靠性、可用性、可维护性和安全性的适用要求,对车辆通信网络系统安全平台进行开发。在该安全平台的开发过程中,应遵循相关标准定义的措施、方法或技术组合。在系统安全计划中定义车辆通信网络系统安全平台的安全活动,在系统开发计划中定义项目的开发过程。车辆通信网络系统安全平台开发 V 模型如图 4 所示。

应依据车辆通信网络系统生命周期各阶段的要求,组织各阶段的安全活动:

- 1) 在系统定义阶段,生成系统安全计划;
- 2) 在系统危害识别和风险分析阶段,生成 PHA(初步危害分析)报告或危害记录册;
- 3) 在系统架构阶段,进行系统危害及接口隐患分析;
- 4) 在适当阶段进行安全审核活动;

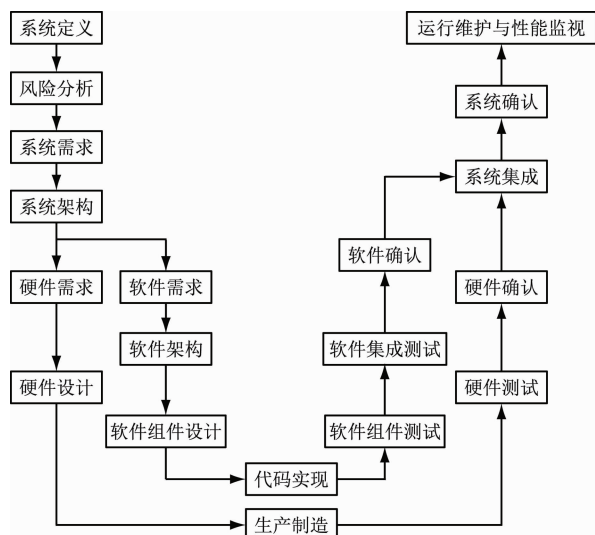


图4 车辆通信网络安全平台开发V模型

Fig. 4 V-model of the security platform development for the vehicle communication network system

5) 危害识别和风险分析阶段结束后,生成系统需求规范,编制测试说明书,对每个功能的测试进行定义和说明。

车辆通信网络系统硬件平台设计应遵循工业标准,采用高性能工业级处理器,满足无风扇设计、关键部件冗余设计等要求,并满足工业环境下宽温、防尘、防潮、防振和高可靠性、电磁兼容等要求。各项试验须符合 EN 50121:2017《轨道交通 电磁兼容》或 EN 50155:2021《铁道应用—机车车辆上使用的电子装置》或等同国际标准的要求。

2.4.2 应用安全

在车辆通信网络系统一体化纵深防御体系中,以安全网关、安全审计和专用防火墙为核心搭建了多层次的防护圈,以抵御外来网络攻击。该体系结合车辆通信网络不同场景下的安全问题,进行全方位、立体化的监测和监视,能够将实时监测数据、告警信息及时告知司机或乘务人员,使运营人员及时掌握网络安全状态,参与安全防护。

从数据安全功能入手,强化协议加密、协议过滤及防护恶意篡改等技术,并在使用前开展协议健壮性测试、软件安全测试及安全系统加固等工作。数据安全防护可采取数据加密、身份识别、权限控制、隔离、私有协议等多种防护措施一体化协同运作的方式。

SDTv2(安全数据传输协议第2版)为1个SDSRC(安全相关/重要数据源)、一个或多个SDSINK(安全相关数据宿)之间提供了安全通信路

径,此路径又被称为“SDTv2 通道”。为保证通信安全,SDTv2 协议针对通信错误部署了应对措施^[10],如表2所示。

表2 针对通信错误的应对措施

通信错误的类型	应对措施						
	序列号	时间戳	信源/宿标志	反馈报文	认证	安全编码	加密技术
重复	✓	✓					
删除	✓						
插入	✓		✓	✓	✓		
重排序	✓	✓					
损坏						✓	✓
延时		✓					
伪装				✓	✓		✓

注:“✓”表示采取了该应对措施。

车地通信采用私有协议,关键信息均为加密传输。对于可能的信息篡改问题,可采用对称或非对称的加密算法,增加多重安全校验,以有效识别并舍弃仿造或被修改的报文。

2.5 安全认证和确认测试

我国实行网络安全等级保护制度,等级保护对象分为5个级别。在安全等级保护的2.0时代,安全等级不再由企业自主确定,而是经过专家评审和主管部门审核后予以确定。

轨道交通车辆通信网络系统目前还没有明确的等级保护级别。根据车辆通信网络系统的安全影响评估要求,车辆通信网络比较符合第三级(监督保护级),即:信息系统被破坏后,会对社会秩序和公共利益造成严重损害,或对国家安全造成损害。因此,建议按照等级保护三级的相关要求,对车辆通信网络进行管理、部署。

SIL 是根据 IEC 61508:2000《功能安全性的通用要求》相关产品进行考核的认证要求,一共分为4个等级。此外,在中国城市轨道交通协会发布的功能安全规范中,车辆通信网络系统被推荐采用SIL2。随着网络功能的增强和运营方对安全的重视,车辆通信网络系统正朝着 SIL4 方向发展。

3 结语

本文结合高速铁路、地铁的车辆通信网络安全需求及相关研究经验,从技术要求和管埋要求2个

方面入手,对轨道交通车辆通信网络进行了信息安全保护设计。提出采取从外到内的纵深防御策略,从安全管理及安全规范需求等方面,系统地设计了车辆通信网络的一体化管控防护方案,组建了安全管理+技术保障的多层次、综合性防御系统,有效提升了轨道交通车辆通信网络的安全防护等级。

参考文献

- [1] 丁超. 城轨列车实时以太网拓扑结构分析及应用思考[J]. 现代城市轨道交通, 2021(12): 79.
DING Chao. RT-Ethernet topology analysis and application for urban rail transit trains[J]. Modern Urban Transit, 2021(12): 79.
- [2] 刘贞, 何跃鹰, 丁欢. 轨道交通列控系统网络安全风险和防护对策研究[J]. 铁路通信信号工程技术, 2020, 17(12): 1.
LIU Zhen, HE Yueying, DING Huan. Research on network security risk and protection countermeasures for train control system of urban rail transit[J]. Railway Signalling & Communication Engineering, 2020, 17(12): 1.
- [3] 李伟, 陈则, 秦元庆, 等. 一种基于移动目标防御的列车通信网络闭环动态安全防护方法[J]. 小型微型计算机系统, 2022, 43(11): 2394.
LI Wei, CHEN Ze, QIN Yuanqing, et al. Closed-loop dynamic security protection method for train communication network based on moving target defense[J]. Journal of Chinese Computer Systems, 2022, 43(11): 2394.
- [4] 陈嘉怡, 燕飞. 城市轨道交通信号系统信息安全风险辨识[J]. 都市快轨交通, 2018, 31(2): 119.
CHEN Jiayi, YAN Fei. Identification of information security risk in urban rail transit signal systems[J]. Urban Rapid Rail Transit, 2018, 31(2): 119.
- [5] 陈宇佳, 曾小清, 袁腾飞. 基于通信的列车控制系统数据安全影响分析[J]. 同济大学学报(自然科学版), 2021, 49(3): 391.
CHEN Yujia, ZENG Xiaoqing, YUAN Tengfei. Analysis of safety impact of data in communication-based train control system[J]. Journal of Tongji University (Natural Science), 2021, 49(3): 391.
- [6] 李思源, 邹宇驰, 杨曼莉. 基于实时以太网的列车网络信息安全防护研究[J]. 中国新通信, 2021, 23(7): 127.
LI Siyuan, ZOU Yuchi, YANG Manli. Research on information security protection of train network based on real-time Ethernet[J]. China New Telecommunications, 2021, 23(7): 127.
- [7] 戴懿, 郭其一. 现代城轨列车通信网络安全性仿真研究[J]. 通信技术, 2020, 53(10): 2573.
DAI Yi, GUO Qiyi. Simulation on security of modern urban rail train communication network[J]. Communications Technology, 2020, 53(10): 2573.
- [8] 朵瑞峰. 列车实时以太网渗透测试与异常检测[D]. 北京: 北京交通大学, 2021.
DUO Ruifeng. Penetration test and anomaly detection of train real-time ethernet[D]. Beijing: Beijing Jiaotong University, 2021.
- [9] 褚腾飞. 面向局域网的网络行为审计系统的设计与实现[D]. 北京: 北京邮电大学, 2017.
CHU Tengfei. Design and implementation of network behavior auditing system oriented to local area network[D]. Beijing: Beijing University of Posts and Telecommunications, 2017.
- [10] 郑艺, 孙可, 孙野, 等. 基于 IEC 61375-2-3 标准的安全数据传输协议设计及测试方法研究[J]. 铁路通信信号工程技术, 2020, 17(9): 33.
ZHENG Yi, SUN Ke, SUN Ye, et al. Design and test method of safe data transmission protocol based on IEC 61375-2-3 standard[J]. Railway Signalling & Communication Engineering, 2020, 17(9): 33.

· 收稿日期:2022-05-13 修回日期:2022-08-20 出版日期:2024-09-10
Received:2022-05-13 Revised:2022-08-20 Published:2024-09-10
· 第一作者:马法运,高级工程师,mafayun123@163.com
通信作者:徐东超,工程师,xdexjtu@163.com
· ©《城市轨道交通研究》杂志社,开放获取 CC BY-NC-ND 协议
© Urban Mass Transit Magazine Press. This is an open access article under the CC BY-NC-ND license

敬请关注《城市轨道交通研究》微信视频号

《城市轨道交通研究》微信视频号聚焦轨道交通行业内的热点问题、焦点问题,以及新技术、新成果,邀请相关专业领域内的专家学者及高级管理人员以视频方式解读和评述,是您及时获知行业资讯、深度了解轨道交通各专业领域的最佳平台。您还可以通过该平台查阅往期论文、查询稿件进度、开具论文录用通知书。敬请关注。

