地铁列车信号控制系统中的数据安全性分析

宋彤　张雨菲　高钰轩
河北省轨道交通集团有限公司

摘　要：随着城市轨道交通的快速发展，地铁列车信号控制系统在保障列车运行安全、提高运输效率方面发挥着越来越重要的作用。然而，由于涉及大量数据的传输和处理，数据安全性问题不容忽视。本文将从地铁列车信号控制系统的概述、安全隐患、数据安全性影响因素、分析方法以及保护措施等方面，对地铁列车信号控制系统中的数据安全性进行分析。

关键词：地铁列车；信号控制系统；数据安全性分析
【DOI】10.12252/j.issn.2096-6261.2022.09.066

引言

地铁列车信号控制系统是保障地铁列车安全运行的重要系统，其数据安全性直接关系到乘客乘坐地铁的安全和顺利。在当前信息化时代，地铁列车信号控制系统也面临着越来越严峻的数据安全挑战，如数据泄漏、黑客攻击、操作失误等问题。因此，对地铁列车信号控制系统的数据安全性进行全面分析和保护是非常必要的。

一、地铁列车信号控制系统概述

（一）地铁列车信号控制系统构成与功能

地铁列车信号控制系统主要由列车控制中心、轨道信号设备、车载信号设备和通信网络等组成。列车控制中心负责监控和控制列车运行，轨道信号设备用于识别轨道上的列车位置和调整信号，车载信号设备用于控制列车的运行速度和方向，通信网络用于传输控制信息和保障系统的正常运行。

（二）地铁列车信号控制系统数据传输方式

地铁列车信号控制系统的数据传输方式主要有有线传输和无线传输两种。有线传输主要采用电缆和光纤，具有传输速率高、抗干扰能力强等优点；无线传输主要采用无线通信技术，如Wi-Fi、蓝牙、无线电波等，具有安装简便、维护成本低等优点[1]。

二、地铁列车信号控制系统中存在的数据安全隐患

（一）数据泄漏和篡改风险

地铁列车信号控制系统中存储了大量的列车运行数据、信号控制信息等，一旦这些数据被未经授权的人员获取，就有可能导致列车运行的混乱或者恶意操作。同时，如果数据被篡改，比如修改列车的运行计划或者信号控制信息，也会对列车的正常运行造成严重影响。

（二）黑客攻击和病毒入侵威胁

随着信息技术的发展，黑客攻击和病毒入侵成了数据安全的主要威胁之一。地铁列车信号控制系统如果受到黑客攻击或病毒入侵，可能导致系统瘫痪、数据被篡改、列车失控等严重后果，极大威胁了列车的运行安全。

（三）数据备份和存储问题

数据备份是保障数据安全的重要手段，然而地铁列车信号控制系统中的数据备份和存储问题常常被忽视。如果系统没有及时进行数据备份，并且存储不安全，一旦系统出现故障或者数据丢失，将无法及时恢复数据，从而影响地铁列车的正常运行。

（四）人为错误和操作失误可能引发的数据安全问题

人为因素是导致数据安全问题的主要原因之一。地铁列车信号控制系统中的操作人员如果疏忽大意、操作失误，可能导致系统发生故障、数据泄漏、列车运行出现意外等问题，因此需要加强对操作人员的培训和监管，确保数据安全。

三、数据安全性影响因素分析

（一）软硬件故障：包括病毒、恶意攻击等

地铁列车信号控制系统的软硬件故障是影响数据安全性的重要因素。病毒和恶意攻击会导致系统运行异常，数据丢失或被篡改。此外，系统硬件故障也可能导致数据传输中断，影响系统的正常运行。

（二）人为因素：误操作、数据泄漏等

误操作、数据泄漏等人为因素也是造成数据安全性问题的重要原因。操作人员的不当操作或泄漏数据可能导致系统数据的丢失或泄漏。

（三）环境因素：电磁干扰、自然灾害等

环境因素如电磁干扰、自然灾害等也可能影响地铁列车信号控制系统的数据安全性。电磁干扰可能导致系统通讯中断或故障，自然灾害则可能导致设备损坏。因此，加强系统的防护设施建设，定期进行设备巡检维护，以应对各种环境因素带来的威胁是非常重要的[2]。

四、数据安全性分析方法

（一）数据加密技术

1、数据加密是保证数据的安全性，提高系统安全，防止非法操作，保护设备和信息。在对通信进行处理时必须采用严格的密钥，为了确保保密性、可靠性、

可扩展等要求而采取各种措施以避免这些技术风险发生概率增加或减少损失。另外还可以利用数字签名来实现加密功能并使其具有一定程度上抵抗攻击能力；最后还要通过数据验证系统加密算法，保证数据安全，提高系统整体安全性和稳定性。

2、数据加密技术是一种比较常见的信号传输安全手段，它通过对输入密码和输出信息进行处理，以达到保护系统的目的。由于地铁列车自身重量较大、结构复杂等原因，在实际应用中需要将列车与外界相连接起来使用到一定程度上的密匙来实现密钥共享功能。为了保证保密性要求我们可以采取加密技术，一是利用计算机程序控制数据传输过程；二是通过对网络资源和存储空间进行管理，以达到保护系统安全目的。

（二）防火墙和网络安全措施

防火墙主要是针对列车的安全，因此，其作用非常重要。首先在地铁车站设置一个专门用来防止黑客攻击的网络防护网；其次就是为了保证系统数据安全性而建立起相应保护措施以达到保护人员及设备不受非法窃取目的。再者就是对防火墙进行定期维护并及时修复漏洞、提高系统运行效率以及保障列车正常安全运作等一系列防范举措来确保整个信息系统能够稳定可靠地工作和运转，从而为乘客提供舒适便利环境。

（三）安全审计和监控机制

在地铁列车的数据管理系统中，安全审计是一个非常重要并且必要的部分。它能够及时发现系统存在着缺陷和隐患，因此，我们必须要采取一定措施来进行监控并对其作出相应处理。对于不需要监测到系统漏洞时可以直接采用人工方式去修复；通过在软件上修改一些不合理或不符合规定要求后再重新安装新硬件；定期检查各个参数值是否符合标准要求等情况的发生[3]。

（四）漏洞管理和及时更新策略

对于列车数据安全的保障，最重要的是要及时更新系统，因为这不仅需要考虑到不同系统之间的协调性和兼容性。因此在对该问题进行改善时应从以下几方面入手，将所有车站信息都纳入一个统一数据库中并建立专门用于维护列车运行信号控制策略、设备管理及运行状态监控等功能模块；另外还应该在数据采集过程上增加监控点与列车间隔器，以便于及时发现故障隐患，从而采取有效的措施来解决这一难题。

五、地铁列车信号控制系统数据安全性保护措施

（一）提升硬件设备安全性：使用抗干扰、防病毒硬件

硬件设备的安全防范措施，在日常工作中，要加强对系统关键器件和元部件的管理，防止由于各种原因造成故障。同时还要注意一些防病毒软件、杀毒软件等软硬件设备是否受到外部干扰以及内部人员操作不规范导致出现问题。预防性抗干扰技术，在进行计算机控制系统设计时必须充分考虑到外界环境因素可能带来的影响。例如，采用屏蔽措施或者安装保护层来加强系统中电子元件和元器件之间的安全距离，防止系统遭到外力损坏而造成故障。

（二）强化软件安全性：实施多层次安全防护，定期更新软件

1、针对列车的数据管理系统，我们可以采用多层次安全防护软件，对每一个子系统都进行有效地管理。在系统运行过程中可能会出现故障或者是异常情况，所以必须要有一套完善的信息监控机制来应对这些突发事件和问题。对于一些比较重要、容易被忽视掉重发点以及比较难发现问题的地方也应该及时地加以解决；最后还需要加强网络化信息系统（包括数据管理系统），使其能够实现与现有设备之间无缝对接，从而保证系统运行时安全稳定。

2、目前，地铁列车的数据管理系统，主要是针对车站、区间进行管理。因此要加强对软件系统的安全防护，在日常检修中经常需要使用到各种计算机网络设备和通讯设施等相关硬件设备来完成信息传输工作。同时还可以通过安装一些先进软件技术手段实现这些功能，例如利用各种通信协议与数据库技术将车站内各站点连接起来以达到相互连接交换站之间数据资源的目的，并且能够保证各个站点都能正常运行，从而提高地铁列车安全管理水平[4]。

（三）建立严格的数据管理制度：确保数据传输、存储的安全性

1、数据管理制度是保证数据安全的一个重要手段，对地铁列车系统而言，它不仅仅要做到信息传输、存储方面有据可依。同时还要做到信息保护，在进行信息系统操作前必须先制定出详细的规章和规范文件要求来约束工作人员行为准则及程序。然后再由专门人员去监督执行情况并记录好这些规则和文档等相关资料，以防止出现漏洞而导致数据丢失或泄漏给用户带来不必要损失，从而保证地铁列车系统能够安全稳定运行下去，并且为企业赢得更多利润空间。

2、数据管理制度是保证信息安全的重要基础，在系统中也同样如此，如果没有严格的数据保护措施和操作流程不规范的话就会造成严重后果。因此要加强对列车管理系统软件、硬件设备等各方面工作内容进行监督检查。首先需要建立一套完善且健全地管理机制，来确保地铁列车运行信号控制系统能正常高效运行。其次就是制定相关规章制度并加以实施，能够有效地防止这些问题发生以及解决系统中所存在的各种漏洞，从而保证

数据安全得到保障和实现。

3、数据管理是地铁列车系统中的重要组成部分，它直接关系着整个车站系统的运行状况。为了保证数据传输、存储和使用过程中各个环节都要严格按照规章制度进行。在日常工作当中经常需要对设备进行维护与保养以确保其安全性，所以必须建立严密地安全监控措施来防止故障问题发生并及时处理突发事件。其次就是加强对信息管理部门工作人员专业技能水平及计算机操作能力的培养，使他们能够熟练掌握各种软件技术以及相关知识等方面内容。

（四）定期对系统进行漏洞扫描和修复

地铁列车的管理系统中，数据安全是非常重要的，所以对系统进行定期不定期地漏洞扫描和修复就显得尤为必要。通过周期性检测、检查、维修等方式来预防故障发生。定期对车站内部设备设施进行扫描，首先在列车运行时需要把监控室安装好并放置好相关设备，然后将相关配置资料上传至调度中心后由调度中心统一管理维护人员。最后再根据地铁列车管理系统的要求，安排专门技术人员负责检修和维护工作，从而保证数据安全性。

（五）定期进行数据备份和灾难恢复演练

1、数据的备份和灾难恢复是一个系统中不可或缺的部分，它在整个系统中是至关重要。由于地铁列车大多数都是通过轨道上移动设备进行运行，所以如果要保证数据安全、完整就必须对其每次出现过或者因为故障而引起信息丢失或损坏。因此应该加强相关人员业务培训工作，并定期组织演练以防范意外事件发生所导致风险事故的发生，同时也需要建立一个应急预案和灾难恢复机制来防止突发事件造成的损失[5]。

2、数据备份是一个系统的关键部分，它可以保障整个系统安全。定期进行数据备份和灾难恢复演练主要包括两个方面，一是对计算机硬件设备、网络通讯介质以及软件等重要信息进行集中管理；二是在突发事件发生时及时应对各种异常情况下，通过对这些重要信息的收集与分析制定出合理有效地维护策略并实施保护措施以确保数据安全性。

3、数据的备份和灾难恢复是一个系统不可缺少且必不可少得环节，所以要在工程中，特别重视数据安全。首先我们应建立起完善的应急预案，当发生突发事件时应该立即采取措施应对；其次就是对重要文件资料进行必要地保护、定期检查以及及时清理文档档案等工作来防止不必要损失出现。最后还应当有计划性和针对性地为紧急事件提供解决方案并做好演练准备以确保数据的安全性与可靠性，使其能够发挥应有作用。

（六）访问控制与身份验证技术

1、在实际的应用中，数据访问控制与身份验证是两者之间非常重要的一个环节。它主要针对的是列车和用户，而对于安全策略来讲。它就是为了确保乘客、车站、地铁站以及相关工作人员都能够遵守相应规定和要求进行操作从而保证整个系统运行时安全性。同时还可以通过对设备状态信息来实现监控并保护铁路轨道上所存储着的信息不被泄漏或者丢失，以避免发生意外事故造成不可估量的损失。

2、在数据的采集和处理过程中，如果有一个设备出现故障，那么就会影响到列车信号控制。所以要对这些系统进行访问控制，身份验证，在程序设计时为了防止非法用户使用合法、安全的软件操作来获取信息，同时保证数据库内存储着一些必要信息等重要内容。最后再利用加密或密钥算法把数据与机密文件分离以保护其安全性和完整性，从而提高系统运行效率及可靠性，使之成为一个完整的体系。

3、在数据管理过程中，为了防止一些不正当操作，保证数据的安全性，需要对列车进行访问控制。首先是对系统数据库内信息的安全防护，通过设置用户名、密码等方式将系统登录权限限制住；其次就是要加强身份验证机制和密钥识别技术。对于普通用户来说使用加密算法时可以采用认证和授权两种形式来确保其身份完全暴露出来并保护好数据在输入端得到有效地存储，从而实现了数据管理的安全性[1]。

结语

地铁列车信号控制系统数据安全问题关系到地铁列车的正常运行和乘客的生命安全，必须引起高度重视。通过分析地铁列车信号控制系统中存在的数据安全隐患，以及影响数据安全性的各种因素，提出相应的数据安全性保护措施，有助于提高地铁列车信号控制系统的数据安全性，保障地铁列正常运行和乘客的安全。

参考文献

[1]左大军.地铁供电系统的可靠性和安全性分析方法研究[J].冶金管理，2023（17）：82-84.

[2]刘孟栋.城市轨道交通综合监控系统的数据安全分析[J].网络安全技术与应用，2023.

[3]孟维佳.地铁信号系统中的智能信号功能分析[J].工程与管理科学，2022，4（9）：44-46.

[4]熊坤鹏，陈硕豪，欧阳敏，等.用于轨道交通列车自动控制系统的自动化测试系统及方法.CN202110048669.8[2024-03-23].

[5]冯宏东.一种地铁信号与屏蔽门的联动控制系统[J].2022（20）.

作者简介：宋彤（1996-04）男，汉族，本科学历，初级职称，信号技工，籍贯河北省涿州市；研究方向：电子工程。