

# 城市轨道交通网络安全防护方案探讨

于大伟

徐州地铁信息科技有限公司 江苏 徐州 221000

**摘要:** 在城市轨道交通的蓬勃发展背后,网络安全问题逐渐浮出水面,成为不容忽视的挑战。本文开篇即强调城市轨道交通网络安全的重要性,随后深入剖析了当前网络安全的现状与隐患。基于此,我们提出了一套综合性的网络安全防护方案,通过多层次、多维度的防护措施,旨在筑牢城市轨道交通网络的安全防线,确保其稳定、高效地服务于广大市民的日常出行。

**关键词:** 城市轨道交通; 网络安全; 防护方案

## 引言

在现代城市的繁华与喧嚣中,城市轨道交通如同城市的血脉,承载着无数市民的出行需求。然而,随着信息技术的迅猛发展,这条血脉也面临着网络安全的严峻考验。为了保障城市轨道交通的安全运行,维护广大乘客的出行权益,我们急需探讨和构建一套行之有效的网络安全防护方案。这不仅是对技术的挑战,更是对城市管理智慧和责任担当的考验。

### 1 城市轨道交通网络安全的重要性

城市轨道交通网络安全的重要性不言而喻,它是城市轨道交通系统稳定、高效运行的重要保障。在现代社会,城市轨道交通已经成为人们日常出行的主要方式之一,其安全性和可靠性直接关系到广大乘客的切身利益。一旦城市轨道交通网络遭受攻击或出现故障,后果将不堪设想。网络攻击可能导致列车运行控制系统失灵,造成列车相撞或脱轨等严重事故,危及乘客的生命安全。此外,乘客的个人信息也可能因网络漏洞而泄露,引发社会安全问题和信任危机。这些不仅会影响城市轨道交通的正常运营,还会对城市的公共安全造成重大威胁。因此,加强城市轨道交通网络安全防护工作刻不容缓。只有确保网络安全,才能保障城市轨道交通系统的稳定运行,为乘客提供安全、便捷的出行服务。同时,这也是维护城市公共安全、促进社会和谐稳定的重要举措。我们必须高度重视城市轨道交通网络安全问题,采取有效措施加以防范和应对。

### 2 城市轨道交通网络安全现状

随着信息技术的迅猛发展和广泛应用,城市轨道交通系统的智能化、网络化进程不断加快,为市民提供了更加便捷、高效的出行服务<sup>[1]</sup>。然而,与此同时,城市轨道交通网络安全问题也日益凸显,面临着多方面的严峻挑战。首先,外部黑客攻击和恶意软件感染等网络安

全事件频发,给城市轨道交通网络带来了严重的安全威胁。黑客利用漏洞和弱点,对城市轨道交通系统进行攻击,可能导致列车运行控制系统失灵、乘客信息泄露等严重后果。例如,近年来,全球范围内发生了多起针对城市轨道交通系统的网络攻击事件,攻击者通过植入恶意软件、篡改数据等手段,破坏了系统的正常运行,给城市轨道交通带来了巨大的经济损失和社会影响。其次,内部人员误操作、设备老化等问题也可能导致网络安全事件的发生。城市轨道交通系统是一个复杂的网络体系,涉及到众多的设备和人员。由于操作不当、设备维护不及时等原因,可能导致网络安全事件的发生。例如,操作人员误操作可能会导致系统崩溃或数据丢失,设备老化则可能引发系统故障或网络中断。这些问题不仅会影响城市轨道交通的正常运营,还可能对乘客的出行安全造成威胁。此外,随着新技术、新应用的不断引入,城市轨道交通网络的复杂性不断增加,网络安全防护的难度也随之加大。例如,物联网、云计算、大数据等新技术的应用,使得城市轨道交通系统的网络架构更加复杂,数据交互更加频繁,同时也带来了更多的安全隐患和漏洞。此外,新技术的应用还可能导致与传统系统的兼容性问题,进一步增加网络安全防护的难度。同时,城市轨道交通网络安全还面临着制度不健全、安全意识不足等挑战。在网络安全管理方面,一些城市轨道交通系统缺乏有效的安全管理制度和应急预案,导致在应对网络安全事件时无法及时响应和有效处置。在安全意识方面,一些操作人员和管理人员缺乏网络安全意识和技能,无法有效识别和防范网络威胁,从而增加了网络安全风险。更为严峻的是,当前城市轨道交通网络安全威胁呈现出多样化、隐蔽化的特点。攻击者可能采用更加复杂、隐蔽的攻击手段,如钓鱼攻击、勒索软件、分布式拒绝服务攻击等,对城市轨道交通系统进行攻

击。这些攻击手段不仅难以被及时发现和防范，而且可能对系统造成更加严重的破坏和影响。

### 3 城市轨道交通网络安全防护方案

#### 3.1 建立完善的网络安全管理体系

在城市轨道交通网络安全防护方案中，建立完善的网络安全管理体系是至关重要的一环。这一体系需要全面考虑城市轨道交通网络的特点和安全需求，从多个层面入手，确保网络安全的全方位管理。首先，制定网络安全政策是建立管理体系的基础<sup>[2]</sup>。政策应明确网络安全的目标、原则和要求，为网络安全工作提供指导。同时，政策还应包括网络安全的标准和规范，确保各项工作符合国家和行业的要求。通过制定网络安全政策，可以统一思想，明确方向，为后续的网络安全工作奠定基础。其次，明确安全管理职责是确保网络安全管理体系有效运行的关键。应建立网络安全管理组织，明确各级管理人员的职责和权限。同时，还应建立跨部门、跨岗位的协同工作机制，形成工作合力。通过明确职责和建立协同机制，可以确保网络安全工作有人负责、有人落实、有人监督，避免出现管理漏洞。此外，实施安全培训也是网络安全管理体系中不可或缺的一环。应定期开展网络安全意识和技能培训，提高员工对网络安全的认识和应对能力。培训内容应包括网络安全基础知识、安全操作规范、应急响应流程等。通过培训，可以增强员工的网络安全意识，提升整体的安全防护能力。在建立完善的网络安全管理体系过程中，还应注重与实际情况的结合。应根据城市轨道交通网络的实际情况，制定切实可行的管理措施和应急预案。同时，还应加强与相关部门和机构的合作与交流，共同应对网络安全挑战。

#### 3.2 加强网络安全技术防护

在城市轨道交通网络安全防护方案中，加强网络安全技术防护是确保网络安全的重要手段。随着网络攻击手段的不断演变和升级，单一的安全防护措施已经难以应对复杂多变的网络安全威胁。因此，我们需要采用多层次、多手段的技术防护措施，构建全方位的网络安全防护体系。首先，部署防火墙是网络安全技术防护的基础措施之一。防火墙能够监控和控制网络之间的数据传输，有效阻止未经授权的访问和恶意攻击。通过配置合理的防火墙规则，可以实现对网络系统的精细化控制，防止潜在的安全风险。其次，入侵检测系统（IDS）是实时监测和识别网络攻击行为的重要工具。IDS能够对网络流量进行深度分析，及时发现并报警异常流量和行为，帮助管理人员快速响应和处置网络安全事件。同时，IDS还可以与防火墙等其他安全设备联动，实现自动化的安

全防御。此外，数据加密技术也是保护网络数据安全的重要手段。通过对敏感数据进行加密处理，可以防止数据在传输和存储过程中被窃取或篡改。在城市轨道交通系统中，数据加密技术可以应用于乘客信息传输、控制系统通信等关键环节，确保数据的安全性和完整性。除了以上措施外，还应定期对网络系统进行安全漏洞扫描和风险评估。安全漏洞扫描可以帮助管理人员及时发现系统存在的安全漏洞和弱点，为修复漏洞提供依据。风险评估则可以对网络系统的安全性进行全面评估，识别潜在的安全威胁和风险，为制定针对性的安全防护策略提供参考。

#### 3.3 建立网络安全应急响应机制

在城市轨道交通网络安全防护方案中，建立网络安全应急响应机制是至关重要的一环。网络安全事件具有突发性、传播速度快、影响范围广等特点，一旦发生，将对城市轨道交通系统的正常运行和乘客的出行安全造成严重影响<sup>[3]</sup>。因此，建立健全的网络安全应急响应机制，对于保障城市轨道交通网络安全具有重要意义。首先，制定详细的应急响应计划是建立应急响应机制的基础。应急响应计划应明确应急响应的流程、责任分工、资源调配等关键要素，确保在发生安全事件时能够迅速启动应急响应程序。同时，应急响应计划还应包括不同安全事件的分类和分级，针对不同类型的事件制定相应的处置措施，提高应急响应的针对性和有效性。其次，组建专业的应急响应团队是保障应急响应机制有效运行的关键。应急响应团队应具备丰富的网络安全知识和实践经验，能够迅速定位并处置安全事件。团队成员之间应建立紧密的协作关系，形成高效的工作机制。同时，还应定期对团队成员进行培训和演练，提高其应对复杂网络安全事件的能力。此外，定期进行应急演练也是检验和提升应急响应机制有效性的重要手段。通过模拟真实的安全事件场景，组织相关人员进行应急演练，可以检验应急响应计划的可行性和有效性，发现存在的问题和不足，并及时进行改进和完善。同时，应急演练还可以提高相关人员的应急意识和处置能力，增强整体的安全防护能力。

#### 3.4 加强网络安全监测和预警

在城市轨道交通网络安全防护方案中，加强网络安全监测和预警是保障网络安全的重要手段。随着网络技术的不断发展和网络攻击的不断升级，城市轨道交通系统面临着越来越复杂的网络安全威胁。因此，建立网络安全监测和预警系统，实时监测网络系统的安全状况，及时发现和处置安全威胁，对于保障城市轨道交通网络

安全具有重要意义。首先,建立网络安全监测和预警系统是加强网络安全监测和预警的基础。该系统应具备实时监测、智能分析、快速响应等功能,能够对网络系统的安全状况进行全面监测和分析。通过对网络流量、系统日志、安全事件等信息的采集和分析,可以及时发现异常行为和潜在威胁,为管理人员提供准确的预警信息。其次,加强与政府、行业组织等的合作与交流是提升网络安全监测和预警能力的重要途径。政府和相关行业组织通常具有丰富的网络安全资源和经验,可以为城市轨道交通系统提供有力的支持。通过合作与交流,可以共享网络安全信息、技术和资源,共同应对网络安全挑战。同时,还可以及时了解最新的网络安全动态和趋势,为制定针对性的安全防护策略提供参考。此外,为了确保网络安全监测和预警系统的有效运行,还应建立完善的管理制度和操作规范。管理制度应明确监测和预警的流程、责任分工、响应机制等关键要素,确保各项工作有序进行。操作规范则应对监测和预警的具体操作进行规定,包括信息采集、分析处理、预警发布等环节,提高工作的规范性和准确性。

### 3.5 提升人员网络安全意识和技能

在城市轨道交通网络安全防护方案中,提升人员的网络安全意识和技能是至关重要的。人是网络安全的第一道防线,也是最容易被攻击的环节<sup>[4]</sup>。因此,加强对城市轨道交通网络相关人员的网络安全培训和教育,提升其网络安全意识和技能水平,对于保障城市轨道交通网络安全具有深远的意义。首先,网络安全意识和技能的提升有助于减少因人为因素导致的网络安全事件。在城市轨道交通系统中,许多网络安全事件往往是由于人员的疏忽、误操作或恶意行为引起的。通过加强网络安全培训和教育,可以让相关人员充分认识到网络安全的重要性,了解常见的网络攻击手段和防御方法,从而在日常工作中更加谨慎地处理网络安全问题,减少人为因素导致的安全漏洞。其次,提升网络安全意识和技能可以增强人员对网络安全的认识和理解。网络安全是一个复

杂而又不断变化的领域,新的攻击手段和防御技术不断涌现。通过持续的网络安全培训和教育,可以让相关人员及时了解最新的网络安全动态和趋势,掌握先进的网络安全技术和工具,从而更好地应对网络安全挑战。此外,提升网络安全意识和技能还可以促进城市轨道交通网络安全文化的建设。网络安全文化是一种注重安全、强调责任、倡导合规的文化氛围。通过加强网络安全培训和教育,可以在城市轨道交通系统中形成一种人人关注网络安全、共同维护网络安全的良好氛围,从而有效提升整个系统的网络安全水平。为了提升人员的网络安全意识和技能,可以采取多种形式的培训和教育手段。例如,可以定期组织网络安全知识讲座、技能培训课程、应急演练等活动,让相关人员全面了解网络安全的基本知识和实践技能。同时,还可以建立网络安全知识库和在线学习平台,方便人员随时随地进行自主学习和交流。

### 结语

在数字化浪潮席卷全球的今天,城市轨道交通网络安全防护的重要性愈发凸显。通过本文的探讨,我们深刻认识到,这是一项系统工程,需要多管齐下、综合施策。只有建立完善的网络安全管理体系,加强技术防护,建立应急响应机制,加强监测预警,并提升人员的网络安全意识和技能,才能为城市轨道交通筑起一道坚不可摧的安全屏障,确保城市的公共交通安全和广大乘客的出行安全无虞。

### 参考文献

- [1]王伟,李强.(2022).城市轨道交通网络安全挑战与对策研究.信息安全,6(6),112-115.
- [2]张涛,刘洋.(2021).基于大数据的城市轨道交通网络安全监测方法.计算机工程与应用,(23),17-21.
- [3]陈晓明.(2022).城市轨道交通信息系统安全管理实践.中国交通信息化,(4),44-47.
- [4]赵新宇,杨帆.(2021).城市轨道交通网络安全态势感知技术研究.电子技术应用,(12),24-26.