智能建筑弱电系统网络安全防护体系构建

赵峻鹰

中能国源（北京）咨询有限公司　北京

【摘要】随着信息技术的快速发展，智能建筑已成为现代城市建设的重要组成部分。在智能建筑中，弱电系统扮演着关键角色，但随之而来的网络安全问题也日益突出。本文探讨了智能建筑弱电系统的网络安全防护体系的构建方法。通过分析现有弱电系统面临的主要安全威胁与挑战，提出了一套全面的安全防护方案，包括网络隔离、数据加密、入侵检测等技术手段的应用。本文还从风险评估、技术标准和应急响应等多个方面进行了深入探讨，旨在为智能建筑提供一个全方位、可持续的网络安全防护体系，以保障智能建筑在日常运营中的安全与稳定。

【关键词】智能建筑；弱电系统；网络安全；防护体系；技术手段

【收稿日期】2025 年 5 月 16 日　　【出刊日期】2025 年 6 月 7 日　　【DOI】10.12208/j.aics.20250038

Construction of network security protection system for weak current systems in intelligent buildings

Junying Zhao

ZhongNengGuoYuan(Beijing) Consulting Co., Ltd., Beijing

【**Abstract**】With the rapid development of information technology, intelligent buildings have become an important part of modern urban construction. In intelligent buildings, weak current systems play a crucial role, but the accompanying network security issues have become increasingly prominent. This paper explores the methods for constructing a network security protection system for weak current systems in intelligent buildings. By analyzing the main security threats and challenges faced by existing weak current systems, it proposes a comprehensive security protection scheme, including the application of technical measures such as network isolation, data encryption, and intrusion detection. The paper also conducts in-depth discussions from multiple aspects such as risk assessment, technical standards, and emergency response, aiming to provide an all-round and sustainable network security protection system for intelligent buildings, so as to ensure the safety and stability of intelligent buildings in daily operations.

【**Keywords**】Intelligent building; Weak current system; Network security; Protection system; Technical measures

引言

智能建筑的快速发展为城市管理和运营带来了许多便利，但也伴随着越来越多的网络安全挑战。弱电系统作为智能建筑的重要组成部分，涉及监控、通信、自动化等多项关键业务，其安全性直接影响到建筑的整体安全运行。随着弱电系统的网络化与信息化程度的提高，外部攻击、数据泄露等安全威胁日益严重。构建一套科学的网络安全防护体系显得尤为重要。本文将围绕智能建筑弱电系统的网络安全防护展开，重点分析当前系统所面临的主要安全风险，并提出相应的防护方案，旨在为智能建筑的可持续发展提供理论支持与技术保障。

1 智能建筑弱电系统面临的网络安全威胁

智能建筑的弱电系统包括监控、通信、安防、照明等多个子系统，而这些子系统的运行依赖于计算机网络和云平台，这也使得其面临着较为复杂的网络安全威胁。在信息化和智能化程度不断提高的今天，弱电系统在提供便利的也为黑客攻击、数据泄露等风险打开了大门。由于弱电系统的设备多样，且经常与外部网络相连接，因此其攻击面较大，容易遭遇网络攻击。网络攻击者可能通过入侵建筑内的通信系统或安防系统来窃取敏感信息、控制系统设备，甚至发起拒绝服务（DoS）攻击，造成系统瘫痪。恶意软件和病毒也可能通过外部设备或网络漏洞传播，从而危害整个建筑的网络安全。

除了外部的黑客攻击，建筑内的内部员工和设备也可能成为潜在的威胁来源。在智能建筑中，弱电系统

需要进行大量的数据传输与存储，一旦管理不当，数据泄露风险加剧。尤其是在个人信息与商业机密的保护方面，如果安全措施不足，可能导致重要数据的泄露或篡改[1]。而智能建筑中的设备一般连接于广域网或互联网，设备之间的协议差异与系统的复杂性使得其防护工作更加艰难。网络攻击者可以通过扫描、植入恶意程序或利用设备之间的漏洞进入弱电系统，给系统的安全性带来巨大的威胁。

智能建筑的弱电系统还面临着传统网络安全防护措施难以适应的问题。由于这些系统涉及的设备多且复杂，传统的防火墙、入侵检测系统等安全技术难以有效地覆盖所有潜在的攻击点。网络设备如传感器、摄像头、楼宇自动化控制系统等普遍缺乏足够的安全防护措施，且许多设备具有远程控制和管理功能，这也增加了远程攻击的风险。智能建筑弱电系统需要结合新型技术手段，如数据加密、身份认证、异常检测等方式，来加强对系统的安全防护。

2 智能建筑弱电系统网络安全防护的关键技术

要确保智能建筑弱电系统的网络安全，必须依赖于多种关键技术手段的综合运用。网络隔离技术是确保建筑弱电系统安全的基础之一。通过合理设计网络架构，将弱电系统的不同子系统隔离开来，形成层次化的安全防护措施，可以有效防止黑客攻击通过一个系统蔓延至其他系统。网络隔离还能够限制潜在的安全风险，尤其是在设备与设备之间的通信时，避免重要信息在无保护的情况下泄漏。

数据加密技术在智能建筑弱电系统中起着至关重要的作用，特别是在保护敏感数据方面。随着系统中监控视频、门禁权限、环境监测数据等信息的频繁传输和处理，这些数据一旦未加密处理，就容易成为黑客攻击的目标，导致信息泄露或篡改。黑客可以通过截取未加密的视频数据或门禁权限信息，从而绕过安全控制，获取未经授权的访问权限[2]。为了避免这种情况，实施端到端加密技术至关重要。端到端加密能够确保数据从发送端到接收端的整个传输过程中都受到保护，防止在中途被截获或篡改。强密码策略和密钥管理机制同样不可忽视，它们能够为系统增加一道额外的防护屏障，确保即使在设备被攻破的情况下，数据依然无法轻易访问或解密，提升系统的整体安全性。

入侵检测与防御技术是确保智能建筑弱电系统安全防护的重要组成部分，能够为系统提供全天候的实时监控。入侵检测系统（IDS）通过实时监控网络流量，能够识别出异常流量和潜在的安全威胁，如未经授权的访问尝试或数据篡改行为。一旦发现异常，IDS 能够立即向管理员发出警报，帮助其迅速采取措施，防止安全事件的扩大。结合入侵防御系统（IPS）与防火墙的部署，可以在攻击发生之前就识别并有效阻断外部威胁，防止恶意行为进入系统，最大程度地减少潜在的风险。随着人工智能技术的不断发展，基于 AI 的安全监测与预测系统也逐步应用于智能建筑中。通过机器学习和大数据分析，这些系统不仅能够识别现有的威胁，还能有效预测并预防未知的安全攻击，为系统增添了额外的智能防护层。

3 构建智能建筑弱电系统网络安全防护体系的策略

在构建智能建筑弱电系统网络安全防护体系时，首先需要深入分析系统的安全需求。这包括对硬件、软件、网络环境以及数据传输过程的详细评估。通过评估，能够明确各个环节中潜在的脆弱点以及可能遭遇的威胁，例如网络接口、设备漏洞、传输过程中的数据泄露等。根据评估结果，制定相应的防护策略，强化系统的安全性，确保建筑中每个子系统能按预定的安全目标正常运行。对于不同类型的子系统，如监控、门禁、环境调节等，其安全需求不同，防护措施也需因地制宜。环境监测系统可能更注重数据完整性，而安防系统则需要防范实时视频数据被恶意篡改。通过针对性设计，能够最大限度降低安全威胁对整个系统的影响。

技术标准和规范是确保智能建筑弱电系统网络安全的基础。在构建安全防护体系时，必须建立起系统性和规范化的标准，涵盖设备选型、通信协议、系统接口等关键方面。这些标准能够确保不同设备和系统之间的兼容性与有效对接，避免因技术不统一导致的漏洞和冲突。在选择摄像头和传感器等设备时，需要明确规定其数据传输协议，以确保设备在联网时不会引入不必要的安全风险。严格的安全管理制度至关重要，它要求对所有系统的访问权限、操作记录以及数据传输过程进行全面监控和审计。这种管理方式不仅有助于实时掌握系统运行状态，还能在出现问题时快速追溯源头，确保及时解决。

应急响应与灾难恢复策略是网络安全防护体系的重要组成部分。面对可能发生的网络攻击或系统安全事件，能够快速启动应急响应机制至关重要。应急响应的核心在于及时发现问题并迅速采取行动，首先是隔离攻击源，避免攻击进一步蔓延。系统备份、漏洞修补和流量分析等措施能在事件发生后尽快恢复服务[3]。通过对安全事件进行深入分析，能够找出问题根源并优

化现有防护策略，从而减少未来安全事件的发生概率。灾难恢复策略则为建筑的运营提供了保障，确保在发生重大安全事件时，能够迅速恢复正常运作，避免因系统瘫痪造成的服务中断，减少经济损失和客户信任的损害。

4 智能建筑弱电系统网络安全防护体系的实施与评估

智能建筑弱电系统网络安全防护体系的实施首先需要建立一支专门的安全团队，负责安全防护策略的落实与系统的持续监控。这支团队需要具备丰富的安全技术背景，能够对建筑弱电系统的各个部分进行安全审核，并提出针对性的改进措施。实施过程中，必须确保所有安全技术的集成与兼容，避免在实施过程中因技术冲突而导致新的安全隐患。系统的安全防护措施必须结合建筑实际情况进行调整，尤其是在跨多个子系统的整合过程中，要确保各子系统之间的安全协同作用。

系统实施后，必须对弱电系统的网络安全进行定期评估与测试。通过模拟各种攻击场景，如网络入侵、病毒传播、数据泄露等，测试系统的防护能力，检查其漏洞与不足。这些测试不仅能验证已有安全防护措施的有效性，也能帮助发现新的潜在威胁。通过不断优化和调整防护方案，确保系统始终处于最优的安全状态。应对网络安全事件进行定期的复盘和分析，总结应急响应中的经验教训，进一步提高系统防护的准确性和有效性[4-8]。网络安全防护体系的持续优化是保证智能建筑弱电系统长期安全的关键。随着技术的不断发展，新的安全威胁不断出现，防护体系不能一成不变。定期更新安全策略，采用新兴的技术手段，并对现有防护措施进行升级，是保持建筑系统安全的长久之计。通过实施持续的监控、检测、评估等手段，能够有效应对未来的网络安全挑战，确保智能建筑的弱电系统始终在安全可控的环境中运行。

5 结语

智能建筑弱电系统的网络安全防护至关重要，随着技术的不断进步，弱电系统面临的安全威胁也日益复杂。构建一个全面、有效的安全防护体系，需要从各个方面入手，包括脆弱性分析、技术标准制定、应急响应机制和灾难恢复策略等。通过数据加密、入侵检测与防御技术等先进手段的综合运用，可以显著提高系统的抗攻击能力。随着人工智能和大数据技术的发展，基于AI的安全监测系统也为智能建筑提供了更加智能化的防护手段。面对日益严峻的网络安全形势，智能建筑弱电系统必须持续优化其安全防护体系，以应对未来可能出现的各种挑战，保障建筑的安全运行，促进智慧城市的健康发展。

参考文献

[1] 喻潮华.建筑电气智能化弱电系统安装及质量管理[C]//《中国招标》期刊有限公司.新质生产力驱动第二产业发展与招标采购创新论坛论文集（二）.杭州佳康机电安装工程有限公司;,2025:216-217.

[2] 曹焕,何雁,庄湘荣,等.智慧产业园智能化方案设计探索[J].智能建筑与智慧城市,2024,(S1):68-71.

[3] 但国良.智能建筑弱电系统信息化建设应用与对策分析[J].新城建科技,2024,33(09):137-139.

[4] 陈敏岷.强化智能建筑弱电系统施工管理工作的对策[J].中国建设信息化,2024,(14):72-75.

[5] 施成桂.建筑电气技术在智能建筑中的作用[J].低碳世界,2024,14(07):103-105.

[6] 罗锦波.智能建筑弱电系统施工常见问题及其防范对策[J].中国高新科技,2023,(17):124-126.

[7] 李伍林.智能建筑弱电工程设计与施工措施探讨[J].江西建材,2023,(04):274-275.

[8] 何小勇,赵俊杰,白显军,等.消防弱电系统在建筑工程中的应用[J].智能建筑与智慧城市,2022,(12):154-156.