建筑智能化系统网络安全体系分析

张金宇
江苏大美天第文化产业有限公司，江苏 南京 210000

DOI: 10.61369/ME.2024090013

摘　　要： 随着建筑智能化系统的快速发展和广泛应用，网络安全问题日益突出。本文从建筑智能化系统的特点出发，分析了其面临的网络安全威胁，探讨了建立建筑智能化系统网络安全体系的必要性。在此基础上，从技术、管理、法律法规三个方面提出了构建建筑智能化系统网络安全体系的策略，以期为保障建筑智能化系统的安全运行提供参考。

关 键 词： 建筑智能化系统；网络安全；安全体系；安全策略

Analysis of Network Security System of Intelligent Building System

Zhang Jinyu
Jiangsu Damei Tiandi Cultural Industry Co., LTD., Nanjing, Jiangsu 210000

Abstract： With the rapid development and widespread application of intelligent building systems, cybersecurity challenges have become increasingly prominent. This paper analyzes the characteristics of intelligent building systems and examines the cybersecurity threats they face, highlighting the necessity of establishing a cybersecurity framework for these systems. Building on this foundation, it proposes strategies to construct a cybersecurity system for intelligent building systems from three perspectives: technology, management, and legal regulations. These strategies aim to provide practical references for ensuring the secure operation of intelligent building systems.

Keywords： **intelligent building systems; cybersecurity; security framework; security strategies**

引言

建筑智能化系统是以建筑物为平台，兼备通信、办公自动化、建筑设备监控、信息管理等多种功能，集成多种智能化子系统，实现建筑物的智能化管理和服务。但是由于建筑智能化系统具有开放性、集成性、网络化等特点，使其面临着诸多网络安全威胁。因此，构建完善的建筑智能化系统网络安全体系势在必行。

一、建筑智能化系统面临的网络安全威胁

（一）数据泄露与窃取

建筑智能化系统汇聚了大量业主的个人信息，如姓名、住址、电话、车牌号等隐私数据，以及楼宇的各种控制参数，如电梯运行状态、空调温度设置、门禁权限分配等敏感信息。这些数据一旦泄露，不仅会侵犯业主的隐私权，还可能被不法分子利用，进行精准营销、电信诈骗等违法活动，给业主造成财产损失和精神困扰。同时，楼宇控制参数的泄露也会给犯罪分子提供可乘之机，如掌握了电梯控制逻辑，就可能实施故意卡停电梯、改变运行速度等危害公共安全的行为 [1]。

（二）系统入侵与控制

数据泄露的途径多种多样，黑客可以利用建筑智能化系统的各种漏洞，如软件漏洞、硬件后门、弱口令等，非法入侵系统，窃取数据。一些智能化系统为了便于远程维护，设置了远程访问接口，但如果认证措施不够严密，也可能成为数据泄露的突破口。此外，内部人员的泄密也是一个重要隐患，如系统管理员滥用职权，将数据非法出售给第三方，或工作人员误操作，将数据错误地公开等。由于建筑智能化系统规模大、结构复杂，数据量巨大，传统的安全防护手段难以完全应对数据泄露与窃取的风险，需要建立多层次、全方位的数据安全保护体系。

（三）拒绝服务攻击

拒绝服务攻击是一种常见的网络攻击方式，攻击者通过向目标系统发送大量虚假请求，耗尽系统的计算、存储、网络等资源，使系统无法正常响应正常用户的服务请求，从而达到瘫痪系统的目的 [2]。建筑智能化系统往往依赖网络通信，各子系统之间、系统与外部之间需要频繁地交换数据和控制指令，一旦遭受拒绝服务攻击，可能严重影响楼宇的智能化服务。

（四）恶意代码传播

恶意代码传播是建筑智能化系统网络安全面临的另一个重要

威胁。恶意代码，如计算机病毒、蠕虫、特洛伊木马等，通过网络传播，感染智能化系统中的各种设备，破坏系统的正常运行，窃取系统的敏感数据。与传统的信息系统相比，建筑智能化系统更容易受到恶意代码的侵害。

二、构建建筑智能化系统网络安全体系的必要性

（一）保障系统安全稳定运行

建筑智能化系统集成了楼宇的各种核心设备和服务，如暖通空调、供配电、给排水、电梯、门禁、消防等，这些系统的运行直接关系到建筑物的正常使用和人身财产安全。一旦建筑智能化系统遭受网络攻击，导致关键设备失灵或服务中断，将给建筑物的运营管理和使用者带来严重的负面影响。因此，构建完善的建筑智能化系统网络安全体系势在必行。网络安全体系应从物理层、网络层、应用层等多个层面入手，采取有效的安全防护措施，全方位守护建筑智能化系统的安全。

（二）保护用户隐私和财产安全

随着建筑智能化系统的不断发展，其采集、存储和处理的用户隐私信息日益增多，一旦发生数据泄露事件，将给用户的隐私安全和财产安全带来极大威胁。构建建筑智能化系统网络安全体系，加强对用户隐私和财产信息的保护，是维护用户合法权益的必然要求[3]。网络安全体系应重点围绕数据安全展开，贯穿数据采集、传输、存储、处理、销毁等各个环节，防止隐私数据被非法获取、篡改、泄露或滥用。例如，对采集的隐私数据进行脱敏处理，加密存储和传输隐私数据，严格限制隐私数据的访问权限，及时删除过期或无用的隐私数据等。同时还应建立健全的数据安全管理制度，明确各方的数据安全责任，加强内部人员的安全意识教育，提高用户隐私保护水平。

（三）维护国家安全和社会稳定

首先，政府机关、军事设施、科研院所等涉及国家机密和核心利益的建筑物，其智能化系统一旦被入侵或破坏，可能导致国家机密泄露、军事指挥失灵、科研成果外流等严重后果，危害国家安全和主权完整。其次，交通枢纽、能源设施、医疗机构等关系国计民生的公共建筑，其智能化系统一旦瘫痪，可能引发连锁反应，导致城市运转陷入瘫痪，给人民群众的工作和生活带来严重影响。最后，金融中心、证券交易所等关系经济命脉的建筑物，其智能化系统一旦失守，可能引发金融风险，甚至触发经济危机。黑客可能利用智能化系统的漏洞，操纵金融交易，窃取商业机密，这不仅会给相关机构造成重大经济损失，还可能动摇投资者信心，引发市场恐慌，进而影响整个国民经济的健康运行。因此，加强建筑智能化系统的网络安全建设，对维护国家安全和社会稳定具有十分重要的意义[4]。

三、建筑智能化系统网络安全体系构建策略

（一）技术策略

为了加强建筑智能化系统的身份认证与访问控制，系统管理员应采取多种措施。系统应引入双因素认证机制，要求用户在登录时不仅提供密码，还需使用硬件令牌或手机应用生成的一次性验证码，以确保只有授权用户才能访问系统。对于重要的系统管理功能，还可以引入生物识别技术，如指纹或人脸识别，进一步提高身份认证的安全性。在访问控制方面，系统应基于用户角色和职责分配权限，采用最小权限原则，只授予用户完成工作所需的最小权限，并定期审核和调整权限设置。系统管理员应在网络边界、核心交换机、服务器等关键节点部署入侵检测系统（IDS），实时监测进出网络的流量，分析其行为特征，及时发现可疑活动。同时，还应部署入侵防御系统（IPS），对检测到的攻击行为进行实时阻断。IDS 和 IPS 系统应定期更新攻击特征库，提高检测和防御的有效性[5]。此外，系统管理员还应关注 IDS 和 IPS 系统的告警信息，对可疑事件进行分析和处置。建筑智能化系统中存储和传输的数据通常具有较高的敏感性，因此必须采取数据加密措施。对于静态存储的数据，应使用强加密算法进行加密，并妥善保管加密密钥。对于跨网络传输的敏感数据，应采用安全传输协议，并使用数字证书进行身份验证，防止数据在传输过程中被窃听或篡改，同时还应对数据备份进行加密，防止备份数据泄露。此外，系统管理员应建立漏洞管理流程，定期对系统软硬件进行漏洞扫描，并关注厂商发布的安全公告和补丁信息。对于发现的漏洞，应及时评估其危害性，制定修复方案，并在测试环境中验证补丁的有效性和兼容性后，再应用于生产环境。对于暂时无法修复的漏洞，应采取临时防护措施，如访问控制、入侵检测等，降低漏洞被利用的风险。构建安全隔离区域是控制建筑智能化系统内部访问的有效手段，系统管理员应根据业务需求和安全要求，将系统划分为不同的安全域，如管理域、业务域、外联域等。在安全域之间部署防火墙，根据预定义的安全策略控制各域之间的访问，如仅允许特定 IP 地址或端口的访问。同时还应对防火墙日志进行分析，及时发现可疑的跨域访问行为。在安全域内部也应根据业务和安全需求进一步划分子网或虚拟局域网，通过访问控制列表等技术手段实现细粒度的访问控制。

（二）管理策略

建筑智能化系统的运营单位应建立健全的安全管理制度体系，成立网络安全管理委员会，明确各部门和个人在网络安全方面的职责和任务，制定全面的网络安全管理制度，涵盖系统规划、建设、运维、应急响应等各个环节，规范操作流程和标准，并定期开展网络安全教育和培训，提高全员的安全意识和技能。管理制度的制定应充分考虑建筑智能化系统的特点和实际情况，确保制度的可操作性和有效性[6]。权限管理是建筑智能化系统安全管理的核心内容，系统管理员应根据用户的角色和职责，设置相应的操作权限。权限设置应遵循最小权限原则，仅授予用户完成工作所需的最小权限，避免过度授权带来的安全风险。对于关键操作，如系统配置修改、数据库管理等，应实行双人复核制度，防止单一用户的错误操作或恶意行为。同时还应定期审核和调整权限设置，及时撤销离职人员的权限，确保权限设置与实际需求相符。日志管理和审计是建筑智能化系统安全管理的重要手段，系统应对用户的登录、退出、操作等行为进行详细记录，包

括时间、地点、操作内容等关键信息。日志应采用集中存储和管理的方式，防止被篡改或删除。安全管理人员应定期对日志进行分析和审计，及时发现可疑行为和安全事件。审计过程中如发现问题，应深入调查，查明原因，并采取相应的纠正和预防措施，审计结果应形成报告提交管理层审阅。此外，安全管理人员应定期对系统进行全面的安全检查，评估现有安全措施的有效性，发现安全隐患和薄弱环节。安全评估应包括外部渗透测试和内部配置核查等方面，全面评估系统的安全状况。对于发现的安全问题应及时制定整改方案，明确责任部门和整改期限，并跟踪整改进度，确保问题得到有效解决。安全评估结果应形成报告，作为管理决策和安全改进的重要依据。运营单位应制定完善的网络安全事件应急预案，明确应急组织架构、职责分工、处置流程等内容。应急预案应针对不同类型和级别的安全事件，制定相应的处置方案和措施。同时成立应急响应小组，配备专业人员和必要的技术设施，确保在安全事件发生时能够迅速响应和处置。应急响应小组应定期开展应急演练，检验应急预案的有效性，提高实战处置能力。在安全事件发生后，还要及时启动应急预案，控制事态，减少损失，并总结经验教训，完善应急机制。

（三）法律法规策略

国家应加快建筑智能化系统网络安全相关法律法规的建设步伐，为行业发展提供有力的法治保障。立法机关要充分调研建筑智能化系统网络安全的特点和需求，制定专门的法律法规，明确建筑智能化系统运营单位、设备供应商、安全服务商等各方主体的安全责任和义务，规范行业行为。同时及时修订现有的法律法规，如《网络安全法》《数据安全法》等，将建筑智能化系统纳入监管范围，弥补法律空白。在法规制定过程中，应广泛听取行业专家和企业代表的意见，确保法规的针对性和可操作性[7]。执法部门应加大对建筑智能化系统网络安全的监管力度，严厉打击各类违法犯罪行为。公安机关应成立专门的网络安全执法队伍，配备专业人员和技术设备，提高执法能力。对于发现的网络攻击、数据泄露等违法犯罪行为，应及时立案侦查，依法惩处。对于情节严重、后果恶劣的案件，应从重处罚，形成威慑。同时，执法部门还应加强与建筑智能化系统运营单位的沟通协作，建立信息共享和联动机制，及时发现和处置安全隐患，执法过程中应严格依法办案，保护企业和个人的合法权益。建筑智能化行业协会应发挥行业自律的重要作用，制定行业网络安全规范和标准，引导企业加强安全防护。行业协会应组织行业专家和企业代表，研究制定建筑智能化系统网络安全的技术标准、管理规范、评估指标等，为企业提供可操作的指引[8]。同时，还应建立行业网络安全信息共享平台，促进企业间的经验交流和威胁情报共享。行业协会还应定期开展网络安全评估和检查，对企业的安全状况进行评价，督促企业整改问题。对于安全防护不力、屡次出现安全事故的企业，行业协会应予以通报批评，情节严重的可以实施行业处罚，如限制市场准入等。此外，行业协会还应积极开展网络安全教育和培训，提高从业人员的安全意识和技能。协会应定期举办网络安全专题讲座、研讨会等活动，邀请行业专家和优秀企业代表分享经验，传播最新的安全理念和技术。同时，还应制定行业人才培养计划，与高校、科研机构合作，培养建筑智能化系统网络安全领域的专业人才，为行业发展提供智力支持。行业自律与政府监管相结合，能够有效提升建筑智能化系统的整体安全防护能力，促进行业健康有序发展。

四、结束语

综上所述，建筑智能化系统网络安全问题事关建筑物的安全运行和人民生命财产安全，必须高度重视。构建完善的建筑智能化系统网络安全体系需要多方共同努力，通过采取有效的技术、管理和法律手段，全面提升建筑智能化系统的安全防护能力，为智能建筑的健康发展提供坚实保障。

参考文献

[1] 田晓霞 . 弱电智能化系统网络安全体系研究 [J]. 中文科技期刊数据库（文摘版）工程技术，2022(3)：3.

[2] 葛欣欣 . 学校建筑智能化系统的设计要点探讨 [J]. 江西建材，2023,(05)：208-210.

[3] 席攀锋 . 新型智能建筑中的网络安全策略研究 [J]. 现代工业经济和信息化，2021,11(07)：111-115.

[4] 云洁 . 建筑智能化系统网络安全研究 [J]. 数字技术与应用，2017,(01)：211+213.

[5] 李志敏 . 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，2022,23(6)：3.

[6] 江好 . 智能建筑中的网络安全策略探讨 [J].IT 经理世界，2023(11)：25-28.

[7] 高凡 . 智能建筑系统网络安全问题行业解决方案制定进行时 [J]. 中国建设信息化，2020(3)：1.

[8] 朱伊华 . 智能楼宇系统中网络安全技术分析 [J]. 中国设备工程，2021(19)：2.

