建筑智能化系统网络安全研究

陈佶思
厦门兆翔智能科技有限公司　福建　厦门　361000

摘　要：建筑智能化系统网络安全涉及楼宇自控、安防监控等子系统数据安全，随物联网、5G技术普及，系统互联性增强导致风险激增。本文从物理层防护、数据加密、权限管理三方面构建防御体系，分析架构漏洞、设备接入短板、传输风险及运维疏漏四大风险，提出架构优化、设备管控、传输加密、运维体系完善四大路径，为智慧建筑可持续发展提供安全保障。

关键词：建筑智能化系统；网络安全；防护优化

引言：随着物联网、5G技术的深度渗透，建筑智能化系统已广泛融入多个核心应用领域，成为智慧建筑高效运行的核心支撑。系统互联性的持续提升，使得网络安全边界不断模糊，非法设备接入、数据泄露、恶意攻击等风险频发，严重威胁建筑运行安全与用户隐私。强化网络安全防护、构建科学完善的动态防御体系，已成为推动建筑智能化行业健康、可持续发展的迫切需求。

1 建筑智能化系统网络安全概述

建筑智能化系统网络安全是保障现代建筑高效运行的核心环节，直接关系到各类智能设备协同运行、业务流程稳定开展与整体建筑的安全管控水平，是建筑数字化、智能化发展的关键前提，涉及楼宇自控、安防监控、能源管理等子系统的数据传输与设备控制安全。随着物联网、5G技术在建筑领域的深度应用，系统互联性增强导致网络安全风险呈指数级增长，需从技术防护、管理机制、人员意识三方面构建综合防御体系。（1）物理层防护：通过电磁屏蔽、专用网络隔离等措施阻断外部非法接入，确保设备接口、通信线路的物理安全，防止硬件被篡改或信号被窃取。（2）数据传输加密：采用国密算法对关键指令、用户身份信息进行端到端加密，避免数据在传输过程中被截获或篡改，保障指令执行的准确性与用户隐私安全。（3）权限动态管理：基于最小化原则分配系统访问权限，结合生物识别、多因素认证等技术实现身份精准核验，同时通过行为分析模型实时监测异常操作，及时阻断潜在攻击。当前，建筑智能化系统网络安全面临技术迭代快、攻击手段隐蔽等挑战，需持续优化防护策略。未来应聚焦自主研发核心安全芯片、构建智能威胁感知平台等方向，提升系统主动防御能力[1]。通过技术革新与管理创新双轮驱动，推动建筑智能化系统网络安全向更智能、更可靠的方向演进，为智慧建筑可持续发展提供坚实保障。

2 建筑智能化系统网络安全现存风险与隐患

2.1 系统架构层面的安全漏洞

建筑智能化系统架构层面的安全漏洞需从底层设计逻辑切入分析。系统硬件接口若缺乏统一安全认证机制，可能被非法设备接入导致数据篡改风险，例如传感器与控制终端的通信协议若未加密，攻击者可截获传输数据并注入恶意指令，破坏设备正常运行逻辑。（1）协议适配层漏洞：不同厂商设备采用私有协议时，若未实现标准化安全封装，易产生协议解析错误或缓冲区溢出风险，攻击者可利用此漏洞发起拒绝服务攻击或执行任意代码。（2）数据链路层缺陷：网络拓扑结构若采用扁平化设计，未划分安全域与隔离区，会导致横向渗透风险加剧，例如办公区与生产区网络直接互通，攻击者突破办公终端后可快速横向移动至核心控制设备。（3）系统组件耦合风险：模块间依赖关系若未实施最小权限原则，单一组件被攻破可能引发连锁反应，例如门禁系统与照明系统的联动接口若未做权限隔离，攻击者可从照明系统渗透至门禁控制模块。当前架构设计需强化纵深防御理念，通过分层防护与动态监测机制降低安全风险，同时需定期开展架构安全评估与渗透测试，确保安全措施与业务需求同步演进。

2.2 设备接入环节的安全短板

设备接入环节的安全短板需从设备身份验证、权限管控、传输安全三方面深入剖析。海量终端接入使设备准入安全面临更大挑战，若设备接入流程缺乏严格认证机制，非法设备可能通过伪造标识或绕过认证流程接入系统，埋下数据泄露与系统破坏隐患。（1）认证机制薄弱：部分设备采用静态密码或简单密钥进行身份验证，攻击者可利用暴力破解或中间人攻击获取合法凭证，进而冒充合法设备接入网络，实施数据窃取或恶意操作。（2）权限分配粗放：设备接入后若未实施动态权限管

理，可能长期持有过高访问权限，例如监控摄像头若被赋予修改系统配置的权限，攻击者可通过摄像头渗透至核心控制模块，破坏系统运行逻辑。（3）传输过程未加密：设备与系统间通信若采用明文传输，攻击者可截获传输数据并解析业务逻辑，甚至注入恶意指令篡改设备行为，导致系统功能异常或数据失真[2]。当前设备接入安全需构建动态防护体系，通过多因素认证、零信任架构、端到端加密等技术手段强化安全边界，同时结合行为分析引擎实时监测设备异常行为，实现风险早发现、早阻断。

2.3 数据传输过程的安全风险

数据传输过程的安全风险涉及协议安全性、加密强度及数据完整性等多个维度，若防护措施不到位，可能导致数据泄露、篡改或系统功能异常，需从底层逻辑到应用层面全面审视。（1）协议兼容性问题：不同设备或系统间若采用不兼容的传输协议，可能引发数据解析错误或安全机制失效，例如部分老旧设备仅支持基础协议，无法适配现代加密标准，导致传输链路存在明文暴露风险。（2）密钥管理缺陷：密钥生成、存储或轮换机制若不完善，易被攻击者利用进行密钥破解或中间人攻击；长期静态密钥或简单轮换策略可能降低加密有效性，增加数据被截获或篡改的概率。（3）流量监测不足：传输链路若缺乏实时流量监测与异常行为分析，可能无法及时发现并阻断恶意流量，例如重放攻击或数据注入行为可能因监测盲区而持续影响系统运行，造成决策偏差或功能失效。为提升传输安全性，需构建动态防护机制，通过协议标准化改造、密钥全生命周期管理、智能流量分析等技术手段强化安全边界，同时结合行为基线学习实现异常流量精准识别，确保数据传输全流程安全可控且风险可追溯。

2.4 运维管理中的安全疏漏

建筑智能化系统网络安全运维管理中，安全疏漏常源于多环节衔接不紧密与细节把控不足，例如权限分配若缺乏动态调整机制，易导致权限滥用风险。（1）权限管理粗放：部分系统采用通用账户或长期不更新的权限设置，非授权人员可能通过共享账户访问敏感区域，造成数据泄露隐患。（2）日志监控薄弱：运维日志未定期检查或缺乏自动化分析工具，难以追踪异常操作和潜在攻击，安全事件溯源效率低下。（3）应急响应滞后：缺乏定期演练或预案更新，面对突发安全事件时响应流程混乱，故障恢复时间延长，影响系统稳定性。运维团队需强化日常巡检与权限审计，定期评估系统访问权限的合理性，及时回收离职人员或岗位变动人员的访问权限。同时，应引入智能日志分析系统，通过机器学习识别异常行为模式，提升威胁检测能力。此外，建立分级应急响应机制，针对不同等级的安全事件制定差异化处置流程，并通过模拟演练验证预案有效性[3]。安全运维需贯穿系统全生命周期，通过技术手段与管理措施双管齐下，构建动态防御体系，有效抵御潜在网络威胁。

3 建筑智能化系统网络安全防护优化路径

3.1 完善系统架构安全设计

建筑智能化系统网络安全防护需从架构设计层面强化本质安全，通过系统性优化构建可信赖的智能环境基础。在物理层，需对传感器、控制器等终端设备实施严格准入控制，采用国密算法加密通信链路，防止非法设备接入或数据截获。网络层应采用微分段技术划分安全域，结合零信任架构动态验证设备与用户身份，避免横向渗透风险。（1）分层防御机制：通过物理隔离、网络分段、系统权限分级等措施构建多层次安全屏障，降低单点故障风险，例如在核心业务区部署工业防火墙，在管理区实施访问控制列表，形成纵深防护体系。（2）动态安全评估：定期进行渗透测试和漏洞扫描，结合威胁情报实时更新防护策略，提升系统自适应能力；通过模拟攻击验证防御有效性，及时修复安全漏洞，确保防护措施与威胁态势同步进化。（3）冗余与容错设计：关键节点采用双活或热备架构，确保在硬件故障或网络攻击时业务连续性不受影响，例如数据中心采用分布式存储与负载均衡技术，避免单点失效导致服务中断。优化系统架构安全设计需兼顾前瞻性与实用性，通过技术迭代与持续改进，实现从被动防御向主动免疫的转变，为建筑智能化系统提供坚实的安全底座。

3.2 强化设备接入安全管控

建筑智能化系统网络安全防护需以设备接入安全管控为核心抓手，通过多维度技术手段构建安全屏障。（1）严格身份认证机制：采用多因素认证方式对设备接入进行验证，如物理标识、数字证书与生物特征结合，确保仅授权设备可接入网络，杜绝非法设备渗透风险。（2）动态访问控制策略：基于设备类型、接入时间、网络位置等属性，实施差异化访问权限管理，例如对关键设备设置最小化权限范围，对临时接入设备采取“一次一密”临时授权模式，降低权限滥用可能性。（3）实时安全状态监测：通过部署智能监测节点，对设备接入后的运行状态、流量特征、异常行为进行持续监控，结合AI算法实现异常行为自动识别与预警，及时阻断潜在安全威胁。设备接入安全管控需贯穿全生命周期管理，从设备入网前的安全检测、入网中的实时防护到入网后的

持续监控，形成闭环管理机制。同时，需注重技术手段与管理措施协同，通过定期安全评估、人员培训、应急演练等措施，提升整体安全防护能力[4]。该路径的实施可有效降低设备接入环节的安全风险，为建筑智能化系统稳定运行提供坚实保障，推动网络安全防护从被动防御向主动预防转变。

3.3 优化数据传输安全机制

建筑智能化系统数据传输安全机制需聚焦传输链路的安全加固，筑牢传输安全防线，防范网络窃密与数据篡改风险，通过技术手段与流程优化双重保障数据传输的保密性、完整性与可用性。（1）传输加密算法升级：采用国密算法或国际主流高强度加密算法对传输数据进行端到端加密，结合动态密钥交换技术，确保数据在传输过程中无法被窃取或篡改，提升传输通道的抗攻击能力。（2）传输协议安全强化：对现有传输协议进行安全改造，增加身份验证、数据完整性校验、重放攻击防护等功能模块，避免传输过程中数据被截获、伪造或篡改，保障数据传输的可靠性。（3）传输链路实时监控：部署智能监控系统对传输链路进行实时状态监测，包括流量异常、传输延迟、数据包丢失等情况，结合自动预警机制，及时发现并阻断异常传输行为，确保传输链路稳定运行。数据传输安全机制的优化需结合系统实际运行环境与业务需求，持续迭代升级安全策略与技术手段。通过构建多层次、多维度的安全防护体系，可有效提升建筑智能化系统在数据传输环节的安全防护水平，为系统整体网络安全提供有力支撑，助力智能化系统在安全环境下高效运行。

3.4 健全运维安全管理体系

建筑智能化系统网络安全防护需以运维安全管理体系为核心，强化日常运维管控，筑牢系统安全防护底线，构建动态防御机制。运维安全管理体系的健全需从流程、人员、技术三方面协同推进，形成闭环管理生态。（1）规范运维流程：建立标准化操作规范，涵盖设备巡检、漏洞修复、日志审计等环节；通过流程固化减少人为失误，确保每项操作可追溯、可验证，提升运维效率与安全性。（2）强化人员管理：实施分级权限控制，依据岗位职责分配系统访问权限；定期开展安全技能培训与应急演练，提升运维团队对网络攻击的识别与处置能力，培养安全意识与责任意识。（3）完善技术支撑：部署实时监控系统，对网络流量、设备状态进行全维度监测；结合人工智能算法分析异常行为，提前预警潜在威胁，实现从被动响应向主动防御的转变。运维安全管理体系需持续迭代优化，适应不断变化的网络威胁环境。通过定期评估体系有效性，结合行业最佳实践与技术发展趋势，动态调整管理策略与技术手段，确保体系始终处于最佳防御状态[5]。此路径不仅能提升建筑智能化系统的网络安全防护水平，还可为其他领域智能化系统提供可复制的运维安全管理经验，推动整体网络安全能力的提升。

结束语：建筑智能化系统网络安全需技术革新与管理创新双轮驱动。未来应聚焦核心安全芯片自主研发、智能威胁感知平台构建，提升主动防御能力。通过分层防御机制、动态安全评估、冗余容错设计优化架构，强化设备身份认证与实时监测，升级传输加密算法与协议安全，健全运维流程规范与技术支撑，推动系统向更智能、更可靠方向演进，支撑智慧建筑可持续发展。

参考文献

[1]方东.基于网络通信技术的建筑智能化系统研究[J].通讯世界,2024,31(6):169-171.

[2]郑庆林,郑庆贵.人工智能技术在建筑智能化安全监控系统中的应用研究[J].移动信息,2025,47(7):410-412.

[3]翟继斌.建筑智能化工程安全防范系统研究[J].移动信息,2024,46(11):376-378.

[4]王钊.建筑智能化系统在工程中的应用研究[J].科学技术创新,2025(1):198-201.

[5]苑玉霞.网络通信技术下弱电智能化建筑系统分析[J].信息记录材料,2024,25(1):100-102.