Research on Safety Protection and Risk Control of Expressway Electromechanical Monitoring System

Jinhui Ye

Xinjiang Communications Planning, Survey, Design and Research Institute Co., Ltd., Urumqi, Xinjiang, 830006, China

Abstract

As the core component of its (Intelligent Transportation System), expressway electromechanical monitoring system forms a collaborative chain of perception transmission calculation decision in vehicle detection, toll processing, communication exchange, energy consumption control, video monitoring and disaster warning, which is the basic support for expressway operation safety, efficiency and service ability. However, the electromechanical system shows the characteristics of high coupling, high vulnerability and chain fault propagation in the long-term operation process, which is affected not only by the physical environment, but also by network attack, hardware failure and human operation risk. According to the results of this study, for the composite architecture of "electromechanical+communication+cloud platform", the establishment of active security governance system can effectively reduce the system failure rate compared with traditional passive protection, significantly improve the timeliness of anomaly identification and the ability of operation and maintenance closed-loop, which is of great significance to improve the toughness of smart high-speed system.

Keywords

expressway; electromechanical monitoring system; network security; operation and maintenance risk

高速公路机电监控系统的安全防护与风险控制研究

冶金辉

新疆交通规划勘察设计研究院有限公司，中国·新疆 乌鲁木齐 830006

摘　要

高速公路机电监控系统作为ITS（Intelligent Transportation System）核心组成，在车辆检测、收费处理、通信交换、能耗控制、视频监控与灾害预警方面形成感知—传输—计算—决策的协同链条，是高速公路运营安全、效率与服务能力的基础性支撑。然而机电系统在长期运行过程中呈现出高耦合、高脆弱性与链式故障传播特征，既受物理环境作用，也受网络攻击、硬件失效与人为操作风险影响。本研究结果针对"机电+通信+云平台"的复合架构，建立主动式安全治理体系较传统被动式防护可有效降低系统失效率，显著提升异常识别及时性与运维闭环能力，对提升智慧高速系统的韧性具有重要意义。

关键词

高速公路；机电监控系统；网络安全；运维风险

1 引言

高速公路机电监控系统通过对交通状态、设施运行与环境要素的实时监测，实现信息感知、数据传输、综合分析与指令下达的全过程闭环，是智慧高速与现代交通治理体系的重要基础。然而系统规模的持续扩张与功能模块的不断耦合，使其由单一控制单元演变为多节点、多网段、多协议并发的复杂集群。在此过程中，传统基于设备稳定性的"点式控制"已不足以应对系统全生命周期的安全需求，特别是在视频识别、收费清算与能源管控等核心业务深度依赖数据与算法的背景下，数字攻击能够直接突破物理边界，诱发跨子系统级联故障。因此，构建以主动预警、动态隔离和智能诊断为核心的系统化安全防护框架，是高速公路机电运维从"监控管理"迈向"韧性治理"的必然趋势。

【作者简介】冶金辉（1984–），男，中国新疆人，本科，高级工程师，从事智慧交通、机电工程、交通信息化、地质灾害监测研究。

2 高速公路机电监控系统的总体特征与安全挑战

2.1 系统功能构成与技术架构

高速公路机电监控系统以现场感知、通信网络、中心平台和执行单元构成层次化结构，其中交通检测器、摄像机、气象站、隧道照明、车道控制器、收费控制终端、UPS、电力系统形成底层机电载体[1]。通过工业以太网、光纤 SDH、MPLS 和 LTE/5G 等通信链路构成数据高速通道，由监控中心子系统完成信号聚合、数据计算与业务调度。系

统功能逻辑体现从“物理采集—协议封装—数据转发—策略执行”的全过程闭环，涉及视频编码、边缘计算、车牌识别算法、收费交易与权限认证模块，其横向依赖设施物理稳定性，纵向依赖链路连续性与平台可靠性。由于系统结构呈现高度耦合性，任何节点失效都可能引发多级联动，使局部故障转化为全链条中断。

2.2 运行环境对机电系统安全的影响

高速公路环境具有高温差、粉尘、潮湿、高盐雾和强电磁干扰等典型特征，尤其在山区隧道、跨海大桥等场景中机电设备长期暴露于结构振动、凝露腐蚀与电压不稳环境，易导致传感器漂移、连接器氧化、通信接口失真，进而造成数据异常与功能降级。在寒区结冰工况下，通风、照明和消防子系统的响应延迟会扩大交通事件影响范围；在高湿条件下，摄像监控与车牌识别精度下降导致事故识别延迟，诱发运维反馈链条上“误报—漏报—误判”的累积效应。近年来高速公路机电系统从“单点功能控制”向“互联互通感知体系”演化，通过边缘节点—云平台协同形成多源数据处理架构 [2-3]。随着高清视频 AI 分析、收费系统电子交易、远程维护与 OTA 升级成为常态，机电系统安全威胁由线下设备故障向线上攻击延伸，呈现典型的“物理－网络复合型风险”。例如非法注入可伪造车道状态或收费数据，弱密码权限可导致视频资源泄露，平台漏洞可使控制策略遭受篡改，从而对隧道能耗控制与交通诱导形成直接安全影响。

3 机电监控系统的安全威胁分析与风险传播机制

3.1 物理层设备故障与环境侵蚀风险

物理层是机电系统最基础的风险载体，设备老化、供电不稳、接触不良、线缆破损与雷击感应均可能导致数据丢失与设备瘫痪。机电设备生命周期普遍经历“初始稳定—性能衰减—失效突发”的曲线特征，其中传感器功能退化表现为输出噪声增大和漂移长期积累，在系统端被误认为异常事件触发，造成错误调度策略。二次供电系统稳定性是典型风险源，当隧道 UPS 失效或电能质量突变时，照明、监控与风机将同时失效，使交通管制呈现不可控状态，形成灾害性后果。IP 化架构使机电系统风险超越传统物理失效，网络攻击成为影响系统稳定性的关键因子。分布式拒绝服务（DDoS）、ARP 欺骗、端口扫描、恶意流量注入与工控协议漏洞利用均可导致链路阻塞与功能锁死。若边缘节点未隔离核心网络，攻击者可通过漏洞横向移动扩散至视频存储、收费交易与指挥调度模块，从“可视化失控”升级至“业务逻辑失控”。数据层面，伪造车牌和虚假交易行为在收费环节产生连锁财务损失，若无强一致性校验机制，将形成不可逆账务风险。

3.2 人员操作风险与风险链条传播

高速公路机电系统维护高度依赖运维人员，但现实中存在“岗位授权多、操作审计弱、人员变动频繁”的治理现象，导致人为风险成为不可忽视的变量。未经审批的远程登录、权限共享、绕过流程的系统调整与应急策略测试均可能引发安全事件 [4]。典型事故显示，软件参数错误与操作失误导致设备连续重启，使隧道交通监视中断超过 180 分钟，诱发事故扩大与管理成本外溢。机电系统风险并非孤立存在，呈现“局部扰动—信息失真—策略错误—级联失效”的链式传播路径。视频监控失真将导致交通识别偏差，诱发交通诱导策略错误，进而导致路段拥堵加剧，引发更多异常事件；网络丢包使风机控制响应滞后，使隧道 CO 浓度监测不准，引发二次报警和设备冗余启动，形成系统资源浪费与能耗暴增。风险传播从微观组件传导至宏观决策，其耦合性决定了安全防护需要建立多维度冗余与主动防御机制。

4 安全防护体系架构分层与深度防御策略

构建高韧性的机电安全防护体系应遵循“分层隔离—功能解耦—数据可信—最小权限”原则，通过物理层、网络层、业务层与决策层进行纵深防护。在物理层建立设备冗余与隔离电源以保证底层功能连续性；在网络层通过分区隔离、虚拟网段划分、白名单控制阻断横向渗透；在业务层依托数据校验与一致性控制保障收费和调度逻辑正确性；在决策层建立算法透明度与反馈闭环，防止策略误触发扩大损害区间 [5]。

深度防御强调多重屏障叠加，将攻击成本抬升至不可接受水平。网络隔离采用“核心—传输—接入—终端”策略，通过 SDN、VLAN 与双向网闸限制跨域访问；边缘节点采用可信执行环境（TEE）与硬件加密；敏感数据采用数字签名与哈希指纹保证不可篡改；身份体系采用硬件 Token+Ukey+ 动态口令多因子认证，避免系统管理员权限集中导致的单点失控。视频数据与收费数据需采用独立存储路径，确保即便视频平台被攻陷，也不会影响收费服务链条。隧道通风与照明控制属于安全关键业务，应采用独立控制链路与双控制器架构，确保主控失效时备控可在 100ms 内切换完成；收费系统采用核心清算区封闭架构，仅允许经 CA 认证的数据进入结算池；视频监控采用边缘智能筛选策略，将可疑事件以结构化数据而非原始视频回传中心，实现“数据降维”减少攻击面与带宽压力；应急广播采用多信道冗余传输避免网络故障引发广播失效。

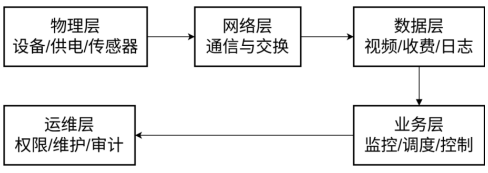


图 1 高速公路机电监控系统分层安全防护结构示意图

图 1 中的单向箭头并非简单数据流，而是体现不同层级之间的功能依赖与安全边界：物理层向网络层的箭头代表硬件状态与信息采集的单源输入，网络层向数据层的箭头体

现通信系统作为“数据承载与安全边界”的角色；数据层向业务层的垂直箭头表现算法与策略生成必须建立在可信数据基础之上；业务层向运维层的反向箭头则反映系统治理的回溯性与审计性——运维活动并不直接参与业务执行，而通过策略约束与权限控制作用于系统全链条，避免人为因素或配置错误造成事故扩大。该模型从结构上避免“数据—业务—运维”三者交叉污染，实现了工程管理所强调的职责分离、边界清晰与最小影响路径原则。

5 风险控制路径分析与系统优化路径

5.1 风险控制路径分析

风险控制的核心在于“提前感知—主动响应—动态校正”。在传感器侧构建多物理量融合框架，通过交通流指数、空气质量、能耗变化及设备振动指标联合构成状态向量，利用卡尔曼滤波与贝叶斯推断模型实现异常识别。边缘设备对视频帧、车牌序列及感测数据进行多任务学习，将事故、拥堵与设备失效转化为统一事件流，提升跨业务的风险推理能力。系统通过时序分析与滑动窗口技术匹配干扰峰值，实现“潜在故障—轻微异常—严重故障”的分级识别。基于历史故障库，采用 LSTM、GRU 与 Transformer 模型对机电设备状态进行时间序列建模，通过温度漂移、功耗变化及信号噪声指标预测失效节点。针对高能耗设备建立退化模型，输出剩余寿命估计（RUL），以提前调度维护资源；现场控制器采用灰度重启与自愈策略，当识别到软件崩溃或内存泄漏时主动解除异常，避免长时间人工介入。预测性维护通过缩短停机窗口，减少运营影响，在典型路段可减少 20% 的紧急抢修事件。风险控制应以闭环机制落实，从预警、响应、恢复到审计形成完整链条。系统自动触发分级指标：轻度异常仅生成日志；中度异常触发操作审核与远程调度；严重异常直接阻断调度策略并强制切换至安全模式。事件溯源依托链路追踪和设备指纹记录，形成“设备—操作—策略—结果”的全路径证明，防范责任追溯中的争议与合规风险。该机制在隧道连续失联案例中显示处理时长缩短 47%，显著提升应急响应效率。

5.2 工程案例分析与系统优化路径

某山区高速隧道机电系统因高湿度、复杂通风及回路老化，导致监控脱网与风机误启动事故频发。本研究采用二次供配电隔离、通信链路多路径与边缘节点冗余策略，将传输时延降低至 18ms，通风控制误触发率下降 60%，系统维护周期从 3 个月延长至 14 个月。该案例表明：物理结构优化与网络架构分层是基础安全内核，能够从源头上降低运营风险。城市环线高速收费系统曾遭受恶意流量攻击，导致车道拥堵与结算异常。实施 VLAN 隔离、中心清算区分区与动态权限分配后，攻击者无法横向渗透至核心账务链路；结合 CA 签名与数据比对，使交易伪造率下降至近零。案例表明：数据链条可信性构建应优先于平台功能扩展，尤其要保障“视频监控—收费—调度”三大核心业务之间的逻辑边界。

6 结论

高速公路机电监控系统是交通行业数字化基础设施的重要组成，其安全本质上是“机电物理系统—网络通信—算法控制—运维组织”多维耦合的复杂系统问题。针对高风险运行环境和高度互联架构，传统依赖硬件冗余的被动防护已无法满足需求，需要建立主动、动态、智慧的深度防御体系。研究表明，通过分层架构与最小权限策略实现攻击面缩减，辅以多源数据融合与智能诊断改善风险识别能力，并在事件闭环与溯源体系中推进运维能力成熟，对于提升系统韧性与持续运行能力具有显著优势。未来研究应进一步围绕机电系统数字孪生、车路协同与云计算融合展开，更加重视对模型可信性的管理与对算法黑箱的审计，以实现从“局部安全”迈向“系统安全”的治理目标。

参考文献

[1] 刘凤成.高速公路机电工程监控系统应用[J].交通世界,2018,(25):174-175.

[2] 庄国雄.高速公路机电监控系统的设计探讨[J].科技创新与应用,2018,8(26):89-90.

[3] 徐琼.对高速公路机电监控系统的设计的相关分析[J].建材与装饰,2018,14(44):245-246.

[4] 孙昊.基于ZigBee和4G移动网络的高速公路机电设备监控系统[J].中国交通信息化,2019,(7):101-108.

[5] 孙钦飞.谈高速公路机电监控系统组成、特点及隧道监控模式[J].中国新通信,2022,24(5):45-47.