探讨轨道交通信号的可靠性和安全性

许 珂
徐州地铁运营有限公司 江苏 徐州 221000

摘 要：随着轨道交通快速发展，信号系统作为行车安全与效率的核心保障，其可靠性与安全性愈发关键。本文以轨道交通信号系统的可靠性和安全性为研究核心，界定了信号系统基本构成与可靠性、安全性内涵，再从硬件、软件、人为操作三方面分析可靠性影响因素，进而提出硬件冗余设计、软件优化验证、智能化运维等提升可靠性的技术措施，同时识别行车安全、设备故障、外部干扰三类安全风险点，并构建信号联锁安全设计、网络安全防护、应急故障恢复的防护体系。研究表明，通过技术与管理协同发力，可有效提升信号系统可靠性与安全性，为轨道交通运营安全提供支撑。

关键词：轨道交通信号；可靠性措施；安全性；防护体系

引言：当前轨道交通运营环境复杂，信号系统易受硬件老化、软件漏洞、外部干扰等因素影响，引发故障甚至安全事故，威胁乘客生命与财产安全。徐州地铁运营过程中，亦需持续优化信号系统性能以应对运营挑战。基于此，本文围绕轨道交通信号系统的核心概念、可靠性影响因素、提升措施、安全风险及防护体系展开研究，旨在为轨道交通信号系统安全稳定运行提供理论与实践参考。

1 轨道交通信号系统的概念与功能定位

1.1 信号系统的基本构成

轨道交通信号系统是保障列车安全高效运行的核心技术体系，主要由车载设备、地面设备与传输网络三部分构成。（1）车载设备负责监测列车运行状态、接收并执行信号，是实现列车自主控制的关键；（2）地面设备包含信号机、道岔转辙机、轨道电路及联锁设备，实时采集轨道占用、道岔位置等信息，生成符合行车规则的控制指令；（3）传输网络作为数据交互“神经中枢”，依托高可靠性通信技术，实现车载与地面设备、各地面设备间实时数据传输，保障控制指令与状态信息精准高效传递。

1.2 可靠性与安全性的定义及内涵

按行业标准，轨道交通信号系统的可靠性，指系统在规定时间、条件下完成规定功能的能力，核心体现为运行稳定性与连续性，需通过低故障发生率、快速故障恢复能力等指标衡量；安全性指系统避免因自身故障或外部干扰引发行车事故的能力，遵循“故障导向安全”原则，即故障时系统必导向安全状态，而非危及安全的不确定状态。二者关联且各有侧重：可靠性是安全性的基础，唯有系统稳定运行，才能规避故障引发的安全风险；安全性是可靠性的核心目标，系统可靠性设计需以保障行车安全为首要前提，共同构成信号系统运行保障的核心维度[1]。

2 轨道交通信号可靠性的影响因素分析

2.1 硬件设备可靠性影响因素

硬件设备是信号系统运行的物理基础，其可靠性决定系统整体稳定度：（1）元器件质量，核心元器件的材质标准、生产工艺精度及出厂质检严格度，直接影响设备抗损耗能力与使用寿命；（2）老化损耗，设备持续使用中，电子元件参数漂移、机械部件磨损等老化现象，会逐步降低性能稳定性；（3）环境适应性，运营环境中的温度波动、湿度变化、粉尘侵蚀及振动冲击，会加剧设备故障概率，缺乏针对性防护设计易引发非预期停机。

2.2 软件系统可靠性影响因素

软件系统稳定性关乎指令传输与执行：（1）程序漏洞，软件开发中需求分析不全面、代码编写不规范或测试覆盖不足，易遗留逻辑缺陷，复杂工况下可能触发程序异常；（2）兼容性问题，系统需与多类设备协同，软件版本不匹配、接口协议不统一，易导致数据交互中断或指令误解读；（3）升级维护风险，软件升级时参数配置偏差、补丁兼容性问题，或维护操作失误，可能造成软件功能失效。

2.3 人为操作与管理对可靠性的影响

人为因素贯穿系统运行全周期：（1）操作规范，工作人员未严格遵循标准化流程，在设备调试、参数设置或应急操作中出现偏差，易引发系统异常；（2）人员素质，工作人员对设备原理、系统逻辑的掌握程度及应急处置能力，影响问题发现与解决的及时性；（3）维护流程，日常维护计划不科学、巡检频次不足或故障排查流

程不清晰，易导致潜在问题累积，增加故障风险。

3 提升轨道交通信号可靠性的技术措施

3.1 硬件冗余设计与容错技术

硬件层面通过冗余配置与容错机制降低单点故障影响，具体措施包括：（1）采用多类型硬件冗余架构，对联锁机、列车自动监控系统服务器等核心设备部署双机热备模式，确保主设备故障时备用设备毫秒级切换且不中断运行；对关键传感器、信号传输接口采用三取二表决冗余设计，通过多设备数据比对排除单点误差或故障导致的错误信号。（2）引入硬件故障自诊断技术，在核心硬件内集成专用诊断模块，实时监测元器件电压、电流、温度等参数及设备状态，参数异常时自动触发诊断程序，定位故障部件与类型并生成报告，同时通过故障隔离功能防止故障扩散。（3）强化硬件环境适应性设计，对设备进行抗振动、抗冲击处理，采用加固外壳与内部缓冲结构；电路中加入防雷击、抗电磁干扰模块，通过接地保护与电磁屏蔽涂层降低干扰；选用宽温域元器件，确保设备在-40℃至70℃稳定运行。

3.2 软件优化与验证技术

软件系统通过开发优化与全流程验证减少漏洞，提升可靠性，具体措施包括：（1）推行模块化软件开发模式，按功能划分列车自动防护、自动运行、数据传输等独立模块，采用标准化接口设计，降低模块耦合度；建立模块版本管理机制，全程记录开发、修改、升级过程，确保迭代可追溯、可回滚。（2）实施多阶段软件验证流程，开发初期通过需求评审、模型仿真验证需求与功能目标一致；开发中开展单元测试验证代码逻辑，集成测试检测模块接口兼容性；开发完成后进行系统级测试，模拟复杂运营场景验证极端工况下的稳定性。（3）建立软件漏洞动态修复机制，定期用专业工具结合人工审计扫描漏洞；对漏洞分级修复，高危漏洞24小时内完成补丁开发与测试，中低危漏洞按周期修复；修复后开展回归测试，确保不影响原有功能且无新兼容性问题。

3.3 智能化运维技术的应用

借助智能化技术优化运维流程，实现精准管控与提前预警，具体措施包括：（1）构建设备状态实时监测网络，在硬件设备部署物联网传感器，采集运行参数、能耗与环境数据，通过5G或工业以太网传输至运维平台；平台用实时数据处理技术清洗整合数据，生成状态曲线与报表，供运维人员实时查看并发现异常。（2）引入预测性维护技术，基于历史运行与故障数据构建设备寿命预测模型，通过机器学习分析参数变化与故障关联性，预测剩余寿命与风险等级；据此制定差异化维护计划，高风险设备提前维护，低风险设备延长周期；维护时用数字化工具记录过程，形成维护档案。（3）搭建大数据分析运维平台，整合长期运行的设备状态、故障与维护数据，通过大数据分析识别故障高发时段与部件，分析共性原因；基于结果优化运维资源配置，调整人员驻点、储备备品备件；结合运营计划预判高峰时段系统负载，提前调整参数提升应对能力[2]。

4 轨道交通信号安全性的关键风险点识别

4.1 行车安全相关风险

行车安全相关风险是信号系统安全核心威胁，聚焦信号指令与逻辑控制层面：信号误发指系统因内部异常输出错误行车指令，打破正常行车秩序；联锁失效是信号与道岔、轨道电路间逻辑关联中断，无法实现“道岔未到位则信号不开放”等安全约束，导致设备状态与信号指令不匹配；列车冲突风险是前两类风险的直接后果，错误信号或失效联锁可能使列车进入同一轨道区间或未按安全距离行驶，引发碰撞事故，危害人员与设备安全。

4.2 设备故障引发的安全隐患

设备故障易通过系统关联效应扩大风险，形成连锁隐患：单点故障扩散指核心设备（如联锁机、传输模块）故障后，因缺乏有效隔离机制，故障信号或异常状态向其他设备传导，导致局部故障演变为多设备协同失效；系统瘫痪风险是故障扩散的极端结果，关键设备集群故障或核心功能模块失效时，信号系统无法生成、传输或执行控制指令，行车指挥停滞，既影响运营效率，又因失去安全管控能力埋下多重隐患。

4.3 外部环境对信号安全性的干扰

外部环境通过物理或技术手段干扰系统运行：电磁干扰来自周边工业设备、通信设施的电磁辐射，可能导致信号传输链路数据丢包、误码，影响指令传递准确性；自然灾害直接损坏地面信号设备与传输线路，破坏系统硬件基础；恶意攻击是人为技术入侵，如非法访问控制系统、植入恶意代码，可能篡改信号数据或控制逻辑，引发系统性安全风险[3]。

5 保障轨道交通信号安全性的防护体系构建

5.1 信号联锁系统的安全设计

信号联锁系统作为保障行车安全的核心逻辑层，需通过严谨设计强化安全约束，具体措施包括：（1）强化逻辑校验机制，在联锁软件设计中嵌入多重安全校验逻辑，对列车进路请求、道岔位置状态、轨道占用情况等关键信息进行交叉验证，确保只有当所有安全条件满足（如道岔精准到位、轨道无占用）时，才允许开放信号；同时，设置逻辑冗余校验，对同一指令的生成与传输过程

进行多次数据比对，避免单一逻辑模块故障导致的错误联锁结果。（2）严格遵循故障导向安全原则，在联锁系统硬件与软件设计中预设故障安全响应模式，当检测到设备故障、数据异常或逻辑冲突时，系统自动触发安全保护动作，如强制关闭相关信号机、锁定道岔位置、切断危险进路等，确保故障状态下系统始终处于不危及行车安全的稳定状态，而非不确定的风险状态。（3）优化联锁数据存储与备份策略，采用双机热备存储架构存储联锁关键数据（如进路参数、设备状态记录），确保主存储设备故障时，备用存储可实时接管数据读写；同时，定期对联锁数据进行异地备份，备份频率不低于每日一次，且备份数据需经过完整性校验，防止因数据丢失或损坏影响联锁系统正常运行。

5.2 Cybersecurity防护技术

针对信号系统面临的网络安全威胁，需构建多层级防护技术体系，具体措施包括：（1）部署数据加密防护机制，对信号系统内部数据传输（如车载与地面设备间的控制指令、设备状态数据）采用国密算法进行端到端加密，确保数据在传输过程中不被窃取或篡改；对系统核心数据库（如联锁逻辑数据库、运维管理数据库）采用存储加密技术，设置访问权限密码与加密密钥，且密钥需定期更换，防止未授权访问获取敏感数据。（2）建立严格的访问控制体系，采用“最小权限原则”划分信号系统用户权限，将用户分为运维人员、管理人员、系统管理员等不同角色，每个角色仅授予完成本职工作必需的操作权限；同时，引入多因素认证机制，用户登录系统时需同时验证账号密码与动态验证码（如短信验证码、Ukey认证），防止账号被盗用引发的非法操作。（3）构建入侵检测与防御系统，在信号系统网络边界部署工业防火墙，过滤非授权网络访问请求，阻断异常数据流量；在系统内部部署入侵检测设备，实时监测网络数据包与系统操作行为，当发现疑似攻击行为（如多次失败登录、异常数据篡改请求）时，自动触发告警机制，并记录攻击源信息、攻击时间与攻击行为，同时对攻击流量进行拦截，防止攻击扩散至核心控制模块。

5.3 应急处置与故障恢复机制

为快速应对信号系统故障，降低安全风险，需建立完善的应急与恢复机制，具体措施包括：（1）制定标准化快速响应流程，明确信号系统各类故障（如信号机故障、联锁失效、网络中断）的应急处置责任人、响应时限与操作步骤，确保故障发生后10分钟内启动应急处置；同时，建立故障上报机制，现场运维人员需在故障发现后5分钟内将故障类型、故障位置、影响范围上报至应急指挥中心，便于指挥中心统筹调度资源。（2）设计多级别备用模式切换方案，根据故障严重程度设置不同备用模式，如单点设备故障时切换至设备级备用模式（启用备用设备），局部系统故障时切换至区域级备用模式（启用备用控制区域），全局系统故障时切换至降级备用模式（如采用人工调度指挥行车）；每个备用模式均需提前预设切换条件与操作流程，且定期开展备用模式切换演练，确保切换过程快速、顺畅，不引发新的安全风险。（3）建立故障恢复与复盘机制，故障处置完成后，运维人员需在24小时内完成故障恢复验证，通过系统测试、数据比对等方式确认信号系统功能恢复正常，且无遗留安全隐患；在故障恢复后3个工作日内开展故障复盘，分析故障原因、处置过程中的问题与改进方向，形成复盘报告并更新应急处置流程，避免同类故障重复发生[4]。

结束语：本文系统梳理了轨道交通信号系统的可靠性与安全性相关问题，明确了影响可靠性的关键因素，提出了针对性技术措施，且构建了全面的安全防护体系，形成了一套覆盖“概念-影响-措施-风险-防护”的研究框架。研究成果可直接为徐州地铁及同类轨道交通运营企业提供借鉴，助力提升信号系统运行质量。

参考文献：

[1]邹定锋.探讨轨道交通信号的可靠性和安全性[J].低碳世界,2021,11(9):209-210.

[2]魏业恒.城市轨道交通信号系统安全性与可靠性分析[J].人民公交,2025(10):90-92.

[3]赵倩.轨道交通信号系统可靠性与安全性探讨[J].中文科技期刊数据库(全文版)工程技术,2021(10):473-474.

[4]江泽欣,谭雄富,商晖.探讨轨道交通信号的可靠性和安全性[J].科学与信息化,2025(16):169-171.