Life Is On | Schneider Electric

A Practical Framework for Cyber Secure, Cloud Connected Smart Building Control Systems

by Hugh Lindsay, Paul Forney, Jay Abdulla, Gregory Strass, and Nasir Mundh

Table of Contents

Introduction

Smart buildings can characteristically be defined as buildings which augment intelligent control systems with new, digital 'Internet of Things (IoT)' technologies with connectivity to analytic and often cloud-based software systems with an aim to:

- Identify and implement efficiencies (particularly in the areas of sustainability, energy efficiency and operating costs)
- Extend the performance and longevity of building infrastructure assets
- And improve the experience, comfort and productivity of building occupants

Current research confirms that smart building performance gains in efficiency, building valuation and occupant satisfaction are authentic. In a recent report[1] professional services firm Deloitte identified numerous opportunities for smart buildings to capture value through efficiencies, differentiation and even new sources of revenue. Further to this, a similarly themed JLL white paper concludes with,

"Forward-looking building owners, tenants and managers are already realizing the competitive advantages gained from smart building technologies. Soon, buildings that don't have smart, connected systems are going to feel the impact, whether it be in terms of asset classification, valuation, rental rates, or even brand perception (from both current and prospective employees – and even clients)."[2]

But while the benefits are increasingly clear, smart buildings that leverage large numbers of IoT devices and connectivity to the Internet and cloud services are also exposed to cybersecurity threats. Research group Gartner has estimated that,

"By year-end 2018, 20 percent of smart buildings will have suffered from digital vandalism."[3]

For many buildings (including critical facilities like banks, hospitals and data centers) that cybersecurity risk may be seen as an impediment that can keep these organizations from investing in otherwise valuable smart building enhancements. Breaches of building control systems or sensitive data can cost millions in regulatory penalties, disrupt core business functions, and threaten business reputations to a level that could impair consumer, employee and investor confidence.

To effectively realize the benefits of a smart building approach and simultaneously mitigate the cybersecurity risks building owners, operators and even occupiers need to change the way that smart building control systems are architected and managed from a cybersecurity perspective. This paper will introduce a pragmatic and standardized framework for securing both existing and new building control systems against cybersecurity threats as an enabler of IoT and Cloud connected smart buildings.

---

[1]Deloitte, "Smart buildings: How IoT technology aims to add value for real estate companies," https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/real-estate/deloitte-nl-fsi-real-estate-smart-buildings-how-iot-technology-aims-to-add-value-for-real-estate-companies.pdf. PDF, 2016.

[2]JLL, "Are Smart Buildings Smart for Business?" https://www.jll.com/Documents/research/pdf/apac/2016-JLL-Are-smart-buildings-smart-for-business.pdf, PDF, 2016.

[3]Gartner, "Gartner Reveals Top Predictions for IT Organizations and Users for 2016 and Beyond," https://www.gartner.com/newsroom/id/3143718, Website, 2015

Understanding the Challenges

Another Deloitte report titled "Evolving cyber risk in commercial real estate: What you don't know can hurt you" (Deloitte, 2015) makes the statement,

"Today's building systems fall short of effectively managing any potential cyber intrusion …"

The reasons for this are typically related to the historical disconnect between information technology (IT) and building operational technology (OT) groups in an organization. Building management systems (BMS) required specialized knowledge of proprietary systems and protocols and, since BMS didn't require access to corporate network resources or the Internet, the cyber secure protection of a BMS network relied on obscurity and lack of external connectivity (often referred to as an "air-gapped" network). Over time the sophistication of cyber attackers and the proliferation of malware have combined to a point where an unprotected and unmonitored system is a vulnerable and potentially compromised system. In fact, there are hacker communities and research groups that specialize in cyber-attacks targeting air-gapped control networks.[4]

Building control systems have evolved as well. A typical BMS now leverages a combination of standardized OT protocols (such as Modbus and BACnet), standard IT protocols (HTTP, FTP, XML, etc.), and connectivity to Internet-based resources. Yet the disconnect between IT groups (where the cybersecurity knowledge resides) and OT groups (where the BMS operational knowledge is) is still the de facto operational model for most buildings. Smart building technologies and connectivity simply compound these challenges and increase the potential security threats smart building enhancements expose.

There is, however, strong support in the OT control systems industry to address these challenges and industry associations have risen to the need for common OT cybersecurity best practices, specifically in the development of the IEC 62443 global set of cybersecurity standards.

An overview of the IEC 62443 Standards

A focus of the International Society of Automation (ISA) that was recently combined with the International Electrotechnical Commission (IEC) is the ISA/IEC 62443 global set of standards, a technical specification for the secure development and protection of industrial control systems (ICS). As highlighted in the ISA's "62443 Series of Standards"[5] introductory document,

The goal in applying the IEC 62443 series is to improve the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, and to provide criteria for procuring and implementing secure industrial automation and control systems.

The IEC 62443 framework contains thirteen documents organized into 4 categories: General, Policies and Procedures, Systems, Components.

[4]Dr. Mordechai Guri runs the Advanced Cybersecurity Research Lab with a specialization in Air Gap vulnerabilities at Ben-Gurion University of the Negev, Israel, https://cyber.bgu.ac.il/advanced-cyber/airgap

[5]ISA, "The 62443 Series of Standards, https://cdn2.hubspot.net/hubfs/3415072/Resources/The%2062443%20Series%20of%20Standards.pdf PDF, 2018

Figure 1
IEC 62443 DOCUMENTS

General	**62443-1-1** Concepts and models	**62443-1-2** Master glossary of items and abbreviations	**62443-1-3** System Security conformance metrics	**62443-1-4** IACS security life-cycle and use cases	**62443-1-5** IACS Protection levels
Policies & Procedures	**62443-2-1** Requirements for an IACS security management system	**62443-2-2** Implementation guidance for an IACs security management system	**62443-2-3** Patch management in the IACS enviornment	**62443-2-4** Security program requirements for IACS service providers	
System	**62443-3-1** Requirements for an IACS security management system	**62443-3-2** Requirements for an IACS security management system	**62443-3-3** Requirements for an IACS security management system		
Component	**62443-4-1** Secure product development life-cycle requirements	**62443-4-2** Technical security requirements for IACS components			

General: These documents define the core terminology, concepts and models and outline common conformance metrics
Policies and Procedures: These documents define the requirements for effective ICS cybersecurity management from design and through the operational life cycle of the systems
System: Here the focus is on cyber secure ICS system level design and risk assessments
Component: And finally, these documents relate to secure product development and ongoing life cycle maintenance of the intelligent devices in an ICS.

For smart building control systems, IEC 62443 is an excellent foundation for guidance through the framework for the following reasons:

- We can first leverage the focus on risk assessment to evaluate and identify the potential threats to existing and legacy building control systems, and to design a cyber secure system and management protocol to protect and maintain those systems.
- As new building control systems are anticipated and new IoT technologies introduced, IEC 62443 further outlines recommendations for evaluating suppliers and IoT component and system level technologies by defining the basis of Secure Development Life-cycle (SDL) best practices.
- IEC 62443 also defines concepts of secure OT network segmentation intended to maintain protection from both internal and external threats.

Ultimately, the goal is to design, implement and maintain a building control system following IEC 62443 such that the system could be audited and certified in compliance with the standards and guidelines.[6]

Of course, this essential guidance should be considered within the broader IT focused cybersecurity guidance from organizations. For example, the National Institute of Standards and Technology's (NIST)

[6]Note: At the time of writing this document, the ISA Security Compliance Institute (the standards body that maps the standard to certification criteria) has determined that while the IEC 62443 standards and certification are applicable to building control systems, they had not yet completed the work to fully adapt the specific guidelines.

Cybersecurity Framework 1.1[7] defines a number of core outcomes (108 in total) that map to the OT specific details of IEC 62443, including a seven-step gap analysis model for the assessment and prioritization for implementing a comprehensive cybersecurity plan. Additionally, the International Organization for Standardization (abbreviated as ISO) has created a model for setting up and operating an enterprise information security management system called ISO / IEC 27000[8]. Like the NIST Framework, the IEC 62443 focus on ICS standardization and certification is fully compatible with ISO 27000 family of standards and should be included in a comprehensive enterprise cybersecurity strategy.

A Practical Cybersecurity Framework for Smart Building Control Systems

Setting aside organizational barriers and acknowledging and addressing the IT/OT disconnect is the critical first step towards implementing and operating cyber secure smart building control systems, but such organizational change is not the focus of this document.[9] Nevertheless, assuming that intention, there are a number of practical actions based on IEC 62443 guidance that can be taken as a framework for creating secure OT building control systems connected with secure IT systems and Cloud services. At a high level, these actions can be summarized as follows:

1. Assess and protect legacy OT building control systems
2. Choose IoT devices and vendors that follow a Secure Development Lifecycle (SDL) approach
3. Implement secure OT building control system architectures
4. Bridge the secure OT building control systems through an IT Security Monitoring Zone

1. Assess and protect legacy OT systems

One of the primary challenges that relates to existing and legacy control systems is that these systems are often intentionally kept outside the view and scope of IT cybersecurity teams. The reason for this is that historically there has been a sufficiently wide gap between the technologies, protocols and operations of the IT world as compared to the OT world. OT industrial and building control protocols were, and commonly still are, not well understood by IT networking and cybersecurity teams. As a result, building control systems were relegated to entirely separate and isolated networks with a mix of strategies for connections to other systems; some with rogue connections through corporate networks, some connected to the Internet, and some with no external connections. As a consequence, these networks and systems were not designed with a view to robust and reliable cybersecurity protections, leaving a typical legacy building control system exposed to:

- Unknown vulnerabilities either internal or external
- Few, if any, cybersecurity protections
- Frequently lax enforcement of IT policies for things like server operating system and anti-virus/anti-malware software updates
- No structured monitoring or maintenance

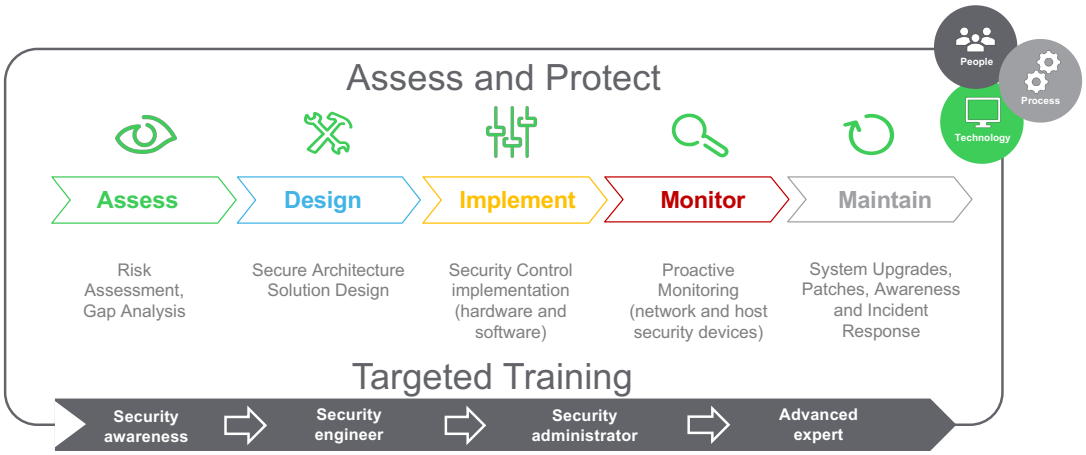
[7] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, PDF, 2018.

[8] https://www.iso.org/isoiec-27001-information-security.html, Website, 2018.

[9] Note: Gartner identified first this need and proposed a path forward in 2011. For a review of their perspectives read: Gartner, C. Petty, "When IT and Operational Technology Converge," https://www.gartner.com/smarterwithgartner/when-it-and-operational-technology-converge/, blog, January 2017.

Under the guise of protecting the operational stability of the building control system, legacy BMS have been left desolate from a security perspective. A comprehensive assessment and protection initiative, as outlined in Figure 2, can address many cybersecurity deficiencies.

Figure 2
ASSESS AND PROTECT INITIATIVE



From a programmatic perspective, protecting legacy systems follows a path of:

- Assessing the threats and documenting the current system
- Designing and implementing a solution for isolating and segmenting the most vulnerable components of the network
- Leveraging tools to monitor and maintain the operation of the system for abnormal behavior or possible intrusions
- Implementing a program of periodic cybersecurity audits and reporting to ensure protections are maintained over the system life cycle
- Initiating a targeted, roles-based cybersecurity training path for the people who use, interact with and administrate the system

In addition to the General Policies and Procedures foundation, two documents from the IEC 62443 series are most relevant to guiding a cybersecurity expert in the assessment and protection of existing control systems:

- IEC 62443-3-2: Security risk assessment and system design
- IEC 62443-3-3: System security requirements and security levels

This guidance can be framed as part of a comprehensive Defense in Depth[10] information security methodology which takes into consideration all of the people, process and technology vectors of cybersecurity strategy. Defense in Depth is an IT best practice, but it has equal application in the analysis and protection of OT systems, as well. This process and the implemented protections and monitoring may not identify and address every possible vulnerability, but it will form a basis for continuous improvement over time.

[10]Note: For more information related to Defense in Depth as it applies to securing building management systems read Schneider Electric whitepaper: "Defending Against Cyber Threats to Building Management Systems," https://download.schneider-electric.com/files?p_enDocType=White+Paper&p_File_Name=998-2095-12-08-15AR0_EN.pdf&p_Doc_Ref=998-2095-12-08-15AR0_EN, Daniel Paillet, PDF, 2015

Having addressed the need to assess and protect the legacy building control systems you can begin to consider how to assess the cybersecurity protections of new IoT technologies and how to design, implement, monitor and maintain new secure building control systems, beginning with Secure Development Life-cycle best practices.

2. Choose IoT devices and vendors that follow a Secure Development Life-cycle (SDL) approach

As you consider and evaluate new IoT technologies to enhance a smart building, an important first step is to evaluate the products and processes of vendors who consider cybersecurity a strong priority. IEC 62443 establishes a number of best practices for an IoT technology and software designer and manufacturer. Figure 3 outlines a high-level summary of Schneider Electric's SDL process.

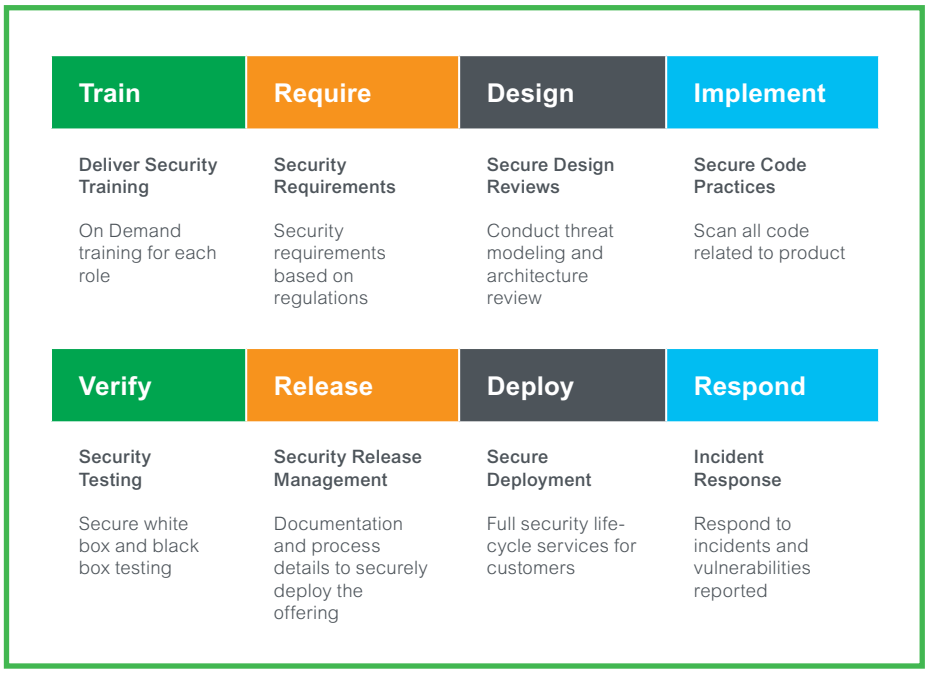


Figure 3
SCHNEIDER ELECTRIC SECURE DEVELOPMENT LIFECYCLE

Fundamentally, the SDL integrates relevant and timely cybersecurity training and development best practices with a set of cybersecurity related checkpoints into the IoT technology and software development processes. Given that the cybersecurity domain is constantly changing, these processes are designed to evolve and adapt as new vulnerabilities and attacks are identified over the life-cycle of the products.

In the standards, IEC 62443-4-1 lays out the process for designing and implementing secure products, and at the component or endpoint level the IEC 62443-4-2 standard lays out the requirements by which a developer would implement capabilities to provide the right level of security for the product deployment. These processes consider the components, hosts, applications and software in the context of a hierarchy of security levels relevant to control applications. These levels can be summarized as:

- Basic – considers elements such as secure communication, cryptographic services, and root of trust (which encapsulates device identity and integrity).
- Enhanced – adds endpoint configuration and management.

- Critical – adds an additional layer of security information and event handling.

Depending on where the product fits in the continuity of a system, the appropriate level of secure development rigor would apply.

The main point is that IoT component and software development teams who follow the IEC 62443-4-1 and 4-2 standards can establish a secure foundation as a basis for full, system level security. Cyber protections at the component and software levels focus on first securing every device, host and application, as well as the connection and communication between these devices, the building control system software, and ultimately through to Cloud services.

3. Implement secure OT system architectures

At the system level, IEC 62443 guidance provides an overview of current network security technologies, including the inherent advantages and limitations, and expands on this by detailing recommendations for system network design and security risk assessments. However, the following documents provide useful guidance in the creation and maintenance of a building control system:

- IEC 62443-2-1: Requirements for an industrial automation and control system (IACS) security management system
- IEC 62443-2-2: Implementation guidance for an IACS
- IEC 62443-3-1: Secure technologies for an IACS
- IEC 62443-3-2: Security risk assessment and system design
- IEC 62443-3-3: System security requirements and security levels

In the aggregate, a system designed using these principles would ensure protections from intrusions that originate from both within the network and from connections through to other external networks, such as a typical corporate network or a specialized network dedicated to critical infrastructure - including appropriately secure connections to external networks like the Internet and cloud platforms. Similar to the component level, IEC 62443 also identifies a hierarchy of four security assurance levels. The level of intended protections is aligned to the anticipated source of an attack, as outlined in Table 1.

TABLE 1:
IEC 62443 SECURITY ASSURANCE LEVELS

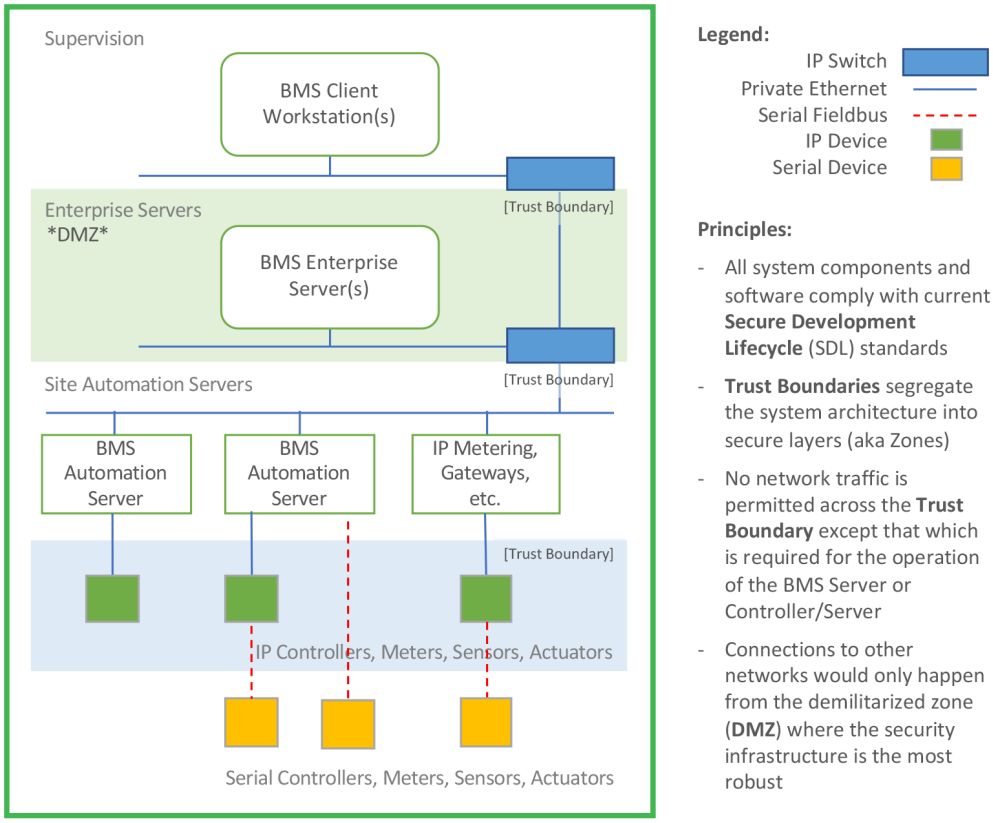
Security Level	Profile	Skills	Motivation	Resources
SL1	Casual or coincidental violations	No attack skills	Mistakes	Individual
SL2	Cybercrime, hacker	Generic	Simple	Low (isolated individual)
SL3	Hacktivist, terrorist	ICS specific	Sophisticated (attack)	Moderate (hacker group)
SL4	Nation state	ICS specific	Sophisticated (campaign)	Extended (multidisciplinary teams)

For many buildings, a targeted level of SL1 or SL2 would be sufficient to thwart opportunistic cybercriminals and hackers, but for more critical buildings like banks, hospitals, and data centers it would be wise to consider an architecture and protections at SL3 and approaching SL4.[11]

Example: IEC 62443 Cyber Secure BMS, Architecture and Principles

At a high level, the standard recommends that control systems should be organized into segments, or zones, such that devices of similar trust levels are grouped together, and access is restricted to mitigate threat exposure. Figure 4 shows how this guidance could be applied to a BMS to improve cybersecurity protections.

FIGURE 4:
CYBER SECURE BUILDING CONTROL SYSTEM ARCHITECTURE HIGHLIGHTING ZONES AND TRUST BOUNDARIES



In this example, the network is segmented into three distinct "trust boundaries", or zones, where IP switches are leveraged to filter out all network traffic between the boundaries except that which is required for the normal operation of the system. This strategy builds upon the component level security by ensuring that, should an attacker manage to compromise a device, the vulnerability would be isolated to that specific zone.

Breaking this down further, the intent and features of each zone are:

- **Supervision:** This zone contains the day-to-day user interface components where the system operator configures and administers the building management system (BMS)

[11]Note: For a more complete understanding of the IEC 62443 security assurance levels and example architectural designs read the Schneider Electric whitepaper titled "Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications." http://download.schneider-electric.com/files?p_Doc_Ref=998-20186845, Daniel DesRuisseaux, PDF, 2018.

controllers and field devices. This interface uses specific software installed on a desktop or laptop PC for monitoring system status, activating alarms, generating reports, etc.

- **Enterprise Servers:** At this level the BMS software manages communication between the Supervision and Site Automation Servers zones and stores data related to the configuration of the complete system as well as data generated by the automation servers, controllers, meters, sensors, etc. for monitoring, alarming, trend logs for reporting, etc. This zone is treated as a "demilitarized zone" (DMZ) and is where connections to external networks would also be managed and protected.

- **Site Automation Servers:** This zone contains the core control elements of the network and manages the communication with the other field devices via IP or serial connections and common BMS protocols. These devices can have local control functions and be configured to manage large HVAC plant and electrical network elements via digital and analogue input and output signals.

- Communication between zones would be restricted through a specific conduit, in this example traffic is managed by the IP Switch(s), with the principle of least privilege used as a configuration baseline. This principle, in effect, ensures that explicitly permitted traffic traverses the conduit into each zone as specifically and operationally required by the security administrator.

It is worth noting that in a secure system design such as this, given that the traffic across the trust boundaries will be strictly managed, changes in programming or updates to system components will require changes to internal processes and procedures. For instance, to update the programming of a BMS Automation Server a system engineer would need to connect directly to the Site Automation Server network with a secure and trusted laptop or tablet, so the physical security of the critical network components is equally important to consider.

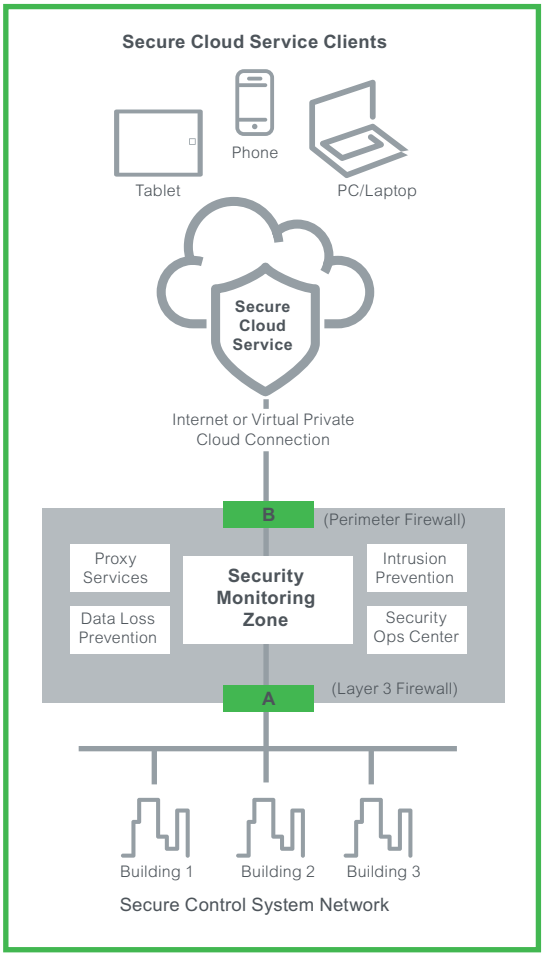
In practice, it would also be important to concurrently build a strategy to monitor the system in real time, sending alerts for any suspect or anomalous behaviors in the network or with any of the monitored devices. The monitoring system would also leverage cyber security tools to engage an active attacker to further protect and defend the system.

A secure design, regularly updated defense in depth security controls and processes, regularly updated infrastructure updates and patches, all combined with active and ongoing monitoring and reporting will ensure that the system remains protected throughout the mission life-cycle and maintains assurances that connections to other networks and the cloud will not compromise the resilience of the core controls network.

4. OT and IT Security Monitoring Zones

While the IEC 62443 standard does not specifically address connections to the Internet or hosted Cloud services, many of the core principles in the standard do still apply. The bridge between secure building control systems, and other potentially less secure networks such as the Internet, can be permitted by applying the best practices from IT cybersecurity perimeter segmentation with the use of secure firewall technologies and a Security Monitoring Zone.

Example: Secure OT Control System Network with IT Security Monitoring Zone



Principles:

- Secure BMS networks connected to a common **Secure Control System Network** can relay encrypted data, as required, to a **Security Monitoring Zone** through a **Layer 3 Firewall (A)**
- Within the **Secure Monitoring Zone** data and network traffic can be inspected and controlled according to rules established by an administrator and conventional security software, such as **Proxy Services, Data Loss Prevention (DLP), Intrusion Prevention (IPS)** and **Security Operation Center (SOC)**, can be leveraged.
- Rules established at the **Perimeter Firewall (B)** enables data flow to the **Secure Cloud Service** through the **Internet** or alternate **Virtual Private Cloud Connection**
- **Secure Cloud Service Clients** can securely interact with the data leverage the analytics offered by the service provider with no direct interaction with the **Secure Control System Network**

FIGURE 5:
SECURITY MONITORING ZONE

In this example architecture, data from the Secure Control System network must pass through a Layer 3 firewall which allows the administrator to set and control rules related to outbound data traffic. The intent of the Secure Monitoring Zone is to filter, monitor and control all data and traffic between the Secure Control System Network and the external networks. In doing this, it is then possible to deploy any number of cybersecurity protection tools including the use of:

- Proxy Servers, that are intended to act as a data intermediary accepting data from the secure control system and relaying that data to the Cloud services
- Data Loss Prevention software (DLP), which detects and prevents potential data breaches
- Intrusion Prevention Systems (IPS), which are devices or software that monitor networks for malicious activities and policy violations
- And in some cases, it may even be appropriate to include the services of a Security Operation Center (SOC) which is a centralized group of cybersecurity experts who leverage specialized tools to address security issues at an organizational level.

Connection through to the Secure Cloud Services occurs through the Perimeter Firewall acting as the primary line of defense for the private Secure Control System network and can be connected through the Internet or a Virtual Private Cloud connection.

Conclusion

Smart building technologies are rapidly evolving, and the benefits are beginning to deliver excellent value, but these systems need to be deployed in a manner that addresses the cybersecurity risks over the life cycle of the system. A comprehensive, well-designed, and efficiently executed cybersecurity strategy can shield existing legacy BMS systems, protect new smart building control system implementations, and can confront the risks of embracing innovative IoT technologies and Cloud services. This practical strategy involves adoption of the best cybersecurity techniques from the IT domain and applying them with a focus on isolating the vulnerabilities of OT devices and systems. The ISA/IEC 62443 series of cybersecurity standards sets out the framework and roadmap to certified conformance to these standards for smart building automation and, in combination with a comprehensive Defense in Depth approach and complementary adoption of the NIST Framework and IOS 27000 standards, can facilitate secure interactions with valuable Cloud services and ultimately smarter and more effective buildings.

Schneider Electric
35 rue Joseph Monier, 92500 Rueil-Malmaison, France Telephone: +33 (0)1 41 29 70 00 software.schneider-electric.com

998-20437895 Rel. 11/18