弱电智能化建筑系统网络信息安全优化探究

张杨帆[1] 王 岩[2]

1.润信智能科技有限公司 陕西 西安 710000

2.润信智能科技有限公司 辽宁 沈阳 110000

【摘 要】：弱电智能化建筑系统是现代建筑的重要组成部分，其网络信息安全优化至关重要。随着智能化水平的提高，系统面临的安全威胁日益增多。文章首先概述了弱电智能化建筑系统的基本构成与功能，随后分析了影响其网络信息安全的多种因素，包括技术漏洞、人为失误及外部攻击等。在此基础上，提出了针对性的优化策略，旨在提升系统的防御能力和数据保护水平，确保建筑智能化进程中的信息安全。

【关键词】：弱电智能化建筑系统；网络信息安全；优化策略

DOI:10.12417/2811-0528.24.20.063

随着科技的飞速发展，弱电智能化建筑系统逐渐成为建筑行业的研究热点。该系统利用现代网络通信技术，在建筑中可以实现控制、监测、管理等功能，从而能够提高建筑的智能化程度和能效。然而，随着连接性的增加，网络攻击和其他安全威胁的风险也随之而来。智能建筑系统涉及大量的数据采集、传输和存储，包括住户的个人信息、建筑物的结构信息等敏感数据。这些数据如果被黑客攻击和窃取，会造成严重的隐私泄露和经济损失。因此，网络信息安全成为弱电智能化建筑系统需要解决的关键问题。为保障建筑系统的正常运行和住户的隐私安全，对弱电智能化建筑系统的网络信息安全进行优化显得尤为重要，这不仅有助于提升建筑系统的智能化水平，还能确保系统的稳定性和可靠性。

1 弱电智能化建筑系统概述

弱电智能化建筑系统是现代建筑领域的重要组成部分，其利用低电压、小电流的信号系统和设备，通过信息技术、自动化技术和通信技术可以实现对建筑物、设施或系统的智能化管理和控制。该系统具有多个显著特点，一是，强调低电压、低功耗，注重通信及控制技术的高效应用。二是，弱电智能化建筑系统通常包括多个子系统，这些系统相互协作，共同为用户提供高效、便捷、安全、舒适的环境和服务。在组成方面，弱电智能化建筑系统主要包括综合布线系统、建筑设备自动化系统以及安全防护系统。综合布线系统能够为各种弱电系统提供统一的传输平台，确保信号和数据在建筑内的稳定传输。建筑设备自动化系统则负责监测和控制建筑物内的空调系统、照明系统、给排水系统等设备，用以提高设备的运行效率和可靠性。安全防护系统则包括视频监控系统、入侵报警系统等，用于保障人员和财产安全[1]。

2 弱电智能化建筑系统网络信息安全影响因素

在弱电智能化建筑系统中，网络信息安全面临着多种复杂的影响因素。这些因素可根据其不同来源和对象进行细致划分。从威胁来源的角度看，网络信息安全隐患主要分为内部与外部两大类别。内部因素通常与人员相关，包括员工的不当操作、疏忽大意或恶意行为，这些行为均会成为系统安全的潜在漏洞。而外部因素则涵盖了更广泛的范围，如来自竞争对手的恶意破坏、黑客的非法侵入等，外部因素会瞄准系统的监控层级、现场控制设备及网络通信链路等关键组件，意图干扰或破坏弱电智能化建筑系统的正常运作，进而对关联企业构成严重的经济损失风险。从威胁的指向性来看，网络信息安全的挑战也呈现出多样化的特征，一方面，攻击者会直接瞄准信息网络和控制网络，利用拦截、篡改数据等手段，试图扰乱系统的正常运行秩序。另一方面，会通过利用互联网接入设备、智能终端设备、应用软件等薄弱环节，绕过系统防护，实现对弱电智能化建筑系统的非法控制。攻击者还会采用更为隐蔽的旁路攻击方式，通过监测设备的能耗特征、电磁辐射强度等物理参数，尝试破解系统的加密机制，进一步威胁到系统的数据安全[2]。此外，在系统内部植入恶意软件、中断通信链路等手段，也是攻击者常用的策略，这些行为不仅会导致系统数据的丢失或损坏，还会对系统的整体稳定性和可靠性造成严重影响。

3 弱电智能化建筑系统网络信息安全优化策略

弱电智能化建筑系统作为现代建筑的重要组成部分，其网络信息安全直接关系到建筑功能的正常发挥及用户数据的安全。为全面提升弱电智能化建筑系统的网络信息安全水平，以下将从安全体系构建、安全服务优化、安全保护对象强化以及具体的安全管理措施等方面，深入阐述网络信息安全优化策略。

3.1 安全体系构建：多维度、多层次的安全防护

在弱电智能化建筑系统中，构建网络信息安全体系应遵循多维度、多层次的原则。首先应明确安全协议层次平面、安全服务平面和安全保护对象平面三大核心要素。安全协议层次平面应依据现有安全协议构建七层模型，确保每一层都能提供针对性的安全服务和安全服务管理机制。同时，应充分考虑物理层、数据链路层、网络层、传输层、会话层等各层的安全需求，确保每一层都能得到全面有效的安全防护。在安全机制方面应充分利用加密机制、访问控制机制、数据完整机制、公证机制等多种安全机制，形成组合拳，提升整体安全服务水平。例如，通过加密与数字签名制度的结合，可以确保数据的机密性和完整性，从而从根本上提升系统安全管理水平。在安全服务方面则应设定明确的安全目标，并为这些目标提供高质量的安全服务。这些服务应跨越多个安全协议层次，确保每一层都能得到全方位的安全保障。此外，安全保护对象平面应明确弱电智能化系统网络安全的保护对象，如传输数据、系统网络实体等。针对这些对象应开展针对性的安全管理工作，确保数据在传输过程中的机密性、完整性和可用性。同时，应加强对网络实体的安全防护，如控制网、管理网和网络互连设备等，确保其能够稳定运行，不受外部攻击的影响。

3.2 安全服务优化：提升服务质量与效率

为满足不同用户对安全服务的需求应提供定制化的安全服务，这包括根据用户的具体需求，设计合适的安全策略、配置安全设备、提供安全培训等。通过定制化服务可以确保用户得到最适合自己的安全解决方案，从而提升整体安全水平。随着人工智能技术的发展，应将智能化技术引入安全服务中。例如，通过利用机器学习算法，可以实现对网络流量的实时监测和分析，及时发现并应对潜在的安全威胁。智能化技术还可以帮助用户自动更新安全策略、优化安全配置等，从而提升安全服务的效率和准确性。此外，安全服务不是一成不变的，而应随着技术的发展和用户需求的变化而不断优化。因此，应定期对安全服务进行评估和改进，确保其能够始终满足用户的需求和期望，这包括更新安全策略、升级安全设备、引入新的安全技术等。

3.3 安全保护对象强化：确保关键数据与系统实体安全

数据传输是弱电智能化建筑系统中最重要的环节之一。为确保数据安全传输应采用加密技术对数据进行加密处理，还应采用数字签名等技术来确保数据的完整性和真实性。同时，应加强对传输通道的监控和管理，确保数据不被非法访问或篡改。系统网络实体包括控制网、管理网和网络互连设备等。为确保系统网络实体安全应采用多种安全防护措施，例如可以通过配置防火墙、入侵检测系统等技术来防止外部攻击，并定期对系统进行漏洞扫描和修复工作，确保系统不存在安全漏洞。同时，应加强对系统用户的管理和监控，防止内部人员的不当操作或恶意攻击。关键数据是弱电智能化建筑系统中的核心资源之一，为确保关键数据的安全，应定期对数据进行备份和恢复测试。通过备份数据可以在系统发生故障或遭受攻击时快速恢复数据，而通过恢复测试则可以验证备份数据的完整性和可用性[3]。因此，应制定完善的备份和恢复策略，并定期对其进行评估和改进。

3.4 具体安全管理措施：实现全面有效的安全防护

（1）建立安全管理团队：为加强弱电智能化建筑系统的网络信息安全管理工作，应建立专业的安全管理团队。安全管理团队应由具备丰富经验和专业知识的安全专家组成，负责系统的安全策略制定、安全风险评估、安全事件应对等工作。同时，还应定期对团队成员进行培训和考核，确保团队成员具备足够的专业素养和技能水平。

（2）制定完善的安全管理制度：安全管理制度是保障弱电智能化建筑系统网络信息安全的基础。因此，应制定包括安全策略、安全操作规程、安全事件处理流程等完善的安全管理制度，这些制度应明确各级人员的职责和权限，确保人员在工作中能够遵守相关规定和流程。同时，还应定期对制度进行审查和更新，确保安全管理制度能够始终适应技术发展和用户需求。

（3）加强安全监测与预警：为及时发现并应对潜在的安全威胁，应加强对弱电智能化建筑系统的安全监测与预警工作。这包括利用先进的技术手段对网络流量、系统日志等进行实时监测和分析，同时还应建立安全预警机制，当发现潜在威胁时及时发出预警信息并采取相应的应对措施，通过加强安全监测与预警工作可以及时发现并消除安全隐患，确保系统的稳定运行。

（4）加强应急响应与恢复能力：当弱电智能化建筑系统遭受攻击或发生故障时应能够迅速响应并恢复系统的正常运行，因此，应加强建设应急响应与恢复能力，这包括制定完善的应急预案和恢复计划，并定期对预案进行演练和评估，确保在关键时刻能够发挥应有的作用。此外，还应加强对系统备份和恢复能力的测试和优化工作，确保在发生故障时能够快速恢复系统的正常运行[4]。

（5）加强用户教育与培训：用户是弱电智能化建筑系统网络信息安全的重要一环，因此,应加强对用户的教育和培训工作，这包括向用户普及网络安全知识、提高用户的安全意识，同时，应教会用户如何正确使用系统、避免不当操作或恶意攻击。通过加强用户教育与培训工作，可以形成用户与系统之间

的良性互动关系，共同维护系统的网络信息安全。

（6）引入第三方安全评估与认证：为确保弱电智能化建筑系统的网络信息安全水平达到行业标准或规范要求，可以引入第三方安全评估与认证机构进行评估和认证工作。这些机构通常具备丰富的经验和专业的技能水平，能够对系统进行全面的安全评估并给出相应的认证结果。通过引入第三方安全评估与认证工作，可以确保系统的安全性能符合相关标准和规范要求，从而提升系统的整体安全水平。

（7）加强国际合作与交流：随着全球化的加速发展，网络安全问题已经成为全球性的挑战。因此，应加强与国际社会的合作与交流工作，共同应对网络安全问题。这包括参加国际网络安全会议、与国际组织建立合作关系、分享网络安全技术和经验等。通过加强国际合作与交流工作可以借鉴其他国家和地区的先进经验和做法，提升自身的网络安全防护能力。

4 结语

弱电智能化建筑系统的发展，在带来便捷与高效的同时，也面临着严峻的网络信息安全挑战。本文深入剖析了系统安全的影响因素，并针对性地提出了优化策略。通过构建多维度、多层次的安全防护体系，优化安全服务，强化安全保护对象，以及实施具体的安全管理措施，可以有效提升系统的网络信息安全水平。这些策略的实施，对于保障建筑智能化进程的顺利进行，维护用户隐私和数据安全具有重要意义。未来，弱电智能化建筑系统的网络信息安全优化工作仍需持续加强，以应对不断变化的安全威胁。

参考文献：

[1] 赵鹏.网络通信技术下弱电智能化建筑系统研究[J].数字通信世界,2023,(08):58-60.

[2] 吴君.基于网络通信技术下弱电智能化建筑系统[J].数字技术与应用,2023,41(04):74-76.

[3] 罗金成.建筑智能化系统中物联网技术应用[J].四川建材,2023,49(02):31-32+41.

[4] 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(06):179-181.