Current Practices in BAS Security Management

Xinwen Fu*, Ziyue Vivian Tang†, Annabelle Cheng ‡, Qun Zhou Sun §
*University of Massachusetts Lowell; Email: xinwen_fu@uml.edu
† Emma Willard School; Email: ztang@emmawillard.org
‡ Neuqua Valley High School; Email: acgpsv8686@gmail.com
§University of Central Florida; Email: qz.sun@ucf.edu

***Abstract*—Building automation systems (BAS) are critical to the operation of modern buildings but are increasingly exposed to cybersecurity threats as connectivity expands. This paper presents the first ever survey of current BAS security management practices conducted with 10 building management practitioners. The survey examines organizational context, security governance, technical and operational controls, vendor management, incident response, and training. Our findings reveal significant gaps between threats and deployed protections, including limited use of secure BAS protocols, inconsistent patching and monitoring, weak vendor security requirements, and uneven incident preparedness and training. Budget constraints, legacy systems, and coordination challenges between facilities and IT teams are identified as key barriers. These results highlight the need for more systematic and coordinated approaches to improving BAS cybersecurity.**

I. Introduction

Buildings are critical infrastructure affecting our daily life. A building automation system (BAS) can be deployed inside of buildings and perform automated management of HVAC (heating, ventilation, air conditioning), lighting control, physical security such as access control, energy management such as metering, fire safety such as alarm integration, and vertical transport such as elevator. A typical BAS consists of three levels: the management level (e.g., control center), the automation level (e.g., controllers for scheduling), and the field level (e.g., sensors and actuators). BAS differs from smart home systems from many aspects. A BAS is a local, standards-based *industrial* control system designed to reliably monitor and control building services with deterministic and predictable behavior, decades-long operational lifecycles, and strong interoperability through protocols such as BACnet, BACnet/SC, KNX, Modbus, and LonWorks. By contrast, smart home systems are consumer IT products for individual end users. They may combine low-power wireless protocols (e.g., Zigbee, Z-Wave), WiFi/IP networking, and messaging protocols (e.g., MQTT), along with application-layer ecosystems (e.g., Google Home, Amazon Alexa, SmartThings, Matter, HomeKit) to prioritize convenience, cost efficiency, and ease of deployment.

However, BAS face growing cybersecurity threats in practice. In 2016, a Mirai botnet distributed denial of service (DDoS) attack disabled heating systems in Finnish housing blocks [1]. In 2021, hackers locked out hundreds of building automation devices in a German firm by changing security keys on Internet-exposed devices [2], while engineering computers for BAS in Pakistan, Afghanistan, and Malaysia were compromised by the ShadowPad backdoor [3]. In January 2024, malware exploiting the Modbus protocol caused over 600 apartment buildings in Ukraine to lose heat for two days, marking the first ICS (Industrial Control System) malware to physically disrupt operational technology via Modbus [4]. Johnson Controls reported a major ransomware attack against the Company's IT infrastructure in September 2023 that disrupted operations and caused about $27 million in losses. [5].

In this paper, we conduct a survey of current BAS security management practices to understand the gap between ever-increasing cybersecurity threats and the security measures implemented in BAS. Our survey captures multiple dimensions of building automation system (BAS) security practices, including the organizational context and characteristics of the BAS systems, such as the number and type of buildings managed and the protocols deployed; security governance and responsibility, including which teams or personnel oversee cybersecurity; technical and operational controls, such as network monitoring, patching, and access restrictions; vendor and third-party management, including policies, certifications, and remote access practices; incident response and training, covering formal plans, past incidents, and staff cybersecurity awareness; and finally, practitioners' perspectives and challenges, exploring the obstacles they encounter and their suggestions for improving BAS security.

We conducted the first ever survey with 10 qualified building management practitioners, and the results provide informative insights. Respondents manage a wide range of facilities and BAS functions, often across multiple buildings, and use diverse protocols spanning traditional BAS standards and IP-based IoT technologies. Governance of BAS cybersecurity is frequently shared between facilities and IT teams, yet significant gaps remain: many organizations lack formal security policies, risk assessments, regular patching, or comprehensive asset inventories. Internet connectivity is common, sometimes without sufficient segmentation or controls, and adoption of secure BAS protocols and monitoring remains limited. Vendor access is widespread, while enforcement of vendor security requirements is relatively rare. Incident preparedness and workforce training are also inconsistent, with notable portions of respondents reporting suspected incidents, missing response plans, or no cybersecurity training. Overall, practitioners identify budget constraints, legacy systems, and coordination challenges as major obstacles, and emphasize the need for system upgrades,

979-8-3315-7111-5/26/$31.00 ©2026 IEEE

increased investment, staff training, and stronger IT-facilities collaboration to improve BAS security.

II. Survey Questions

We design a survey that captures multiple dimensions of practice, including organizational context and BAS system characteristics; security governance and responsibility; technical and operational controls; vendor and third-party management; incident response and training; and practitioners' perspectives and challenges.

A. Organization and Systems Overview

We seek to understand the roles individuals play in building management. Accordingly, the first survey question is an open-ended item asking respondents to report their role or job title ("Your role / title"). The responses will enable us to characterize the range of roles and titles among building management practitioners.

In our second survey question, we aim to identify the "type of facility" using the BAS, recognizing that buildings may or may not employ BAS protocols.

- Office or commercial building
- Industrial facility
- Hospital or healthcare building
- University or campus
- Government or public building
- Residential complex
- Other

The question "Approximate number of buildings or sites under your management" is designed to capture the scope or scale of responsibility of the respondent in building management.

- 1
- 2–5
- 6–20
- More than 20

We aim to understand "What types of building automation systems are deployed in your facilities?" This question captures the specific areas or systems within buildings where BAS technologies are implemented.

- HVAC (heating, ventilation, air conditioning)
- Lighting control
- Access control / physical security
- Energy management / metering
- Fire safety / alarm integration
- Elevator / vertical transport
- Other

A building may implement multiple BAS protocols. The question, "Which communication protocols are used in your BAS networks? (check all that apply)," is designed to identify the prevalence of different BAS protocols in current practice.

- BACnet
- BACnet/SC
- KNX
- Modbus
- LonWorks
- MQTT / IP-based IoT protocols
- Not sure
- Other

B. Security Governance and Responsibility

The Internet is increasingly integrated into our daily lives, and remote building management is becoming more common. However, Internet technologies and building automation systems (BAS) rely on different protocols and require distinct expertise, such as IT and Operational Technology (OT), to manage effectively. It is critical to ensure that the appropriate personnel are responsible for managing the entire system. The question, "Who is primarily responsible for BAS cybersecurity in your organization?" is designed to capture this aspect.

- Facilities team
- IT / cybersecurity team
- Shared responsibility (joint IT + facilities)
- Outsourced to a service provider
- Not formally assigned

A policy provides guidance to personnel on required actions. The question "Do you have a documented BAS cybersecurity policy or procedure?" is designed to determine whether such a policy exists within the respondent's organization.

- Yes, organization-wide policy
- Yes, limited to certain systems
- No formal policy
- Other

Risk assessments and audits are common practices in IT security. The question, "Do you perform formal risk assessments or audits of BAS networks?" is designed to determine whether such practices are applied to building automation systems.

- Yes, regularly (annually or more often)
- Occasionally (every few years)
- Only after incidents or upgrades
- Never

C. Technical and Operational Controls

When a BAS is connected to the Internet, the potential attack surface increases significantly. The question, "How are your BAS networks connected to the corporate IT network or the Internet?" is designed to capture these connectivity practices.

- Fully isolated (air-gapped)
- Segmented with firewalls / VLANs
- Connected directly (shared network)
- Not sure
- Other

The question "Do you use any of the following controls? (check all that apply)" is designed to determine whether security controls are implemented to mitigate the attack surface.

- Network firewalls separating BAS from IT
- VPNs or secure remote access for vendors
- Multi-factor authentication (MFA)
- Network monitoring or intrusion detection
- Role-based access controls
- Patch and update management

- Physical access control to BAS hardware
- None of the above
- Other

With many BAS protocols offering secure versions, this question, "Do you use secure protocols such as BACnet/SC or encrypted communications for BAS traffic?", assesses whether such security measures are implemented in practice.

- Yes, fully implemented
- Partially (some systems)
- No, not supported
- Not sure

While network monitoring and intrusion detection are standard in IT, this question, "Do you monitor network activity or logs from your BAS systems?", captures whether such practices are implemented for BAS.

- Yes, integrated with IT security monitoring (e.g., SIEM)
- Yes, using a dedicated OT/BAS monitoring tool
- Basic manual log checks only
- No monitoring in place
- Other

Device firmware and management software often contain security vulnerabilities, and automatic patching is standard in IT security. This question, "How often are BAS devices or servers patched or updated?", assesses how regularly such updates are applied to BAS.

- On a scheduled basis (quarterly or more frequent)
- Occasionally (when vendor updates are available)
- Rarely (only during major upgrades)
- Never / not applicable
- Other

D. Vendor and Third-Party Management

The question "How do vendors or contractors access your BAS for maintenance? (check all that apply)" assesses how vendors or contractors access BASs, capturing both on-site and remote access methods and the associated security practices.

- On-site only
- Remote VPN access
- Cloud-based management portal
- Remote desktop or jump host
- Shared passwords or generic accounts
- Other

The question "Do you require vendors to follow any specific security policies or certifications (e.g., IEC 62443, BACnet/SC)?" assesses whether vendors are required to comply with specific security policies or certifications.

- Yes, formally required in contracts
- Recommended but not enforced
- No requirements
- Other

The question, "Do you maintain an inventory of all BAS devices and software versions?" assesses whether the organization keeps an up-to-date inventory, which is critical for risk assessment identifying the attack surface.

- Yes, complete and up to date
- Partial inventory
- No formal inventory
- Other

E. Incident Response and Training

The question "Have you experienced or suspected any cybersecurity incident affecting your BAS (e.g., unauthorized access, malfunction, ransomware)?" assesses whether the organization has experienced or suspected cybersecurity incidents affecting its BAS and the types of such incidents.

- Yes, confirmed incident
- Yes, suspected but not confirmed
- No incidents
- Prefer not to say
- Other

The question "Do you have an incident response plan that includes BAS systems?" assesses whether the organization has an incident response plan that specifically includes BAS systems when incidents occur.

- Yes, integrated with IT incident response
- Separate BAS-specific plan
- Not formally documented
- Other

Humans are often the weakest link in system security. The question, "Do facilities or building engineers receive cybersecurity training or awareness education?" assesses whether operational staff receive BAS-related cybersecurity training or awareness education.

- Yes, regularly
- Occasionally
- No training offered
- Other

F. Perspectives and Challenges

Practitioners working in the field often have the clearest understanding of security challenges. The question, "What are your top challenges in securing your BAS? (check all that apply)" identifies the primary obstacles organizations face in securing their BAS.

- Legacy / outdated devices
- Limited vendor support
- Budget constraints
- Lack of staff expertise
- Coordination between IT and facilities
- Difficulty applying patches or updates
- Other

Given their field expertise, the open-ended question, "What improvements would most help you strengthen BAS security?" captures practitioners' perspectives on enhancing BAS security.

III. Survey Results

Given that buildings are critical infrastructure, we do not describe the survey distribution sensitive information regarding

an organization's security. However, all respondents are qualified. The following section presents the survey results from 10 participants.

A. Organization and Systems Overview

Per our survey, the range of roles and titles among building management practitioners includes BMS Manager, Building Manager, Facility Manager, facilities maintenance/engineering personnel, Utilities Smart Infrastructure Director, information technology (IT)/cybersecurity personnel, third-party service providers or integrators, and building or property management personnel. Figure 1 shows the type of facility is very diverse and ranges from Office or commercial building to Residential complex. The personnel often manage more than one building, with 40% of respondents managing more than 20 buildings. Our survey shows that the types of managed BAS are highly diverse, ranging from HVAC systems to elevator and vertical transportation systems. Deployed BAS protocols are also very diverse and Figure 2 demonstrates they range from BACnet to MQTT/IP-based IoT protocols.

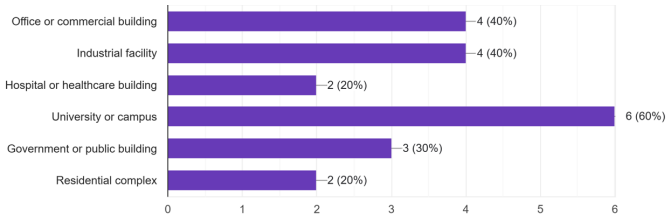

Fig. 1. Type of facility you manage

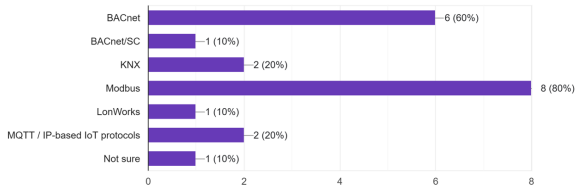

Fig. 2. Which communication protocols are used in your BAS networks?

B. Security Governance and Responsibility

Figure 3 shows that BAS cybersecurity governance often involves both facilities and IT/cybersecurity teams, with joint IT-facilities responsibility accounting for 50% of responses. Notably, Figure 4 indicates that 30% of respondents report having no formally documented BAS cybersecurity policy or procedure. Figure 5 shows that 20% never performed formal risk assessments or audits of BAS networks.

C. Technical and Operational Controls

Figure 6 shows that 20% of BAS are directly connected to the Internet, a risky practice, while 40% are connected via firewalls or VLANs. Figure 7 indicates that security controls are commonly adopted in BAS, although 10% of respondents report using none. Figure 8 reports only 10% of BASs fully implement secure BAS protocols. Figure 9 shows 20% of BASs have no monitoring in place. Figure 10 demonstrates that most BAS are not updated as regularly as IT-managed devices.

D. Vendor and Third-Party Management

Our survey shows that vendors or contractors can remotely access 60% of BAS for maintenance purposes and 40% use on-site maintenance only. Figure 11 shows that only 30% of respondents require vendors to follow specific security policies or certifications. Figure 12 indicates 50% of respondents maintain partial inventory of all BAS devices and software versions while 20% have no formal inventory.

E. Incident Response and Training

Figure 13 indicates that 50% of respondents report suspected but not confirmed incidents and 10% report confirmed incidents. Figure 14 shows that 30% have no formally documented incident response plan. Figure 15 demonstrates 20% of respondents receive no cybersecurity training or awareness education at all.

F. Perspectives and Challenges

Per Figure 16, top challenges in securing BASs are diverse, notably 60% report budget constraints. For improvements to most help strengthen BAS security, respondents report controller upgrades and training staff on cybersecurity best practices, increasing budget for upgrades, and enhancing collaboration between IT and facilities teams.

IV. Conclusion

This paper presented a the firsr ever survey of current building automation system (BAS) security management practices conducted with 10 qualified building management practitioners. The results reveal a clear gap between the growing cybersecurity threats facing BAS and the security measures implemented in practice, including limited adoption of secure protocols, inconsistent patching and monitoring, insufficient formal policies and asset inventories, and widespread vendor remote access with weak security enforcement. Organizational and human factors-such as budget constraints, legacy systems, lack of training, and coordination challenges between facilities and IT teams, further compound these issues. These findings underscore the need for improved governance, stronger technical and operational controls, enhanced workforce training, and closer IT-facilities collaboration to strengthen the security and resilience of building automation systems.

References

[1] L. Mathews, "Hackers use ddos attack to cut heat to apartments," Forbes, Nov 2016.
[2] "Cyberattacks shut down building automation systems," Veridify Security Inc., December 2021.
[3] "Attacks on industrial control systems using shadowpad," Kaspersky, June 2022.
[4] C. Vasquez, "Simple 'frostygoop' malware responsible for turning off ukrainiansâĂŹ heat in january attack," Cyberscoop, July 2024.
[5] M. Kapko. (2024) Johnson controls reports $27m hit from ransomware attack. Industry Dive.

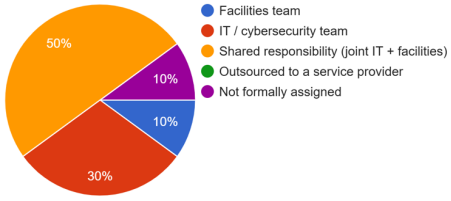

Fig. 3. Who is primarily responsible for BAS cybersecurity in your organization?

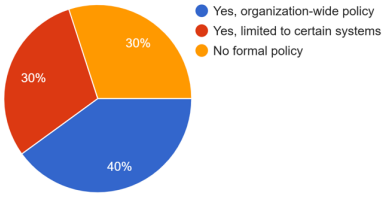

Fig. 4. Do you have a documented BAS cybersecurity policy or procedure?

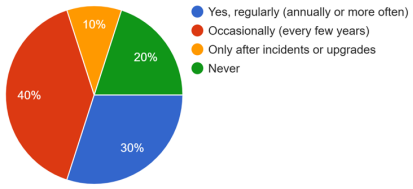

Fig. 5. Do you perform formal risk assessments or audits of BAS networks?

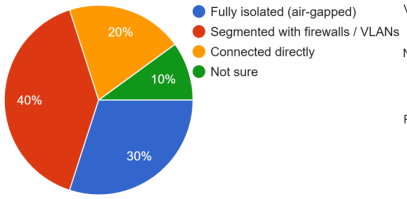

Fig. 6. How are your BAS networks connected to the corporate IT network or Internet?

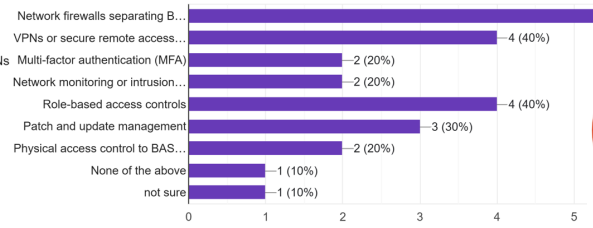

Fig. 7. Do you use any of the following controls? (check all that apply)

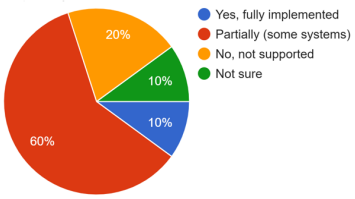

Fig. 8. Do you use secure protocols such as BACnet/SC or encrypted communications for BAS traffic?

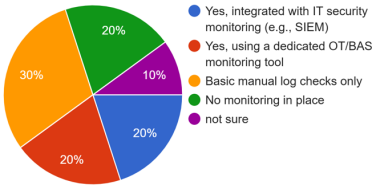

Fig. 9. Do you monitor network activity or logs from your BAS systems?

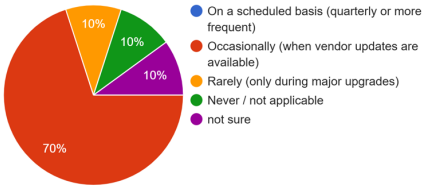

Fig. 10. How often are BAS devices or servers patched or updated?

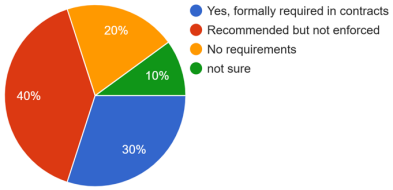

Fig. 11. Do you require vendors to follow any specific security policies or certifications (e.g., IEC 62443, BACnet/SC)?

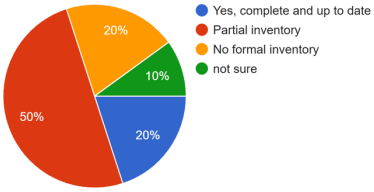

Fig. 12. Do you maintain an inventory of all BAS devices and software versions?

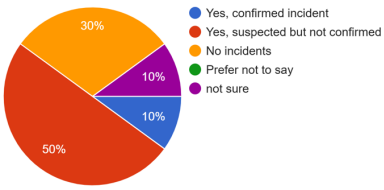

Fig. 13. Have you experienced or suspected any cybersecurity incident affecting your BAS (e.g., unauthorized access, malfunction, ransomware)?

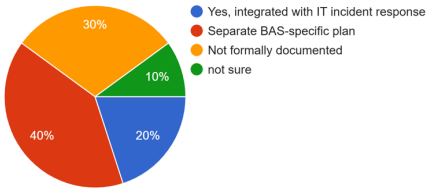

Fig. 14. Do you have an incident response plan that includes BAS systems?

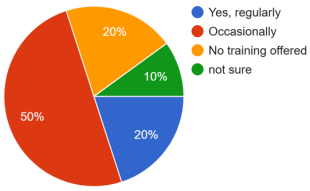

Fig. 15. Do facilities or building engineers receive cybersecurity training or awareness education?

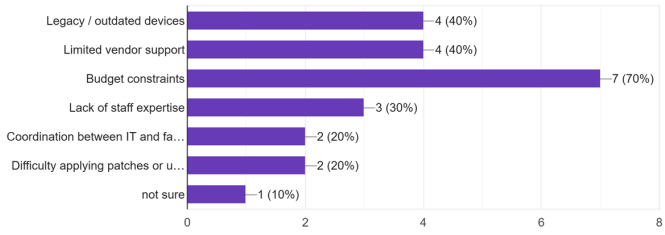

Fig. 16. What are your top challenges in securing your BAS? (check all that apply)