 DOI: https://doi.org/10.12349/iser.v5i12.4053

Problems and Prevention Strategies of Railway Network Information Security

Peizhi Zheng

Institute of Computing Technology, China Academy of Railway Sciences, Linzhi, Xizang Autonomous Region, Linzhi, Xizang, 860100, China

Abstract

Railway network information security is very important to ensure transportation safety and social stability. With the development of information technology, the railway network information system is becoming increasingly complex and faces more security threats. This paper analyzes the problems existing in technology, management, regulations and personnel awareness, and puts forward the corresponding prevention strategies. At the technical level, strengthening encryption technology and system protection capability are key; at the management level, improving security mechanism and strengthening training to enhance employees' security awareness; at the regulation level, formulating and implementing relevant regulations to provide legal support for security; at the personnel awareness level, it is crucial to improve security awareness and establish security culture. These measures jointly build a three-dimensional line of defense of railway network information security.

Keywords

railway network information security; technical prevention; management strategy; laws and regulations; personnel safety awareness

铁路网络信息安全存在的问题及防范策略

郑培志

西藏自治区林芝市中国铁道科学研究院电子计算技术研究所，中国 · 西藏 林芝 860100

摘　要

铁路网络信息安全对保障运输安全和社会稳定至关重要。随着信息技术的发展，铁路网络信息系统日趋复杂，面临更多安全威胁。论文分析了铁路网络信息安全在技术、管理、法规及人员意识方面存在的问题，并提出了相应的防范策略。技术层面，强化加密技术和系统防护能力是关键；管理层面，完善安全机制和加强培训提升员工安全意识；法规层面，制定和执行相关法规为安全提供法律支撑；人员意识层面，增强安全意识和建立安全文化至关重要。这些措施共同构建了铁路网络信息安全的立体防线。

关键词

铁路网络信息安全；技术防范；管理策略；法律法规；人员安全意识

1 引言

随着信息技术的飞速发展，铁路网络已经成为国家重要的交通命脉和关键信息基础设施之一。铁路网络信息安全问题直接关系到铁路运输的安全与效率，甚至影响到国家的经济运行和社会稳定。在此背景下，探讨铁路网络信息安全存在的问题及防范策略显得尤为重要。铁路网络信息系统的安全性和可靠性一直是铁路运输领域关注的焦点。近年来，随着高速铁路的快速发展和信息技术的广泛应用，铁路网络信息系统日益复杂，面临的安全威胁也日益增多。从国内外轨道交通网络安全事件中不难发现，恶意攻击、人员误操作、系统漏洞等问题时有发生，给铁路运输安全带来了严重威胁。

【作者简介】郑培志（1994–），男，中国河南鹤壁人，本科，从事网络信息安全研究。

2 相关理论概述

铁路网络信息安全是确保铁路运输系统稳定运行和数据不受威胁的关键领域。随着信息技术的不断发展，铁路网络信息系统的复杂性日益增加，面临的安全挑战也日益严峻。

2.1 铁路网络信息安全的定义与范畴

铁路网络信息安全所涵盖的领域，旨在保护铁路系统中的关键网络设施、信息系统以及数据不受未授权的访问、破坏、修改或泄露等威胁的影响。这包括但不限于列车调度指挥系统、客票发售预订系统、铁路运输管理系统等关键信息基础设施。这些系统构成了铁路运输的神经中枢，一旦遭到破坏或数据泄露，可能会对国家安全、经济运行和社会秩序造成严重影响。铁路网络信息安全的定义不仅包括技术层面的防护，还涉及管理、法律、人员培训等多个维度，以确

保铁路网络的完整性、可用性和保密性得到全面保障。

2.2 铁路网络信息安全的关键技术

确保铁路网络信息安全的关键技术是构建网络安全防御体系的基石。这些技术包括但不限于防火墙、入侵检测系统、防病毒软件、数据加密技术、安全信息和事件管理（SIEM）系统等。防火墙作为网络的第一道防线，能够有效地监控和控制进出网络的流量，防止恶意软件和攻击者入侵。入侵检测系统和入侵防御系统则进一步监控网络和系统是否有被攻击的迹象，并在潜在攻击发生时立即采取措施。数据加密技术则确保了数据在传输和存储过程中的安全性，防止敏感信息被非法截获和解读。

2.3 铁路网络信息安全的相关法规与标准

铁路网络信息安全的法规与标准是确保其安全性的基石。《中华人民共和国网络安全法》为铁路网络信息安全提供了基础性框架，确立了网络安全等级保护制度、关键信息基础设施的保护要求、网络安全监测预警和应急处置等关键制度。这些规定为铁路网络的安全运行提供了法律依据和操作标准，确保了在遇到安全威胁时，能够依法采取有效措施。《铁路关键信息基础设施安全保护管理办法》进一步细化了铁路关键信息基础设施的安全保护要求。该办法明确了铁路关键信息基础设施的定义，即在铁路领域中，一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生和公共利益的重要网络设施和信息系统。

3 铁路网络信息安全现状

铁路网络信息安全是确保铁路运输系统稳定运行和数据不受威胁的关键领域。随着信息技术的不断发展，铁路网络信息系统的复杂性日益增加，面临的安全挑战也日益严峻。

3.1 铁路网络信息安全的主要威胁

铁路网络信息安全所面临的主要威胁涵盖了恶意攻击、人员误操作、系统漏洞、网络安全威胁以及数据安全问题等多个方面。随着新的攻击手段，如 APT（Advanced Persistent Threat）的出现，铁路通信网络覆盖面积的增加，以及系统对外界依赖性的增强，针对铁路信号系统网络的恶意攻击呈现出多样化和复杂化的趋势。这些攻击可能包括对铁路网络的非法侵入、干扰、破坏，以及数据泄露，严重时甚至可能危害国家安全、国计民生和公共利益。在人员误操作方面，由于技术水平跟不上铁路信息化发展的要求，加之人员素质及责任心的问题，人为因素已成为造成安全隐患的重要原因。

3.2 铁路网络信息安全防护的现状分析

铁路网络信息安全防护体系的构建是一个复杂且持续的过程，涉及技术、管理、人员等多个层面。当前，铁路网络信息安全防护主要从内网物理隔离的角度出发，在必要的地方增加外围防护。这种策略在一定程度上能够抵御外部攻击，但同时也存在一些局限性。外围防护和系统本身的功能安全防护并未协同考虑，这导致了在实际防护中存在一定的脱节。功能安全防护侧重于系统的可靠性和稳定性，而信息安全防护则更关注数据的保密性、完整性和可用性。这两者的结合是实现系统内生安全的关键，但目前在这方面还存在巨大差距。高速铁路信号系统的网络安全防护措施包括调度集中网的建立，该系统采用新一代分散自律调度集中系统，综合了计算机技术、网络通信技术和现代化控制技术，以提高列车运行的安全性和效率。这种系统的设计原则是“故障导向安全”，即在设计阶段就采用热备、容错、冗余等机制来保障设备和系统的高可靠性、高可用性、高可维修性和高安全性。

4 铁路网络信息安全存在的问题

铁路网络信息安全是确保铁路运输系统稳定运行的关键，随着信息技术的不断发展，铁路网络信息系统的复杂性日益增加，面临的安全挑战也日益严峻。

4.1 技术层面的安全隐患

铁路网络技术层面的安全隐患主要涉及网络设施和信息系统等关键组件的脆弱性。随着铁路系统数字化转型的深入，运营技术（OT）系统与信息技术（IT）系统的融合带来了新的安全挑战和风险。例如，传统的 OT 系统在设计时往往侧重于功能的实现和系统的稳定性，而缺乏对网络安全威胁的充分考量，导致系统在面对恶意攻击时显得脆弱。老旧系统可能由于缺乏内置的安全特性而难以适应当前的网络安全要求，增加了安全防护的难度。系统的广泛分布和数量众多也使得标准化和管理变得更加复杂。铁路网络的覆盖面积不断扩大，系统对外界的依赖性增强，使得针对铁路信号系统网络的恶意攻击越来越多样化和复杂化。对供应商的依赖性、安全问题的复杂性以及更新系统的安全性问题都是技术层面需要关注的重要问题。应用层的自主开发能力虽然在提升，但在操作系统、芯片以及数据库等方面仍然依赖国外厂商，这在一定程度上限制了对漏洞的主动辨识和应对能力。

信号系统网络的相对封闭性虽然有助于防止外界入侵，但也易遭到多样化、隐蔽性的攻击。信号系统采用的安全计算机平台虽然关注了可靠性、可用性、可维修性和安全性等指标，但计算性能相对有限，难以实现有效的安全防护，直接对抗攻击的能力较弱。信号系统基本按照等级保护的要求安装了基本的安全设备，但区域防护能力不完善，设备接入控制技术有限，非法接入风险较大，边界防护能力亟待提升。

4.2 管理层面的安全隐患

铁路网络信息安全的管理层面安全隐患是一个多维度的问题，它不仅涉及组织结构的合理性，还与人员素质和内部流程的规范性密切相关。在组织结构方面，一个明确、高效的管理框架对于确保铁路网络信息安全至关重要。当前，

一些铁路运营单位在组织结构上可能存在职责不明确、协调不充分等问题，这些问题可能导致安全管理上的盲点和漏洞，从而增加网络信息安全的风险。人员素质的提升也是管理层面的一个重要议题。技术人员和相关工作人员的专业技能、安全意识以及对网络安全威胁的识别和应对能力，直接影响到铁路网络信息安全防护的有效性。

4.3 法律法规层面的安全隐患

铁路网络信息安全的法律法规层面安全隐患主要体现在相关法律法规及标准的完善程度及其执行力度上。当前，铁路领域的网络安全法规尚处于完善阶段，现有的铁路特定法规可能尚未全面涵盖网络安全的各个方面，导致基本服务运营商（OES）在遵守网络安全要求时面临源自不同法规的、非统一的标准和要求。这种法规间的不一致性，不仅增加了企业合规的难度，也可能导致安全防护措施的执行不到位，从而影响铁路网络信息安全的整体水平。对于网络安全指令的理解和遵从可能需要大量的工作来集成信息并执行管理任务，这对 OES 在遵守不同国家法规施加的网络安全要求时构成了挑战。根据《铁路关键信息基础设施安全保护管理办法》（以下简称《管理办法》），国家铁路局负责制定铁路关键信息基础设施认定规则，并报国务院公安部门备案，抄送国家网信部门。这要求运营者不仅要理解《管理办法》的具体要求，还要能够将其与现有的网络安全实践相结合，确保法规得到有效执行。

4.4 人员安全意识层面的安全隐患

铁路网络信息安全不仅受制于技术与管理层面，人员的安全意识同样扮演着至关重要的角色。在铁路部门的网络安全实践中，员工对于网络安全的认识水平参差不齐，整体而言，对网络安全需求的意识仍然偏低。尽管安全要求至关重要，但面对频繁更新的网络安全规定，安全团队必须投入额外的时间与资源以确保安全机制的完整性，这无疑增加了保护信息的难度。

5 铁路网络信息安全对策

针对铁路网络信息安全现存的问题，采取全面的解决对策是保障铁路运输安全的关键。这些对策需要从技术、管理、法律法规及人员安全意识等多个层面进行综合施策。

5.1 技术层面的防范策略

技术层面的防范策略是确保铁路网络信息安全的基础。加强加密技术的应用是提升数据传输和存储安全性的关键。通过采用先进的加密算法和协议，如 TLS/SSL 协议，可以有效地保护数据在传输过程中不被窃取或篡改。提升系统安全防护能力是另一项重要措施。这包括但不限于强化网络边界的防火墙配置、定期进行系统漏洞扫描和补丁管理，以及部署入侵检测系统和入侵防御系统来及时发现和响应潜在的安全威胁。

5.2 管理层面的防范策略

管理层面的防范策略是确保铁路网络信息安全的重要组成部分。完善信息安全管理机制要求建立一套全面的安全政策和程序，以规范员工的行为并减少人为错误。加强人员安全培训则要求定期对员工进行安全意识教育和技能培训，以提高他们对网络安全威胁的认识并提升其应对能力。

5.3 法律法规层面的防范策略

铁路网络信息安全的法律法规防范策略构成了维护网络安全的基石。在数字化时代，网络空间已成为国家安全的重要组成部分，铁路网络作为关键信息基础设施，其安全性直接关系到国家安全和经济社会的稳定运行。《中华人民共和国网络安全法》（以下简称《网络安全法》）的实施为铁路网络信息安全提供了基础性的法律框架，对保护个人信息、治理网络诈骗、保护关键信息基础设施等方面作出了明确规定。

5.4 人员安全意识层面的防范策略

人员安全意识层面的防范策略是提升铁路网络信息安全的关键。增强全员安全意识要求通过教育和培训提高所有员工对网络安全重要性的认识。建立安全文化则要求在组织内部营造一种重视网络安全的氛围。

6 结语

铁路网络信息安全是确保铁路运输系统稳定运行的关键领域。随着信息技术的不断发展，铁路网络信息系统的复杂性日益增加，面临的安全挑战也日益严峻。论文从技术、管理、法律法规及人员安全意识等多个层面，深入分析了铁路网络信息安全现存的问题，并提出了相应的解决对策。

参考文献

[1] 闫莉,岳涛,方旭明.铁路应急场景下无人机通信感知一体化无线网络资源智能分配算法[J].电子与信息学报,2024,46(9):3510-3519.

[2] 赵茹英.新质生产力对铁路运输网络影响的实证分析[J].理论学习与探索,2024(4):71-74.

[3] 郭首江,张德栋,冯凯亮,等.铁路信息系统信创迁移网络安全风险分析及对策研究[J].网络安全技术与应用,2024(8):92-95.

[4] 程智博,刘忠东,周亮瑾,等.基于应用现代化的铁路信息系统统型方法研究[J].铁路计算机应用,2024,33(7):41-46.

[5] 王春杨,侯朝慧.高速铁路网络建设对企业投资效率的影响研究[J].铁道运输与经济,2024,46(8):180-189.