电梯远程检测系统漏洞问题与安全加固对策分析

胡　镒
四川立方维特科技有限公司　四川成都　610000

摘　要：随着智能化和远程监控技术的广泛应用，电梯远程检测系统在提升运维效率和故障响应能力方面发挥了重要作用。该系统也暴露出通信协议不安全、权限管理混乱、数据加密薄弱以及更新机制滞后等多重安全隐患。文章系统分析了当前常见漏洞类型及其技术成因，针对性地提出加密链路优化、访问控制分级、补丁机制完善以及态势感知构建等加固对策。同时，从行业制度层面给出标准制定、协作联防、安全运维自动化等保障建议，旨在构建全面、安全、可持续的电梯远程检测安全体系。

关键词：电梯远程检测系统；通信加密；权限控制；漏洞分析

引言

电梯作为城市垂直交通的核心载体，其安全运行直接关系到公众生命财产安全。随着物联网和远程监测技术的快速发展，电梯远程检测系统已成为现代电梯维保的重要组成部分，助力企业实现故障预测与精准运维。然而，系统的开放性与网络连接属性也带来了严重的信息安全挑战。近年多起智能终端遭受攻击事件表明，若系统防护薄弱，可能导致电梯被远程干扰、数据被篡改，甚至发生安全事故。因此，研究电梯远程检测系统中的安全漏洞并提出有效加固策略，已成为提升行业整体安全水平的紧迫任务。本文围绕漏洞问题与加固方案展开深入分析，期望为行业提供可行的技术指导与制度支撑。

一、电梯远程检测系统常见漏洞问题分析

（一）通信协议存在安全缺陷

目前的电梯远程检测系统大多使用Modbus，CAN，MQTT三种通信协议进行通信，它们原生地缺少强制加密与认证的机制，易被攻击者用于实施中间人攻击，伪造命令注入或者重放攻击等。一旦通信数据遭到拦截或者篡改，就会造成监测数据失真的问题，甚至会造成系统远程失控的问题，极大地影响电梯运行的安全性[1]。同时一些设备采用私有协议而没有公开的安全标准造成了安全审计和评估的困难，增加了系统的风险。通信协议缺乏安全性既来自历史兼容性，也体现出物联网场景下对于协议加固的支持滞后。所以在城市复杂运行环境下，以安全通信协议为基础的电梯远程检测系统所面临的攻击面不断扩大的情况不容忽视。

（二）远程控制权限分配不当

电梯远程检测平台普遍面临权限粒度过粗和认证方式单一的问题。部分系统将运维、监控、调试等高权限功能集中分配给单一的账号或角色，而缺乏必要的角色隔离和行为约束机制。一旦突破高权限账户，攻击者就可以绕开安全策略对电梯控制逻辑进行远程介入，导致系统瘫痪或者引发安全事故。相当多的平台缺少多因素认证和实时审计的机制，不能有效地检测并屏蔽异常登录及越权操作。这类权限管理不到位的现象常常被人们所小觑，但它是电梯系统裸露于网络空间的直接隐患。所以权限分配机制不平衡急需用精细化访问控制与动态授权体系来弥补。

（三）数据采集与传输环节加密不足

数据采集和上传时，海量设备仍然以明文方式传输或者采用陈旧的加密算法进行加密，特别是传感器层和边缘计算节点间数据交互环节加密较弱或者缺失的情况屡见不鲜。这样电梯的运行状态，故障日志和实时视频等敏感信息就很容易被盗用，篡改或者侦听，既暴露了用户的隐私，也会被黑客用来构造攻击路径。部分设备部署时密钥管理能力不足，加密模块的禁用或者默认配置时间较长，安全威胁进一步放大[2]。数据传输过程中加密不充分已经成为黑灰产对电梯系统打击的一个重要突破点，需要系统架构设计者及安全管理者予以高度重视。

（四）系统软件更新与补丁机制滞后

电梯远程检测系统核心软件，固件以及其依赖组件等都有很多已知的漏洞，但是系统部署零散，设备访问复杂等原因使得补丁更新周期长，覆盖率不高，是攻击

者重复使用的对象。有些陈旧的设备连远程更新的能力都没有，只能够依靠人工在现场进行作业，严重落后于漏洞的响应节奏。一些厂家对软件版本控制和更新管理没有统一平台，更新过程不够透明，验证机制欠缺，有可能出现二次污染或者更新失败等问题。补丁机制落后既妨碍安全闭环建设，又影响系统的长期可维护性等问题，急需借助集中化和自动化的补丁推送平台来改善。

二、漏洞成因与技术分析

（一）嵌入式设备防护能力薄弱

电梯远程检测系统大量终端设备使用嵌入式硬件平台进行检测，一般都面临着处理能力有限和安全模块欠缺的情况，不能携带复杂加密运算或者接入控制逻辑。这类设备一般都是预装固定固件且更新机制不够完善，在部署完成之后几乎没有进行维护，这使其很容易成为破解黑客攻击问题的首选突破口。嵌入式系统开发主要集中在功能实现上，缺少系统化安全设计思路，易产生缓冲区溢出，默认口令和开放端口这些典型漏洞。这一底层防护缺口，使得整个远程检测系统面临网络攻击表现出“木桶短板”，是安全保障链条上最容易打通的环节。

（二）物联网平台安全策略缺失

很多电梯远程检测平台建设之初并没有建立起完整的物联网安全架构，没有统一身份认证体系，传输加密机制以及设备接入控制策略，致使该平台在设备识别，信道保护和数据隔离上都存在着明显的不足。有些平台甚至让未认证设备注册和数据上传构成了“裸接入”安全漏洞的问题。平台对于设备生命周期的管理不到位，无法动态感知和应对设备状态，漏洞风险等问题，为黑客的长期潜伏和控制提供空间。安全策略缺失实质上体现了平台建设重功能集成、轻系统安全设计的问题，需要补全安全能力模块来根治。

（三）第三方接口安全管控不足

电梯检测系统往往需要连接各种第三方服务平台，运维系统或者监管接口，有些接口设计时访问控制和数据校验不到位，有可能出现逻辑绕过，参数篡改和信息泄露的问题。有些界面采用静态认证机制或者暴露敏感路径使得攻击者可以很方便地伪造请求或者注入恶意数据。一些开放接口缺少调用频次限制和访问日志的记录，很难追溯和保护自动化攻击的发生[3]。接口安全问题通常来自开发阶段忽视安全和平台之间协同机制不强，这是系统连通性增强的同时也引入了一个“隐性漏洞”，需要在平台连接策略上重点加强管控能力建设。

（四）风险评估与安全测试机制缺位

大多数电梯远程检测系统上线之前缺少系统性的风险评估和专业化的安全测试，不能发现架构漏洞，配置缺陷以及可能的攻击路径。开发流程中普遍存在“重功能、轻安全”的现象，未建立代码审计、静态分析、安全基线核查等机制，导致产品上线即带漏洞。系统运行时缺少连续的漏洞扫描，渗透测试和安全加固等迭代机制不能适应动态攻击态势。这一机制性缺位，直接造成安全漏洞在系统中潜伏已久，不能及时发现和应对，成为威胁系统持续安全运行的主要原因。

三、电梯远程检测系统安全加固对策

（一）强化通信与控制链路加密机制

为了确保数据传输和控制时的完整性和保密性，需要综合部署强加密通信机制并建议使用TLS1.3协议实现链路的端到端的加密，并且将动态密钥协商，双向身份验证相结合，加强了安全性。特别是对关键控制指令必须引入报文签名和序列验证机制以防伪造指令和重放攻击。同时要淘汰明文通信和弱加密算法并定期对加密参数进行更新，以规避加密算法衰老所造成的危害。加密既要涵盖数据通道又要延伸到设备之间的通信，平台API调用以及其他各种交互环节以达到对系统通信进行全生命周期防护和增强整体抗攻击能力的目的。

（二）构建多级访问权限与审计体系

远程检测系统安全防线需要依靠精细化权限控制和可追溯操作审计体系来实现。要按照岗位职责进行操作权限划分，构建多级角色模型和最小权限原则对高敏操作的曝光范围进行约束。系统需要强行启用多因素认证与动态口令机制来防止账号的非法登录[4]。同时要建设综合的操作日志系统来记录每一次接入行为，对操作和异常事件进行控制，并且配置实时告警和追溯能力以方便对风险源头进行迅速定位。通过“人—机—操作”全链条监管机制可以有效防范内部滥用和外部渗透叠加风险。

（三）引入安全固件管理与远程补丁机制

加强终端设备固件生命周期安全管理是抑制已知漏洞不断被曝光的关键。系统要配置远程安全更新机制对固件，驱动和平台组件进行统一版本控制和差分升级。全部补丁首先要经过数字签名校验和沙箱测试以保证来源可信和兼容性好。固件更新要支持分批推送，断点续传和异常回滚等机制，以避免大范围更新失败导致的服务中断。同时要针对老旧设备制定安全兼容策略并划分

更新优先级和安全缓冲区以实现异构设备环境渐进式安全修复。

（四）建立系统级安全态势感知能力

为了实现电梯远程系统攻击面与安全状态的实时控制，要建设多维度，智能化安全态势感知体系。系统要综合运用网络流量监测，行为分析和日志聚合的方法来实时识别异常行为和潜在攻击信号。介绍了基于AI进行威胁建模和事件关联分析技术能够有效地提高告警准确率和响应速度。同时要构建风险等级评估模型对设备，平台和接入节点进行动态分级管理。态势感知平台应具有可视化展示，安全趋势预测以及自动化响应等功能，促使电梯检测系统朝着“主动防御”，“自适应修复等”的方向发展。

四、安全保障体系建设建议

（一）制定行业级远程检测系统安全标准

为解决电梯远程检测系统所面临的安全共性问题，在原监管机构的领导下，会同行业龙头企业和科研机构建立了统一安全技术标准，内容涉及通信规范，设备认证，数据加密，权限管理等关键环节。标准要体现可操作性和前瞻性，综合考虑技术发展和实地部署的需要，促进产业链上下游协同安全生态的形成[5]。要建立安全合规认证机制对系统开发商、运营方进行分级评估与认证，诱导市场优胜劣汰，从根本上增强全行业安全基线与风险抵抗力。

（二）构建多主体联防联控协作机制

电梯远程检测系统由制造商、平台商、运维单位和监管部门共同参与，仅依靠单一的力量很难形成有效的防护合力。要促进参与各方建立联防联控协同机制、搭建信息共享通道和应急响应联动流程、提高安全事件集体应对效率。同时鼓励在行业内建立安全联盟，共同进行漏洞通报、技术研讨和攻防演练，建立横向贯通和纵向协同全链条保护体系。通过机制化合作和资源整合可以有效地应对正在演变中的跨平台攻击危险。

（三）推进安全运维自动化与智能化

随着系统规模和复杂度的日益增加，常规人工运维已经很难同时满足实时性和精准性需求。应当加速推进安全自动化工具的部署，这包括但不限于漏洞扫描、配置基线核查、行为分析和合规检测等多个模块，以实现对安全事件的迅速识别、分类和响应。同时要引入机器学习和大数据分析技术实现运维数据趋势建模和异常溯源，建立自学习自适应智能运维体系。通过将自动化和智能化深度结合，既可以减少人力成本又可以提高安全防护精准性和系统恢复高效性。

（四）定期开展安全评估与红蓝对抗演练

为验证系统防护效果和及时发现可能存在的风险，要建立覆盖静态代码审查，配置项审计和攻击面分析的定期安全评估机制以保证系统一直处于可控风险之内。同时要组织红蓝对抗专业演习，在模拟攻击场景中验证安全策略有效性和运维团队应急响应能力。演练结果要形成闭环的改进意见，促进制度优化和技术加固同时进行。通过制度化演练机制可以达到“以攻促防”，持续增强系统对复杂威胁环境适应能力和抵御能力。

结束语

电梯远程检测系统在提高运行效率与维护水平方面具有显著优势，但其系统性安全风险不容忽视。通过本研究可见，当前系统普遍存在通信协议薄弱、权限配置不当、接口管控缺失等漏洞问题，其根源在于嵌入式防护不足与缺乏规范化安全设计。为此，必须从技术手段与制度建设双轮驱动入手，强化链路加密、权限管理与补丁更新能力，同时构建态势感知平台提升主动防御能力。在此基础上，结合行业标准制定、协同机制构建与智能运维推动，可形成电梯远程检测领域“技术—制度”并重的安全保障体系，实现系统长期稳定与可信运行的目标。

参考文献

[1]王英权，陈永强，周曹军.电梯安全性能影响因素及电梯检验探讨[J].中国科技期刊数据库 工业A，2023.

[2]李颖杰，谭杰.电力终端嵌入式组件信息源数据安全检测系统[J].信息技术，2023，47（2）：178-184.

[3]王启刚，蒋炜，彭世喆.物联网环境下多元共治的电梯安全监管体系研究[J].上海管理科学，2023，45（3）：43-48.

[4]胡范芝.基于物联网的电梯远程监控与故障诊断技术[J].2024（16）：40-42.

[5]李小珊.电梯物联网的应用领域与面临的挑战[J].中国电梯，2024，35（11）：83-85.