

轨道交通自动售检票系统安全性分析及解决方法

石维光

重庆市轨道交通（集团）有限公司 重庆 400020

摘要：轨道交通自动售检票系统（AFC）作为城市轨道交通管理的核心，其安全性关乎日常运营、乘客体验及财务安全。本文深入分析了AFC系统在数据安全、设备安全及网络安全方面存在的风险，并针对性地提出了加强数据安全、提高设备安全性、强化网络安全防护及加强人员安全管理的综合安全防护策略。通过实施这些策略，可确保AFC系统在面对各种威胁时保持稳定运行，为乘客提供安全、便捷的出行服务。

关键词：AFC系统安全性；多维度风险分析；安全性解决方法

引言

随着城市轨道交通的快速发展，自动售检票系统（AFC）作为客流与票务管理的关键，其安全性日益受到重视。AFC系统不仅承载着大量乘客的个人信息和出行数据，还直接关系到轨道的日常运营效率和乘客的出行体验。因此，全面分析AFC系统的安全风险，并采取相应的防护措施，对于保障城市轨道交通的安全运行具有重要意义。

1 轨道交通自动售检票系统安全性的重要性

轨道交通自动售检票系统（AFC）作为城市轨道交通客流管理与票务管理的核心系统，其安全性至关重要。该系统关乎城市轨道交通的日常运营，更与乘客的出行体验及运营公司的财务安全紧密相连。AFC系统的安全性体现在多个层面。车票的安全性是基础。车票中存储着乘客的个人信息和支付金额，如果车票数据被非法篡改或伪造，将直接损害乘客和轨道交通运营部门的利益。采用先进的IC卡技术和综合安全措施，如数据加密传输、SAM卡认证等，是保障车票安全的有效手段。系统整体的安全性也不容忽视。AFC系统承载着大量的业务数据，这些数据需要在服务器和 workstation 之间进行高效、安全的流通和处理。为确保系统稳定运行，需采用冗余和集群等技术配置中央计算机系统，并实施严格的身份认证和权限控制。建立完善的软件审计和防病毒机制，也是提升系统安全性的重要措施。数据的安全性同样关键。AFC系统作为数据管理系统，需确保数据的准确采集、可靠传输、存储及统计处理。选择功能强大、成熟可靠的数据库系统，并采用数据加密、数据备份和异地容灾备份等手段，是保障数据安全的有效策略。轨道交通自动售检票系统的安全性是多维度的，需要从车票、系统、数据等多个层面进行综合考量与防护。通过采用先进的技术手段和管理措施，有效提升AFC系统的

安全性，为城市轨道交通的顺畅运营提供有力保障。

2 轨道交通自动售检票系统安全风险

2.1 数据安全风险

轨道交通自动售检票系统（AFC）作为现代城市轨道交通的重要组成部分，承载着大量乘客的个人信息和出行数据。然而，这一系统在数据安全方面面临着诸多风险，其中数据泄露和数据篡改尤为突出。数据泄露是AFC系统面临的一大安全隐患。系统数据库中存储着乘客的姓名、身份证号、乘车记录等敏感信息。若系统的安全防护措施存在漏洞，或数据库管理不当，这些数据便有可能被不法分子窃取。如果数据泄露，乘客的隐私将受到严重威胁，可能导致个人信息被滥用，进而引发安全问题。除了数据泄露，数据篡改也是AFC系统数据安全风险的重要方面。在数据的传输和存储过程中，若系统遭受恶意攻击，数据便有可能被篡改。如黑客可能通过技术手段修改车票信息，导致乘客无法正常乘车，这会扰乱轨道交通的正常运营秩序，还给乘客带来不必要的困扰和经济损失。数据篡改还可能造成轨道交通运营方的经济损失，如车票收入减少、运营成本增加等。数据安全风险是轨道交通自动售检票系统不可忽视的重要问题。为了保障乘客的隐私和轨道交通的正常运营，必须加强对AFC系统数据安全的防护和管理，确保数据的完整性和保密性。

2.2 设备安全风险

在轨道交通自动售检票系统（AFC）的运行过程中，设备安全风险是一个不容忽视的重要方面。这一风险主要体现在硬件故障和设备被破坏两个方面。（1）硬件故障是AFC系统设备安全风险的主要来源。由于自动售票机、闸机等设备长时间运行且使用频率高，其内部硬件组件会因磨损、老化等原因出现故障。硬件故障不仅会导致设备无法正常工作，影响乘客的购票和乘车

体验,还对轨道交通的运营秩序造成干扰。更为严重的是,某些硬件故障可能会引发安全事故,对乘客和运营方的安全构成威胁。(2)设备被破坏也是AFC系统设备安全风险的一个重要方面。恶意破坏者会出于制造混乱、发泄情绪或其他不良目的,故意损坏自动售检票系统的设备。这种行为不仅会导致设备无法正常运行,影响乘客的出行和轨道交通的运营,还会增加维修成本和影响运营秩序,给轨道交通运营方带来经济损失。(3)需要指出的是,设备安全风险对轨道交通自动售检票系统的稳定性和可靠性构成了严重威胁。为了降低这一风险,运营方应加强设备的日常维护和保养,及时发现并处理潜在的硬件故障;还应加强设备的安全防护,防止恶意破坏行为的发生。通过这些措施,确保AFC系统的稳定运行,为乘客提供更加安全、便捷的出行服务^[1]。

2.3 网络安全风险

(1)网络攻击是AFC系统面临的重大网络安全威胁。随着系统的网络化程度不断提高,黑客通过网络入侵系统服务器的可能性也随之增加。如果黑客成功入侵,他们会获取系统的敏感信息,如乘客的个人数据和交易记录,甚至可能控制设备的运行。如分布式拒绝服务攻击(DDoS)能通过大量无效的网络请求使系统服务器过载,导致系统瘫痪,使乘客无法正常购票和乘车,给轨道交通运营带来巨大压力。(2)网络通信故障也是AFC系统网络安全风险的一个重要组成部分。网络线路中断、路由器故障等问题都可能导致数据传输的中断,使得自动售票机、闸机等设备之间无法正常通信。这种通信故障会直接影响乘客的购票和乘车体验,可能导致乘客无法及时获取票务信息,或者使闸机处无法正常通行。网络通信故障还可能影响系统的整体运行效率,给轨道交通运营带来不必要的困扰。(3)需要强调的是,网络安全风险对轨道交通自动售检票系统的稳定性和可靠性构成了严重威胁。为了降低这一风险,运营方应加强对系统网络的安全防护,定期更新安全补丁,提高系统的抗攻击能力;还应建立完善的网络通信故障应急响应机制,确保在网络通信出现故障时能迅速恢复系统的正常运行。

3 轨道交通自动售检票系统安全性解决方法

3.1 加强数据安全

(1)数据加密技术是保障数据安全的关键所在,尤其在轨道交通领域,乘客的个人信息和出行数据至关重要。为了确保这些数据在传输和存储过程中的安全性,我们要采用先进的加密技术。具体来说,结合使用对称加密算法和非对称加密算法,为数据提供多层次的加密

保护。对称加密算法以其高效性,能够快速加密大量数据;而非对称加密算法则确保了密钥交换的安全性,增强了数据的保密性。这样的双重保护机制,能有效防止数据泄露,还能确保数据的完整性,为乘客信息安全筑起一道坚实的防线。(2)访问控制机制的建立对于防止数据泄露至关重要。应设定严格的访问权限,仅允许经过授权的人员访问和操作系统的数据库。对这些授权人员的操作行为进行实时审计和详细记录,以便在必要时进行追溯和调查。这一措施能够有效防止内部人员滥用权限,确保数据的安全使用。(3)数据备份与恢复策略的制定也是不可或缺的环节。定期对系统的数据进行全面备份,并将备份数据存储在安全、可靠的地方,以确保在数据泄露、数据篡改等意外事件发生时,能够及时、准确地恢复数据,最大限度地减少损失。这一策略能保障数据的持续性可用性,还能为系统的稳定运行提供有力支持。加强数据安全是提升轨道交通自动售检票系统安全性的重要途径。通过实施数据加密、访问控制以及数据备份与恢复等措施,能全面保障乘客个人信息和出行数据的安全性^[2]。

3.2 提高设备安全性

在轨道交通自动售检票系统(AFC)的安全性构建中,提高设备安全性是确保系统稳定运行的关键环节。这主要涉及到设备的维护与保养、故障应急预案的制定以及设备防护措施的加强。设备的维护与保养是确保AFC系统设备安全性的基础。应加强对自动售检票系统设备的日常维护和保养,通过定期检查设备的运行状态,及时发现并处理潜在的硬件故障,从而降低因设备故障导致的安全风险。为应对可能出现的设备故障,应制定详细的故障应急预案,确保在设备出现故障时能够迅速响应,并采取有效措施进行处理,以保障系统的连续运行。在设备防护方面,应采取多重措施以防止恶意破坏。安装防护设施,如坚固的防护栏和高清监控摄像头,可以有效防止破坏者对设备进行物理破坏。加强对设备的巡查力度,定期巡查和实时监控相结合的方式,及时发现并制止破坏行为,确保设备的安全运行。为提高设备安全性,还应注重提升设备的技术防护能力。如采用先进的传感器技术和远程监控技术,实时监测设备的运行状态和异常行为,提升设备的自我保护能力。加强对设备操作人员的培训和管理,提高其安全意识和操作技能,确保设备在操作过程中的安全性和稳定性。提高设备安全性是轨道交通自动售检票系统安全性解决的关键措施。通过加强设备的维护与保养、制定故障应急预案以及加强设备防护措施,全面提升AFC系统的设备

安全性,为乘客提供更加安全、便捷的出行服务^[3]。

3.3 强化网络安全防护

(1) 防火墙的设置是网络安全防护的基础。作为系统的网络边界防御,防火墙的重要性不言而喻。通过在AFC系统的网络边界部署防火墙,可以构建起一道坚实的防线,有效阻止未经授权的网络访问,降低系统遭受恶意攻击和网络入侵的风险。防火墙能够依据预设的安全规则,对网络流量进行严格的过滤和检测,及时发现并拦截潜在的威胁,为系统的安全运行提供坚实的保障。(2) 入侵检测与防范系统的部署是提升系统安全性的重要手段。安装入侵检测系统(IDS)和入侵防范系统(IPS),能够实现对网络活动的实时监测,及时发现并报告异常行为。结合定期更新病毒库和安全补丁,可以提升系统的抗攻击能力,确保在面对新型网络威胁时,系统仍能保持稳定运行,为乘客提供不间断的出行服务。(3) 网络冗余设计是提升系统稳定性的关键措施。通过采用双线路接入、冗余服务器等冗余设计,在部分网络设备出现故障时,迅速切换至备用设备,确保系统仍能正常运行。这一设计提高了系统的可靠性和稳定性,还为乘客提供了更加稳定、便捷的出行体验,增强了轨道交通的吸引力和竞争力。强化网络安全防护是提升轨道交通自动售检票系统安全性的重要策略。精心设置防火墙、部署入侵检测与防范系统以及实施网络冗余设计,确保系统在面对各种网络威胁时仍能保持稳定运行,为乘客提供更加安全、可靠的出行服务。

3.4 加强人员安全管理

(1) 提升员工安全意识与技能对轨道交通运营至关重要。应定期组织自动售检票系统安全培训,涵盖安全原理、风险及应对措施。强调数据安全,禁止随意连接外部网络;规范设备操作,避免故障。通过考核机制确保员工掌握知识与技能,激励员工提升安全素养,确保运营安全。(2) 规范乘客行为对保障自动售检票系统安全意义重大。在车站显著位置设置宣传标识,通过图文

并茂的形式向乘客展示正确使用自动售检票设备的方法以及破坏设备、违规乘车等行为的危害。利用车站广播系统,在不同时段循环播放安全提示信息,提醒乘客文明乘车。对于故意破坏自动售检票设备的行为,应加大处罚力度,通过在车站张贴处罚公告等方式起到威慑作用。积极引导乘客文明出行,鼓励乘客相互监督,营造良好的乘车环境,减少因乘客不当行为导致的设备损坏和系统运行异常。(3) 构建高效人员应急响应机制,关键在于制定详尽预案,清晰界定各岗位责任。遇数据泄露,安全管理人员即刻加密备份,技术人员全力追溯;设备受损,维护人员速赴现场抢修,安保人员管控局面。通过定期应急演练,模拟各类安全事件,锻炼员工应急响应与团队协作能力,确保突发时刻能迅速、有效应对,竭力减少损失与影响^[4]。

结束语

综上所述,轨道交通自动售检票系统的安全性是一个复杂而多维的问题,需要从数据安全、设备安全、网络安全及人员安全管理等多个方面进行综合考量与防护。通过实施本文提出的综合安全防护策略,可以有效提升AFC系统的安全性,为城市轨道交通的顺畅运营提供有力保障。未来,随着技术的不断进步,还需持续优化和完善安全防护措施,以适应新的挑战 and 威胁。

参考文献

- [1]宋伟.轨道交通自动售检票系统安全性分析及解决方法[J].今日自动化,2023(4):117-119.
- [2]杨岗,汪小勇,余颜丽,等.基于弹性运力需求的轨道交通列车运行控制系统及装备研发与应用[Z].中铁二院工程集团有限责任公司.2023(1):17-19.
- [3]周麟真.轨道交通自动售检票系统设备维修策略优化研究[D].北京:北京交通大学,2023(4):11-12.
- [4]张振华.轨道交通自动售检票系统安全性分析及解决方法[J].数码-移动生活,2022(12):257-259.