DOI 10.15302/J-SSCAE-2023.06.005

轨道交通行业网络空间安全现状与未来发展

彭轶华，刘明远*，郜帅，苏伟，张宏科

（北京交通大学电子信息工程学院，北京 100044）

摘要：随着网络技术的广泛应用，轨道交通行业关键基础设施面临着更为复杂的网络环境挑战；开展轨道交通行业网络空间安全发展研究，是实施网络强国战略的重要组成部分。本文阐述了轨道交通行业网络空间安全的基本概念与主要特征，从国外战略、国内战略、安全制度与规范等角度总结了轨道交通行业网络空间安全的宏观态势；着重从基础防护、强化防护、协同防护三方面梳理了轨道交通行业网络空间安全防护体系的发展现状，深入剖析了相应安全风险及成因，涉及传统网络威胁、数据攻击威胁的实际案例。研究认为，内外风险因素成为行业专网的双重威胁、传统网络架构制约安全与可靠性；研究建议，加强网络原创基础研究和体系化创新、构建行业网络安全自主可控产业链、深化行业网络安全运维管理、注重行业网络安全人才培养，以此提升轨道交通行业网络空间安全发展水平。

关键词：轨道交通；网络空间安全；网络体系架构；专用网络；网络攻击

中图分类号：U285.8　　**文献标识码：**A

Current Status and Future Development of Cyberspace Security in Rail Transit Industry

Peng Yihua, Liu Mingyuan*, Gao Shuai, Su Wei, Zhang Hongke

(School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

Abstract: The wide application of network technologies has meanwhile brought about increasingly complex challenges regarding network environment for the key infrastructure of the rail transit industry. Therefore, deepening the research on cyberspace security in the rail transit industry becomes increasingly important. This study expounds on the basic concept and major characteristics of cyberspace security in the rail transit industry and summarizes its macro situation from the perspectives of strategies in China and abroad as well as security system and standards. It sorts out the development status of cyberspace security protection systems in the rail transit industry from three aspects: basic, enhanced, and collaborative protection. Moreover, the study analyzes the corresponding security risks and causes, involving practical cases of traditional network threats and data attack threats, and concludes that internal and external risk factors become the double threats to the industry's dedicated network and the traditional network architecture restricts network security and reliability in the rail transit industry. Furthermore, we propose the following suggestions: (1) strengthening the original basic research and systematic innovation of networks, (2) building an independent and controllable industrial chain of network security, (3) improving the operation and management of network security, and (4) enhancing talent cultivation for network security in the rail transit industry.

Keywords: rail transit; cyberspace security; network architecture; customized network; network attack

收稿日期：2023-07-18；**修回日期：**2023-11-21

通讯作者：*刘明远，北京交通大学电子信息工程学院讲师，研究方向为未来网络技术；E-mail: myliu@bjtu.edu.cn

资助项目：中国工程院咨询项目“网络空间安全技术体系与风险应对”(2022-JB-04)；中国博士后科学基金资助项目(2023M730206)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

随着网络空间与物理空间的相互渗透，交通、金融、电力以及能源等涉及国家根本安全的关键信息基础设施已成为网络黑客组织的主要攻击目标[1]。网络空间被视为继陆、海、空、天四个疆域之后的第五疆域，已成为大国博弈的核心与关键，是关乎经济发展以及社会进步的决定因素。保障轨道交通行业关键基础设施网络空间安全是维护公众生命安全的基本要求，更是满足国家网络强国战略需求、提高网络空间竞争力的重要支撑。

《“十四五”现代综合交通运输体系发展规划》（2022年）提出，大力发展以轨道交通为核心的交通网络，保障轨道交通行业的高安全和高效率发展。近年来，我国轨道交通行业大力推进网络空间安全建设，取得了良好效果，但各种新型攻击手段不断涌现，给轨道交通行业网络安全带来了严峻考验[2]。随着技术演进和应用需求发展，轨道交通行业网络信息系统的信息交互接口日益增多，越来越多的通用软件、标准硬件和通用的通信协议被应用，系统安全漏洞问题凸显[3]，各类网络攻击事件频发。除网络攻击影响外，网络移动性和数据传输实时性也会对轨道交通行业的安全运行产生重要影响。传统网络的原始设计并没有充分考虑安全性、移动性和实时性等因素[4]，使其难以满足轨道交通行业使用场景的特殊需求。因此，建立系统有效的网络安全防护体系，解决传统网络架构的不足，提高网络内生安全、移动与实时性，是保障轨道交通行业网络安全的重要措施。

本文从轨道交通行业网络形态、技术及架构等视角分析轨道交通行业网络安全特点，梳理轨道交通网络空间安全战略与防护体系现状，总结轨道交通行业网络空间安全威胁与典型案例，提炼导致当前轨道交通行业网络安全风险的深层次原因，提出针对轨道交通行业网络空间安全的发展建议，以期为我国轨道交通的安全稳定提供借鉴。

二、轨道交通行业网络空间安全的概念及特征

轨道交通行业由众多信息系统构成，各系统运行时同层子系统以及层间子系统均有频繁、大量的数据交互，信息流走向极为复杂，且大部分通过承载在有线或无线链路的传输控制协议 / 网间协议（TCP/IP）网络进行传输[4,5]，在整个过程中，受到攻击威胁与传输不可靠等因素的影响会造成数据泄露，影响行车安全。

（一）轨道交通行业网络空间安全概念

轨道交通行业依赖于包括列车运行控制、列车调度指挥、客票发售预订以及列车供电远动等系统在内的信息传输。系统内部与彼此之间使用基于传统网络技术进行交互，并且各系统传输的网络空间信息直接反映了该系统的状况，网络的安全稳定性对列车运行安全起着至关重要的作用。2019年，国际商业机器公司（IBM）X-Force团队发布的研究报告指出[6]，交通行业已经成为仅次于金融服务业的第二大受攻击的行业。除此之外，IBM的安全研究人员进一步提出破坏交通系统或盗取信息数据可能会被用于恐怖主义行动。严格的网络安全措施是保障各系统之间传输数据和信息安全的重要手段，以防止对社会秩序产生破坏性影响的事件发生。

传统互联网在最初设计时未充分考虑安全性，现行的补丁式安全增强手段难以满足重点行业的网络安全需求。互联网的设计初衷是让可信赖的用户共享信息，在设计初期并未将安全作为首要考虑因素。当新的安全漏洞突破现有安全防护措施时，通常采用发布补丁的方法来进行修复。随着网络技术的发展，网络拓扑逐渐增大，不可信的网络自治域增多，数据包可能会被截获、篡改、伪造。对于安全性要求较低的普通应用场景，如传输敏感性较低的娱乐视频、普通文本或图片信息，现有互联网的安全措施在平衡成本与实用性方面已基本满足需求。轨道交通行业中列车运行控制系统等数据相较于普通应用数据重要性更高，采用补丁修补的方式会产生滞后效应，导致机密数据泄露等问题。

（二）轨道交通行业网络空间安全特征

网络安全是保障信息系统正常运行和数据完整性、可用性和保密性的重要措施。网络安全可以防止或减少信息系统造成的破坏，确保网络系统的功能和服务正常运行。与其他行业相比，轨道交通行业的网络安全具有攻击目的性强、与现实联系紧密以及攻击后果难以预测的显著特征。

轨道交通行业的网络系统具有高度的复杂性和

互联性，针对其攻击具有专业性与目的性强的特点。轨道交通行业各子系统的设备和模块之间形成了复杂的网络体系，数据交互和信息传输频繁，针对其安全威胁也呈现多样化、复杂化的特点。例如，攻击者以破坏轨道交通的正常运营为目的，通过高级长期威胁（APT）等恶意攻击手段，针对性攻击轨道交通信号系统网络，以期达到控制信号设备效果。攻击的专业性和目的性强给轨道交通网络安全防范带来了巨大的挑战和困难。

轨道交通行业中，物理空间与网络空间紧密绑定、交互密切。网络传输数据的安全性以及可靠性直接关系到轨道交通行业的运行安全，关乎生命财产安全。如果列车的调度指挥和运行控制系统受到攻击，这可能导致列车调度混乱、失去正常控制，进而引发碰撞或脱轨等严重的安全事故；客票发售预订系统遭受攻击，会导致票务数据泄露，乘客隐私受损；列车供电远动系统遭到攻击，可能导致列车运行中断，甚至引发供电设备损坏和火灾事故。

与传统的铁路安全标准不同，轨道交通行业的网络安全标准需要更加复杂和灵活的评估方法。传统的铁路安全标准主要基于物理空间的安全性评估，将安全性划分为绝对安全和相对安全[7]，并以此制定相应的可接受极限范围。不同于铁路轨道工程寿命可以通过结构损伤等进行相关安全评估[8]，由于受社会环境等因素影响，轨道交通网络攻击呈现高突发、高隐蔽性等特点，网络攻击的后果难以预测和控制。

综上可见，轨道交通行业信息系统构成复杂，受限于使用传统网络技术等原因，难以应对当前日益严峻的网络攻击。同时轨道交通行业网络安全与现实联系紧密，针对其攻击具有隐蔽性强、破坏性大等特点，这使得维护其网络安全空间充满挑战。

三、轨道交通行业网络空间安全的宏观态势

维护轨道交通行业网络空间安全是保障轨道交通行业安全运行的基础，轨道交通行业网络空间安全问题已经成为全球共同面临的挑战[9]。为提高轨道交通行业网络空间安全，不同国家与行业组织都发布了相应的发展战略与规范体系。

（一）国外轨道交通行业网络空间安全战略

在涉及国家根本安全的轨道交通行业，各国都在加强对其网络安全管理和保护，以防范网络攻击和数据泄露等问题对社会造成的重大威胁。近年来，全球主要经济体针对轨道交通行业（铁路干线、城市轨道交通）的网络空间安全，发布了系列相关战略文件（见表1）。

在铁路干线方面，早在2014年，欧盟为提升铁路行业的竞争力提出了Shift2Rail计划。该计划的重点关注领域包括铁路信号和控制系统的网络安全，为其他欧洲国家制定相关战略提供指导。德国在2016年发布“德国铁路4.0战略”，希望建立一个全面的安全体系，保护旅客和物流信息的隐私和安全，并加强对网络攻击和数据泄露的防范措施。该战略还强调加强员工网络安全教育和培训，提高员工对网络安全问题的意识和应对能力。相较于法国与德国分别在加强网络安全能力与提高员工的网络安全意识，瑞士在2017年提出的SmartRail4.0方案则更重关注系统性网络安全，其中包括确保所有设备和系统的网络安全，通过身份认证和访问控制来保护数据和系统，以及实施安全策略和安全漏洞管

表1　世界各国轨道交通行业网络安全战略

领域	发布时间/年	国家 / 地区	战略名称	主要关注领域
铁路	2014	欧盟	Shift2Rail计划	铁路信号和控制系统
	2016	德国	德国铁路4.0战略	网络攻击和数据泄露的防范措施
	2017	瑞士	SmartRail4.0	身份认证、访问控制安全策略和安全漏洞管理措施
	2018	英国	数字铁路战略	网络安全管理机制
	2019	韩国	2030铁路基础设施发展战略	安全技术研究、强化合作交流
城市轨道	2015	法国	数字化法铁战略	安全责任制、人才培养
	2017	美国	公共交通安全标准纲要	安全标准体系
	2020	日本	技术创新中长期规划	物联网、大数据、人工智能风险预测

理措施来提高网络安全性。英国在2018年发布的“数字铁路战略”明确提出加强网络安全的保障措施，包括构建健全的网络安全管理机制，加强网络安全技术研究和应用，提升网络安全意识和培训，制定相关政策法规并落实到实际操作中。同时，“数字铁路战略”还要求在信息技术系统和设备的设计、采购、部署、维护等环节中，充分考虑网络安全因素，避免因安全漏洞或人为疏忽等因素导致安全风险，提升铁路的可靠性和安全性。韩国《2030铁路基础设施发展战略》（2019年）更加注重铁路系统的网络安全，提出了诸多加强网络安全的措施，包括建立完善的网络安全管理体系、加强网络安全技术的研究和开发、推进铁路系统的网络安全培训和意识提升以及加强监管和安全保障措施等；强调加强信息共享和协作，促进铁路系统各方面的合作和信息交流，提高网络安全的综合防御能力，确保铁路系统的信息安全。

在城市轨道交通方面，法国《数字化法铁战略》（2015年）是保障轨道交通行业网络安全的重要战略文件。该战略的主要目标是强化法国的网络安全基础，增强网络安全防护力量，改进网络安全管理体系，落实网络安全责任制，在此基础上加强网络安全人才培养，提高网络安全技术水平。美国《公共交通安全标准纲要》（2017年）从城市轨道交通模式以及安全标准方面保障乘客和系统的安全，以线路、通信信号、车辆中的乘客设备以及规章程序等为主体共制定了128项标准，构建了完善的城市轨道标准体系[10]。在城市轨道交通较为发达的日本，以东日本铁路公司为代表，率先提出结合物联网、大数据、人工智能等新型技术实现对包括网络安全在内的风险预测，提升运行可靠性。

（二）国内轨道交通行业网络空间安全战略

为了保证轨道交通行业中各部分的网络空间安全，我国近年来分别从政策规划、法律法规以及技术规范等方面出台了相应的文件，充分体现了国家在网络安全保障方面的决心。

在国家政策规划方面，《“十四五”规划和2035远景目标纲要》强调增强网络安全保护，完善国家网络安全法规和标准，同时加强对重要领域的数据资源、关键网络和信息系统的安全保护[11]；《“十四五”现代综合交通运输体系发展规划》提出增强交通运输领域的关键信息基础设施、重要信息系统的网络安全防护，推进信息系统设施设备自主可控[12]。

在法律法规方面，《中华人民共和国网络安全法》（2016年）是我国网络空间安全管理方面的第一部全面规范性的基础法律，旨在保障国家网络空间安全，规范网络行为，强化数据保护，完善监管体制，保护关键信息基础设施，加大对违法行为的惩处力度，并对监测预警和应急处置方案进行法制化，为维护国家安全和网络环境的稳定发展提供了坚实的法律基础[13]。

在技术规范方面，国家标准化委员会发布的《网络安全等级保护2.0国家标准》（2019年）将等级保护对象从原有的狭义信息系统扩展至包括网络基础设施在内的各类系统与平台。此举与《中华人民共和国网络安全法》的实施相辅相成，为不同层级用户提供系统性的等级保护方案[14]。该标准在轨道交通行业的关键作用主要体现在全方位安全性保障，从被动的等级保护1.0升级到主动的安全防御，解决了安全数据分散、单一维度无法抵御高级威胁、响应困难以及缺乏预警手段等问题[15]。《关键信息基础设施安全保护条例》（2021年）明确了关键信息基础设施的定义，规定了运营者的责任、权利以及提供产品和服务的标准。在此基础上，针对交通等重要领域也提出了具体要求，规定了运营者的安全保护主体责任，同时要求建立关键信息基础设施网络安全监测预警体系和信息通报制度[16]。《信息安全技术 关键信息基础设施安全保护要求》（2023年）确立了关键信息基础设施运营者在分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面的安全要求，主要用于指导运营者以及网络安全服务商等相关方协同构建包括网络安全在内的关键基础设施安全保障体系。

（三）轨道交通行业部分安全制度与规范体系

作为我国轨道交通的运行企业，中国国家铁路集团有限公司自2017年以来逐步强化铁路网络安全规章制度和标准规范安全体系架构，发布了《信息系统运行维护管理办法》《铁路综合信息网安全防护要求》《信息化工作管理办法》以及《铁路关键信息基础设施目录》等多项规范文件，同时在产品研发上积极推进“铁网护栏”工程来确保运行安全。

《信息系统运行维护管理办法》对铁路信息系统的运行维护流程进行规范，提升了系统的安全性和稳定性，明确了各部门的职责，规定了故障处理和系统恢复方案。《铁路综合信息网安全防护要求》为铁路信息网提供技术指南，确保网络安全与数据保护，并提出具体的防护措施与技术要求以降低安全风险。通过加强安全防护意识，整体提升了铁路网络安全水平。《信息化工作管理办法》明确了铁路信息化建设与管理的基本要求以提高工作效率。该办法明确了信息化工作的组织实施，推进了铁路行业信息化发展，确保了投资回报和建设质量。《铁路关键信息基础设施目录》明确了铁路行业关键信息基础设施的范围，有助于保护与管理重要信息系统。通过提升关键信息基础设施的安全防护能力，降低了系统安全风险。该目录为铁路行业关键信息基础设施的监管和确保关键信息安全提供了重要依据。

目前，为加速推动“铁网护栏”项目，中国国家铁路集团有限公司正在积极推进企业标准的制定和发布，部分标准状态如下[17]（见表2）。

在城市轨道交通方面，我国交通运输部于2019年发布的《城市轨道交通正式运营前安全评估规范第1部分：地铁和轻轨》与《城市轨道交通运营期间安全评估规范》均提出重点评估城市轨道交通工程项目的网络安全、信息安全、数据安全、通信安全等方面的风险和措施。中国城市轨道交通协会发布的《智慧城轨信息技术架构和信息安全规范》系列标准和《城市轨道交通云计算平台网络安全技术规范》等，规范了城市轨道交通云的架构、安全防护范围和措施，为保障城市轨道网络安全提供指导和参考。

综上可见，世界主要经济体都在持续强化轨道交通行业网络空间安全防护战略。我国也从国家层面对轨道交通行业网络安全进行了制度和法律等多维度保障，但我国网络安全防护工作开展相对较晚，且标准规范框架尚不完善是影响我国轨道交通行业网络空间安全的重要因素之一。

四、轨道交通行业网络空间安全防护体系发展现状

目前，轨道交通行业专网多采用传统网络技术进行建设，在具体的需求与适应场景上进行特殊针对性设计以满足需求。在防护体系上，从网络基础防护、强化防护、协同防护3个层面共同构建安全防护体系。

（一）基础防护

在轨道交通行业中，基础防护主要包括合规性管理、等级保护机制以及软硬件安全防护等。

合规性管理主要建立在我国现行的网络空间安全法律法规和重点行业内部制定实施的标准之上。基于《中华人民共和国网络安全法》，轨道交通行业的合规性管理从网络安全运维、关键信息基础设施运维、个人信息保护、监测预警和应急处置四个方面制定轨道交通行业网络信息安全策略。在网络安全运维方面，《中华人民共和国网络安全法》对网络安全等级保护制度、网络产品和服务、关键网络安全设备产品和网络运营服务等提出了明确要求。轨道交通行业需要严格遵守相关规定，强化网络安全运维。在关键信息基础设施运维方面，《中华人民共和国网络安全法》要求交通等行业应实行重点保护。轨道交通行业应严格落实“三同步”要求，制定完善的网络安全应急计划，执行规范的网络安全审查，确保关键系统和数据库可靠备份。在个人信息保护方面，《中华人民共和国网络安全法》

表2　中国国家铁路集团有限公司网络安全部分标准

序号	标准名称	状态
1	铁路通信网络安全技术要求第1部分：总体技术要求	已发布
2	铁路通信网络安全技术要求第2部分：承载网	已发布
3	铁路通信网络安全技术要求第3部分：GSM-R	已发布
4	铁路通信网络安全技术要求第4部分：综合视频监控系统	已发布
5	铁路通信网络安全技术要求第5部分：安全管理中心	已立项
6	铁路通信网络安全技术要求第6部分：通信安全基线	已立项

明确要求网络运营者对收集的用户信息进行严格保密，采取必要的措施保护用户信息的安全性。轨道交通行业正在积极制定数据分级体系，研究数据脱敏技术，以防止信息泄露、损毁和丢失。在监测预警和应急处置方面，《中华人民共和国网络安全法》要求建立完善的网络安全监测预警以及信息通报制度。轨道交通行业正与第三方深度合作，共同构建系统漏洞发掘通报机制、行业内部安全事件反馈通报机制、信息化部门安全管理评审机制等。

等级保护机制是网络安全的核心，经过不断发展已经在传统保护基础上逐渐演化为对事前、事中、事后的全方位安全控制；适用于传统计算机信息系统、工业控制系统、移动互联网系统在内的各类信息系统，以构建全方位、立体覆盖的等级保护体系。在轨道交通行业中，信息系统等级保护针对关键信息基础设施进行重点保护，实行基于等级保护的分等级的防护机制和基于关键信息基础设施的加强保护措施[18]。

软硬件安全防护是网络空间安全的基石。物理安全是硬件安防技术的核心，目的在于保护计算机设备、网络服务器、打印机和通信链路等设施免遭人为破坏，防止搭线攻击、地震、水灾、火灾、有害气体和其他环境因素导致的损坏[19]。保证计算机及网络系统机房的安全，以及保证所有设备及其他场地的物理安全，是整个计算机网络系统安全的前提。物理安全防护主要包括：环境安全、电磁防护、物理隔离和容灾备份。在软件安全防护层面，以城市轨道交通为例，目前的信息安全防御依照以下部署架构：中央级系统区域安防服务器区包含各种安全设备，如防火墙、入侵监测、一级防病毒服务器、统一认证、漏洞扫描、行为监控、补丁分发服务器等，形成纵深的安全防护层次，重点保障了业务的安全性、可持续性。应用服务器区包含各种应用服务器与应用区防火墙。数据中心系统涵盖各应用系统、用户数据存储区、灾备应急响应系统以及审计溯源系统。车站级系统区域安防服务器区包含各种安全设备，如堡垒主机、安全网关、入侵监测系统、次级防病毒服务器、统一认证代理系统、补丁分发代理系统等。

（二）强化防护

强化防护主要依据《关键信息基础设施安全保护条例》和《信息安全技术 关键信息基础设施安全保护要求》，在基础防护之上，以实时高效为前提、安全可靠为目标、主动防御为手段，围绕轨道交通行业生产运行全生命周期中的关键信息基础设施，从安全保护计划、安全教育培训、边界防护、入侵防御、运维审计等方面建设安全防护体系。

在安全保护计划方面，需要制定具有轨道交通行业特色的网络安全保护计划，从管理体系、技术体系、运营体系、保障体系等方面进行规划，加强机构、人员、经费、装备等资源保障。在安全教育培训方面，建立网络安全教育培训制度，定期开展网络安全教育培训和技能考核，提升关键安全人员的安全意识、安全技能和安全法规知识。在边界防护方面，除了对人员访问进行控制外，还需要在信号系统与外部系统、生产执行网与执行协调网之间设置工控系统安全防护网关，控制不同安全域间的工控协议访问，防止低安全级别网络的非法工控数据入侵高安全级别网络[20]。在入侵防御方面，轨道交通行业入侵防御系统根据部署位置的不同，主要分为两种模式：一是网络核心交换机上部署的旁路入侵检测系统，针对专网内的通信流量做实时入侵攻击的检测和攻击报警；二是在关键业务功能模块前部署直路入侵检测系统，以实时监测与关键业务相关的信号系统通信流量，以便及时拦截入侵攻击。在运维审计方面，部署综合运维安全审计系统，构建行业专网内部运维管理制度和规范的技术化落实平台。采取相应的网络审计措施，监测和记录系统运行状态、日常操作、故障维护、远程运维等，留存相关日志。

（三）协同防护

在轨道交通行业中，协同防护主要分为内部和外部两个部分。协同防护的内部指机务段[21]、车务段[22]、工务段[23]、电务段[24]以及车辆段[25]。机务段主要负责机车的使用以及整备工作。车务段负责列车运营，保证管辖辖区内的各个车站客运、货运的正常运营。工务段负责维护铁路线路和相关设备。电务段管理和维护地面信号、机车信号和道岔的稳定。车辆段负责列车的运营、维护和检修等相关事项。伴随着我国高速铁路的发展，传统的轨道交通行业也在思考数字化管理和运维转型。在轨道交通行业内部，为了实现行业专用网络的安全可靠，需

要五大子系统之间进行密切和深入的数据交互与安全协同。

协同防护的外部是指在轨道交通行业之外，与其他同为关键信息基础设施重点行业的公共通信和信息服务、能源、交通、金融、公共服务、电子政务、国防科技工业等行业和领域进行的协同安全防护与调度。同时也包括与公安部、国家安全局、中央网络安全和信息化委员会办公室等国家与政府职能部门之间的安全协同。

综上所述，基础防护侧重于从标准规范上保证重点行业对关键软硬件的安全防护。强化防护主要是针对轨道交通行业特色制定网络安全保护计划。协同防护要求统筹轨道交通行业内部子系统与相关行业高效协同，实现全方位立体化的安全保证。随着时代的发展，轨道交通行业网络空间安全已经成为事关国家安全的重要问题。面对复杂多变的网络空间安全环境，推进和落实上述3种防护是抵御轨道交通行业网络威胁的有效手段。

五、轨道交通行业网络空间安全风险及成因

（一）轨道交通行业网络空间安全威胁与案例

轨道交通行业中信号控制等子系统，本质上属于计算机网络系统，虽具备封闭性以及专用性，但信息安全仍然是不容忽视的因素。随着轨道交通行业网络对数据共享和大容量数据通信需求的迅速增长，需要与外界进行开放互联，这也使得其不断受到升级和迭代的网络攻击威胁。特别值得注意的是，传统的网络威胁和新兴的数据威胁是当前构成攻击的重要手段。

1. 传统网络威胁

传统网络威胁在轨道交通行业中主要包括恶意软件攻击威胁、漏洞攻击威胁以及拒绝服务攻击。

恶意软件攻击主要是利用木马、勒索软件等各类程序来控制轨道交通行业系统、窃取敏感信息以及干扰正常运营。通过恶意软件，攻击者可以毫无察觉地侵入系统执行攻击者指定的恶意操作，并可能以此进行相应的勒索。2020年5月，瑞士施泰德（Stadler）铁路公司曝光了一起事件，攻击者入侵了其网络并感染了部分计算机，导致泄露敏感数据，攻击者还企图通过威胁勒索公司来获得赎金。

漏洞攻击指攻击者利用软件、硬件或网络系统中的漏洞来获取对系统的控制权或窃取数据。轨道交通行业系统中的一些设备由于使用年限较长，其操作系统和应用程序版本已停止更新，因此存在已知的漏洞。一些设备的配置不安全，如使用默认用户名和密码等，这些漏洞也会成为黑客攻击轨道交通行业系统的入口。攻击者通过利用这些漏洞，可以进入轨道交通行业系统内部，获取敏感信息、篡改数据、破坏系统。新的漏洞不断被披露，加剧了轨道交通行业系统漏洞威胁。上述漏洞如果被黑客利用，则可能造成轨道交通行业系统数据丢失、信息泄露、运行故障等问题。国家计算机网络应急技术处理协调中心（CNCERT/CC）曾针对城市轨道交通行业联网系统进行自动化无损漏洞扫描，共发现425个漏洞，其中高危漏洞33个、中危漏洞184个、低危漏洞208个[26]。2021年7月，伊朗铁路系统受到攻击使得数百项运营被推迟或取消，系统中没有受保护的口令、不更新杀毒软件是导致被攻击的直接原因。

由于技术门槛相对较低且检测与防御复杂性较高，拒绝服务攻击（DDoS）目前被大量应用。攻击者使用工具（如僵尸网络）向轨道交通行业系统中的网络节点发送大量的恶意流量，以占用列车自动控制系统（CBTC）网络的带宽资源。攻击流量通过网络入口路由设备进入网络，然后传递给内部核心设备。这些设备在攻击流量的冲击下，处理能力和网络带宽被耗尽，导致服务不可用，进而严重影响轨道交通行业系统的正常运行。2020年7月，以色列铁路基础设施遭受到大规模DDoS网络攻击，攻击针对以色列铁路150多台工业服务器，影响了28个火车站和地铁站的运营；攻击行动持续了10天，公布了以色列铁路网地图，确定了28个目标车站[27]。在攻击行动结束6天后，由于设备和基础设施受到严重破坏，被攻击车站仍然无法正常运行。

2. 数据攻击威胁

数据完整性攻击是通过修改、删除、篡改、伪造等手段对数据进行非法操作，从而破坏数据的真实性、准确性和完整性。这类攻击可能会导致数据丢失、混淆、误报、错误分析、错误决策等问题，对数据的可靠性和安全性造成威胁。其中数据投毒攻击是一种利用恶意数据来欺骗智能控制系统模型的常见攻击机制。

在轨道交通行业，数据完整性攻击威胁主要表

现为对决策系统生成的数据和在网络中传输的数据进行攻击。其攻击目标涵盖了列车自动监控系统、列车自动防护子系统、列车自动运行系统等智能决策系统所产生的关键数据。这种攻击威胁的结果可能导致列车运行数据和乘客信息等敏感数据遭到未经授权的访问、篡改、破坏或丢失，从而危及轨道交通行业系统的可靠性和安全性。例如，在具体实施过程中，数据完整性攻击主要通过以下两种方式威胁轨道交通行业网络：一种是直接篡改数据包中的内容，另一种是通过中间人攻击方式，篡改数据包的传输路径。通过篡改部分数据，攻击者可以对轨道交通系统中的车辆、信号以及通信等设备进行控制，进而造成列车脱轨、相撞等事故。轨道交通行业数据完整性保护的主要目的是保障轨道交通行业系统的正常运行，防止数据安全问题对轨道交通行业运营和乘客带来的潜在威胁。

数据完整性攻击对轨道交通行业构成的安全影响较为广泛，值得引起高度重视。2022年4月13日，国家安全机关披露了一起涉及为境外提供高铁数据的案件[28]，一家境外公司委托一家上海信息科技公司采集包括物联网、蜂窝和铁路综合数字移动通信系统（GSM-R）等关键铁路信号数据和频谱数据。这些数据直接涉及高铁列车运行控制以及行车调度指挥，一旦被不法分子滥用，将对高铁运行秩序构成严重威胁。类似事件在其他国家也有发生，英国火车站无线网络通信系统（Wi-Fi）提供商C3UK在2020年未能保护包含用户信息的数据库，导致1万名英国铁路乘客的个人数据泄露[29]。另外，美国国家铁路客运公司在2020年遭受网络入侵攻击，导致用户信息泄露。

攻击事件表明，传统网络安全威胁如恶意软件、漏洞和拒绝服务攻击是当前轨道交通行业系统的主要网络攻击手段，但数据攻击威胁如数据投毒和数据篡改也不容小觑。因此，强化传统网络安全和数据安全是确保轨道交通行业系统可靠性和安全性的重要手段。

（二）我国轨道交通行业网络风险成因探究

轨道交通行业的专用网络是由物理隔离专网和基于公共通道形成的专网共同构成，两种构成方式都面临着来自网络内部和外部的众多安全威胁，且由于采用传统网络架构，轨道交通行业的安全性与可靠性面临挑战。

1. 内外风险因素成为行业专网双重威胁

轨道交通行业专用网络形态是造成网络安全问题的根本原因。行业网络形态可以分为两大类：物理隔离的行业专网和基于公共通道的行业专网。物理隔离的专用网络是采用物理隔离方式建设专用网络，具体技术基本上是直接采用公网传统技术或者将公网技术进行专网定制。轨道交通行业专网广泛采用GSM-R窄带技术，由于该技术主要以语音业务为导向，存在数据率低下等问题，这使得其难以满足未来高铁运维安全保障的需求[30]。公网通道的专用网络需要借助公网对物理隔离的专网进行互联（见图1），受到基础设施限制和约束。尽管某些应急通信网络对移动环境下的高质量安全通信有严格要求，但专门建设电信基础设施成本较高，借助公网通道构建行业专网是首选方案。从网络安全角度上看，无论是物理隔离的专网，还是基于公网通道的专网，均采用传统管理与网络体系技术，面临来自内部与外部的双重威胁。

专用网络存在内部威胁，虽然做到了与公共网络的隔离，但内部威胁仍是主要挑战，如安全意识不到位、身份认证不够强、权限管理不精细、审计管理不全面；面临着多种来自公共网络的外部威胁，如网络监听、网络爬虫、暴力破解、网络钓鱼等。

轨道交通行业的内部威胁主要是人员机制和系统设计缺陷造成的，如内部员工使用职员访问权限，将业务系统中的信息违规批量导出贩卖进行获利、系统身份认证单一缺陷造成的身份凭证被假冒等。外部威胁主要来自空中接口。目前，全球主要存在3种用于列车控制的无线通信系统，分别是北美CBTC使用的宽带大容量通用无线通信系统、日本高级列车管理和通信系统（ATACS）的专用无线通

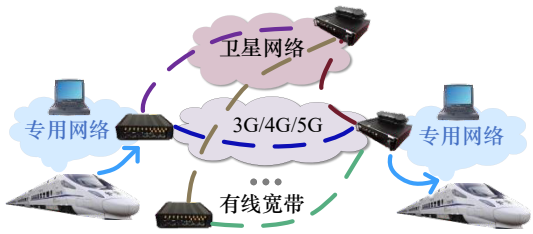

图1　轨道交通行业基于公共通道专网示意图

注：3G为第三代移动通信；4G为第四代移动通信；5G为第五代移动通信。

信系统和欧洲列车控制系统采用的GSM-R无线通信系统。我国轨道交通行业使用的主要是GSM-R无线调度与有线数字调度相结合的方式，主要负责如制动检测、轮轴检测以及供电检测等一系列信息传输任务。基于全球移动通信系统（GSM），GSM-R增加了调度通信和适用于高速移动环境的功能，以便铁路调度人员与列车司机和其他相关人员进行有效通信和协调，这种系统符合国际铁路专用调度通信的要求[31]。然而在GSM-R网络中，存在一种主要的安全威胁，即通过无线接口进行攻击。因为移动设备和通信基础设施之间的通信是通过空中无线接口利用电磁波传输的，而这种接口是开放的，任何拥有合适无线设备的人都能够通过窃听无线信道来获取通信内容。攻击者还可以对通信内容进行修改、插入、删除或重传，以欺骗网络端，假冒合法用户身份[32]。

2. 传统网络架构制约安全和可靠性

在轨道交通行业通信系统的早期研究阶段，主要考虑的是列车操作控制通信需求，而没有考虑到工作人员和乘客对视频、音频等多媒体业务的需求。虽然GSM-R铁路综合数字通信系统被普遍用于轨道交通行业的列车调度管理，但由于该系统使用的是低速率窄带通信方式，不足以应对移动环境下的媒体流传输和通信调度等功能的需要。伴随着移动通信系统研究的不断演进，学术界逐渐基于长期演进（LTE）技术着手研究下一代铁路通信系统。在媒体流数据传输方面，LTE-R由于能够提供比GSM-R更高的传输速率，弥补了GSM-R的缺陷。随着智能轨道交通的高速发展，出现了新的高带宽需求，如在列车上观看实时4K/8K超清视频，对列车进行远程维护等新业务，LTE-R系统能够提供的Mbps级带宽已然不够使用[33]。所以，5G技术成为铁路通信系统新的研究方向，但是技术和成本上的双重困难使新一代智能化铁路网络的建设面临挑战。目前，轨道交通周边存在着丰富的无线资源，如4G/5G蜂窝网络，Wi-Fi、卫星网络、全球微波接入互操作性等非蜂窝网络[34]。因此，如何高效使用现有的多种异构网络资源进行协同传输，满足轨道交通行业高带宽、高安全和高可靠性需求，是智能轨道交通行业车载网络一个值得探索的方向。

在网络架构层面，传统网络体系架构难以满足轨道交通行业的安全性与高可靠需求，其存在资源／位置绑定、用户／网络绑定和控制／数据绑定的三重绑定问题[35]。在网络层，互联网协议（IP）地址存在二义性问题[36]，IP地址同时承担了身份和位置的功能，这种设计使得网络架构只关注网络的连通性，欠缺对应用服务资源内在需求的考虑。此外，传统网络的设计对移动性、隐私性和可扩展性的支持也存在不足[37]，进而引发保护位置隐私、网络移动性、多家连接等一系列难题。在传输层，传统网络体系使用<IP:端口>标识连接，这种传输层名称空间与下层网络名称空间紧密依赖的设计使上层网络应用难以提供移动场景下的无缝通信连接服务[38]。在应用层，通过层次化语义统一资源标识符（URI）来描述服务和内容资源，并通过域名系统（DNS）将URI与IP地址进行映射，从而实现了网络资源的定位和访问。然而，这种依赖于资源与网络位置的方式也带来了一些问题，如资源过剩、网络僵化、传输能力有限等。与此同时，网络层与应用层之间的分离导致网络层无法理解应用层对网络的要求[39]，难以满足轨道交通行业对应用承载网络的多元化需求。

综上可见，针对轨道交通行业专用网络的攻击主要由行业内部管理与系统漏洞等导致的内部威胁以及网络监听和恶意钓鱼等外部威胁共同构成。在网络体系架构方面，传统网络原始设计面向信任体制、固定有线场景，未充分考虑移动性、安全性等问题，以打补丁的方式改进现有网络仍然难以解决原生设计不足。为此亟需开展新型网络理论研究、设计更好满足轨道交通行业需求的网络工作机制和体系，并在新网络基础设计建设的契机下，构建一个高效、安全、灵活、可扩展的新网络架构，满足轨道交通行业的未来发展需求。

六、我国轨道交通行业网络空间安全发展建议

随着我国轨道交通行业的飞速发展，信息技术、人工智能技术和控制技术的逐步完善，轨道交通行业系统智能化水平的不断提高，其外部和内部威胁也在逐渐增加[40]。加强网络创新研究、实现全产业链自主可控以及完善安全运维管理是维护当前轨道交通行业网络空间安全的重要措施，同时强化人才培养是确保未来安全需求得以满足的坚实保障。

（一）加强网络原创基础研究和体系化创新

目前，网络体系化创新架构多样，分别应对不同的需求和场景，如多模态网络、服务定制网络、智融标识网络等，但面向轨道交通行业安全的网络体系架构较少。

轨道交通行业系统和网络的结合日益密切，铁路交通流自动化是一项复杂的制造活动，在开发智能控制系统时，必须确保准确的预测和正确的运输计划，应考虑到所有限制因素，特别要关注到轨道交通行业的网络安全能力[41]。① 从源头出发，重视基础研究与原始创新，向行业纵深发展，探索更广阔的市场空间。② 在吸收引进先进技术的同时坚持原创自主创新，打破碎片式创新的局面，在技术细节上持续创新，稳步提升创新能力。③ 在充分吸收和借鉴国内现有信息网络技术体系优势的基础上，推动体系化引领性创新，由局部分片的创新模式，向大体系、大系统创新转变，形成集整体性、协同性、过程性、全面性和适应性于一身的网络安全体系。

（二）构建行业网络安全自主可控产业链

在当下全球经济竞争越发激烈的大背景下，为防止产业链“断链”“卡链”对国家产业安全造成威胁，亟需增强产业链的韧性，保证产业体系的原始创新、安全可靠。构建智能化、可持续发展、高安全性的轨道交通产业成为行业重点研究方向[42]。

为了构建轨道交通行业网络安全自主可控的产业链，建议采取以下措施。① 着眼于产业链和效益链，从“卡脖子”技术出发，解决由于行业网络关键基础设备来自国外厂商，缺乏突发安全事件预警和控制能力的问题。具体来说，要对关键基础技术进行升级，对基础设备进行更换，摆脱对国外厂商服务的依赖，提升轨道交通行业网络抗风险能力。② 要持续跟踪行业网络安全动态，系统开展行业网络新技术的研究。融合多种新型技术到行业中是未来发展趋势，智能交通系统旨在提高交通的安全性和效率[43]，依靠多要素融合思维智能整合信息资源，以提高系统的安全性、可用性和可靠性。重点突破关键核心技术，推动轨道交通行业体系不断优化，助力全链条网络资源的高效流动，实现行业体系建设的智能规划、部署，确保产业链安全，促进我国轨道交通行业网络技术原始创新、产业高效发展。

（三）加强行业网络安全运维管理

轨道交通行业信息化的发展给交通出行和交通管理带来便利的同时，也带来了诸多风险，信息系统成为不法分子的主要攻击对象和不法利益来源[44]。

为适应现代化产业体系下的行业发展，建议从以下方面着手布局。① 建立健全新形势下的国家和行业层面的网络空间安全多维管理制度，优化网络安全管理体制与协调机制，将责任制度落实落细在全方位各个环节，明确各部分职责分工，强化维护网络安全重要性意识，不断协调、优化管理机制，提高管理的透明度和规范性，确保行业系统的高效性和高可用性。② 结合我国轨道交通行业网络安全运营管理现状，专注行业发展趋势，从多角度分析行业发展需求，充分考虑列车调度指挥系统、列车运行控制系统以及运输调度管理信息系统等对聚集大量数据资源和高安全性的需求，善于运用数字化、信息化、智能化多种新型处理技术，持续应用高效的优化算法和可靠的通信技术完成信息的综合整理分析，构建效率高、综合性强、信息涵盖面广的智能运营管理平台。③ 结合轨道交通行业各系统特点，制定多维度、多层级的管理模式，旨在制定适用不同场景的更细致、更深入、更全面的行业运营管理方案，实现全流程的安全管理。

（四）加强行业网络安全人才培养

人才培养是保障轨道交通行业网络空间安全的关键因素之一。未来智能交通安全态势感知等领域的发展需要大量人才支撑，培养相关网络安全人才是满足需求的重要措施[45]。

近年来，国家对网络空间安全人才的重视程度不断提高。工业和信息化部发布的《网络安全产业高质量发展三年行动计划（2021—2023年）（征求意见稿）》提出，2023年网络安全产业规模超过2500亿元，年复合增长率超过15%。然而，我国重点行业的网络空间安全人才仍存在缺口。在轨道交通行业，原始创新网络体系下的网络安全人才培养的挑战主要表现在人才数量、人才质量以及“产学研”结合等方面。为应对上述挑战，可从5个方面提升人才培养水平。① 政策引导：出台相关政策，支持轨道交通行业网络空间安全人才的培养和发展，如加大资金投入、设置奖励政策等。② 完善培养机制：因地制宜地建立轨道交通行业网络空间安

全人才培养的机制，如建立专业的人才培养机构、设立相关教育和培训计划等。③ 推动“产学研”结合：轨道交通行业相关网络安全企业与高校等教育机构进行紧密合作，共同开展研究和实践活动，培养具有实践能力的人才。④ 加强国际交流：应加强轨道交通行业网络空间安全人才与国际领域的交流与合作，促进国内人才的国际化和国际人才的引进。⑤ 健全人才评价体系：应结合轨道交通行业特点健全人才评价体系，完善相关人才培养质量监测和评价机制，以推动人才质量持续提高。

利益冲突声明

本文作者在此声明彼此之间不存在任何利益冲突或财务冲突。

Received date: July 18, 2023; **Revised date:** November 21, 2023

Corresponding author: Liu Mingyuan is a lecturer from the School of Electronic and Information Engineering, Beijing Jiaotong University. His major research field is future network technology. E-mail: myliu@bjtu.edu.cn

Funding project: Chinese Academy of Engineering project “Cyberspace Security Technology System and Risk Response” (2022-JB-04); China Postdoctoral Science Foundation (2023M730206)

参考文献

[1] 刘大为. 铁路网络安全面临的严峻形势和主要对策研究 [J]. 铁道通信信号, 2023, 59(1): 1–5.
Liu D W. Analysis of the challenges and countermeasures in railway cybersecurity protection [J]. Railway Signalling & Communication, 2023, 59(1): 1–5.

[2] 崔伟健. 基于改进 Apriori 算法的铁路网络安全风险分析方法研究 [D]. 北京: 中国铁道科学研究院 (硕士学位论文), 2021.
Cui W J. Research on railway network security risk analysis method based on improved Apriori algorithm [D]. Beijing: China Academy of Railway Sciences Corporation Limited (Master’s thesis), 2021.

[3] 赵小军, 黄天天, 马金鑫. 列控系统信息安全风险分析与防护技术探讨 [J]. 铁路通信信号工程技术, 2022, 19(9): 46–50.
Zhao X J, Huang T T, Ma J X. Information security risk analysis and protection technology of Chinese train control system [J]. Technology Innovation, 2022, 19(9): 46–50.

[4] Li L, Xu K, Wang D, et al. A longitudinal measurement study of TCP performance and behavior in 3G/4G networks over high speed rails [J]. IEEE/ACM Transactions on Networking, 2017, 25(4): 2195–2208.

[5] Huang X J, Chen Y L, Bian T, et al. Analysis and research on vehicle-ground communication failure of CBTC system [C]. Chongqing: 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), 2019.

[6] Kane K. IBM X-force report: Ransomware doesn’t pay in 2018 as cybercriminals turn to cryptojacking for Profit [EB/OL]. (2019-02-26)[2023-08-10]. https://newsroom.ibm.com/2019-02-26-IBM-X-Force-Report-Ransomware-Doesnt-Pay-in-2018-as-Cybercriminals-Turn-to-Cryptojacking-for-Profit.

[7] 耿幸福, 崔联云. 城市轨道交通运营安全(第 3 版) [M]. 北京: 人民交通出版社, 2022.
Geng X F, Cui L Y. Urban rail transit operation safety (3rd edition) [M]. Beijing: China Communication Press, 2022.

[8] 王平, 陈嵘, 安博洋. 铁路轨道工程长寿命安全保障战略探讨 [J]. 中国工程科学, 2017, 19(6): 66–71.
Wang P, Chen R, An B Y. Discussion on long-life security strategies for railway track engineering [J]. Strategic Study of CAE, 2017, 19(6): 66–71.

[9] 孙远运. 筑牢网络安全防线, 保障铁路数字化升级转型 [J]. 铁路计算机应用, 2021, 30(11): 3.
Sun Y Y. Building a strong defense line for network security and ensuring the digital upgrading and transformation of railways [J]. Railway Computer Application, 2021, 30(11): 3.

[10] 陈燕申, 陈思凯, 李昂. 美国《公共交通安全标准纲要》中城市轨道交通安全标准法规体系结构及其启示 [J]. 城市轨道交通研究, 2019, 22(5): 16–21.
Chen Y S, Chen S K, Li A. Architecture of urban rail transit safety standards and regulations in the *compendium of public safety standards* of US and the enlightenment [J]. Urban Mass Transit, 2019, 22(5): 16–21.

[11] 新华网. 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要 [EB/OL]. (2021-03-13)[2023-04-20]. http://www.xinhuanet.com/politics/2021lh/2021-03/13/c_1127205564.htm.
Xinhuanet. The outline of the 14th Five-Year Plan for national economic and social development and the long-range objectives through the year 2035 [EB/OL]. (2021-03-13)[2023-04-20]. http://www.xinhuanet.com/politics/2021lh/2021-03/13/c_1127205564.htm.

[12] 中华人民共和国国家发展和改革委员会. “十四五”现代综合交通运输体系发展规划 [EB/OL]. (2021-03-13)[2023-03-25]. https://www.ndrc.gov.cn/fggz/fzzlgh/gjjzxgh/202203/t20220325_1320208.html.
National Development and Reform Commission of the People’s Republic of China. Development plan for modern comprehensive transportation system during the 14th Five-Year Plan [EB/OL]. (2021-03-13)[2023-03-25]. https://www.ndrc.gov.cn/fggz/fzzlgh/gjjzxgh/202203/t20220325_1320208.html.

[13] 中华人民共和国网络安全法 [J]. 中华人民共和国全国人民代表大会常务委员会公报, 2016 (6): 899–907.
Cybersecurity law of the People’s Republic of China [J]. Gazette of the Standing Committee of the National People’s Congress of the People’s Republic of China, 2016 (6): 899–907.

[14] 马力, 陈广勇, 祝国邦. 网络安全等级保护 2.0 国家标准解读 [J]. 保密科学技术, 2019 (7): 14–19.
Ma L, Chen G Y, Zhu G B. Interpretation of baseline for classified protection of cybersecurity 2.0 [J]. Secrecy Science and Technology, 2019 (7): 14–19.

[15] 李继元. 铁路通信网络安全防护研究 [J]. 中国铁路, 2022 (6): 94–98.
Li J Y. Research on protection of railway communication network

security [J]. China Railway, 2022 (6): 94–98.

[16] 朱广劼. 对依法依规筑牢铁路网络安全屏障的思考与展望 [J]. 铁路计算机应用, 2021, 30(11): 5–10.
Zhu G J. Thinking and prospect of building solid railway network security barrier in accordance with law and regulations [J]. Railway Computer Application, 2021, 30(11): 5–10.

[17] 国铁集团关于发布《铁路通信网络安全技术要求第1部分: 总体技术要求》等30项技术标准的通知 [J]. 铁道技术监督, 2022, 50(1): 83–85.
Notice of China Railway Group on issuing 30 technical standards, including *technical requirements for railway communication network security part 1: Overall technical requirements* [J]. Railway Quality Control, 2022, 50(1): 83–85.

[18] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 关键信息基础设施安全保护要求: GB/T 39204—2022 [S].
State Administration for Market Regulation, Standardization Administration. Information security technology—Cybersecurity requirements for critical information infrastructure protection: GB/T 39204—2022 [S].

[19] 王丹识, 韩鹏军, 王荣博, 等. 我国煤炭企业网络安全现状、问题分析研究与建议 [J]. 中国煤炭, 2022, 48(7): 34–40.
Wang D S, Han P J, Wang R B, et al. Research and suggestions on the current situation and problems of network security in China's coal enterprises [J]. China Coal, 2022, 48(7): 34–40.

[20] 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(z1): 20–23.
Tao W. Research on the information security for urban rail transit signal system [J]. Urban Mass Transit, 2018, 21(z1): 20–23.

[21] 牛爱成. 对机务段布置形式的探讨 [R]. 北京: 第十届世界轨道交通发展研究会年会, 2013.
Niu A C. Discussion on the layout form of locomotive depot [R]. Beijing: The 10th Annual Conference of World Railway Development and Research Society, 2013.

[22] 柯向喜. 铁路车务段运输安全系统分析方法与应用 [D]. 长沙: 中南大学 (硕士学位论文), 2013.
Ke X X. Transport safety system analysis methods and application in railway train operation depot [D]. Changsha: Central South University (Master's thesis), 2013.

[23] 赵文芳, 孙美. 高速铁路智慧工务安全生产管理模型研究 [J]. 管理现代化, 2015, 35(1): 103–105.
Zhao W F, Sun M. Research on the safety production management model of intelligent works in high speed railways [J]. Modernization of Management, 2015, 35(1): 103–105.

[24] 杨帅. 安全双重预防机制在铁路电务段的应用研究 [D]. 北京: 中国铁道科学研究院 (硕士学位论文), 2023.
Yang S. Research on the application of safety double prevention mechanism in railway telecommunication depot [D]. Beijing: China Academy of Railway Sciences Corporation Limited (Master's thesis), 2023.

[25] 蒋一凡. 地铁车辆段检修工艺设备管理分析探讨 [J]. 中国设备工程, 2021 (24): 90–91.
Jiang Y F. Analysis and discussion on the management of maintenance process equipment in subway depot [J]. China Plant Engineering, 2021 (24): 90–91.

[26] 关键基础设施安全应急响应中心. CNCERT: 城市轨道交通行业网络安全态势分析报告 [EB/OL]. (2020-11-05)[2023-11-15]. https://www.secrss.com/articles/26791.
CISRC. CNCET: Analysis report on network security situation of urban rail transit industry [EB/OL]. (2020-11-05)[2023-11-15]. https://www.secrss.com/articles/26791.

[27] 颉新春. 网络化控制系统的异常检测及安全控制 [D]. 上海: 上海大学 (博士学位论文), 2023.
Jie X C. Anomaly detection and security control of networked control systems [D]. Shanghai: Shanghai University (Doctoral dissertation), 2023.

[28] 石魏. 网络数据动态流动刑事规制的现状审视、反思与探索 [J]. 法律适用, 2022 (11): 98–106.
Shi W. Review, reflection and exploration of the criminal regulation for the dynamic flow of network data [J]. Journal of Law Application, 2022 (11): 98–106.

[29] 周泽岩, 程鹏, 方付生, 等. 基于机器学习的牵引供电远动系统异常攻击检测技术研究 [J]. 软件工程, 2022, 25(2): 1–5.
Zhou Z Y, Cheng P, Fang F S, et al. Research on abnormal attack detection technology of traction power supply SCADA system based on machine learning [J]. Software Engineering, 2022, 25(2): 1–5.

[30] 钟章队, 官科, 陈为, 等. 铁路新一代移动通信的挑战与思考 [J]. 中兴通讯技术, 2021, 27(4): 44–50.
Zhong Z D, Guan K, Chen W, et al. Challenges and perspective of new generation of railway mobile communications [J]. ZTE Technology Journal, 2021, 27(4): 44–50.

[31] 罗丹. GSM-R系统在既有高速铁路上的应用 [D]. 广州: 华南理工大学 (硕士学位论文), 2012.
Luo D. The applications of GSM-R system in high-speed railway [D]. Guangzhou: South China University of Technology (Master's thesis), 2012.

[32] 程学庆, 邓一维, 唐于, 等. 基于GSM-R的列控通信系统安全防控 [J]. 铁道科学与工程学报, 2015, 12(6): 1289–1295.
Cheng X Q, Deng Y W, Tang Y, et al. Safety analysis of communication system in train control system based on GSM-R [J]. Journal of Railway Science and Engineering, 2015, 12(6): 1289–1295.

[33] Ai B, Molisch A F, Rupp M, et al. 5G key technologies for smart railways [J]. Proceedings of the IEEE, 2020, 108(6): 856–893.

[34] 董平, 尹晨洋, 张宇阳, 等. 轨道交通中异构智融车载网络发展综述 [J]. 交通运输工程学报, 2022, 22(2): 41–58.
Dong P, Yin C Y, Zhang Y Y, et al. Review on development of heterogeneous smart cooperative vehicular networks in rail transit [J]. Journal of Traffic and Transportation Engineering, 2022, 22(2): 41–58.

[35] Zhang H K, Quan W, Chao H C, et al. Smart identifier network: A collaborative architecture for the future internet [J]. IEEE Network, 2016, 30(3): 46–51.

[36] 支婷, 刘颖, 周华春, 等. 智慧标识网络服务机理研究进展及安全性分析 [J]. 电子学报, 2021, 49(8): 1653–1664.
Zhi T, Liu Y, Zhou H C, et al. Research progress and security analysis of the service mechanism in smart identifier network [J]. Acta Electronica Sinica, 2021, 49(8): 1653–1664.

[37] 江凌云, 穆晏如, 朱洪波. 物联网命名和寻址技术研究 [J]. 物联网学报, 2018, 2(3): 44–50.

Jiang L Y, Mu Y R, Zhu H B. Research on naming and addressing technology of the Internet of things [J]. Chinese Journal on Internet of Things, 2018, 2(3): 44–50.

[38] 缪静莹. 面向多维标识体系的标识解析映射系统的设计与实现 [D]. 北京: 北京交通大学 (硕士学位论文), 2022.
Miu J Y. Design and implementation of identifier resolution and mapping system for multi-dimensional identifier architecture [D]. Beijing: Beijing Jiaotong University (Master's thesis), 2022.

[39] 黄兵, 谭斌, 罗鉴, 等. 面向业务和网络协同的未来IP网络架构演进 [J]. 电信科学, 2021, 37(10): 39–46.
Huang B, Tan B, Luo J, et al. Future IP network architecture evolution for service and network collaboration [J]. Telecommunications Science, 2021, 37(10): 39–46.

[40] Wang Z R, Xie X Z, Chen L, et al. Intrusion detection and network information security based on deep learning algorithm in urban rail transit management system [J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(2): 2135–2143.

[41] Mikhailova U, Lukyanov G, Kalugina O. Intelligent and secure wireless network management of a railway transportation [C]. Istanbul: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020.

[42] 李义岭, 喻彦喆, 姚克民. 城市轨道交通智能化及可持续发展现状分析与展望 [J]. 现代城市轨道交通, 2021 (11): 90–94.
Li Y L, Yu Y Z, Yao K M. Status analysis and prospect of intelligent and sustainable development of urban rail transit [J]. Modern Urban Transit, 2021 (11): 90–94.

[43] Sedjelmaci H, Hadji M, Ansari N. Cyber security game for intelligent transportation systems [J]. IEEE Network, 2019, 33(4): 216–222.

[44] Deng J, Song L Q, Liang L. Comprehensive information security risk assessment model for transportation industry [C]. Bhubaneswar: 2021 Smart City Challenges & Outcomes for Urban Transformation (SCOUT), 2021.

[45] Sarowa S, Bhanot B, Kumar V, et al. Review of smart transportation and challenges: Cyber security perspective [C]. Gharuan: 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT), 2023.