城市轨道交通信息系统信息安全风险识别

刘柯宏
重庆市轨道交通（集团）有限公司　重庆　400020

摘　要：本文旨在探讨城市轨道交通信息系统中的信息安全风险识别问题。通过对城市轨道交通信息系统的深入了解，结合信息安全风险识别的相关理论和方法，本文分析了信息安全风险的主要来源和类型，提出了针对性的风险识别方法和过程。研究结果表明，城市轨道交通信息系统面临着多种信息安全风险，必须采取有效的措施进行防范和应对。本文的研究为城市轨道交通信息系统的信息安全防护提供了有益的参考。

关键词：城市轨道交通；信息系统；信息安全；风险识别；风险防范

引言：随着城市轨道交通的快速发展，信息系统在轨道交通运营中扮演着越来越重要的角色。然而，信息系统的广泛应用也带来了信息安全风险的问题。信息安全风险不仅可能导致运营中断、数据泄露等严重后果，还可能对乘客的出行安全构成威胁。因此，对城市轨道交通信息系统的信息安全风险进行识别和分析，采取有效的措施进行防范和应对，具有重要的现实意义。

1 城市轨道交通信息系统信息安全的重要性

1.1 信息安全是城市轨道交通运营的基石

城市轨道交通系统，作为现代都市交通网络的重要组成部分，承担着数百万人的日常出行任务。这一庞大而复杂的系统中，信息系统扮演着至关重要的角色。从列车运行的精确控制到乘客服务的智能化管理，从设备状态的实时监控到故障预警的快速响应，无一不依赖于信息系统的稳定与高效。因此信息安全成为了确保城市轨道交通系统正常运行的基石。一旦信息系统遭受攻击或破坏，不仅可能导致列车运行混乱、乘客服务中断，还可能引发安全事故，对公众生命财产安全构成严重威胁。

1.2 信息泄露与非法访问的潜在风险

在城市轨道交通信息系统中，存储着大量敏感数据，包括乘客个人信息、票务信息、设备监控数据等。这些数据一旦泄露或被非法访问，后果不堪设想[1]。乘客个人信息泄露可能引发个人隐私侵犯、诈骗等社会问题，损害乘客权益，降低公众对轨道交通系统的信任度。票务信息泄露则可能导致票务欺诈、逃票行为频发，影响轨道交通系统的正常运营秩序和票务收入。设备监控数据的非法访问可能被用于恶意破坏或干扰轨道交通设备的正常运行，进而危及行车安全。因此，加强信息安全防护，防止信息泄露与非法访问，是保障城市轨道交通系统安全稳定运行的关键。

1.3 信息安全对于提升服务质量和效率的重要性

信息安全不仅关乎轨道交通系统的安全稳定运行，还直接影响到服务质量和效率的提升。在智能化、信息化的今天，乘客对于轨道交通系统的服务体验要求越来越高。通过信息系统，轨道交通系统可以实现列车运行的精确调度、乘客服务的智能化管理、设备状态的实时监控等功能，从而提升服务质量和效率。然而，这一切的前提是信息系统的安全稳定。只有确保信息安全，才能确保这些功能的正常发挥，进而提升乘客满意度和轨道交通系统的整体竞争力。

1.4 构建全方位的信息安全防护体系

为了应对信息安全挑战，城市轨道交通系统需要构建全方位的信息安全防护体系。这包括加强物理安全、网络安全、数据安全等多个层面的防护。物理安全方面，需要确保信息设备的安全存放和访问控制；网络安全方面，需要部署防火墙、入侵检测系统、安全审计系统等安全措施，防止网络攻击和病毒入侵；数据安全方面，需要采用数据加密、数据备份、数据恢复等技术手段，确保数据的完整性和可用性。同时还需要加强员工的信息安全培训，提升全员的信息安全意识，形成人人参与信息安全防护的良好氛围。

2 城市轨道交通信息系统概述

2.1 系统组成

城市轨道交通信息系统是一个集成了多种高科技子系统的复杂网络，它们共同协作，确保轨道交通的安全、高效运营。以下是其基本组成：（1）传输系统：作为整个信息系统的神经中枢，负责数据的高速、稳定传输，是各子系统间信息交流的桥梁。（2）公务电话系统：为轨道交通内部人员提供便捷的通话服务，保障日常管理和应急通讯的畅通。（3）专用电话系统：针对轨道交通特定需求设计的通信系统，如行车调度电话、紧急救援电话等，确保行车指挥和应急响应的高效性。

（4）无线集群调度系统：为移动中的列车驾驶员、维修人员等提供无线通信服务，实现即时调度和指令传达。（5）闭路电视监控系统：对车站、列车及沿线关键区域进行全天候监控，保障行车安全和乘客秩序。（6）广播系统：用于车站、列车内的乘客信息播报、紧急通知等，是乘客服务的重要组成部分。（7）时钟系统：为整个轨道交通系统提供统一的时间标准，确保列车运行和乘客服务的准点性。（8）旅客引导显示系统：通过电子显示屏等方式，为乘客提供列车到站、发车时间等实时信息，引导乘客有序乘车。（9）防雷系统：保护信息系统免受雷电等自然灾害的破坏，确保系统的稳定运行。（10）光纤在线监测系统：实时监测光纤线路的状态，及时发现并处理潜在故障，保障信息传输的可靠性。（11）动力环境监测系统：对轨道交通系统的电力、环境等关键参数进行监测，确保系统的正常供电和运行环境。（12）UPS不间断电源系统：为关键信息系统提供持续稳定的电力供应，确保在停电等紧急情况下系统的正常运行。

2.2 系统功能

这些子系统在轨道交通运营中发挥着不可或缺的作用。（1）传输系统、公务电话系统和专用电话系统共同构建了轨道交通的通信网络，为行车指挥、日常管理和应急响应提供了有力的支持。（2）闭路电视监控系统和广播系统则通过实时监控和信息播报，保障了行车安全和乘客服务的及时性。（3）旅客引导显示系统和时钟系统则通过提供实时信息，提升了乘客的出行体验。（4）防雷系统、光纤在线监测系统和动力环境监测系统则通过保障系统的安全性和稳定性，为轨道交通的长期运营提供了坚实的基础。

3 信息安全风险识别方法

信息安全风险识别是确保组织信息系统安全的关键步骤，它涉及对潜在威胁、脆弱性、影响及可能性的系统性分析与评估[2]。有效的风险识别不仅能够帮助组织预防安全事件的发生，还能在事件发生后迅速响应，减少损失。

3.1 基于证据的方法

基于证据的风险识别方法侧重于利用历史数据和现有证据来预测未来的风险趋势。这种方法的核心在于数据的收集与分析，通过量化分析来揭示潜在的安全隐患。（1）检查表法：通过预先设计的检查表，对信息系统的各个组件、流程进行逐一审查，对照已知的安全标准和最佳实践，识别出不符合项或潜在风险点。这种方法简单易行，适合作为初步筛查工具。（2）历史数据审查：通过分析过去发生的安全事件、漏洞报告、审计结果等历史数据，识别出常见的攻击模式、漏洞类型及其发展趋势。这有助于预测未来可能遭遇的风险，并据此制定预防措施。基于证据的方法的优势在于其客观性和可重复性，但也可能受限于数据的完整性和时效性。因此，持续的数据收集与更新是保持其有效性的关键。

3.2 系统性的团队方法

系统性的团队方法强调团队合作与系统化流程在风险识别中的重要性。这种方法通过组建跨职能的专家团队，利用集体智慧和多样化的视角来全面识别风险。（1）专家评审：邀请信息安全领域的专家，通过研讨会、工作坊等形式，对信息系统进行深入分析，利用他们的专业知识和经验来识别潜在风险。（2）结构化提示与问题：设计一套结构化的提示或问题列表，引导团队成员从不同维度（如技术、管理、法律等）思考风险点。这种方法有助于确保风险识别的全面性和深度。系统性的团队方法能够弥补个人认知的局限性，提高风险识别的准确性和完整性。然而，它要求团队成员之间有良好的沟通与协作，以及较高的专业素养。

3.3 归纳推理技术

归纳推理技术如危险与可操作性分析方法（HAZOP），通过系统地分析系统的功能、操作条件及其可能的偏差，来识别潜在风险及其后果。HAZOP分析：该方法特别适用于复杂系统的风险识别，通过引导团队成员对系统的每个功能单元进行“如果……会怎样？”的提问，识别出操作过程中的偏差及其潜在后果。HAZOP不仅关注直接风险，还考虑到了风险之间的相互作用和连锁反应。归纳推理技术的优势在于其能够深入挖掘潜在风险，特别是那些不易被直接观察到的风险。但这种方法对分析者的要求较高，需要他们具备深厚的专业知识和分析能力。

3.4 其他支持性技术

除了上述方法外，还有一些支持性技术，如（1）头脑风暴法：通过自由讨论和思维碰撞，激发团队成员的创造力，鼓励提出尽可能多的风险点。这种方法能够打破常规思维，发现一些常规方法难以识别的风险。（2）德尔菲法：通过多轮匿名问卷调查，收集并整合专家意见，逐步逼近共识。德尔菲法适用于处理复杂、模糊或争议较大的风险问题，能够确保风险识别的客观性和科学性。这些支持性技术各有特色，可以根据具体情况灵活选用，以弥补其他方法的不足，提升风险识别的效果。

4 信息安全风险识别过程

信息安全风险识别过程是组织保障其信息系统安

全、防范潜在威胁与损害的关键环节。这一过程涉及从风险源的初步识别到风险事件的具体分析，再到风险评估的量化处理，并最终提出风险处理建议，形成一个完整的闭环管理体系。

4.1 风险源识别

风险源识别是信息安全风险管理的第一步，旨在确定可能导致信息安全风险的各类因素。这些因素大致可以分为（1）人为因素：包括内部员工的疏忽、恶意行为（如内部欺诈）、以及外部攻击者的入侵尝试。人为因素往往难以完全预测和控制，但通过建立严格的访问控制、安全培训和合规性检查，可以有效降低其风险。（2）技术因素：涉及信息系统本身的漏洞、过时或配置不当的安全策略、以及第三方软件和服务的安全隐患。技术因素的风险识别需要定期进行系统审计、漏洞扫描和更新管理，确保系统的安全性和稳定性。（3）管理因素：涵盖组织在信息安全政策、流程、监控和响应机制等方面的不足[3]。有效的风险管理需要建立全面的信息安全管理体系，包括明确的责任分工、定期的审计和审查、以及应急响应计划的制定。风险源识别的过程应尽可能全面和深入，确保不遗漏任何可能导致风险的因素。这通常需要通过跨部门协作、专家咨询和数据分析来实现。

4.2 风险事件识别

在识别了风险源之后，下一步是分析这些风险源可能导致的事故或事件。风险事件识别需要明确风险事件的发生条件、演变过程及潜在后果。（1）发生条件：指触发风险事件的具体情境或条件，如特定的攻击手段、系统漏洞的利用方式等。（2）演变过程：描述风险事件从触发到造成实际损害的过程，包括攻击者可能采取的行动步骤、系统可能的响应方式等。（3）潜在后果：评估风险事件对组织可能造成的财务损失、声誉损害、数据泄露等后果。风险事件识别的关键在于对风险源的深入理解和对潜在威胁的敏锐洞察。这通常需要对信息系统进行详细的安全分析，包括威胁建模、场景构建和攻击模拟等。

4.3 风险评估

风险评估是对识别出的风险进行量化评估的过程，旨在确定风险的严重程度和发生概率，为后续的风险处理提供依据。（1）严重程度：评估风险事件对组织可能造成的直接和间接损失，包括财务、声誉、法律和运营等方面的影响。（2）发生概率：基于历史数据、行业趋势和专家判断，估计风险事件发生的可能性。风险评估通常使用定性和定量相结合的方法，如风险矩阵、风险评分卡等。这些方法能够帮助组织直观地了解风险的大小和优先级，从而制定更有效的风险管理策略。

4.4 风险处理建议

根据风险评估的结果，组织需要提出针对性的风险处理建议，以减轻或消除风险。这些建议通常包括以下几种策略：（1）风险规避：通过避免高风险行为或活动来消除风险。例如，不使用易受攻击的软件、不存储敏感数据等。（2）风险降低：通过实施安全措施来降低风险的严重程度或发生概率。如加强访问控制、定期更新系统补丁、进行安全培训等。（3）风险转移：通过购买保险、签订服务级别协议（SLA）等方式，将风险的部分或全部责任转移给第三方。（4）风险接受：在评估了风险和收益之后，决定不采取额外措施来减轻风险。这通常适用于那些风险较小或成本效益比不高的情况。风险处理建议的制定应基于组织的实际情况和风险偏好，确保措施的有效性和可行性。同时组织应定期审查和更新风险管理策略，以适应不断变化的安全环境和业务需求。

结语

城市轨道交通信息系统的信息安全风险识别是一个复杂而重要的过程。通过对信息安全风险的深入分析和识别，我们可以采取有效的措施进行防范和应对，确保轨道交通的安全、高效运营。未来，随着技术的不断发展和应用，我们还需要不断探索和创新信息安全风险识别的方法和手段，为轨道交通的信息安全防护提供更加全面、有效的支持。

参考文献

[1]王德文,葛健,费瑞东等.城市轨道交通信号系统的信息安全[J].运输经理世界,2022,(13):139-141.

[2]陈燕.城市轨道交通信号系统信息安全方案研究[J].自动化应用,2021,(07):62-63+66.

[3]杨瑾,张亚.城市轨道交通运营安全风险管理研究[J].科技与创新,2023,(08):133-135.