TIA

BRIEFING PAPER

SMART BUILDING CYBERSECURITY:

DESIGN APPROACH FOR MULTI-STAKEHOLDER ENVIRONMENTS

SMART BUILDING CYBERSECURITY:
DESIGN APPROACH FOR MULTI-STAKEHOLDER ENVIRONMENTS

AUTHORS:

Brian Ensign, Superior Essex

David Brearly, HDR

Gayla Arrindell, Corning

Jared Morello, Legrand

Jason Christman, Johnson Controls

Jon Williamson, Johnson Controls

Seth Ely, Stantec

Sudhi Sinha, UL

Terry Haley, Haley Solutions

Tim Koch, HDR

Travis Rosiek, BluVector, a Comcast Company

EXECUTIVE SUMMARY

Smart buildings encompass a greater number of connected systems and devices that provide data-driven insight and enable measurable information shared across multiple converged operational technology (OT) and information technology (IT) systems to increase efficiency, optimize operations, and enhance overall occupant productivity and wellbeing. As these systems converge via open, interoperable IP-based protocols to support smart building initiatives, they are increasingly at risk for cybersecurity and ransomware attacks that come with significant expense and the potential to halt facility operations and put lives at risk.

Stakeholder engagement during the early design phase of a Smart Building is vital to achieving owner and operator goals for efficient operations and improved occupant experience. All stakeholders must align to achieve a common vision by addressing the value and impact of smart building Technologies and balancing their expectations and responsibilities. This is critical to ensuring constructability, efficiencies, operability, and maintainability of smart building technologies to achieve and sustain return on investment (ROI). The same holds true for ensuring cybersecurity in the Smart Building.

This white paper describes proven processes for multiple smart building stakeholders to come together during the early design phase to achieve a common vision and parameters for improving cybersecurity. These processes engage all stakeholders in key design decisions that address Smart building technologies to identify normal operations, as well as define acceptable failure modes and cybersecurity requirements for each system and the building as a whole. Just as is required for meeting owner and operator goals for efficient operations and improved occupant experience, early engagement of construction entities across all building systems is vital to assessing constructability and identifying potential methods and value-engineered solutions to achieve cybersecurity goals.

TABLE OF CONTENTS

SMART BUILDING
CYBER ECOSTRUCTURE

The market for the global smart building environment is evolving with greater data-enabled and connected services that provide the next wave of digital innovation. This shift is fundamentally driven by increased convergence of historically isolated building systems and the demand for greater access to rich data sets. With this convergence comes a need to ensure a connected environment that is also secure from internal and external threats. In the same way that the IT cyber domain has evolved to address greater threat levels, a similar demand is increasingly evident in building OT environment as smart building critical systems and services become interconnected. According to a recent cyber threat report, the number of cyberattacks reached an all-time high in 2021 [1], and researchers found that of the 3,000 data leaks originating from ransomware attacks, more than 1,300 occurred on OT infrastructure [2].

With more IP-connected systems and devices and the convergence of IT/OT, a traditionally-closed, airgap approach is no longer acceptable. Just as the cyber-IT industry has shifted from reactive and perimeter-focused protection to zero-trust strategies, real-time threat intelligence, and a more cohesive security approach in response to expanding threats and sophisticated attack strategies, the OT industry must now develop new levels of active cyber defense.

[1] [18]. 2022 Cyber Threat Report, SonicWall -- https://www.sonicwall.com/2022-cyber-threat-report/

[2] [19]. Incident report, Mandiant -- https://www.mandiant.com/resources/ransomware-extortion-ot-docs

Smart Buildings are increasingly vulnerable to cyberattacks due to several reasons:

- Cyber threat actors are opportunistic and Smart Buildings will garner more of their attention.
- Smart Buildings have a high proliferation of OT and IT connected devices and systems that are increasing by the day.
- The higher diversity of technologies and connection methods in Smart Buildings increases the threat surface.
- To improve efficiency and reduce workforce requirements, Smart Building systems are increasing being monitored remotely, which further expands the threat surface
- Many OT building systems and networks use older technologies that do not have the foundational capabilities to implement current safeguards.
- The same level of scrutiny for cyber protection in IT networks is often not applied to building OT systems.
- Access to building systems is highly distributed and sometimes not properly controlled.

Smart building cybersecurity is implemented at multiple levels of the system architecture, extending from sensors, controllers, and servers at the edge to cloud-based systems that process and analyze information. Building cybersecurity must address each of the following:

- **Building components and devices** – e.g., thermostats, chillers, controllers, cameras, elevators, appliances
- **Building systems** – e.g., heating, ventilation, and air conditioning (HVAC) systems, security and life safety systems (e.g., access control, surveillance, emergency lighting, fire detection and alarm)
- **Building networks** – e.g., IP-based cabling infrastructure and Wi-Fi, Zigbee or LoRa WAN wireless networks for building systems
- **Interface of building components/systems/networks to internal enterprise IT systems** – e.g., integration of access control systems with human resources (HR) systems
- **Interface of building components/systems/networks to external systems** – e.g., integration of building automation systems (BAS) with utility/smart grid demand response (DR) and/or cloud-based systems

The last few years has seen several well-publicized OT cyber incidents targeting critical infrastructure through endpoints such as closed-circuit television (CCTV) and HVAC devices and peripherals such as printers and retail point-of-sale (POS) machines. These attacks are increasing and becoming more sophisticated in their exploitation of OT resources due to traditionally flat network configurations and lack of well segmented network resources. As networks become more software defined and leverage technologies like machine learning (ML) and artificial intelligence (AI) to create a new level of network-based intelligence (i.e., intent-based networking), visibility and control of connected devices are supported through network micro-segmentation. Micro-segmentation creates an opportunity to provide a true end-to-end securely connected Smart Building that dynamically allocates resources across systems, control planes, and devices/sensors and reduces the cost to maintain these complex systems via fewer site visits and more targeted utilization of assets.

Cybersecurity implementation should ideally:

- Prevent attacks from becoming an intrusion.
- Ensure that the safety aspects of the building are not compromised in the event of an attack/intrusion.
- Ensure a good response mechanism to enable business continuity.
- Include special considerations and protection for life-safety systems.

To better understand cybersecurity implementation in smart buildings, the following tasks need to be accomplished:

- Identify specific threat vectors at different levels of security implementation.
- Define the best practices for security implementation.
- Translate the cybersecurity assessment into a series of multiple-choice questions to help indicate increasing levels of maturity.

A best-in-class smart building cybersecurity implementation should include the following practices across various functional areas:

- Data and cryptography
- Malware analysis
- Logical security
- System management
- Communication security
- Process documentation (e.g., system as-builts, functional narratives, etc.).
- Secure configuration
- Secure remote access
- Vulnerability management and penetration testing
- Secure software/firmware updates and patching
- Security logging and monitoring
- Security audits
- Incident response
- System upgrades and decommissioning (i.e., end-of-life)
- Stakeholder training and documentation

Based on the National Institute of Technologies (NIST) Cybersecurity Framework (CSF) [5] that integrates industry standards and best practices to help organizations manage their cybersecurity risks, the following functions/use-cases should be part of the system integration and implementation for cyber protection in OT systems:

1. IDENTIFY

- Asset discovery / Inventory
- Vulnerability testing
- Penetration testing
- Red teaming
- Threat intel trending

2. PROTECT

- Endpoint protection
- Cyber secure infrastructure, including intrusion detection systems (IDS), intrusion prevention systems (IPS), and distributed denial of service (DDoS) management
- Sensor tuning
- Hardening (cyber hygiene)

3. DETECT

- Anomaly detection
- User and entity behavior analytics (UEBA)
- Log management
- Alerts
- Network traffic analytics overflow

4. RESPOND

- Anomaly detection
- User and entity behavior analytics (UEBA)
- Log management
- Alerts
- Network traffic analytics overflow

5. RECOVER

- Data loss prevention (DLP)
- Disaster recovery plan
- Remediation

BUILDINGS COMPRISE OF A LOT OF SYSTEMS, SOME ARE INTERCONNECTED, SOME EXIST IN SILOS

1. Chilled Water System
2. Ventilation System
3. Air Handling System
4. High Temperature Chilled Water Heat Exchangers
5. Tenant Retail Condenser Water System
6. Heating Water System
7. Tertiary Chilled Water System
8. Floor Controls
9. Supplementary FCU/ACU/PAC System
10. Lighting System
11. Vertical Transport System
12. Access Control System
13. End of Trip System
14. Electrical Power Supply
15. Onsite Renewable Energy – Solar/Geo.
16. Hydraulic Controls
17. Occupancy Controls
18. Digital Signage
19. Intelligent Maintenance Management
20. Dynamic Envelop
21. Indoor Environment Quality
22. Building Cybersecurity
23. Refrigerated Spaces
24. Plumbing System
25. Public Address System
20. Fire Detection System
21. Fire Suppression System
22. Video Surveillance System
23. Intrusion Detection System
24. UPS
25. Emergency Lighting System
26. Visitor Management System
27. Parking Management System
28. EV Charging System
35. Occupant Engagement System
36. Space Management System
37. Automated Blind System
38. Indoor Navigation System
39. Wi-Fi System
40. Telecommunication System
41. Meeting Room System
42. Rainwater Harvesting System
43. Seismic Monitoring System
44. Baggage Scanning System
45. Weather Stations
46. Water Leak Detection System
47. Rodent Repellant System
48. Air and Surface Sterilization Systems
49. VESDA System
50. Sewage System

+ many more systems

FIGURE 1: Common Building Systems, Courtesy of Sudhi Sinha

The number and types of systems that support a Smart Building may vary based on the building type, its occupants, and overall function. Figure 1 above contains a list of common systems in a building that should be considered in scope for cybersecurity.

DEFINING STAKEHOLDERS

Smart buildings offer owners, operators, and occupants vast potential for improved efficiency, sustainability, and user experience. These same stakeholders are also affected by the security of the facility and how systems respond during an incident.

Design of a Smart Building can be successful with proper early interaction between all stakeholders that will design, construct, operate, and maintain systems within the Smart Building ecostructure. Figure 2 identifies common stakeholders and their impact on the building lifecycle from a design, construction, and operation/maintenance perspective.

LIFECYCLE IMPACT

STAKEHOLDER GROUP	DESIGN	CONSTRUCTION	OPERATE/MAINTAIN
Designer / AE	Design Requirements	Commission	
Facility Owner	Cost, Risks, ROI	System Accept/Training	Asset management, Maintenance, Monitoring, IR
Facility Maintenance	Cost, Skills, Tools Required	Acceptance, Training, Security Coordination	Monitor, Maintain, enforce policies and procedures
Cyber Monitoring	Determine Responsibility & Tools	Commission	Vulnerability Patching, Maintenance Contracts, Support
Contractor / Subs & Solution Providers	Constructability / Cost	Follow Specifications, Adhere to Policies and Procedures	Operate & Maintain Occupant Systems connected to building network
Occupants / Visitors / Tenants	Consequence & ROI for costs		
IT Groups (Different mandates and operations	Design Requirements if managing OT	Building Network Commissioning	Disaster Recovery Support
Local Authorities & Ecosystem (Campus, City, Etc)	Design Threat Basis Input		
Utility Provider	Design Requirements (i.e., load shedding connections)		
Inusrance Providers	Design Requirements		Verification of monitoring & maintenance
Auditors and Assessors			Maintaining security posture

FIGURE 2: Common smart building stakeholders and their impact on the building lifecycle

DEVELOPING THE VISION

The fundamental strategy behind information security and associated practices is to support the smooth operations of a business by preventing disruption, minimizing regulation penalties, and ensuring that leadership is aware of circumstances with potential risk to operations. That means that an organization must first develop its vision based on identified risks. A simple exercise in that endeavor is to start asking the following questions:

1. What would happen if certain key personnel were no longer available due to illness, or otherwise?
2. What information does the organization maintain and what industry regulations protect that information?
3. What would happen if a disruptive event prevented access to an information system or a supplier?

These questions, while not comprehensive, represent key functional areas of an organization that can be divided into three domains: people, processes, and technology.

LEADERSHIP

The first step in identifying risk is to recognize that each domain (i.e., people, processes, and technology) requires two key foundations—oversight by at least one individual and ultimate accountability. Many organizations suffer from not having these foundations in place for their processes. At a basic level, the highest-ranking HR officer, operations officer, and technology officer should oversee the three domains of people, processes, and technology, respectively.

If an organization has an information security officer (ISO), that role should support the other three individuals on topics related to organizational risk. It is important to note that because the ISO does not have authority in the domains, they typically cannot mandate within those areas. Officers of those domains must therefore advocate for and ensure implementation of the ISO's recommendations. Getting this leadership approach right is vital for businesses to have a smooth and successful security program.

RISK TOLERANCE

Each domain must determine its tolerance for risk based on the functions they support within the business. For example, does HR have policies in place for vetting hires such as pre-hiring background check for individuals in sensitive roles that will have broad access to data? If not, the risk of those specific roles is high and requires more scrutiny. This underlying principle applies to all domains as follows:

Human Resources: Identify roles in the business and rate their sensitivity levels. Determine how much scrutiny the organization requires to hire only qualified and reliable individuals.

Operations: Identify all the processes within the organization that are critical and determine if those processes warrant contingency plans.

Technology: Identify all critical information systems and determine if those systems warrant highly-available backups.

The bottom line is that each component within the three domains of the business needs to be reviewed using a "what-if scenario" approach. If the outcome of a potential failure is identified as minor, the risk tolerance of the component is higher than if the outcome were moderate or high. It is acceptable to be subjective here—the point is that rating components and comparing them with each other provides a good spectrum of risk. At this point in the vision development process, an organization should have identified oversight and the chain of accountability for each of the three domains and conducted a basic internal risk assessment across all components within the domains. The next step is determining what to do with this information.

RISK MANAGEMENT

Cybersecurity in considered risk management and begins with recognition and identification of potential risks via assessments that should be conducted for both existing and new systems. Once the risks are identified, they can be managed via one of the following five methods.

1. Acceptance – The business has accepted an identified risk as a part of doing business. Addressing this risk may cost more than the exploitation of the vulnerability.
2. Remediation – The business is actively working to resolve the vulnerability by adopting or implementing a best practice solution to reduce the risk or impact.
3. Avoidance – The business has chosen to eliminate the function identified as vulnerable due to the cost of remediation or limited impact generated by its elimination.
4. Sharing – The business has chosen to implement a solution in which a third-party shares part of the risk. This is most common with components that rely on solution providers or contractors.
5. Transference – The business has adopted legal waivers for their clients and partners to acknowledge their willingness to accept the risks associated with the transaction or through cybersecurity insurance policies providing protections to stakeholders.

Each of these methods can, and should, apply to each of the risks identified—and it is okay to be as broad or as detailed in this strategy as needed. There are benefits and potential drawbacks for each method, so they should be considered carefully. For example, business often host information in third-party cloud environments (e.g., Azure, Google Cloud). Rather than sharing the risk with these third-party entities, a business may decide to exclude sensitive data from being hosted by a third party and instead locally host and manage that information on-prem. On the other hand, a simple strategy could be for the business to share as much risk as possible by partnering with other organizations, especially if there is limited internal staff. Managing too much with too little can be a risk in and of itself.

EXTERNAL FACTORS

To comprehensively review security domains, there are several security frameworks available that ask key questions related to how an organization manages its security program, such as NIST CSF [5], the Building Cyber Security (BCS) risk framework [1], and the ISA/IEC 62443 series of standards [3].

These frameworks are designed to help organizations navigate through the waters of information security by asking questions that many business leaders may not be considering. If an ISO is part of the cybersecurity stakeholder team, their role should include assisting domain officers in applying these frameworks, complying with standards, and passing cybersecurity audits.

DEVELOPING VISION
GOVERNANCE

Governing cybersecurity for smart buildings means putting cybersecurity in context of the building's mission and desired outcomes and experiences. Governance begins with asset owners and operators establishing a security controls framework and lifecycle approach for managing risk and bolstering resilience to threats. Proper governance will minimize risk to the intended outcomes of a smart building, such as establishing safe and healthy environments and achieving energy efficiency, sustainability, productivity, and amazing occupant experiences.

A security controls framework includes setting policy and processes that leverage internationally-recognized cybersecurity standards that are suitable to the converged OT/IT ecosystem within the smart buildings of today and tomorrow. For example, the BCS risk framework [1] provides a useful model for a converged, data-enabled environments by integrating OT security controls from ISA/IEC 62443 [3] and IT security controls from ISO/IEC 27001 [4] and CIS Critical Security Controls [2] in a way that reduces risk and drives value through market-aligned incentives for asset owners. These standards and control sets map to many other national and local standards and regulatory requirements, such as NIST 800-53 [7].

With a security controls framework and policies in place for minimum security levels and requirements, initial and continuous risk assessments will identify gaps and weaknesses in system security design and operational practices. Remediation and improvement actions, when completed, will be reassessed to determine compliance and security rating or level, as described by the BCS risk framework [1].

In addition, privacy regulations and considerations must be part of the controls framework, policies, and processes, particularly where personal data is collected and processed, such as with security surveillance, physical access control systems, health and location-based services, and others.

USE CASES AND CYBER PROTECTED SMART BUILDING

A smart building utilizes data to provide a safer, energy efficient, and flexible environment for occupants. Sources of Smart Building data include the electrical, lighting, and mechanical equipment and devices that serve the building. Both equipment and devices are becoming inherently smart and continue to be capable of providing greater value by enhancing smart building capabilities. But they also introduce new cyber risks.

Cyber protection has many facets, including limiting network connected devices to only-as-required and limiting or eliminating communication between devices that have no identified need to communicate. Therefore, it would appear that the goals of achieving open communication across Smart building systems and limiting communication for cyber protection are opposing forces. This is where use-cases come in.

Use-cases identify the need to integrate data to achieve desired outcomes. In other words, use-cases serve as a conscious effort to identify the purpose of why two or more systems (or devices) need to communicate. A desired outcome is the result of use-case(s). How the use-cases are represented and documented is the decision of the design engineer. A consistent method should be adopted such that all desired outcomes are tracked by use-cases through all project phases, including design, bid, construction, commissioning, and cyber protection. Also, the adopted method should speak to stakeholders, including the cyber protection engineer.

A simple example of an outcome is the desire for a networked light switch in a conference room to turn on certain conference room lighting fixtures. The use-case would identify the light switch/fixture relationship, hence the need for data communication. What might appear to be an obvious use-case to both the designer and construction contractor may not be obvious to a cyber protection engineer who only sees each device as a network address. When a lighting control scheme use-case is represented in an easily recognizable matrix format for an entire building, a cyber protection engineer can quickly assess the data flow requirements. The level of communication (allowed or inhibited) within the entire lighting control system is based on the cyber risk governance documents for the project.

A more advanced outcome to consider is a building's HVAC system. The mechanical engineer and mechanical contracting industry have extensive history and experience in writing, programming, and commissioning sequences-of-operations to keep buildings comfortable and running efficiently. Since digital signals from many devices are communicated across a network, these building control sequences may be classified as a set of use-cases in that network data is shared to achieve an outcome. HVAC sequence-of-operations include inputs from numerous sensors, data analytics, and outputs to complex equipment including air-handlers, chillers, boilers, pumps, and fans.

For this advanced outcome, it is prudent for the cyber protection engineer to be engaged with the design engineer to assure HVAC system data flow requirements when implementing the cyber protection strategy. For example, the use-cases may require communication between the chiller or the boiler and the BAS but if there are no use-cases or permissions for data flow between the chiller and the boiler, communication between these systems may be prohibited. The purpose of locking down chiller to boiler communication is such that if a cyber incident caused by a vendor's infected laptop compromised the chiller control panel, the malware would not have easy access to the chilled water system.

Use-cases provide clarity for data integrations in the built environment. Use-case documentation is necessary to ensure that desired outcomes are constructed, commissioned, and cyber protected. Smart Buildings don't just happen—they are thoughtfully designed and cyber-protected.

SECURITY CONSIDERATIONS

Smart buildings incorporate many devices that may have limitations for how to monitor and secure, such as not supporting the installation of endpoint security software. Another challenge in protecting these devices is that they often use default passwords (or guessable passwords) and only required single-factor authentication. Identifying available patches at scale and deploying them for each of the relevant devices is also a challenge for smart building network administrators, leading to a potentially large attack surface awaiting action. Secure architecture design is therefore imperative. Network segmentation and isolation of these critical and often susceptible devices/systems are key. Adding a layer of authentication before accessing these systems is best practice, as well as enhanced network monitoring to look for known and unknown threats.

Considerations should be given to adopting the principle of "least functionality" to reduce the overall attack surface by disabling those ports, protocols, services, features, and connectivity that are not required for a use-case or function.

Potential risks for connected smart buildings include any system of devices that are connected for the means of exchanging information. These systems can provide significant benefits to building owners, operators, and occupants, but they also pose potential risks if not addressed properly during system design, installation, and commissioning. Systems that could be vulnerable if not properly secured include the following:

Considerations should be given to adopting the principle of “least functionality” to reduce the overall attack surface by disabling those ports, protocols, services, features, and connectivity that are not required for a use-case or function.

Potential risks for connected smart buildings include any system of devices that are connected for the means of exchanging information. These systems can provide significant benefits to building owners, operators, and occupants, but they also pose potential risks if not addressed properly during system design, installation, and commissioning. Systems that could be vulnerable if not properly secured include the following:

- **IT data network – foundational (internet) network**
- **Dedicated systems networks**
- **Access control**
- **Surveillance**
- **Lighting**
- **HVAC**
- **Power Generation/ Distribution**
- **Fire / Life Safety**
- **Remote Access**

BUILDING SYSTEM ENVIRONMENTS

The environment for a building system will have an impact on assessing security risk and determining which security controls should be implemented. Defining what type of environment is in scope and where the system components are to be located within that environment is therefore essential when planning for cybersecurity in the early design phase.

When assessing the environment under consideration, it is important to identify the risk potential should an incident occur and how it can impact occupants, data, and operations. Facilities and environments that support business and mission-critical functions will have a lower risk tolerance.

It is important to realize that while an overall facility may be categorized as high risk, the same risk level may not encompass every environment within the facility. Each environment should therefore be addressed independently for risk. For example, a building's lobby will likely not require the same protection as a controlled area where sensitive information and processes are managed. There can even be varying degrees of risk tolerance within the controlled areas. Data centers and operational areas (e.g., mechanical rooms, manufacturing floors, electrical rooms, etc.) are likely to be more sensitive to risk than office space that has less impact on safety, data, and operational loss.

The location of system components and the role each plays also factors into the risk calculation. Some components reside within the life-space of a building (e.g., sensors, thermostats, door readers, and mobile applications) and are physically available to occupants and visitors while others may reside in a controlled space (e.g., servers, operator workstations, controllers, and actuators) that cannot be accessed by the general population. It is important to limit the ability to view sensitive data and execute changes in configuration and control to only those who are properly trained and authorized.

Providing occupants with the ability to interact with the living space can improve efficiency and user experience, but it should not compromise the security of a system. For example, it may be reasonable to enable users to select conference room presets and minor adjustments for temperature and lighting via wall-mounted control panels. These panels however should ensure that unauthorized users do not have access to functions beyond those intended for public use.

Within controlled spaces, appropriate physical security should be in place to limit access to authorized individuals only. Mechanical locks, electronic access control, video surveillance, and tamper detection methods can be used to ensure restricted access to components in controlled spaces. To ensure components can operate as designed, physical security should also include protection of the infrastructure (e.g., wiring, cables, pathways, ducts, etc.) that feeds into the controlled space from less secure areas. This can be achieved by placing cables in conduit or inaccessible pathway systems and maintaining proper environmental conditions (i.e., temperature, humidity). Refer to NIST 800-82 [6], TIA-5017 [12], UFC 4-10-06 [13], UL 60730-1 [15] for more information.

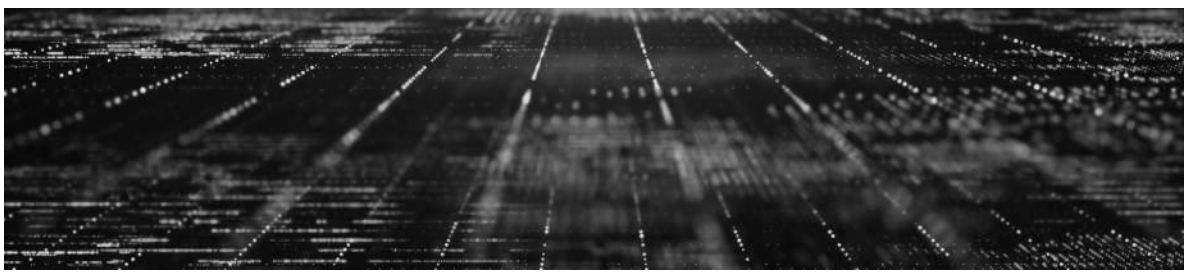
SYSTEM LEVEL CONSIDERATIONS

One critical aspect to remember when designing and deploying smart building systems is that with every added feature comes added risk, and system architects should always be cognizant of the risk-reward aspect of choosing features. There should be a deep understanding for each system component as it relates to controlling physical access, logical access, supply chain, and trust relationships/interconnections. (See NISTIRs 8259 and 8259A [8], SP 800-213 [9], TIA SCS 9001 [11], UL 1376 [14].)

Many times, innovative technology is implemented without full awareness of every network port and protocol (including versions) that are accessible to a system, both with wired and wireless connectivity. Another key area is trust relationships between system components. For example, it can often be easy to focus on securing system component A and overlook the fact that system component B is "trusted" by system component A. Therefore, if system component B is also not hardened and secured, it has the potential to be compromised and provide an easy and direct attack path to system component A. In other words, only securing system component A can provide a false sense of security. The growing number of interconnected devices in a smart building can be a challenge to keep track of but is a critical task as systems and buildings are only as secure as the weakest link. And that weakest link could be a human.

When considering IT/OT building networks, network topology and structure are critical aspects for a successful physical and cyber security strategy. Many aspects of these networks may vary significantly, such as physical infrastructure (e.g., wired, wireless), communication protocols (e.g., serial, Ethernet), topology and hierarchy, processes, policies, building and business systems interaction, and overall business objectives. IT/OT convergence is trending in the industry based on the potential advantages of designing, constructing, and operating these networks more closely to achieve economic and operational efficiency. However, IT/OT convergence also has security implications, for both physical security and cybersecurity. The degree of convergence and the specific implementation (e.g., physical, data link, network layer convergence) need to consider all aspects during technology and solutions assessments to meet desired outcomes and business goals without sacrificing security beyond acceptable risk.

Several security best practices and approaches can provide better outcomes and network uptime, depending on the current and desired future network physical infrastructure (wired or wireless) and functionality (e.g., IoT devices, futureproofing).



The wired structured cabling infrastructure in a building can use different combinations and topologies of copper, fiber, and hybrid fiber cabling. For example, backbone infrastructure between floors may use optical fiber cable, while the horizontal or floor-level infrastructure may use copper cabling or hybrid copper-fiber cabling. Horizontal infrastructure cables can often deliver both data and power to devices using remote powering technology such as IEEE 802.3 power over Ethernet (PoE). Today's cables also support higher bandwidth requirements to support a variety of IT-based applications. From a security perspective, access to cabling infrastructure needs to be fully defined in the overall security strategies. For example, access to cabling in mission-critical or data-sensitive environments may need to be controlled through physical means, such as protected distribution systems, hardened pathways, and secure connectivity.

Wireless communications that are becoming ubiquitous in today's commercial buildings also need to be considered. Wireless connections to devices are a component of the IT network but can also reside within OT networks to communicate with wireless sensors and other devices that collect data and control applications.

Choosing between wired and wireless communications for devices depends on several considerations, such as new construction versus renovation/retrofit, device location, and the desired functionality. Deciding between wired and wireless requires assessment on a case-by-case basis. The same considerations for determining protection level, security protocols, and best practices for wired connections should also be applied to wireless. The actual methods, technologies, and implementation will however differ depending on media type and acceptable risk. For any current and future designs, it is critical to consider the network and how devices are connected when determining requirements for both cyber and physical security.

DEFINING INTEGRATION FAILURE MODES

As part of risk management, smart building design must account for system integration failures or loss of communication due to any reason (e.g., incident, equipment failure, maintenance, etc.). This allows all stakeholders to know what to expect during an incident and recovery. Each system should have a defined functionality for how it will operate during loss of communication and when communication is restored. To achieve this, a best practice is to assess what failures are possible. Designers can start by visually mapping and analyzing all interactions within the building. This should include all logging and reporting of building system data, including logs, heartbeat, commands, readings, events, configuration, failure reporting, and alerts messages. Identifying where different systems interface with each other can also help identify potential risks in integrated systems. Common interfaces include security and access control, lighting and HVAC control, and building systems that access the Internet for cloud-based solutions.

Another often-overlooked risk is where systems interface with each other. Varying versions or composite systems sometimes do not follow a default sequence or operations if communication is lost, even if those systems come from a single manufacturer. Examples of inter-manufacturer integrations include cameras and access control, thermostats and variable air volume (VAV) controls, lighting and window treatments, wired and wireless controls, and panel-based and distributed control architectures. These interactions are often not published and may not be easily identifiable. It is therefore important to rely on manufacturers for a better understanding of their architecture and where potential failure may exist between systems.

In many cases, a supervisory system may control subordinate systems within a building. It is important to identify which products or services control other systems and the processes used to do so. These systems may be from a multitude of manufacturers, such as a supervisory system that monitors a central utility plant in addition to systems within individual buildings. In most commercial building designs, primary systems take control over other systems during an event. For example, an occupancy sensor may signal for a VAV control to turn off air flow to an unoccupied space, overriding the thermostat that would have normally maintained conditioned air in the presence of occupants. It is important to understand which system is in control of your building during a building event to ensure that occupant experience is not compromised by a system failure. In the event of a failure, knowing exactly which system had control at the time also facilitates troubleshooting.

PROVIDING TOOLS TO MAINTAIN AND RECOVER

A comprehensive smart building design should also include considerations for system operation, maintenance, and cyber incident handling. Monitoring and maintenance are key countermeasures for many common cybersecurity attacks but often the tools to perform these functions are not considered during the design phase. When developing stakeholder roles and responsibilities during the early design phase, consider the following questions:

- Who will be responsible for monitoring each smart building system?
- What tools and skills exist, and do they apply to the systems planned for this project or will the project provide cyber tools to the stakeholders to perform their responsibilities?
- Will training be provided on systems, tools, and security features?
- Will the monitoring and maintenance be performed on-site or remotely?
- Do policies and procedures exist for patching and patch frequency?
- Is a test bed available or warranted to allow for patching within acceptable risk tolerances?

The ability to recover a system after an incident is the last line of defense. The design team should determine which stakeholders have responsibility for incident response and what documentation and tools will be required. The development of incident response and recovery processes should consider the following:

- Include requirements to provide a comprehensive asset inventory spreadsheet and as-installed network diagrams. We can only defend and recover what we know about.
- Include requirements for contractors to provided backups for all as-built applications at a minimum. Bare-metal backups (i.e., restoration on new equipment) should also be considered.
- Determine if the responsible parties have on-site and off-site backup tools or if they should these be included within the new networks (i.e., network attached storage [NAS] for on-site repository).
- Testing and documentation of the backup recovery procedures as part of project training.

SMART BUILDINGS CYBERSECURITY CONCLUSION

Cybersecurity is one of the most critical emerging threats. The rise of technology and increased number of connected devices in today's commercial buildings expands the threat surface and increases the vulnerability. A report by Ponemon Institute puts the average cost of an attack to industrial control systems and other OT systems at around $3 million[3]. The issue of cybersecurity in smart buildings is especially complicated due to the multiplicity of systems, the legacy OT systems, and the complex integrations being implemented between various IT and OT systems. Traditionally, cybersecurity has been the domain of IT departments in most organizations. However, given the rising significance of cybersecurity concerns in the OT environment, property managers, facility managers, and maintenance managers have to increase their understanding and engagement in protecting buildings from cyber vulnerabilities.

The SPIRE Smart Building Program created by TIA and UL [10] takes a comprehensive view of assessing various cybersecurity vulnerabilities that might exist in a building or be introduced due to addition of new smart building systems and technologies. This program also examines how the building management team is positioned in terms of its awareness, policies, processes, and preparedness in dealing with cyber events. The SPIRE framework takes into account the best practices espoused by existing cybersecurity standards, regulations, and guidelines.

More importantly, the SPIRE framework creates a connective tissue between various aspects of smart buildings represented by is criteria dimensions of energy and power, health and wellbeing, life and property safety, connectivity, cybersecurity, and sustainability. The overall objectives of Smart Buildings need a fine balance between all of these factors. For example, a greater density of sensors and control devices can help to effectively manage the indoor environment via more granular data, however, this can also increase exposure to cyber threat. SPIRE helps building owners and operators sort through such conflicts by ensuring the right balance between objectives, technologies, policies, and operational processes. As building technologies continue to evolve, SPIRE will continue to adapt to address new forms of risks and improvement opportunities.

[3] [20] . 2021 State of Industrial Cybersecurity, Ponemon Institute -- https://hub.dragos.com/hubfs/Reports/2021-Ponemon-Institute-State-of-Industrial-Cybersecurity-Report.pdf?hsLang=en

APPENDIX A: STANDARDS

I. **BCS (Building Cyber Security) Risk Framework**
https://buildingcybersecurity.org/

II. **CIS Critical Security Controls**
https://www.cisecurity.org/controls

III. **ISA/IEC 62443** – Series of standards for managing security vulnerabilities in industrial automation and control systems (IACSs)
https://www.isa.org/

IV. **ISO/IEC 27001:2013** – Information technology – Security techniques – Information security management systems – Requirements, Geneva, Switzerland, International Organization for Standardization, 2013
https://www.iso.org/standard/42103.html

V. **NIST CSF –** National Institute of Technologies (NIST) Cybersecurity Framework (CSF) –
https://www.nist.gov/cyberframework

VI. **NIST 800-82** – NIST Special Publication (SP) 800-82 Guide to Industrial Control Systems (ICS) Security, Rev 2, May 2015 –
https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

VII. **NIST 800-53 –** Security and Privacy Controls for Information Systems and Organizations, Rev 5, December 2020 -
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

VIII. **NISTIRs 8259 and 8259A**

- **NISTIRs 8259 -** Foundational Cybersecurity Activities for IoT Device Manufacturers --
https://csrc.nist.gov/publications/detail/nistir/8259/final
- **NISTIRs 8259A IoT Device Cybersecurity Capability Core Baseline** --
https://csrc.nis- t.gov/publications/detail/nistir/8259a/final

IX. **SP 800-213 -** IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements --
https://csrc.nist.gov/publications/detail/sp/800-213/final

X. **SPIRE** – Smart Buildings Assessment Program
https://spiresmartbuildings.ul.com/

XI. **TIA SCS 9001** – FDIS/SCS 9001® Supply Chain Security Management System

XII. **TIA-5017** – Telecommunications Physical Network Security Standard, February 2016

XIII. **UFC 4-10-06** – Cybersecurity of Facility-Related Control Systems

XIV. **UL 1376** – Verified IoT Device Security Rating, December 2020

XV. **UL 60730-1** – UL Standard for Safety Automatic Electrical Controls – Part 1: General Requirements; August 3, 2016

XVI. **2022 Cyber Threat Report, SonicWall**
https://www.sonicwall.com/2022-cyber-threat-report/

XVII. **Incident report, Mandiant**
https://www.mandiant.com/resources/ransomware-extortion-ot-docs

BRIEFING PAPER

THANK YOU

TIA SMART BUILDING PROGRAM SPONSORS

AECOM

CORNING