 DOI: https://doi.org/10.12349/iser.v7i6.10793

Research on Railway Communication Security Protection System Construction and Technology

Yating Yun

Guoneng Shuohuang Railway Yuanping Branch, Xinzhou, Shanxi, 034100, China

Abstract

Railway communication systems play a critical role in train scheduling, line monitoring, and operational coordination, with their stability directly impacting transportation safety and efficiency. As railway networks expand and technologies advance, these systems have exposed vulnerabilities to multi-source threats—including traditional environmental interference, equipment aging, as well as emerging risks like cyberattacks and data breaches. Establishing a systematic, secure, and sustainably evolving protection framework has become a key research focus in the railway industry. Based on the structural characteristics, operational patterns, and security requirements of railway communication systems, this study analyzes communication network architectures, critical equipment, data links, and management mechanisms. It explores the formation mechanisms of communication security risks, evaluates applicable conditions and development trends for technical safeguards, and proposes future-oriented systematic construction approaches. The research aims to provide theoretical support and practical references for ensuring high-reliability operations in railway communication systems.

Keywords

railway communication; safety protection; network architecture; technical research; operational support

铁路通信安全防护体系建设与技术研究

运亚婷

国能朔黄铁路原平分公司，中国 · 山西 忻州 034100

摘　要

铁路通信系统在列车调度、线路监测和运营协调中发挥着关键作用，其稳定性直接影响运输安全与效率。随着铁路网络的扩展和技术进步，通信系统暴露出多源威胁和脆弱性，包括传统环境干扰、设备老化，以及网络攻击和数据泄露等新型风险。如何构建一个系统化、安全、可持续演进的防护体系，已成为铁路行业的研究重点。本文基于铁路通信系统的结构特点、运行规律与安全需求，围绕通信网络架构、关键设备、数据链路和管理机制展开分析，探讨通信安全风险的形成机制，并梳理技术防护措施的适用条件与发展趋势，提出面向未来的体系化建设路径，旨在为铁路通信系统的高可靠运行提供理论支持与实践参考。

关键词

铁路通信；安全防护；网络体系；技术研究；运行保障

1 引言

铁路通信系统的安全是铁路运输安全的重要基础。随着铁路建设全面推进、高速铁路密度不断提高、智能化调度手段广泛应用，通信系统在任务复杂度与承载能力方面均面临显著挑战。传统通信系统以稳定性为核心，但在当前网络化、数字化背景下，安全威胁呈现技术化、隐蔽化和场景化趋势，使防护体系建设的紧迫性不断提高。通信系统的关键节点、传输链路与监控平台一旦受到破坏，可能造成调度滞后、区段控制失灵、信号指令错发等严重后果，甚至引发系统级安全事件。为此，有必要构建结构清晰、技术先进、管理完善的通信安全防护体系，使其能够应对复杂环境变化，并在实际运行中保持高可靠、高冗余与高自适应能力。本文基于铁路通信系统的实际特点，对安全风险来源与防护机制展开深入研究，旨在提出可操作、可落地的系统化建设方案。

【作者简介】运亚婷（1988–），女，中国河北大名人，本科，工程师，从事铁路通信设备维护研究。

2 铁路通信安全风险的构成特征

2.1 通信网络架构的脆弱性分析

铁路通信系统结构庞大，由骨干传输网、无线通信系统、沿线设备、调度平台等多层级构成，区域跨度大、设备类型多、运行环境复杂。网络架构在长期扩展和改造中形成不同年代、不同技术体系的混合结构，使整体耦合关系复杂，潜在兼容性问题较多。部分线路存在链路冗余不足、节点布局

不均衡的情况，导致某些区段在遭遇强干扰、线路中断或设备故障时，系统恢复能力有限。通信架构的脆弱性还体现在部分老旧传输设备的抗干扰能力下降，无法满足高速铁路对时延、抖动和带宽的高要求，当运行负荷急剧增加时，易出现瓶颈或短时失效。此外，通信架构在设备部署过程中受地形、站场结构及施工条件限制，局部区域形成信号覆盖盲区，使得某些场景下通信链路稳定性难以保证。

2.2 多源干扰环境下的安全隐患

铁路沿线通常穿越城市、乡村、隧道、山区等多种环境，外部电磁环境复杂，雷击、强电磁辐射、大型输电线路干扰都会影响通信质量。高速列车运行过程中产生强烈气动噪声与滑动摩擦电荷，也会对无线通信信号形成扰动。某些区域由于沿线建筑密集或新建设施的电磁排放超标，使现场通信信号衰减严重。外部环境干扰往往具有突发性和不可控性，在极端情况下可能导致通信链路中断。部分设备在长期暴露于高湿、高盐、高温环境中，其性能衰退速度加快，内部元器件易产生接触不良，进而引发短时故障。此外，设备检修周期与现场环境变化可能存在偏差，使潜在隐患难以及时被发现，增加通信失效概率。

2.3 网络安全威胁的隐蔽化特点

随着铁路调度系统与通信网络进一步融合，信息系统逐步采用开放式接口和分布式架构，引入更多外部访问点，使系统暴露面积显著扩大。网络入侵、恶意代码注入、拒绝服务攻击等威胁呈现组织化特征，攻击者可利用系统漏洞实施持续渗透。部分调度终端与后台服务器存在访问控制不足、加密强度不够的问题，使非法访问风险提高。随着云计算、边缘计算平台引入铁路行业，数据在多节点间交换的频率提升，攻击路径也更加多样化。

3 铁路通信安全防护体系的基础构成

3.1 通信网络冗余体系的构建原则

通信系统的冗余设计是抵御突发故障的重要手段，涉及传输链路、交换节点、供电系统与无线覆盖等多方面内容。冗余体系建设需遵循多路径、多节点与多层级原则，使单点故障不会影响整体网络的连续运行。对于骨干传输网，采用光纤环网或双向保护链路结构能够显著提升容错能力；对站场级网络，可增加核心节点的旁路通道，使其在主链路失效时迅速切换到备用链路。无线通信系统可结合沿线布局设计重叠覆盖区域，通过优化基站间距与功率配置提高覆盖连续性。冗余体系不仅依赖硬件结构，也需要配套的智能切换算法，确保链路切换过程不影响数据完整性。科学的冗余体系能够有效提升系统抗破坏能力，并为后续的故障诊断与恢复提供稳定基础。

3.2 关键通信设备的可靠性强化措施

关键设备包括传输节点、调度控制服务器、无线基站、路由交换设备等，其运行状态直接影响通信质量。设备可靠性强化需要从选型、安装、运行监测与维护策略等多个方面展开。设备选型应考虑长期运行环境，通过耐高温、抗振动、抗潮湿等指标筛选适配型号；安装阶段结合沿线环境配置防雷、防水和防鼠害措施，确保设备在极端条件下保持稳定运行。运行监测可利用智能巡检系统实时采集温度、电流、信号强度等指标，通过阈值分析和趋势判断及时发现异常。维护策略需结合设备寿命曲线制定检修计划，使关键元器件在性能下降前完成替换，避免因突发损坏导致链路中断。可靠性强化的核心在于形成动态调节机制，使设备始终保持在最佳运行区间。

3.3 通信系统管理机制的安全支撑作用

管理机制是通信安全体系的重要支撑，包括运维规范、权限管理、应急预案与审计追踪等内容。运维规范通过统一标准实现设备管理的可控性与一致性，使安装、调试与检修过程可追溯。权限管理需根据岗位职责进行严格分级，通过身份认证、双因素验证和操作记录系统减少人为失误或恶意操作的风险。应急预案是处理突发事件的重要保障，通过明确处置流程、人员职责与资源配置，使系统在面对干扰、攻击或设备故障时能够迅速恢复。审计追踪机制可记录系统的访问行为与参数变更，为风险分析与事后调查提供依据。管理机制的系统性建设能够有效降低人为因素造成的安全隐患，并为技术防护体系提供制度保障。

4 铁路通信安全技术的关键路径

4.1 网络隔离与边界控制技术

铁路通信系统通常采用生产网、管理网和业务网分层隔离的结构，通过边界控制设备实现数据路径的可控性。网络隔离可阻断外部网络对核心系统的直接访问，削弱潜在攻击的渗透能力。边界控制包括防火墙、入侵检测系统与数据过滤设备，通过协议识别、行为分析和访问策略匹配对异常流量进行识别与阻断。部分系统可采用单向传输技术，使数据只能向外发送无法回流，避免关键平台被外部访问者利用。边界控制技术不断演进，引入深度包检测与基于行为模型的识别方式，使系统能够应对复杂攻击手段。合理的边界控制能够显著降低网络威胁的影响范围，使通信系统的核心部分保持高可靠性。

4.2 数据加密与身份认证体系

数据在传输过程中存在被截取、篡改或伪造的风险，为此需构建完善的数据加密体系，通过加密算法与密钥管理机制保护通信内容的完整性与机密性。加密体系包括链路层加密、端到端加密与存储加密，使不同层级的数据交换过程均具备保护能力。身份认证体系可在用户访问关键系统前进行验证，通过数字证书、生物特征识别或硬件密钥等手段确保使用者的合法性。铁路系统在认证过程中可结合调度权限、岗位级别和操作场景进行细分，使访问行为受到严格限制。密钥管理是加密体系的核心环节，通过密钥轮换、分级

存储和权限隔离避免密钥泄露。加密与认证技术的融合能够有效增强系统安全性，使数据交换过程具有更高可信度。

4.3 主动式安全监测与智能分析技术

主动式安全监测以实时感知系统状态为核心，通过采集网络流量、设备日志、用户行为等数据并进行智能分析，实现对潜在威胁的提前发现。监测系统通常采用多模型融合方式，通过异常识别、特征匹配与机器学习算法构建安全态势感知平台，使系统具备快速响应能力。智能分析技术可识别攻击行为的模式，并通过预测模型判断风险发展趋势，为运维人员决策提供依据。部分平台可实现自动化处置，在识别严重威胁时自动隔离受影响区域，减少攻击扩散的可能性。主动式监测技术的应用使铁路通信系统不再依赖被动防御，而是具备自感知、自诊断与自恢复的能力，为构建真正意义上的动态安全体系提供技术基础。

5 铁路通信安全防护体系的建设路径

5.1 体系化顶层架构的构建

铁路通信安全防护体系的构建首先需要通过顶层架构设计明确系统的边界、功能分区、技术路线和协同机制。顶层架构的核心目标是保证系统各个部分在通信、信号、供电及调度等方面的统一性与一致性。在构建过程中，需将所有相关子系统纳入统一框架，以避免由于各技术平台标准不一致导致的安全漏洞。在设计架构时，应考虑铁路行业的长期发展趋势，包括网络规模扩展、线路延伸和设备更新等因素，确保防护体系具备可持续性和扩展性。顶层设计不仅要统筹当前的安全需求，还应预见未来的技术变革与行业发展，从而为系统的长期发展奠定坚实基础。

5.2 先进技术的工程化应用模式

铁路通信安全建设不仅依赖理论方案，还需要通过工程化应用模式确保新技术能够在实际铁路环境中稳定实施。在技术应用过程中，必须结合实际运营需求、施工组织、设备布局及环境特点，使每一项技术措施在实际运行中具有可操作性。例如，加密系统在铁路通信中的应用需要特别关注其在长距离传输和大规模节点环境中的性能表现，确保其在复杂网络环境下保持高效能。而智能监测技术的应用则需要考察其数据采集频率、实时分析能力和报警的准确性。工程化模式应强调系统的稳定性和可维护性，因此，在设计时必须考虑模块化、标准化，减少系统间的接口障碍，使技术能够在广域铁路网络中快速推广。通过优化技术和系统架构设计，不仅可以提高系统的安全防护能力，还能实现技术建设的高效落地，推动铁路通信安全水平的整体提升。

5.3 安全管理体系与技术系统的融合机制

铁路通信安全的有效保障不仅依赖于先进的技术措施，也需要与完善的管理体系紧密结合，形成协同工作机制。安全管理体系的建设应与技术系统深度融合，确保技术措施能够在制度化管理下落实到位。管理体系通过制度化要求来确保设备的定期检修、数据监测和应急响应等工作能够按计划高效开展，从而使运行行为有据可依。在此基础上，技术系统应为管理体系提供量化的实时数据支持，帮助管理决策更加科学合理。信息化平台的建设则是实现技术与管理深度融合的关键，通过该平台可以实时监控各类安全事件的发生，并使各部门能够迅速协同处理，从而提高整体体系的响应效率。融合机制的核心是实现安全管控过程的自动化与数据化，避免传统管理方式过度依赖人工经验判断，而是基于数据分析、规则设定和自动化流程来进行精准、高效的安全管理。这种融合机制将大大提升铁路通信系统在面临突发事件时的应急响应能力和安全防护水平。

6 结语

铁路通信安全防护体系建设是一项系统性、长期性工程，需要技术、管理与制度多维协同。面对铁路运输组织持续扩展与通信需求的不断增长，通信系统的安全风险呈现多样化趋势，使防护体系的建设必须兼顾架构稳定性、技术先进性与运行可持续性。通过优化网络架构、强化关键设备、完善管理体系、引入智能监测技术，可逐步构建适应未来铁路发展的安全保障体系。通信安全防护不仅是技术问题，更关乎运行组织、应急处置与行业治理能力的整体提升。随着智能铁路建设的推进，通信系统将承担更加复杂的任务，对安全性的要求也将不断提高。持续推进安全防护体系建设，有助于支撑铁路行业的高质量发展，并确保铁路运输在多源威胁环境下保持稳定、安全与高效运行。

参考文献

[1] 陈继仲,蒋明亮,摆晓军,等.基于云架构的集中式铁路通信网络安全防护方案研究[J].铁道通信信号,2025,61(12):41-49.

[2] 张卫军,郭桂芳,刘清涛.铁路通信网网络安全体系架构研究[J].铁道通信信号,2018,54(09):37-42.

[3] 陈丹晖,周耀胜.铁路通信骨干网云安全技术保障体系研究[J].铁道通信信号,2023,59(02):50-54.

[4] 李继元.铁路通信网络安全防护研究[J].中国铁路,2022,(06):94-98.

[5] 李东阳.铁路通信光缆故障及防护技术分析[J].科技创新与应用,2020,(34):135-136.