铁路信号电路设计安全性研究与分析

丁向涛
通号工程局集团有限公司　北京　100070

摘　要：铁路信号电路是保障列车运行安全的核心，设计安全性关乎铁路运输效率与人员安全。本文分析了其组成、分类和功能特点，从硬件故障、软件漏洞、人为操作失误三方面剖析设计隐患，提出基于定性、定量和综合评估方法的安全性评价体系，并针对关键风险点给出硬件冗余、软件安全编码、强化人员培训、优化安全管理制度等改进措施。结果表明，多维度防护可降故障率、提可靠性。

关键词：铁路信号电路；设计安全性；故障分析；安全防护

1 铁路信号电路概述

1.1 铁路信号系统的组成与功能

铁路信号系统是确保列车按计划有序运行的“指挥系统”，主要由信号设备、联锁设备、列控设备及传输设备四部分组成。信号设备包括信号机、轨道电路、道岔转辙机，负责向列车司机传递线路状态信息（如停车、减速、通行）；联锁设备通过逻辑控制实现进路、道岔、信号机的协同动作，防止敌对进路同时开通；列控设备（如CTCS-3级列控系统）根据线路条件、列车位置动态调整行车速度，保障高密度、高速度运行场景下的安全；传输设备依托光纤、电缆构建数据传输网络，实现各子系统间的信息交互。从功能来看，信号系统核心是通过“指令生成-信息传输-执行反馈”的闭环流程，实现列车运行的安全防护、效率提升与调度管理，而信号电路作为各设备的“连接纽带”，是功能落地的关键载体，其稳定性直接影响整个信号系统的运行效果。

1.2 铁路信号电路的分类与特点

铁路信号电路根据功能可分为轨道电路、道岔控制电路、信号机控制电路及联锁电路四类。轨道电路沿钢轨敷设，通过发送与接收电磁信号检测列车占用状态，具有“无间断监测”特点，能实时反馈轨道空闲/占用信息，但易受钢轨锈蚀、电磁干扰影响；道岔控制电路负责道岔定/反位转换与锁闭，包含动作电路与监督电路，需满足“快速转换、可靠锁闭”要求，其设计需考虑道岔转换时间、缺口监测等关键参数，防止转换不到位引发脱轨风险；信号机控制电路驱动信号机灯光切换（如红灯、绿灯、黄灯），并通过灯丝监督电路监测灯泡状态，具备“故障导向安全”特性，即灯泡故障时自动切换至红灯或灭灯，避免误导列车；联锁电路是信号系统的“逻辑核心”，通过继电器或电子元件实现进路与信号机、道岔的联锁关系，具有“逻辑严谨性”特点，需严格规避时序冲突与逻辑漏洞。整体而言，铁路信号电路普遍遵循“故障-安全”原则，即故障时需导向安全状态（如信号关闭、道岔锁闭），同时需具备抗电磁干扰、适应复杂环境的能力[1]。

2 铁路信号电路设计中的安全隐患分析

2.1 硬件方面的安全隐患

硬件故障是铁路信号电路安全事故的主要风险源。常见问题包括元件老化，长期使用后电子元件性能衰减，影响信号传输稳定性；接触不良，连接点松动或氧化导致电流传输不畅；设计缺陷，从初始就埋下隐患。以继电器触点为例，频繁通断易产生电弧烧蚀，使接触电阻增大，引发信号误显示，威胁列车运行安全。电源模块若无过压保护装置，雷击或电网波动时强大电流冲击会损坏电路板。部分老旧线路的机械式道岔转换设备，机械部件长期磨损后动作不可靠。这些硬件隐患源于选型不当、降额设计不足及维护周期过长。

2.2 软件方面的安全隐患

铁路信号电路设计中，软件缺陷如“定时炸弹”，可能导致联锁逻辑错误或系统崩溃。典型问题有代码漏洞，特定条件下使软件系统异常；实时性不足，延误列车运行调度；配置错误，导致软件无法按预期运行。曾有线路因软件未二次校验道岔位置冲突，致两列车同入一区间，险酿大祸。还有通信协议栈存在缓冲区溢出漏洞，攻击者可篡改信号指令。软件隐患成因包括开发流程不规范，未形式化验证难保正确性；测试覆盖不全，难发现潜在问题；版本管理混乱，更新维护困难。

2.3 人为因素导致的安全隐患

人为操作失误是铁路信号电路事故重要诱因，贯穿设计、施工、运维三阶段。设计阶段，工程师经验不足，可能未考虑极端工况影响，如低温致电缆脆化埋下隐患。施工阶段，工人误接线路、未按规范接地，可能

引发短路故障。运维阶段，维护人员未定期巡检，难及时发现问题；误操作设备，如未确认道岔状态开放信号，会致列车运行方向错误[2]。

3 铁路信号电路设计安全性的评估方法

3.1 定性评估方法

定性评估方法围绕“风险识别与逻辑验证”展开，借助经验判断和规范对照来评估电路设计的安全性，尤其适合在设计初期进行隐患筛查。常见的方法有故障类型与影响分析（FMEA）、危险与可操作性分析（HAZOP）以及规范符合性检查。FMEA通过梳理电路中各个元件、模块可能出现的潜在故障类型，像继电器粘连、电缆断线等情况，分析这些故障对电路功能产生的影响程度，进而确定风险的优先级。例如在评估轨道电路时，要分析“发送器故障”对列车占用检测功能的影响，并标注出高风险的项目。HAZOP则是组建一个包含设计、运维、安全等多专业人员的团队，采用“引导词+参数”的形式，例如“信号延迟-传输时间”，来识别电路设计中存在的偏差和隐患，以此确保逻辑的严谨性。在一条高铁信号电路的评估中，通过HAZOP就发现了“道岔缺口监测电路未设置冗余”这一隐患。规范符合性检查是对照TB/T、IEC等相关标准，如IEC61508功能安全标准，核查电路设计是否满足安全要求，像元件安全等级、防护措施等方面。这种方法操作简便、成本较低，但比较依赖评估人员的经验，主观性相对较强。

3.2 定量评估方法

定量评估方法借助“数据建模与指标计算”来量化电路设计的安全性，以客观数据为评估结论提供支撑，适用于设计后期的性能验证。常用的方法有故障树分析（FTA）、事件树分析（ETA）以及可靠性指标计算。FTA把“信号电路故障”作为顶事件，自上而下地分解导致故障的底层原因，如元件失效、设计缺陷等，通过计算最小割集和故障概率，确定关键的风险点。例如在评估信号机控制电路时，可通过FTA计算“信号机误亮绿灯”的概率，如果该概率超过10^{-9}/小时（安全阈值），就需要对设计进行优化。ETA以“初始事件”，比如电缆断线为起点，分析事件发展的不同路径以及可能产生的后果，计算安全后果和危险后果发生的概率。在一条轨道电路的评估中，通过ETA分析“钢轨锈蚀”事件，得出“列车误判空闲”的概率为5×10^{-8}/小时。可靠性指标计算是通过统计平均无故障时间（MTBF）、故障恢复时间（MTTR）来评估电路的稳定性，像道岔控制电路的MTBF需要达到10^{4}小时以上，才能满足设计要求。定量评估需要依赖大量的故障数据和仿真工具，虽然结果准确性较高，但计算复杂度也相对较高。

3.3 综合评估方法

综合评估方法融合了定性与定量评估的优势，通过“多维度融合”的方式对信号电路设计的安全性进行全面评估，适用于复杂的信号系统，例如高铁CTCS-3级列控系统电路。常用的方法有层次分析法（AHP）和模糊综合评价法。AHP通过构建“目标层（电路安全性）-准则层（硬件、软件、人为因素）-指标层（元件可靠性、逻辑严谨性等）”的层次结构，确定各个指标的权重，再结合定性分析结果，如FMEA的风险等级，以及定量数据，如MTBF值，计算综合安全评分。在一条铁路信号电路的评估中，通过AHP得出硬件可靠性权重为0.45、软件逻辑权重为0.35、人为因素权重为0.2，综合评分为82分（满分100分），判定该电路处于“较安全”等级。模糊综合评价法针对电路安全评估中存在的“模糊性”问题，例如“电磁干扰影响程度”，通过建立模糊集合与隶属函数，将定性描述转化为定量数据，再结合权重计算综合评价结果[3]。综合评估方法能够兼顾主观性与客观性、定性与定量，评估结果较为全面，但需要投入更多的时间和资源，对评估人员的专业能力要求也比较高。

4 提高铁路信号电路设计安全性的措施

4.1 硬件安全防护

硬件安全防护需从元件选型、电路拓扑、环境适应三个维度入手，构建“可靠-冗余-防护”的硬件体系。元件选型方面，优先选用符合安全标准的元件（如SIL4等级继电器、耐高低温电容），并开展元件寿命测试与环境适应性验证；例如高寒地区信号电路选用工作温度-40℃~+70℃的电阻，确保低温下性能稳定。电路拓扑设计方面，关键电路采用冗余设计（如“二取二”“三取二”表决逻辑），核心设备（如信号机、道岔转辙机）采用双电源供电，信号传输采用双通道备份，避免单点故障影响全局；如轨道电路发送与接收端均设置双模块，模块故障时自动切换。环境适应防护方面，针对电磁干扰，在电路中加装防雷模块、电磁屏蔽层，电缆采用铠装屏蔽电缆并规范接地；针对高低温、潮湿环境，对元件进行密封处理，在设备箱内加装加热/除湿装置；针对物理损坏，电缆敷设时穿镀锌钢管防护，设备箱采用防鼠设计，减少外部环境对硬件的影响。

4.2 软件安全防护

软件安全防护需围绕“逻辑严谨-容错可靠-测试充分”构建防护体系，保障电子联锁、列控系统等软件驱动的电路安全。逻辑设计方面，采用模块化编程，明确各模块功能边界，避免逻辑耦合；关键逻辑（如联锁关

系、故障导向安全）采用“双重校验”，如进路开通前需同时满足“道岔位置正确”“轨道空闲”两个条件，缺一不可。容错设计方面，植入故障自诊断算法，实时监测软件运行状态（如数据传输完整性、模块响应时间），发现异常时自动启动备用模块或导向安全状态；例如软件检测到“信号机状态反馈丢失”时，立即输出“关闭信号”指令。测试验证方面，开展全场景测试（正常工况、故障工况、极端工况），采用静态测试（代码审查）与动态测试（仿真运行）结合的方式，覆盖所有逻辑分支；例如针对道岔控制软件，需模拟“道岔转换超时”“缺口超限”等20余种故障场景，验证软件容错能力。此外，软件需定期更新迭代，修复已知漏洞，保障长期运行安全[4]。

4.3 人为因素控制

人为因素控制需通过“培训-规范-监督”的闭环管理，减少设计、调试、维护阶段的人为失误。培训方面，建立分层培训体系：对设计人员开展规范培训（如TB/T标准、“故障-安全”原则）与现场调研培训，确保设计方案贴合实际；对调试人员开展操作技能培训（如仪器使用、故障模拟测试）与安全意识培训；对维护人员开展定期复训，更新技术知识（如新型信号电路维护方法）。规范方面，制定全流程操作规范：设计阶段明确“三级审核”制度（设计人自审、专业审核、总工审定），确保设计方案无漏洞；调试阶段制定标准化测试流程，明确测试项目、仪器精度要求与故障处理流程；维护阶段出台定期检修计划，明确检修周期、内容与参数标准（如继电器触点电阻需 ≤ 0.1Ω）。监督方面，建立质量监督机制，引入第三方机构对设计、调试过程进行抽查，对违规操作进行追责；同时，在电路设计中增加“防误操作”设计（如关键参数锁定、操作权限分级），从技术层面减少人为失误。

4.4 安全管理制度建设

安全管理制度是保障信号电路设计安全性的“长效保障”，需构建“责任-流程-考核”的管理体系。责任体系建设方面，明确各参与方（设计单位、施工单位、运维单位）的安全责任，设计单位对设计方案安全性负责，施工单位对施工质量负责，运维单位对运行维护负责，建立责任追溯机制，出现安全问题时可精准追责。流程制度建设方面，制定信号电路设计全生命周期管理制度，涵盖设计立项、方案评审、施工调试、验收交付、运维更新各环节；例如设计方案需通过安全评审（邀请行业专家参与），验收交付需完成全场景测试并出具安全评估报告。考核与改进制度方面，建立安全考核指标（如电路故障次数、MTBF值），定期对设计、运维单位进行考核，考核结果与项目合作挂钩；同时，建立故障数据库，收集信号电路故障案例，分析故障原因并形成改进措施，反馈至设计环节，实现“故障-分析-改进-优化”的持续改进闭环，不断提升信号电路设计安全性。

结束语

铁路信号电路设计安全性是铁路运输安全的基石，需从硬件、软件、人为及管理四方面构建全方位防护体系。通过冗余设计、安全编码、标准化作业及制度保障，可显著降低系统故障率，提升应对突发事件的能力。未来，随着物联网、人工智能等技术的融入，铁路信号电路将向智能化、自适应方向发展，进一步增强安全冗余与动态防护能力。持续优化设计方法与评估体系，是保障铁路运输安全、推动行业高质量发展的关键所在。

参考文献

[1]冯旭.铁路信号设备电路原理仿真教学系统设计及应用研究[J].中国新通信,2022,24(04):38-40.

[2]刘春平.铁路信号室内通用电路测试系统设计[J].铁道建筑技术，2021，(09):72-74+151.

[3]严金鹏.基于物联网的铁路信号设备智能检测与故障诊断系统设计[J].装备制造技术,2024,(02):132-134.

[4]安卓.铁路信号系统安全保障策略研究[J].工程建设与设计，2024，(03)：214-216.