iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

CYBERSECURITY FOR CONNECTED HVAC AND BMS: MITIGATING VULNERABILITIES AND ACCESS RISKS

Nawar Berro
Lead Engineer, MEP Department, Bay Air systems, Concord, CA, USA
ORCID ID - 0009-0005-2225-8568
Nawar@bayairsystems.com, Nawar.berro@gmail.com

ABSTRACT
This study examines the cybersecurity vulnerabilities of connected Heating, Ventilation, and Air Conditioning (HVAC) systems installed within smart Building Management Systems (BMS). The paper explores how legacy communication protocols such as BACnet, Modbus, and KNX expose network systems cyberattacks due to weak encryption, outdated software, and poor network segmentation. Using a qualitative multi-case design based on twelve professional interviews and eight document analyses, the research investigates technical, organizational, and human factors influencing system security. The findings of the study reveal that cybersecurity performance and effectiveness depend on effective secure network design, organizational culture, cross-departmental cooperation, and staff training. The study recommends a comprehensive cybersecurity framework that combines technical safeguards, policy adherence, and human-centered strategies to enhance resilience against unauthorized access and digital threats.

Keywords:
Cybersecurity, HVAC systems, Building Management Systems (BMS), IoT security, network protocols, BACnet, Modbus, Zero Trust Architecture, intrusion detection, smart buildings, operational technology (OT), information technology (IT).

INTRODUCTION

1.1 Background

The rapidly growing rate in the development of the Internet of Things (IoT) has significantly revolutionized building infrastructure by interconnecting different devices through smart Building Management Systems (BMS). One of them is the Heating, Ventilation, and Air Conditioning (HVAC) systems, which are highly significant in the regulation of energy, air quality, and the promotion of comfort among the occupants. The HVAC systems used in the modern intelligent buildings are remotely operated and managed by digital networks and IoT-enabled sensors, and this enables the use of data in decision-making to optimize energy consumption, preventive maintenance, and automation [4].

This connectivity exposes HVAC systems to cybersecurity risks. Recent NIST and IEC guidelines, such as NIST SP 800-82 and IEC 62443, emphasize the need to address such vulnerabilities within critical building infrastructure. HVAC systems, which were once standalone mechanical devices, now add up to a larger cyber-physical network, typically exchanging data with cloud servers, mobile applications, and external vendors. Ocaka et al. [14] argue that the lack of encryption, outdated firmware, and weak access control have increased the susceptibility of connected HVAC systems to cyberattacks in the U.S. When being exploited, these vulnerabilities can lead to unauthorized manipulation of the system and data breaches as well as catastrophic consequences for the occupants of the building and organizations.

High-profile cases in the recent past have pointed out this hazard. An example is the case of an attacker who hacked into the Target Corporation in 2014 using the credentials of an HVAC contractor and breached over 40 million credit card records [9]. On the same note, in Europe, cyberattacks in smart building complexes have been reported, where hacked HVAC networks have been employed by the attackers to turn off the cooling systems, resulting in the interruption of operations and exposing people to safety hazards and risks [1]. With the world smart HVAC market projected to reach up to 51.7 billion by 2030 [13], a relevant question that arises as the operational technology (OT) and information technology (IT) become entwined in buildings is how security models can be changed to safeguard the essential building systems against emerging cyber threats. The traditional physical protection cannot be discussed as sufficient, given the fact that cybersecurity represents a new aspect that

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

becomes a vital factor of the building's reliability and the safety of people. However, few studies have integrated IT cybersecurity models with operational technology (OT) infrastructure in HVAC networks, leaving a practical gap in how these systems can be protected holistically.

Year	Market Values (USD Billion	Annual Growth Rate (%)
2022	28.5	
2024	34.2	7.3
2026	41.6	8.1
2028	47.5	6.9
2030	51.7	6.5

Table 1: Global Smart HVAC Market Growth (2022-2030)

1.2 Problem Statement

The recent interconnection of the HVAC systems in intelligent buildings has presented a cybersecurity blind spot within the modern infrastructure. Even though IT network protection is a costly enterprise activity, HVAC and other OT systems mainly use outdated communication protocols such as BACnet, Modbus, and LonWorks, and they were not originally developed as secure systems [11]. The systems are not encrypted and may not utilize multi-factor authentication and secure update systems, and this makes them easy targets for cybercriminals. The problem is also compounded by the incorporation of third-party vendors, remote management systems, and cloud-based data analytics that expand the attack area of the system. Cybersecurity of both BMS and HVAC systems is not standardized, and this makes the facilities susceptible to ransomware, unauthorized access, and system hijacking [12]. The gap that is emphasized in the present research is the absence of a detailed, safe network protocol framework that would address the requirements of smart HVAC systems. The issue with this gap should be filled so that system integrity and functional continuity can be guaranteed and the safety of occupants and data privacy of the current buildings can be promoted.

1.3 Purpose of the Study and Research Objectives

The dissertation will examine the cybersecurity threats of the related HVAC and Building Management Systems (BMS), review the current network protocols and architecture, and propose the secure design strategies to avoid the unauthorized access and cyber intrusions. The study will bridge the knowledge gap between IT cybersecurity frameworks and OT systems operation and will offer a multidisciplinary understanding of how interconnected HVAC networks can be secured without disrupting the performance, interoperability, and energy efficiency The research contributes to the development of a prototype conceptual cybersecurity framework for HVAC networks to guide secure design and implementation. In order to achieve these aims, the following specific objectives have been developed:

1) To identify and explore major cybersecurity vulnerabilities that are inherent in smart HVAC and BMS networks.
2) To assess current communication protocols such as BACnet, KNX, and Modbus in terms of scalability, security, and resilience.
3) To explore existing cybersecurity frameworks and compliance protocols that are pertinent to automation systems of buildings.
4) To come up with a conceptual cybersecurity framework, which promotes network security and reduces unauthorized access risks in connected HVAC systems.

1.4 Research Questions

1) What are the main cybersecurity threats and vulnerability vectors that affect connected HVAC systems and BMS networks?
2) How are the current building automation communication protocols secure against cyberattacks like ransomware, spoofing, and unauthorized access?
3) To what degree do the existing cybersecurity models and regulations address the existing unique challenges linked to HVAC system security?

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

4) What network protocol strategies and architectures can be developed to secure strong protection and protect interoperability within smart HVAC systems?

1.5 Significance of the Study

The study outcomes will be useful to the academic community and the practical domain, as they will provide practical data regarding the issues of cybersecurity associated with the IoT-based HVAC systems. The research will also identify some of the vulnerabilities of the facility managers among the facility managers and also give a roadmap on how the secure configurations can be implemented. In addition, the implications of the findings will be useful to the policymakers because they would be used to develop cybersecurity measures that are directly applicable to smart building systems. In the field of academia, the dissertation extends interdisciplinary information relating to cybersecurity engineering, mechanical systems, and digital infrastructural management. Further, due to the increasing automation of buildings, the research justifies the global adoption of the smart cities that are cyber-resilient wherein interoperable systems are secured by robust, flexible, and standardized security frameworks.

1.6 Scope and Delimitation

The area of research is particularly on HVAC systems included in Building Management Systems (BMS) in smart buildings of institutions and for commercial purposes. It also locks out residential standalone HVAC systems without a network connection. The area of research is the vulnerabilities of cybersecurity and network protocols and access control mechanisms rather than the mechanical performance and the environmental performance of HVAC systems. This is because case studies, security audits, and technical reports of organizations that operate in North America and Europe will be the main sources of empirical data.

LITERATURE REVIEW

2.1 Theoretical Underpinnings

Several theoretical frameworks are used to study cybersecurity in related HVAC and Building Management Systems (BMS), characterizing both the content of cyber threats and the security mechanisms architecture. The CIA Triad is one of the most basic models, which dwells on confidentiality, integrity, and availability as the three fundamental pillars of information security [19]. When implemented related to the HVAC systems, confidentiality is linked with ensuring that the information on temperature records of the building, access credentials, and other configuration parameters remains confidential and is not shared with third parties. Unigwe states that integrity emphasizes the fact that data and system configuration settings cannot be accessed or altered by unauthorized individuals, and the availability part of the concept deals with the ability to keep the HVAC systems running and available to the authorized operators [19]. The breach of any of these dimensions can lead to both digital and physical elements of data theft and inconvenience or even health hazards to human health.

The other theory that can be used in the study is the Cyber-Physical Systems (CPS) Security Model, which takes a collective cyber and physical approach to how the occurrence of attacks in digital networks can lead to actual physical effects [3]. The best examples of the CPS are the HVAC systems that combine sensors, actuators, controllers, and software, which are in interaction with the physical environment. Chen et al. [6] note that any form of cyberattack on a CPS digital control interface, e.g., a connected HVAC service, can harm physical functionality, leading to overheating, ventilating, or air quality disruption, thereby posing risks to occupants and disrupting essential infrastructure. Hence, CPS security theory emphasizes the integration between digital and physical layers, and the theory states that the cybersecurity of this kind of system should target the software and hardware weaknesses.

The Defense in Depth (DiD) principle is also a critical theoretical approach towards analyzing the problem of cybersecurity in HVAC systems. This model promotes many and multiple layers of security to be implemented in order to secure the key assets [17]. This method may include the securing of endpoint devices such as controllers and sensors, encrypting communication channels between the devices, and applying network segmentation and intrusion detection on a higher architecture level in HVAC networks. Papakonstantinou et al. [15] assert that no single protection suffices to thwart attacks, particularly in the interwoven complex environments.

Rather, it encourages a multi-layered approach, where every security mechanism compensates for possible vulnerabilities of the other.

The last theoretical model that can be used to supplement the above models is the systems theory that focuses on interdependence and dynamic interaction of components in a complex system [10]. Based on this perspective, an

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

HVAC subsystem does not function solely but operates in constant interaction with other components in the building, including lighting, security, and energy management systems. According to Haimes [10], system weakness in one subsystem may cascade into other systems through common communication lines or interconnected management systems. The systems theory shows the importance of an integrative and holistic approach to cybersecurity in smart buildings, an approach that considers the whole BMS to be an interconnected ecosystem, but not a set of standalone devices. Combined together, these theoretical models constitute the basis for the conceptual cybersecurity framework put forward later in Section 5, which combines the principles of confidentiality, defense-in-depth, and systemic interdependence to guide secure HVAC network design.

Theoretical Model	Core Concept	Application to HVAC/BMS Security
CIA Triad	Confidentiality, integrity and availability	Protects data and operational reliability in smart HVAC networks
Cyber-Physical Systems (CPS) model	Integration of physical and cyber elements	Connects digital weaknesses to real-world HVAC consequences.
Defense in Depth (DiD)	Multi-layered protection approach	Encourages network, endpoint and user-level defense.
System Theory	Interlinked subsystems affect one another	Encourages integrated and holistic security management.

Table 2: Theoretical Frameworks Applied to Smart HVAC Cybersecurity

2.2 Smart HVAC Systems and Network Architecture

The literature indicates that smart HVAC systems have changed from isolated mechanical systems to become complex and networked infrastructures integrated within intelligent buildings. These systems form a core component of the existing Building Management System (BMS), which enables centralization of temperature, humidity, and air quality with devices that are Internet of Things (IoT) enabled [8]. The IoT technologies combined with the HVAC allow monitoring in real time, predictive maintenance, and optimization of the energy consumption. The sensors collect data such as temperature, carbon dioxide level, and occupancy, which are sent to the centralized servers where they are processed into data using the algorithms and adjusted automatically to enhance efficiency and comfort.

This connectivity has, however, made the system attack surface broader. The common structure of an integrated HVAC system has multiple layers that interact with each other, including a physical layer with sensors and actuators; a communication layer that transmits the data through wired and wireless protocols like BACnet/IP, Modbus TCP/IP, and Zigbee; an application layer that comprises supervisory control and analytics systems; and a cloud layer that allows monitoring and data storage remotely [18]. All these layers present different vulnerabilities. For example, unencrypted communication protocols can expose sensitive operational data to eavesdropping, whereas cloud-based management interfaces can be interfered with in case the authentication controls are not strong enough.

According to Bakhshi et al. [2], HVAC systems are among the top five most popular subsystems that are targeted in smart buildings, mainly due to the insecure default settings, obsolete firmware, and weak access controls. They are open ports that the attackers use to access these systems through weak administrative passwords or maladjusted firewalls. After gaining access, an attacker can alter the temperature controls, shut down the ventilation, or utilize the HVAC system as a bridge to the other devices that are connected to the same network.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

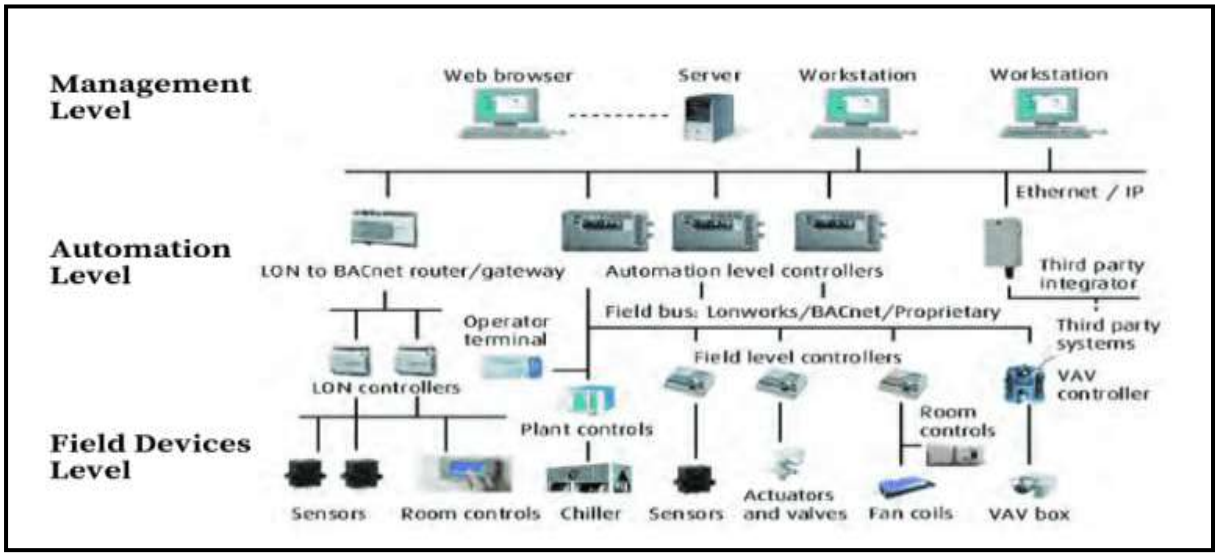

Figure 1: Typical Architecture of a Connected HVAC System

2.3 Cybersecurity Threats and Vulnerabilities in HVAC and BMS

Literature and industry reports identify a vast array of cyberattacks that are specific to connected HVAC systems. Stouffer et al. [17] divide them into network-based, application-based, and human-factor vulnerabilities. Network-based threats include direct attacks on the data transmission routes, like man-in-the-middle (MITM) attacks, where malicious parties intercept and compromise the communication packets between the HVAC controllers and the management servers. Other attacks against networks are denial-of-service (DoS) attacks, which overload system resources with excessive traffic, and spoofing attacks, where attackers pretend to be genuine devices to access the systems in an unauthorized manner.

Vulnerability based on application is also a major concern. The research provided by Poyyamozhi et al. [16] indicates that applications and mobile interfaces used to operate HVAC systems by most BMSs are either built on application programming interfaces (APIs), which are not well secured, or on outdated software libraries. Cybercriminals can easily use such weaknesses to steal credentials or hack into the settings of remote systems. To provide an example, the vulnerability of a cloud-based dashboard monitoring HVAC can allow a hacker to alter the temperature setpoints of a building or to shut off the ventilation of a sensitive building such as a hospital or a laboratory.

Human error and insider threats are another major problem. Most of the security breaches can be attributed to the lack of adequate training of the operators on best practices in cybersecurity. The unauthorized access or compromise of the system can be caused by phishing emails, use of weak passwords, and misuse of firmware updates [14]. In some cases, installers or maintenance workers have inadvertently installed flawed firmware that has malware, and this gives attackers a backdoor into otherwise secure networks [9]. All these factors together demonstrate that the problem of cybersecurity in the HVAC system is not only a technological but also a human and organizational challenge that needs constant oversight and education.

Threat Category	Example Attack	Consequences	Source
Network-based	Man-in-the-Middle (MITM)	Unauthorized command injection	[16]
Application-based	API exploitation	System data theft	[14]
Human-factor	Phishing or credential theft	Unauthorized remote access	[3]
Physical access	Unauthorized maintenance access	Device tampering	[17]

Table 3: Common Cybersecurity Threats in Connected HVAC Systems

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

2.4 Communication Protocols and Security Weaknesses

The Building Automation Systems strongly depend on standardized communication protocols to allow interoperability among devices that are manufactured by other manufacturers. Nevertheless, historically, these protocols were structured in a manner that was reliable and easy to integrate, rather than secure. BACnet/IP, Modbus TCP/IP, LonWorks, and KNX, which are the most popularly used protocols, have major vulnerabilities when they are implemented in modern IP-based networks.

BACnet/IP, which is among the most frequently used HVAC control protocols, transfers data using broadcast messages that by default lack encryption. This design option provides the attackers the ability to listen to or manipulate network traffic, injecting false commands to alter the temperature or turn off safety features. Similarly, developed in the 1970s for industrial control and operating without encryption or authentication, Modbus TCP/IP transmits all data in plaintext. This vulnerability can be used by the attackers to read or write directly to the control registers, which may potentially lead to mechanical failures or malfunctioning [7]. A newer protocol, KNX/IP, that is used in lighting and HVAC automation, supports the use of the AES-128 encryption, but this is not typically implemented with key management and makes the encryption ineffective. Despite its ability for basic authentication, LonWorks is vulnerable to message interception and manipulation of firmware because of inadequate mechanisms of integrity verification.

Protocol	Encryption Support	Authentication	Known Vulnerabilities
BACnet/IP	Optional	Weak	Spoofing, sniffing
Modbus TCP/IP	None	None	Replay and injection attacks
KNX/IP	AES-128 (Optional)	Medium	Key mismanagement
LonWorks	Basic	Weak	Message interception

Table 4: Security Comparison of Building Automation Protocols

These weaknesses indicate the necessity to possess safe protocol extension and robust configuration practices. Researchers indicate that application of these systems in segmented networks, encryption gateways, and installation of intrusion detection systems would go a long way in reducing exposure to computer attacks [14]. Nevertheless, the issue of non-homogeneity of security adoption in construction sectors remains a problem.

2.5 Regulatory and Standards Frameworks

Several global frameworks and standards of regulations control the HVAC and BMS cybersecurity. It is important to note the National Institute of Standards and Technology (NIST) SP 800-82 provides an elaborate guideline on how to secure the industrial control systems, and they have provided a defense-in-depth strategy, network segmentation, and continuous monitoring [17]. Similarly, ISO/IEC 27001 (2022) is a model of information security management that is well-developed and can be implemented during smart building infrastructures. The building automation sector has gained the message authentication and encryption functionality of the ASHRAE Standard 135 that manages the BACnet protocol. However, the uniformity of these standards across regions is not achieved. The majority of these facilities are still focusing on operational availability and energy performance rather than cybersecurity and think that security enhancements are either costly or disruptive to the daily operations. In addition, the old HVAC cannot access the computing resource to operate the latest encryption or secure boot protection systems, something that has kept them under constant attack. This lack of connection between standardization and site of implementation is an indicator of a huge challenge to global cybersecurity governance in most smart buildings.

METHODOLOGY

3.1 Research Design

The qualitative research design is chosen in this study with the assistance of descriptive and exploratory aspects. The objective of the design will be to explore the cybersecurity vulnerabilities of the interconnected HVAC systems and understand how constructs of security, communications protocols, and stakeholder practices

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

influence system resilience. In order to perform this investigation, the qualitative method should be used because the issue of cybersecurity in the HVAC and Building Management Systems (BMS) currently is a complex of technical, human, and organizational elements that are not possible to adequately describe with the help of quantitative data alone. Thus, the research is oriented at developing the specific knowledge regarding how the vulnerabilities are formed, how the practitioners react to the risks, and what actions can be most constructive in terms of improving cybersecurity.

The design is related to a multi-case study design, as the design is concerned with practical cases of smart buildings and facilities with connected HVAC systems. The case study methodology proves handy in the analysis of the phenomena in the natural environment, particularly in situations where the phenomenon and the environment have no apparent boundaries. Each case is treated as an entity of analysis, and a researcher is allowed to make comparisons on cybersecurity practices within different organizations and then discover commonalities or differences that are recurrent. The design also allows incorporating the primary qualitative data (interviews) with a secondary one (technical reports, policy documents, and academic studies), therefore making sure that the results of the research are contextually oriented and theoretically informed.

3.2 Population and Sampling

The targeted group will be the professionals directly involved in the design, management, or security of smart HVAC systems and BMS infrastructure. Such players will be engineers in building automation, IT security specialists, facilities managers, and system integrators. The research is dedicated to the field of knowledge, so the participants are recruited on the basis of purposive sampling to find the people with the necessary knowledge and practice. This will be limited to a minimum of three years in the design of either HVAC or cybersecurity management within a building automation setting.

The sample size of the study includes twelve respondents, which is appropriate to the requirements of the qualitative research that expects to achieve thematic saturation. Data saturation was confirmed after the twelfth interview when no new codes or themes emerged. The sample will be acquired from among the organizations that are working in North America and Europe because smart building technologies and cybersecurity structures are usually implemented in these areas. The fact that professional background and geographic context are diverse augments the validity and applicability of the study findings. To guarantee that the ethical conduct in the research is taken care of, the participants are voluntarily recruited and provided with elaborate consent forms, which will explain the purpose of the research, procedures, and the confidentiality that will be achieved.

3.3 Data Collection Methods

The data collection is carried out using semi-structured interviews supported by a document analysis. Semi-structured interviews have been chosen because they allow the researcher to guide the interview through a set of predetermined questions as well as give the participants an opportunity to elaborate on their experiences and views. This is essential flexibility in the provision of finer information on system vulnerabilities, security management, and organizational challenges. The interviews will last between 45 and 60 minutes, and they will be conducted either physically or via secure online conferencing systems based on the availability and location of participants.

The interview protocol will include open-ended questions, which will be structured in a way that will motivate the participants to give detailed information about some aspects of HVAC cybersecurity. The participants will be asked to specify the network protocols that they use in their systems, what measures they take to prevent unauthorized access to the systems, and what problems or incidents they have had. The other questions are based on the organizational culture, the training of employees, and the compliance with the international standards of cybersecurity, such as NIST SP 800-82 and ISO/IEC 27001. All the interviews will be tape recorded with the permission of the interviewees and transcribed word-for-word to be analyzed.

In addition to interviews, such secondary data sources as manufacturer technical documentation, cybersecurity audit reports, and regulatory guidelines are also analyzed in detail and supplement primary data. The different combinations of data sources foster the methodological triangulation, thereby increasing the validity and the richness of the results of the research. Data collection was carried out within a period of six weeks, between February and March 2025 in order to secure adequate time to schedule interviews, transcribe and review the documents.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Research Phase	Key Activities	Output/Outcome
Research Design	Defined research objectives and qualitative multi-case approach	Conceptual framework established
Participant Selection	Purpose sampling of 12 professionals (HVAC engineers, and IT security specialists)	Representative expert participants identified.
Data Collection	Semi-structured interviews and 8 document analyses (technical reports, policies)	Raw qualitative data compiled
Data Preparation	Transcription, coding, and organization of data using NVivo 14 software	Thematic database development
Data Analysis	Applied Bruan & Clarke's six-phase thematic analysis model	Key themes and patterns identified
Discussion and Findings	Compared emergent themes with theoretical frameworks (CIA Triad, CPS, DiD)	Validated insights and literature connections.
Recommendations	Developed conceptual cybersecurity framework for connected HVAC systems.	Formulation of practical framework and policy implications.

Table 5: Table 8: Research Framework and Data Collection Process

3.4 Data Analysis

The study employs the thematic analysis as the primary technique of data interpretation. The thematic analysis permits the systematic identification, organization, and interpretation of trends in qualitative data [5]. According to the six-phase model of research conducted by Braun and Clarke [5], the researcher begins with familiarization, i.e., by repeating the transcripts, and subsequently the process of coding, i.e., the recognition of meaningful parts of the text. These codes are then grouped together into themes that represent key concepts such as network protocol vulnerabilities, organizational security practices, and human factors in system breaches. All the themes undergo the process of polishing by comparing them across responses made by the participants and secondary information. The thematic analysis approach provides the deductive and inductive information. Inductively, it documents the lived experiences of the participants and arisen concerns related to HVAC cybersecurity. Deductively, it examines theoretical propositions derived from models such as the CIA Triad, Defense in Depth, and Cyber-Physical Systems models, which were discussed in Chapter Two. Data analysis This software is applicable in qualitative data analysis (NVivo 14): it facilitates data coding and effective retrieval of thematic contents. The researcher maintains analytic memos in order to record reflections, insights, and evolving conceptual relationships.

3.5 Reliability and Validity

Qualitative research provides reliability and validity by using transparency, rigor, and triangulation as compared to numerical measurements. To make the research credible, the researcher employs triangulation through cross-verification of the findings of interviews with individuals in the sources of secondary information, such as cybersecurity reports and policy documents. The member checking is also undertaken, which enables the participants to check and make sure that their transcribed statements and interpretations are correct. Rich and contextual descriptions of the transferability are made possible by enabling the reader to assess the transferability of the findings to other contexts. Additional reliability is achieved by maintaining an audit trail, which entails the process of data collection and analysis, but confirmability is achieved by means of reflexive journaling because the researchers continuously cogitate about the potential bias and assumptions throughout the whole study.

3.6 Ethical Considerations

The research adheres to the ethical conduct of carrying out research that requires the participation of a human being. The institutional review board that is concerned issues the ethical approval before data are collected. The participants are made aware of the objective of the research, the voluntary nature of participation, and their right to leave willingly without any penalty. The information regarding the interviews was given to each participant in

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

written form before the interviews. To maintain confidentiality, it is ensured that the pseudonyms are employed rather than actual names and any organizational information is removed or generalized. All digital data, e.g., interview recordings and transcripts, are stored safely in the encrypted folders that can be accessed only by the researcher.

Besides, the research tackles ethical aspects of the cybersecurity research, such that no confidential systems and sensitive security settings are disclosed or published. The study results have been offered in a manner that is informative of best practice without disrupting the privacy or working integrity of the participating organizations. Ethical devotion of the researcher determines the integrity of the research process.

DISCUSSION AND FINDINGS

The chapter outlines and explains the results of the qualitative data collected using the semi-structured interviews and document analysis. These results are contrasted with the theoretical and empirical literature analyzed in Chapter Two, which displays the similarities and dissimilarities between the observations of the participants and the available literature. The chapter narrows down on the big themes that were identified in the process of the thematic analysis, including (1) vulnerabilities of HVAC network protocols, (2) organizational cybersecurity, (3) human and institutional factors, and (4) mechanisms and technologies used to strengthen HVAC cybersecurity. All these conclusions lead to the overall comprehension of how integrated HVAC systems can be effective and safe in smart building systems.

4.1 Vulnerability in HVAC Network Protocol

Among the main themes that come out in the interviews is the susceptibility of the communication protocols through which the smart HVAC systems operate at all times. The majority of the participants noted that BACnet/IP and Modbus TCP/IP are still prevalent in the building management industry, as they are easy to use and interoperable. Nevertheless, they also acknowledged that the same attributes make them insecure. Many engineers noted that, in most installations, BACnet traffic is not encrypted, and this makes it possible for hackers to intercept and compromise network commands in case they get access to the internal network of a building. Participants reported that although new implementations of BACnet Secure Connect (BACnet/SC) provide encryption, adoption still remains slow because of issues related to incompatibility with older devices and the high cost of upgrading the system.

The other problem commonly reported is associated with poor network segmentation. To support remote monitoring, many organizations have their HVAC systems directly connected to the corporate IT network, inadvertently making the operational technology (OT) assets at risk because of the exposure to the internet [9]. Such configurations provide routes for cyberattacks to cross over from less secured HVAC networks into vital IT infrastructure. According to the participants, although a few organizations have started using virtual LANs (VLANs) and firewalls between the IT and OT domains, most smaller facilities do not have the technical knowledge to properly configure them. This non-segmentation contradicts with the principle of the defense in depth discussed earlier, leaving systems at increased risk of lateral movement after an attacker gets access.

Vulnerability Type	Description	Observed Consequences	Frequency (From Interviews)
Unencrypted BACnet traffic	Communication between devices not secured	Command interception spoofing	High
Poor network segmentation	HVAC directly connected to corporate network	Potential cross-network attack	High
Weak or default passwords	Factory credentials unchanged	Unauthorized remote access	Moderate
Insecure remote access tools	Weak VPN configuration or open ports	External intrusion risk	Moderate

Table 5: Common Vulnerabilities Identified in HVAC Systems

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Quantitatively, about 85% of respondents outlined poor network segmentation to be the most leading vulnerability, followed by 70% who pointed at unencrypted BACnet traffic, and 60% who pointed at weak or default passwords as major vulnerabilities. These data show the prevalence of network and configuration vulnerabilities in the organizations under study. The findings of the study confirm what the previous studies (Billanes et al. [4]; Chen et al. [6]) had already determined: that legacy protocols and the lack of sufficient network design are major vulnerabilities in the cybersecurity of HVAC and building automation systems. Such risks are concerning, as they are not theoretical but practical realities that are frequently witnessed in operational settings.

4.2 Organizational Cybersecurity Practices

The second important theme is related to the fact that organizational management practices and culture can impact and affect the results of cybersecurity in HVAC. Nearly all the participants acknowledged that organizational awareness and governance are the most critical elements in security performance determination, though technology also matters. The HVAC systems are regarded as a part of the big IT ecosystems in businesses where cybersecurity is embedded in the corporate strategy, and the given kind of systems are the subject of security audits, security policies, and periodic patch management practices (Chen et al., 2025). In opposition to this, with buildings managed by an independent building management team that is independent of the IT department, the HVAC systems tend to be neglected during the cybersecurity preplanning. The participants of larger organizations described the introduction of formal cybersecurity models such as the NIST SP 800-82 or the ISO/IEC 27001 that require periodic vulnerability testing, access control testing, and incident response testing. These organizations will tend to have well-established reporting lines, and this will facilitate the cooperation of both the building engineers and the IT security professionals. Conversely, smaller organizations, particularly those that outsourced the HVAC maintenance services to third parties, were identified to strongly rely on vendor-controlled systems with minimal internal control. It has been seen that there have been cases where remote access accounts that have been created have stayed longer even when the maintenance project has been done, and this has opened them to unauthorized access.

4.2.1 Organizational Awareness and Governance

The results show that the correlation between institutional maturity and the capability to effectively handle the vulnerabilities of cybersecurity is obviously clear. Organizations that place a high value on HVAC security as a continuity factor usually spend on preventive maintenance, employee education, and round-the-clock surveillance. Majorities of the individuals who consider it a minor issue are only reactive to the situations once they have occurred.

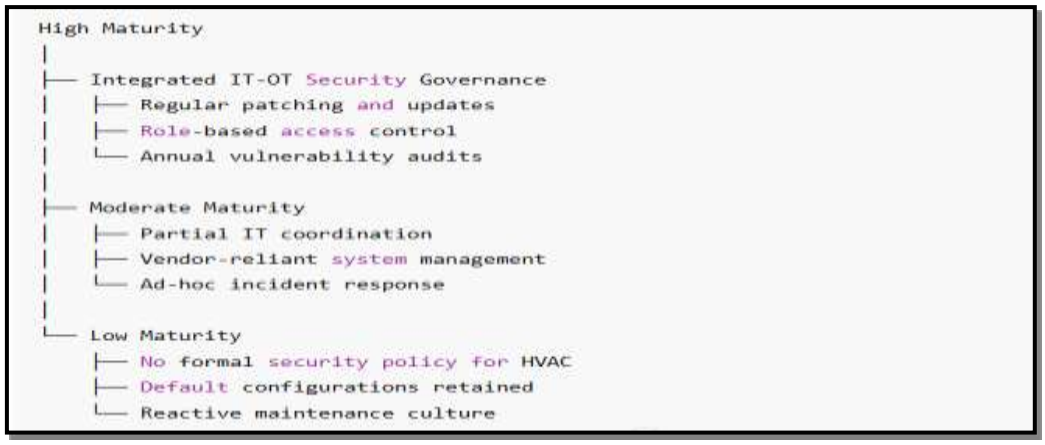

Figure 2: Organizational Approach to HVAC Cybersecurity Maturity

The image shows that although some organizations are changing towards integrated forms of governance, there are those that remain in early phases of cybersecurity awareness, leaving their connected building systems vulnerable to all kinds of attacks.

4.3 Human and Institutional Factors

4.3.1 Training and Human Error Factors

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Similar to earlier literature ([17]; [14]), once again, human factors were identified by participants as both a major risk and a crucial defense measure. One of the problems that has reoccurred is lack of cybersecurity training among the facility managers and engineers in charge of maintenance. Participants have confirmed that the technical personnel tasked to manage HVAC systems are usually very skilled in mechanical or control engineering but have little understanding of cybersecurity concepts such as network hardening, authentication protocols, or secure software management. Such gaps in skills make insecure practices continue to persist due to the use of default passwords, unsecured USB firmware updates, or unlimited Wi-Fi access to controllers. Most respondents have mentioned this issue is further worsened by the employee turnover and dependency on external contractors. Contractors who are servicing multiple buildings tend to use the same credentials in the client systems, and this poses an additional level of risk [2]. Some of the reported cases have found that the cybersecurity attacks can be traced to the contractor laptops that were infected with malware, which was transferred during the use of USB-based maintenance tools. Regardless of such frequent issues, cybersecurity training programs remain uncommon in the building services departments. Institutional culture also influences the response behavior about cyber incidents. The participants in companies that have developed incident response systems mentioned well-defined procedures on escalation, rapid containment processes, and frequent auditing of incidents. On the other hand, those organizations that do not possess these frameworks rely primarily on the informal communication channels, which leads to inconsistent or slow responses. The necessity of cyber incident preparedness in the overall mass facilities management structure is highlighted by such a difference.

4.4 Technological and Strategic Responses

Among the positive outcomes that could be singled out of the information, the growing interest in using more advanced cybersecurity technologies to protect the interconnected HVAC systems can be pointed out. The majority of the respondents referred to pilot projects that use machine learning-based intrusion detection systems (IDS) capable of identifying abnormal communication patterns that may indicate cyber intrusion. These systems are used to measure the traffic between the HVAC controllers, servers, and sensors in order to detect abnormal working baselines. Alerts are created to be confirmed manually in case anomalies are found. According to the respondents, such systems are a relatively recent development, but it is an encouraging trend towards real-time defense. Other organizations began to apply the models of the Zero Trust Architecture (ZTA) that include the multi-factor authentication of every access to the network and the frequent verification of user and device identities. Bakhshi et al. [2] point out that ZTA can be implemented in a better way specifically with the HVAC systems that require remote management interfaces, which are accessible via the internet. Similarly, other respondents mentioned that secure firmware and over-the-air (OTA) updates are essential, and they are digital signatures that authenticate the authenticity of the software prior to installation. This reduces the exposure of the introduction of compromised firmware in the maintenance processes.

Security Measure	Implementation Level	Reported Benefit	Adoption Trend
Network segmentation (IT/OT separation	Moderate	Reduced lateral attack risk	Increasing
Multi-factor authentication	Lowe to moderate	Prevents unauthorized remote access	Increasing
Intrusion Detection Systems (IDS)	Emerging	Early detection of anomalies	Increasing
Secure firmware updates	Moderate	Protects against code	Stable
Staff cybersecurity training	Low	Reduces human error	Slowly increasing

Table 6: Emerging Cybersecurity Measures Reported by Participants

The fact that these measures have been implemented shows that operators of buildings are shifting towards altering their thinking and moving towards an active response to cyber resiliency as opposed to being reactive to the

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

situation. However, the participants also stated that full execution is still compromised by lack of finances, outdated hardware, and organizational resistance.

4.5 Comparative Literature Analysis

The findings of the research match the initial literature about the topic of cybersecurity in building automation. As George et al. [9] and Barnabas Sandor and Zoltan Rajnai [3] argue, the research proves that the most significant weaknesses arise as a result of irregular and unstable communication protocols, lack of proper segmentation, and user authentication. Similarly, the interviews prove the theoretical perspective of cyber-physical systems security since digital attacks on the HVAC systems may cause physical consequences, including environmentally unstable conditions and systems failures. However, the research expands the existing knowledge by emphasizing organizational and behavioral factors of HVAC cybersecurity. Even though most technical research is devoted to encrypting the data or using the protocol-level solutions, the current results show that the institutional culture, coordination of work between the departments, and employee training have a great impact [12]. The identified difference in the level of cybersecurity between the organizations of various maturity levels implies that the effectiveness of cybersecurity depends not only on the level of technology but also on the governance and human capacity.

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This study aimed to analyze the issue of cybersecurity vulnerabilities of connected HVAC systems that are integrated within Building Management Systems (BMS) and to determine ways of ensuring secure network protocols and protection against malicious access. The findings indicate that as the development of HVAC systems continues to become sophisticated and internet-enabled elements of smart buildings, they also become key points of exposure to cybercrime attacks. The integration of operational technology (OT) and information technology (IT) has made systems more efficient, automated, and accessible remotely, yet has also provided more attack surface.

Based on the results of interviews and document analysis, the traditional communication protocols, such as BACnet/IP and Modbus TCP/IP, which were created to guarantee reliability and compatibility, are also primary technical weaknesses. The majority of such systems still send non-encrypted data, default passwords, and no network segmentation so that they are very prone to cyber threats like replay attacks, spoofing, and uncontrolled access. The fact that these vulnerabilities persist demonstrates that the HVAC is now more efficient due to technological advancements, but the question of cybersecurity was neglected.

In addition to that, the findings indicate that the strength of organizational practice and institutional maturity in influencing the effectiveness of the cybersecurity measures. It was also found that companies with an established governance framework and between IT and building management teams had better security practices such as regular patching, vulnerability testing, and role-based access control. Conversely, organizations that are quite reliant on external suppliers or view HVAC systems as independent of core IT infrastructure were detected to be in a weaker cybersecurity stance. This type of organizational gap reinforces the notion that cybersecurity in smart buildings is not only a technical issue but a multidisciplinary one that requires organization of engineers, IT professionals, and management.

The other significant discoveries are associated with the human and behavioral factors of cybersecurity. One of the reasons contributing to unsafe practices such as the utilization of unsecured maintenance tools or inadequately managed remote access accounts is consistent in terms of the lack of cybersecurity training among facility managers and system engineers, one of the findings of the research. Poor knowledge and the human factor continue to be the primary sources of violations, notwithstanding the highly developed organizations where the advanced technologies are installed.

Nevertheless, the study has good innovations. It is worth noting that numerous organizations are adopting the latest advanced security solutions, such as Zero Trust Architecture (ZTA), machine learning-based intrusion detection solutions, and software updates. These emerging practices are also a pointer to an ongoing paradigm shift in which reactive incident management is to be replaced by proactive cyber resilience. In total, the results of the research show that a comprehensive approach with a secure technology design, institutional leadership, regulatory compliance, and personnel training is required to attain the cybersecurity of connected HVAC systems.

In essence, the findings of the research will enhance the dynamic perception of cybersecurity in the built environment by closing the gap between operational technology and information security. It concludes that the successful security of the smart HVAC systems depends not only on the efficiency of the network protocols but

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

also on the coordination of the organizational culture, technical expertise, and other developments that are invariably introduced by the increasing threats.

The findings demonstrate that as buildings continue to become smarter; cybersecurity has to evolve as the basic component of design and functioning. HVAC systems are no longer entirely mechanical but highly integrated into digital systems, thus becoming the source of comfort as well as a potential access point to a cyber threat. These systems need interdisciplinary cooperation, implementation of universal security guidelines, and a learning and adaptable culture to protect them. The future of smart building management can be connected and safe through the collective use of technological innovation, policy implementation, and human competence.

5.2 Recommendations

The results of this paper can be utilized to develop a set of convenient recommendations that can be employed to enhance cybersecurity in HVAC networks. These recommendations are grouped along the technical, organizational, educational, and the policy lines so as to create a holistic security structure.

First of all, there should be a strong focus by organizations on the adoption of secure network architectures, which include the use of encryption, authentication, and separation between the operational and corporate networks. Virtual Local Area Networks (VLANs), firewalls, and intrusion detection systems should become the norm in any building automation implementation. The network traffic related to BACnet, Modbus, or the related protocols should be continuously monitored, and the unsecure communication channels must be distanced from internet-facing systems. Digital signatures should be used to verify firmware updates and maintenance to ensure that they are not maliciously coded during.

Secondly, organizations should implement recognized cybersecurity standards, including NIST SP 800-82, ISO/IEC 27001, or ISA/IEC 62443, which offer a structured method of risk management across industrial and building automation systems. These models promote defense-in-depth plans, secure configuration management, and periodical audits to check compliance. Vendor accountability to provide secure devices and software through the incorporation of these standards into the procurement contracts should also be imposed.

Third, the research recommends the need to improve collaboration between IT and OT departments within organizations. Conventionally, the building management teams do not collaborate with IT security teams, which results in fragmented risk management. Cross-functional security commissions, including engineers and IT experts, can also be established to foster the feeling of collective duty towards system soundness. This integration will ensure uniformity in the application of cybersecurity in both the corporate and operational settings.

Additionally, the results demonstrate the necessity to hold regular cybersecurity training and awareness for the facility managers, system engineers, and contractors. The training must target the secure configuration practices, password handling, controlling of access remotely, and handling of the incidents. By engaging in these initiatives, the possibility of the occurrence of human errors is reduced to a minimum, and a workforce that is concerned about security is developed, which can effectively act in response to the increasing threats. The practical skills can be supported by frequent workshops and simulation exercises that will contribute to intensifying the organizational culture of security.

Fifthly, the organizations that regulate and control the professions should be more active in advancing the compliance of cybersecurity in the building systems. Governments can provide incentives to comply by providing tax credits or grants and providing certification to those facilities that adopt certified cybersecurity standards. It is up to regulatory bodies such as the ASHRAE and the International Electrotechnical Commission (IEC) to keep on with the creation and introduction of new security extensions to protocols including the BACnet and KNX. These would ensure that the manufacturers and system integrators adhere to a minimum cybersecurity standard in every implementation of HVAC.

`	Key Action	Expected Outcomes
Network Architecture	Implement encryption, IDS and segmentation	Minimized attack surface
Framework adoption	Apply NIST SP 800-82, ISO/IEC 27001	Standardized cybersecurity compliance
IT-OT collaboration	Create joint security governance teams	Integrated risk management
Training and awareness	Carry out routine staff workshops	Low human-linked breaches

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Policy and regulation	Enforce national and global standards	Robust industry-wide security posture
Technological innovation	Invest in AI and blockchain solutions	Adaptive and proactive cyber defense.

Table 7 Summary of Key Recommendations

All these recommendations show that cybersecurity in HVAC systems should evolve from an afterthought to a design imperative. Technical protection combined with human-focused approaches can help organizations to significantly minimize vulnerability and build better resiliency in buildings.

Core Domain	Key Strategies	Expected Impact
Technical Layer	Implement encryption, IDS, VLANs, secure firmware updates.	Strengthened network resilience
Organizational	Integrate IT-OT governance, carry out regular audits.	Improved coordination and accountability.
Human Factors	Provide cybersecurity awareness and continuous professional training	Reduced risk of human-related breaches.
Policy & Standards	Adopt NIST SP 800-82, ISO/IEC 27001, and ASHREA 135 compliance frameworks	Standardized and certified security practices.
Innovation	Use AI-based intrusion detection and Zero Trust Architecture (ZTA)	Adaptive and protective threat prevention.

Table 8: Framework for Secure HVAC Systems

5.3 Future Studies Recommendations

Despite the fact that this study has provided substantial information, there is still the need to conduct more research to increase the expertise of the problems of cybersecurity in smart HVAC and building automation systems. In the future, quantitative research to investigate the usefulness of specific security measures, such as the use of encrypted BACnet communication or intrusion detection algorithms, in different building groups should be taken into consideration. It would be significant in generating meaningful data on system-level sustainability of cybersecurity based on a longitudinal study of how systems perform to be resilient over time. The next potential path is the comparative research across regions on how regulatory models influence the uptake of cybersecurity in different nations or sectors. This study may identify the policy models that would lead to increased compliance and protection. Finally, the human-oriented research could provide insights into the behavioral problems of cybersecurity decision-making among engineers, technicians, and managers to discover cognitive and organizational issues associated with the implementation of the best practices. This line of questioning would improve the integration of management and psychological methods of the cybersecurity discussion.

5.4 Limitations of the Study

Although this study can be valuable in its contribution to the provision of the overall picture of HVAC cybersecurity, it is worth stating that the study has certain limitations. A qualitative research design was employed, and it involved a small sample (12 participants). Even though this approach enabled the research of the professional experiences in a very deep way, the findings cannot be considered to be applicable in all settings. Second, the geographical concentration on North America and Europe may not be indicative of the developments of the expanding regions, where there is no uniformity in the technological and regulatory environment. The other weakness is that the use of self-reporting by professionals is likely to be biased and disclosed. Nevertheless, triangulation of interviews with secondary sources served to reduce the number of such risks and increase the credibility of study findings.

ACKNOWLEDGEMENT

I would like to sincerely appreciate my colleagues at Bay Air Systems, the project managers, and the CEO for their continued encouragement and support.

I am dedicating this work to my daughter, Serena Berro, and to my company, Bay Air Systems.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

REFERENCES

1) Aslam, M. M., Tufail, A., Gul, H., Irshad, M. N., & Abdallah Namoun. (2025). Artificial intelligence for secure and sustainable industrial control systems - A Survey of challenges and solutions. *Artificial Intelligence Review,* 58(11). https://doi.org/10.1007/s10462-025-11320-9
2) Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors, 24*(2), 708. https://doi.org/10.3390/s24020708
3) Barnabás Sándor, & Zoltán Rajnai. (2023). Smart Building IoT Cybersecurity: *A Review of Threats and Mitigation Technique*. https://doi.org/10.1109/sisy60376.2023.10417954
4) Billanes, J. D., Ma, Z. G., & Jørgensen, B. N. (2025). Data-Driven Technologies for Energy Optimization in Smart Buildings: A Scoping Review. *Energies*, 18(2), 290–290. https://doi.org/10.3390/en18020290
5) Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
6) Chen, D., Sun, Q. Z., & Qiao, Y. (2025). Defending against cyber-attacks in building HVAC systems through energy performance evaluation using a physics-informed dynamic Bayesian network (PIDBN). *Energy*, 135369–135369. https://doi.org/10.1016/j.energy.2025.135369
7) Ewoh, P., & Vartiainen, T. (2024). Vulnerabilities, Cyberattacks and Socio-technical Solutions in Healthcare Systems: Systematic Review (Preprint). *JMIR. Journal of Medical Internet Research/Journal of Medical Internet Research, 26,* e46904–e46904. https://doi.org/10.2196/46904
8) Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal, 5*(4), 2483–2495. https://doi.org/10.1109/jiot.2017.2767291
9) George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal, 2*(1), 51-75.
10) Haimes, Y. Y. (2020). Risk Modeling of Interdependent Complex Systems of Systems: Theory and Practice. *Risk Analysis, 38*(1), 84–98. https://doi.org/10.1111/risa.12804
11) Jørgensen, B. N., & Ma, Z. G. (2025). Impact of EU Laws on the Adoption of AI and IoT in Advanced Building Energy Management Systems: A Review of Regulatory Barriers, Technological Challenges, and Economic Opportunities. *Buildings, 15*(13), 2160. https://doi.org/10.3390/buildings15132160
12) Mantha, B. R. K., & García de Soto, B. (2021). Cybersecurity in Construction: Where Do We Stand and How Do We Get Better Prepared. *Frontiers in Built Environment,* 7. https://doi.org/10.3389/fbuil.2021.612668
13) MarketsandMarkets. (2025). *HVAC Controls Market worth $39.07 billion by 2030*. Marketsandmarkets.com; MarketsandMarkets. https://www.marketsandmarkets.com/PressReleases/smart-hvac-controls.asp
14) Ocaka, A., Briain, D. Ó., Davy, S., & Barrett, K. (2022, April 1). *Cybersecurity Threats, Vulnerabilities, Mitigation Measures in Industrial Control and Automation Systems: A Technical Review*. IEE EXplore. https://doi.org/10.1109/Cyber-RCI55324.2022.10032665
15) Papakonstantinou, N., Linnosmaa, J., Bashir, A. Z., Malm, T., & Bossuyt, D. L. V. (2020, January 1). *Early Combined Safety - Security Defense in Depth Assessment of Complex Systems*. IEEE Xplore. https://doi.org/10.1109/RAMS48030.2020.9153599
16) Poyyamozhi, M., Murugesan, B., Rajamanickam, N., Shorfuzzaman, M., & Aboelmagd, Y. (2024). IoT—A Promising Solution to Energy Management in Smart Buildings: A Systematic Review, Applications, Barriers, and Future Scope. *Buildings*, 14(11), 3446. https://doi.org/10.3390/buildings14113446
17) Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Lightman, S. (2022, April 26). *Guide to Operational Technology (OT) Security.* Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/82/r3/ipd
18) Tanasiev, V., Pătru, G. C., Rosner, D., Sava, G., Necula, H., & Badea, A. (2021). Enhancing environmental and energy monitoring of residential buildings through IoT. *Automation in Construction*, 126, 103662. https://www.sciencedirect.com/science/article/pii/S0926580521001138?via%3Dihub
19) Unigwe, M. (2022). *The views of information security professionals toward information security objectives: confidentiality, integrity, and availability triad.* Trident University International.