

基于信息安全的地铁数字化转型探讨

谢波

(南京地铁运营有限责任公司)

摘要: 随着智慧城市的发展,地铁作为城市交通的重要组成部分,其数字化转型对提高运行效率和乘客体验至关重要。然而,这一转型过程中的信息安全问题不容忽视。本文将围绕地铁数字化转型的三个主要方面进行深入研究:首先,强化顶层设计,构建“安全一张网”;其次,围绕业务实施建设纵深防御,为智慧地铁保驾护航;最后,建立常态化信息安全运行机制,确保有效运行。通过这三个方面的研究,旨在为地铁行业的数字化转型提供一套全面的信息安全解决方案。

关键词: 地铁;数字化转型;信息安全

一、地铁数字化转型背景

地铁作为现代都市交通的重要组成部分,随着城市化进程的加快和科技的迅速发展,其运营模式和管理体系正经历着深刻的数字化转型。这一转型不仅关乎地铁系统效率的提升、运营成本的降低,也涉及乘客体验的改善和服务的个性化。数字化转型的背后,是对信息技术的广泛应用,包括但不限于大数据分析、云计算、物联网(IoT)和人工智能(AI)。这些技术的引入,使得地铁系统能够实现更为精准的流量预测、车辆调度、故障预测维护,以及提供更加智能化的客户服务。然而,这种转型同时带来了新的挑战,尤其是在信息安全领域。随着系统的开放和网络的互联互通,地铁系统越来越多地暴露在网络攻击和数据泄露的风险之中。

二、强化顶层设计,构建“安全一张网”

1. 横向安全架构

在构建“安全一张网”的横向安全架构中,关键在于实现地铁系统各个业务单元之间的无缝信息安全集成。这要求建立一个统一的安全管理平台,用于监控和协调各个系统和部门之间的安全策略和措施。例如,通过集成的安全信息和事件管理(SIEM)系统,可以实时收集和分析来自票务系统、监控系统、乘客服务系统等不同源的安全日志,以便及时识别和响应潜在的安全威胁。横向架构还要求在不同系统间建立标准化的数据交换和通信协议,确保信息在传递过程中的安全性和完整性。在实践中,这可能涉及对现有系统的改造或升级,以支持先进的加密技术和认证机制,从而增强整个地铁系统在信息传输和处理过程中的安全性。

2. 纵向安全机制

纵向安全机制的建立,着重于从地铁系统的顶层管理到基础设施的每一个环节,确保信息安全的全面性。这意味着不仅要在技术层面上强化安全防护,还要在管理和操作层面上建立严格的安全规范。从技术层面来看,

需要对关键基础设施如服务器、网络设备和终端设备进行定期的安全评估和加固,以防止恶意攻击和数据泄露。同时,还应实施细致的访问控制和身份验证机制,以确保只有授权人员才能访问敏感数据和关键系统。在管理和操作层面,制定和执行严格的安全政策和程序至关重要。这包括但不限于定期对员工进行安全意识培训,制定应急响应计划,以及建立有效的内部审计和合规检查机制。

三、围绕业务实施建设纵深防御,为智慧地铁保驾护航

1. 安全管理中心

地铁数字化转型中,建立一个全面的安全管理中心是实施纵深防御的关键。安全管理中心的核心职责是统一监控和管理整个地铁网络的安全状况,包括但不限于威胁检测、风险评估、事件响应和恢复。通过部署先进的安全信息与事件管理系统(SIEM),中心能够实时收集和分析安全日志,从而快速识别潜在的安全事件,并采取相应的预防或应对措施。安全管理中心还需与地铁运营的其他关键部门协作,确保安全策略的有效实施,并在发生安全事件时进行快速有效的协调与处理。这不仅提高了地铁系统的整体安全性能,也为快速响应和处理安全事件提供了坚实的基础。

2. 安全通信网络

在智慧地铁系统中,构建一个安全通信网络至关重要。安全通信网络的设计应确保数据传输的完整性、机密性和可用性。为此,需采用强大的加密技术来保护数据在传输过程中不被截取或篡改。采用分层网络架构,将关键系统和普通业务系统分隔开来,可以有效防止潜在的网络攻击向关键系统蔓延。同时,引入入侵检测系统(IDS)和入侵防御系统(IPS)能够及时发现并阻止恶意活动。保证网络的稳定性和可靠性同样重要,这要求持续监测网络性能,及时处理任何可能导致服务中断

的问题。通过这些措施，可以确保智慧地铁系统的关键通信和数据在一个安全、可靠的网络环境中流动。

2.安全区域边界

设立明确的安全区域边界对于保护地铁系统的关键资产至关重要。这涉及物理和网络两个层面的安全控制。物理层面，重点是加强对地铁系统关键设施如控制中心、服务器房和通信枢纽的物理访问控制。这可能包括门禁系统、监控摄像头和安保人员的配置。网络层面，安全区域边界的建立需通过防火墙、虚拟私有网络（VPN）和网络隔离等技术来实现。这些技术能有效隔绝内部网络与外部网络，防止未经授权访问和数据泄露。同时，定期对这些安全边界进行检测和审计，可以确保其持续有效地保护地铁系统不受外部威胁的侵袭。

3.安全计算环境

建立一个安全的计算环境对于智慧地铁系统至关重要。这个环境不仅要保证硬件和软件的安全性，还要确保数据处理和存储过程中的安全。首先，硬件层面上，关键服务器和存储设备需要在物理上得到保护，防止未经授权的访问或破坏。同时，采用可靠的硬件维护和更新策略，确保设备始终运行在最佳状态，减少由硬件故障引起的安全风险。软件层面上，操作系统和应用程序需要定期更新和打补丁，以防止利用已知漏洞进行攻击。此外，引入先进的端点保护和异常行为监测系统，可以及时发现并阻止恶意软件或非授权操作。数据处理和存储的安全也非常重要，这要求使用强加密技术来保护敏感数据，同时实施严格的数据备份和恢复策略，确保在任何情况下数据的完整性和可用性。

4.安全防护服务

为智慧地铁系统提供全方位的安全防护服务是实现纵深防御的关键环节。这包括但不限于实时的威胁监测、定期的安全评估、快速的事件响应以及持续的安全培训。威胁监测服务需利用先进的技术，如人工智能和机器学习，来分析大量数据，及时识别潜在的安全威胁。安全评估服务则要定期对整个地铁系统的安全状况进行全面的检查，包括硬件、软件、网络和数据的安全性评估。在发生安全事件时，快速响应服务能够及时采取措施，减少损失并尽快恢复正常运营。

四、建立常态化信息安全运行机制，确保有效运行

为保证地铁数字化转型的信息安全，建立常态化的信息安全运行机制至关重要。这一机制涉及三个核心方面：制度建设、常态化运行机制的维护，以及定期的攻

防演练。

首先，制度建设是常态化信息安全管理的基础。这要求地铁运营机构制定全面而详尽的信息安全政策和程序，涵盖数据保护、网络安全、物理安全、员工行为规范等多个方面。制度的有效性依赖于清晰的责任分配和严格的执行力。比如，对于数据的访问和处理，需要设定严格的权限管理和审计追踪机制，确保只有授权人员能够访问特定数据，任何操作都有追溯记录。

其次，常态化运行机制的维护是确保信息安全日常管理的关键。这包括但不限于定期的系统和软件更新、持续的安全监控、异常事件的即时响应和处理。运维团队需要对系统进行持续监控，以及时发现并处理安全漏洞和异常行为。同时，建立一个有效的信息沟通机制，确保安全相关信息能够快速传达到每一个相关人员和部门。

最后，定期进行攻防演练是检验和提升地铁信息安全防护能力的有效手段。通过模拟各种可能的安全威胁和攻击场景，如网络攻击、数据泄露、系统故障等，演练能够帮助员工熟悉应急响应流程，并增强其处理实际安全事件的能力。此外，攻防演练还能揭示安全策略的潜在弱点，为进一步加强安全防护提供实际依据。

通过这些措施，地铁运营机构不仅能够应对当前的安全挑战，也能够更好地预防和准备未来可能出现的安全威胁，从而确保地铁系统的信息安全在数字化转型过程中得到有效保障。

五、结语

本研究深入探讨了地铁数字化转型中的信息安全问题，强调了构建安全一张网、实施纵深防御及建立常态化运行机制的重要性。笔者认为，地铁系统的数字化不仅是技术上的革新，更是一种全方位的安全挑战。通过横向和纵向的安全架构，可以确保系统的完整性和协调性。同时，安全管理中心、通信网络、区域边界以及计算环境的加固，为智慧地铁提供了坚实的安全防护。最后，通过制度建设、常态化机制和攻防演练，地铁系统能够有效应对日益复杂的信息安全挑战，保障数字化转型的顺利进行。

参考文献：

- [1]史永飞.厦门轨道交通建设数字化转型实践与思考[J].都市轨道交通,2023,36(04):35-39.
- [2]刘晓溪.信息安全助力深圳地铁数字化转型稳步推进[J].城市轨道交通,2021(08):34-36.