 DOI: https://doi.org/10.12345/gcjsygl.v9i5.24137

Research on Security Assessment and Protection Strategies of Building Intelligent Systems

Li Li Bo Liu

China Architecture Design and Research Institute Co., Ltd., Beijing, 100000, China

Abstract

With the rapid development and application of building intelligent systems, intelligent management of buildings has become an important component of modern cities. Building intelligent systems greatly improve the efficiency and comfort of building use by integrating multiple functions such as control, monitoring, environmental regulation, and safety protection. However, with the increasing complexity of system functions, security issues have gradually become prominent, especially in areas such as network attacks, data breaches, and physical intrusions, which have brought many hidden dangers to the normal operation of buildings. Therefore, this article studies the security assessment method of building intelligent systems and proposes corresponding protection strategies, aiming to improve the overall security of building intelligent systems. By analyzing existing security risks and vulnerabilities, combined with risk assessment and protection technologies, this article provides scientific basis and practical guidance for the security guarantee of building intelligent systems.

Keywords

Building Intelligence System; Security assessment; Protection strategy; Risk management; information security

楼宇智能化系统安全性评估与防护策略研究

李丽 刘波

中国建筑设计研究院有限公司，中国·北京 100000

摘 要

随着楼宇智能化系统的快速发展和应用，建筑物的智能化管理已成为现代城市的重要组成部分。楼宇智能化系统通过集成控制、监控、环境调节、安全防护等多个功能，大大提高了建筑物的使用效率和舒适度。然而，随着系统功能的日益复杂，安全性问题逐渐凸显，尤其是在网络攻击、数据泄露、物理入侵等方面，给楼宇的正常运营带来了诸多隐患。因此，本文研究了楼宇智能化系统的安全性评估方法，并提出了相应的防护策略，旨在提高楼宇智能化系统的整体安全性。通过分析现有的安全隐患及漏洞，结合风险评估与防护技术，本文为楼宇智能化系统的安全保障提供了科学依据和实践指导。

关键词

楼宇智能化系统；安全性评估；防护策略；风险管理；信息安全

1 引言

随着信息技术和物联网技术的飞速发展，楼宇智能化系统已成为现代建筑的标配，其主要功能包括环境调节、安全监控、设备管理等，旨在通过智能化手段提高建筑物的管理效率和居住体验。智能化系统的核心组成部分包括监控系统、照明系统、空调系统、火灾报警系统、安全防范系统等，这些系统通过物联网和大数据技术进行集成和管理，能够实现实时监控、自动控制和远程管理等功能。楼宇智能化系统的广泛应用，不仅提升了建筑物的安全性、舒适性和便利性，还有效降低了能耗，推动了绿色建筑的发展。

然而，随着楼宇智能化系统逐渐成为建筑物运营的核心，其安全性问题也逐渐显现。智能化系统的复杂性和集成性使其成为网络攻击和物理入侵的潜在目标，系统漏洞、数据泄露、设备故障等问题已成为影响智能化系统稳定性和安全性的关键因素。特别是在智能化系统的大规模联网和数据共享的背景下，信息安全、设备防护、网络安全等问题日益突出，成为当前智能楼宇管理中的重要挑战。

本研究旨在探讨楼宇智能化系统的安全性评估方法，分析现有智能化系统中存在的安全隐患，并提出有效的防护策略。通过建立完善的安全评估体系，结合技术手段和管理对策，为楼宇智能化系统的安全提供保障，确保其在高效运行的同时，也能抵御各种潜在的安全威胁。

2 楼宇智能化系统安全性面临的主要问题

2.1 网络安全问题

楼宇智能化系统的网络安全问题是当前面临的最为严

【作者简介】李丽（1981–），女，中国河北保定人，本科，工程师，从事楼宇智能化研究。

峻的挑战之一。随着物联网技术的广泛应用，楼宇智能化系统各组成部分通过无线网络连接，形成了一个庞大的网络系统。尽管这种联网方式提高了系统的灵活性和可操作性，但也带来了网络攻击的风险。黑客可能通过网络漏洞入侵系统，造成数据泄露、信息篡改、系统瘫痪等严重后果。

网络安全问题的主要表现形式包括数据包嗅探、恶意攻击、服务拒绝等。通过对网络中的数据流量进行窃听，攻击者可以获得楼宇智能化系统的敏感信息，如设备状态、用户行为、远程控制指令等。此外，攻击者还可以通过分布式拒绝服务（DDoS）攻击导致系统无法正常工作，影响楼宇的安全管理。为了防止网络安全事件的发生，需要在设计和部署过程中充分考虑网络的安全性，采取必要的加密措施，定期进行漏洞扫描，及时修复系统漏洞，避免潜在的安全隐患。

2.2 数据隐私和泄露问题

楼宇智能化系统在采集和处理大量数据的过程中，涉及大量的个人信息和敏感数据。例如，楼宇智能化系统中的门禁管理、环境控制、视频监控等功能都可能涉及用户的个人隐私和行为数据。如果这些数据未能得到妥善保护，可能会导致个人隐私泄露、商业机密泄露等安全事件。

数据泄露问题通常出现在以下几个方面：一是数据存储不当，导致数据被非法访问或盗用；二是数据传输过程中未进行加密处理，容易被窃听；三是缺乏有效的数据销毁机制，导致敏感数据长期存在系统中。为了应对这些挑战，楼宇智能化系统必须采取严格的数据加密措施，确保数据在存储、传输和处理过程中的安全性。同时，系统应建立完善的数据访问控制和审计机制，确保只有授权人员能够访问敏感数据，并在数据不再使用时及时销毁。

2.3 物理安全问题

尽管楼宇智能化系统的核心功能多为软件和网络驱动，但物理安全问题仍然是楼宇智能化系统安全防护的重要一环。物理安全问题主要表现为非法入侵和设备损坏。智能化系统的硬件设备往往安装在不易被察觉的位置，如机房、天花板、地下室等，这使得攻击者可以通过物理入侵手段直接破坏系统设备，导致设备瘫痪或信息丢失。

此外，楼宇智能化系统的设备维护和管理人员较为分散，缺乏集中化管理的安全防护措施。设备维护人员的权限过大，若管理不当，可能导致系统设备被非法操作或破坏。因此，物理安全问题要求加强对楼宇智能化设备的物理保护，如安装监控、报警系统、门禁控制等，确保设备和控制中心的物理安全。同时，定期对系统设备进行检查，及时发现潜在的硬件故障和损坏，保障设备的正常运行。

3 楼宇智能化系统的安全性评估方法

3.1 风险评估模型

楼宇智能化系统的安全性评估需要从多个维度进行，包括网络安全、数据安全、物理安全等。通过构建风险评估模型，能够全面识别系统中的潜在风险，并评估其对系统安全的影响。风险评估模型通常包括以下几个步骤：

风险识别：通过对楼宇智能化系统的功能和结构进行分析，识别可能的安全威胁和漏洞，如网络攻击、设备故障、数据泄露等。

风险分析：对识别出的风险进行定量或定性的分析，评估其发生的可能性和危害程度。可以采用概率分析、故障树分析（FTA）等方法对风险进行建模。

风险评估：根据分析结果，评估每个风险事件的影响范围、损失程度和发生频率。通过计算风险值，确定哪些风险是最需要优先防范的。

风险控制与管理：根据评估结果，制定相应的防控措施，并对风险进行动态管理。对重要的系统组件，采用多重防护策略，减少系统受到攻击或损坏的可能性。

3.2 安全漏洞扫描与评估

针对楼宇智能化系统中的软件和硬件安全漏洞，定期进行安全漏洞扫描和评估是保障系统安全的有效手段。通过漏洞扫描工具，可以自动识别系统中的已知漏洞，并进行修复。此外，还可以进行渗透测试，模拟黑客攻击，评估系统的防御能力。

安全漏洞扫描不仅应涵盖操作系统和应用程序的漏洞，还应关注网络设备、通信协议、硬件接口等方面的安全风险。定期的漏洞扫描与评估可以帮助及时发现并修复系统中的安全漏洞，从而有效预防安全事件的发生。

3.3 安全监测与审计

楼宇智能化系统需要建立全面的安全监测和审计机制，实时监控系统的运行状态和安全状况，及时发现异常情况。安全监测包括对网络流量、用户行为、设备状态等的实时监控，以便在发生安全事件时能够迅速响应并采取措施。

审计机制则用于记录系统操作日志，包括系统访问、设备操作、数据处理等信息。通过对日志的定期分析，可以发现系统中的异常操作或潜在的安全威胁，为系统的安全管理提供重要依据。

4 楼宇智能化系统安全性防护策略

4.1 加强网络安全防护

针对楼宇智能化系统中的网络安全问题，必须采取多层次的防护措施，以应对不断变化的网络攻击手段。在楼宇智能化系统中，所有的硬件设备和软件系统往往通过网络相互连接和通信，因此其网络安全性直接决定了整个智能化系统的稳定性和可靠性。为了确保楼宇智能化系统在运营过程中的网络安全，应从防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等多个方面进行部署，构建一套全方位的防护体系。

防火墙作为网络安全的第一道防线，通过设定严格的

访问控制规则，能够有效阻止非法访问和恶意攻击。入侵检测系统（IDS）能够实时监控网络流量，识别潜在的安全威胁，及时报警并提供入侵的详细信息。而入侵防御系统（IPS）则不仅能够检测入侵行为，还能采取主动防御措施，自动阻止攻击者的进一步行动，增强系统的防御能力。

此外，网络的划分和隔离也是提升安全性的重要手段。通过划分不同的安全区域，确保关键数据和核心设备与其他系统进行隔离，减少因某个环节被攻击而波及整个系统。不同的网络区域可以根据其安全级别和重要性设定不同的访问权限和保护措施，从而有效降低网络攻击的影响范围。

楼宇智能化系统的无线网络部分尤为容易受到攻击，因此，对无线网络的安全性也需特别重视。通过使用强加密技术，如 WPA3 加密协议，保障数据传输过程中的安全性。此外，采用多重身份认证（例如双因素认证、动态口令认证等）手段，可以大大增强系统的安全性，确保只有授权用户可以访问系统，从而防止网络黑客通过弱密码等方式入侵系统。

4.2 强化数据安全管理

楼宇智能化系统涉及大量敏感数据的采集、传输、存储和处理，这些数据包括但不限于用户身份信息、访问记录、环境控制数据、视频监控内容等。数据安全问题一旦发生，可能导致信息泄露、隐私侵犯等严重后果，因此数据的安全性管理必须得到充分地重视。

为保障数据的安全性，首先需要对敏感数据进行加密处理。无论是在数据传输过程中，还是存储过程中，使用加密算法（如 AES 加密标准）对数据进行加密，能够有效防止数据在网络传输或存储过程中被截获和盗用。加密技术不仅能保护数据的机密性，还能防止数据被篡改，保证数据的完整性。

其次，访问控制机制是确保数据安全的另一个重要环节。在楼宇智能化系统中，敏感数据的访问权限应当严格管理。可以通过角色权限控制和多层次的访问控制策略，确保只有授权人员能够访问特定的数据。对于高敏感度数据，如视频监控记录、控制指令等，可以设置更加严格的权限控制，例如限制某些用户只能进行查看操作，不能进行修改或删除操作。

4.3 优化物理安全保护

尽管楼宇智能化系统的核心功能多为软件和网络驱动，但物理安全问题仍然是保障系统安全的重要一环。物理安全保护主要针对系统硬件设备的保护，防止设备被非法访问、损坏或破坏，确保智能化系统的持续稳定运行。楼宇智能化系统的硬件设备通常部署在机房、控制中心等关键区域，这些区域需要特别的物理防护。

首先，安装高安全等级的门禁系统对楼宇智能化设备进行物理保护。门禁系统可通过身份识别手段（如指纹识别、面部识别、IC 卡等）对进出人员进行严格的身份验证。对于关键区域的设备，应实施多重身份认证，并设定不同的访问权限，以确保只有授权人员才能进入设备管理区域。此举可以有效防止未授权人员通过物理入侵手段破坏设备或篡改系统数据。

5 结语

楼宇智能化系统的广泛应用为现代建筑提供了极大的便利和效率，但也伴随着日益严峻的安全问题。本文通过分析楼宇智能化系统的主要安全隐患，提出了网络安全、数据安全和物理安全等方面的防护策略，强调了多层次综合防护的重要性。随着智能化系统的日益复杂，安全防护手段也需要不断更新和完善，确保系统的稳定性和可持续性。未来，随着技术的进步，楼宇智能化系统的安全防护策略将更加科学和高效，为智能建筑的发展提供有力保障。

参考文献

[1] 厉明,张立博,刘广东.基于5G网络的智能化楼宇自动监控系统设计[J].微型电脑应用,2024,40(12):119-122.

[2] 王雷.楼宇智能化技术在智能建筑中的应用研究[J].智能建筑与智慧城市,2024,(11):138-140.

[3] 付海立.基于楼宇智能化监控系统的施工重点研究[J].工程建设与设计,2024,(12):90-92.

[4] 赵毅.智能楼宇中的自动化技术应用[J].电子技术,2023,52(09):188-189.