SIEMENS

KEY CONSIDERATIONS WHITE PAPER

BACnet Secure Connect: The next generation of OT security for building operations

Index

Introduction

New and evolving technologies, including smart and autonomous building systems, come with a whole host of advantages but also increased vulnerability. Cyber threats now extend beyond the typical purview of IT to include the entire building automation industry. Luckily, for those involved in the operation and design of smart buildings, new technology and security protocols are being created and standardized.

BACnet Secure Connect (BACnet/SC) safeguards communication between building systems and devices in an IT-friendly manner. It applies the same technology to secure and encrypt communication between devices used on the internet for online banking connections and other critical applications, providing a cost-effective solution for standalone and networked facilities alike.

This paper provides current and prospective users with an overview of the BACnet/SC standard, along with key considerations to keep in mind when upgrading a building automation system that supports the standard.

Cyberattacks against buildings

Cyberattacks against buildings are on the rise, due to the rapid growth of attack surfaces and the convergence of IT and Operational Technology (OT) systems.

While attentive IT departments manage and secure computers, networks, servers, and applications, OT departments have historically managed building control systems, machinery, and IoT devices with different infrastructures and protocols. In the past, OT systems could rely on an "air gap" for security—meaning that they were not connected to a larger network or the world wide web, and so could not be externally accessed.

However, this is no longer the case. Many OT systems are now wholly or partly intertwined with a company's IT infrastructure. Integrating these previously isolated OT systems with IT allows for complete network visibility, performance optimization, increased real-time communications, and the ability to leverage the power of the cloud and analytics to save money and protect the environment. The value created by this connectivity and data is what makes smart building technology so attractive.

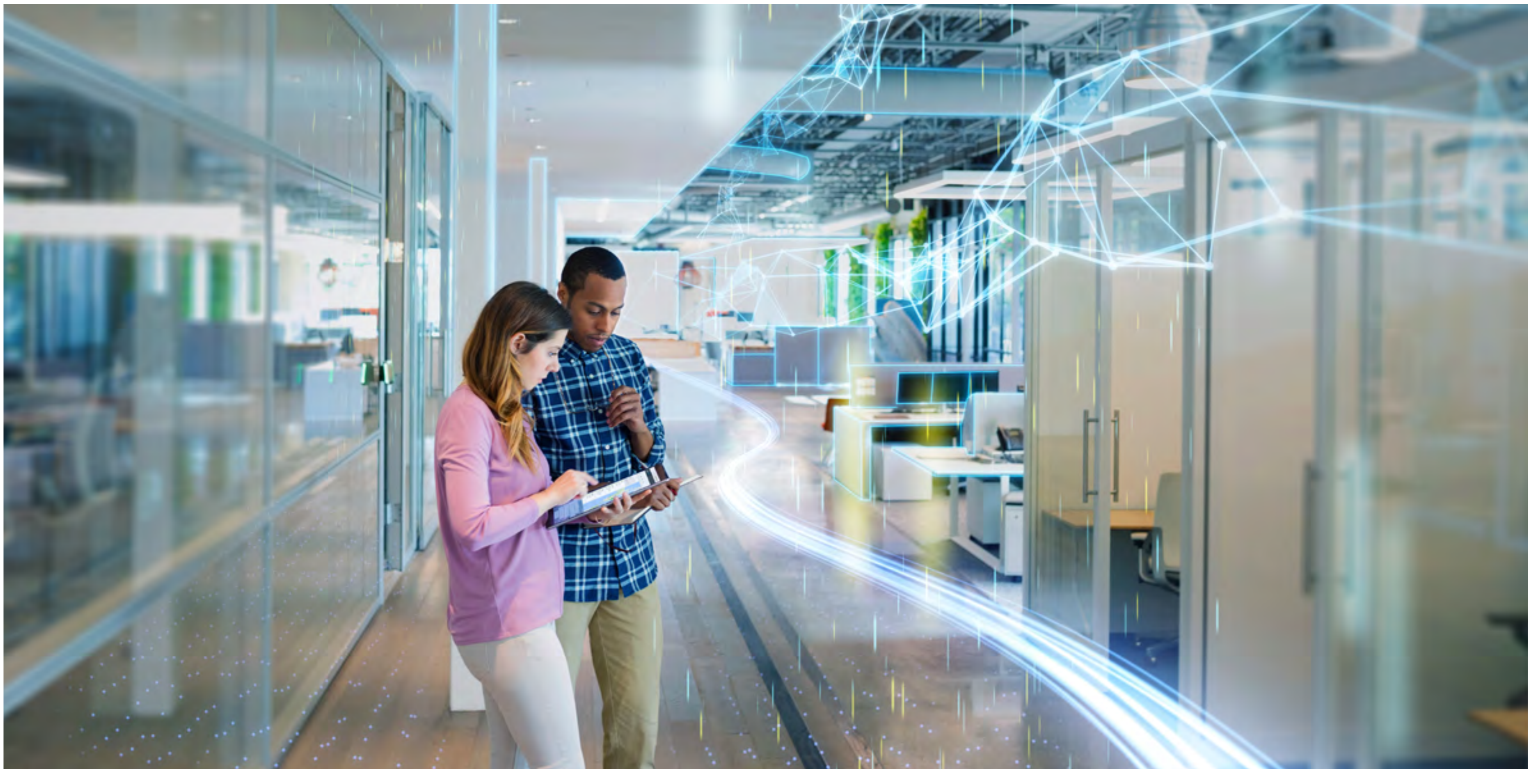
The tradeoff, however, is that as connectivity increases, opportunities for threat actors also increase. Attacks are on the rise by those looking to exploit these newly connected systems to access sensitive data or sabotage operations.

Attacks on building systems come in the form of zero-day exploits, ransomware, phishing, malware, DDoS, social engineering, firmware exploits, and more. Examples of cyberattacks targeting building protocols include:

- A DDoS attack knocked out the heating systems in two apartment buildings in Finland for over a week.[1]
- Hackers accessed the smart thermometer in a casino lobby's fish tank to gain access to a high-roller database.[2]
- A hacker gained access to a parking system's printer through an exposed wireless access point and printed a bomb threat.[3]

Attacks such as these have the potential for drastic consequences. For example, accessing a building's protocols could lead to a data center hack that prevents normal device operation, causing a shutdown. In a hospital setting, a hacker could even access control of lights in a surgery room, leading to life-threatening consequences.

Therefore, developing a robust security architecture that considers this new connectivity between IT and OT is vital. A defense-in-depth approach to cybersecurity that incorporates BACnet/SC can help companies and organizations reap the benefits of connectivity while reducing the risk of cyber threats.



Introduction to **BACnet/SC**

The story of BACnet began in the late 70s as increasingly sophisticated building automation systems began to emerge. Initially, these systems were proprietary, with no simple way to integrate different systems within a single building.

In 1987, the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) convened to solve the problem, creating the original Building Automation and Control Networks (BACnet). This non-proprietary standardized communication protocol enabled interoperability among compatible building-automation devices.

Today, the BACnet communication protocol is used by more than 1,000 manufacturers for building products and systems, including HVAC, lighting, access control, elevators, and security devices. The benefits of BACnet go beyond unprecedented levels of interoperability and efficiency across building systems. They include system scalability, backward compatibility with older versions of BACnet, and flexibility to meet the changing needs of building automation systems.

BACnet **security issues**

In the early days of BACnet, before the convergence of IT and OT systems, security wasn't much of an issue. Traditional BACnet security relied on virtual separation (such as VPN access and VLANs), physical separation, and proprietary protocol solutions.

However, virtual separation methods can increase complexity and cost while still lacking actual security at the device level. Physical separation limits many desirable smart building concepts, and the use of proprietary protocols diminishes the interoperability of smart building systems.

As the building automation industry embraced digitalization, it created a demand for BACnet/IP networks, which expanded communication among OT systems but also introduced new risks as IT and OT systems became increasingly intertwined.

In addition to lacking built-in security functionality, BACnet/IP networks faced issues of IT friendliness and acceptance. For example, the use of unsecure UDP ports, BACnet Broadcast Management Device (BBMD) broadcasts, and dedicated static IP addresses were not accepted by IT departments because they were incompatible with standard IT management and expectations. This created excess traffic and required complicated, manual IT management practices.

The BACnet/SC **standard**

BACnet/SC is a security addendum that eliminates the most troubling elements of BACnet/IP regarding IT network management, such as broadcasts, static IP addresses, and lack of encryption and authentication. It also works well with firewalls, network address translation (NAT), and proxy devices common in IT infrastructure and cloud computing.

BACnet/SC leverages the same interoperable and backward compatible capabilities built over the many years of BACnet protocol support and product development. It just adds a new and more secure data link for the transmission of data.

It uses the same end-to-end communication encryption method banks and governments around the world rely on for financial transactions. Additionally, it requires a mutual (instead of one-sided) Transport Layer Security (TLS) handshake. In other words, the BACnet stack itself is unchanged, while the link-layer is completely different, based on WebSocket Secure (WSS) - accomplished by WebSocket protocol over Transport Layer Security (TLS), and authentication instead of unsecured UDP.

Decades of experience have taught the Web community about best security practices for data exchange over the internet by using encryption. WSS is encrypted using the latest TLS security protocol, thus protecting against man-in-the-middle attacks. Putting BACnet inside brings the most popular building automation protocol on par with the latest security protocols.

BACnet/SC does not rely on the three traditional security approaches (virtual separation, physical separation, and proprietary protocol solutions), though physical/virtual separation may sometimes be needed for other reasons. For example, VLANs on local area networks inside the building, and VPNs for wide area network communication can still be used to complement BACnet/SC for increased security. In general, however, BACnet/SC is secure enough to run on even unsecured networks.

While BACnet/SC itself is not a silver bullet, it plays a critical role in a holistic defense-in-depth approach. BACnet/SC is the most significant advance in BACnet since the BACnet/IP release. The introduction of BACnet/SC is critical to providing a standard protocol with interoperability AND a secure network, all while addressing issues associated with IT friendliness and acceptance.

Defense in depth: An overview, and where BACnet/SC fits

A comprehensive cybersecurity strategy must integrate security across IT and OT systems. The defense-in-depth approach treats organizations like an onion with multiple layers of security placed throughout the combined IT/OT system. This provides broad, redundant protection using multiple independent defense methods.

Layers of the defense-in-depth include:

- Data/process security
- Device security
- Application security
- Host security (OS)
- Network security
- Perimeter security
- Physical security
- Organizational culture

Layered security puts more barriers in the way of attackers, making it more difficult for them to succeed. OT systems typically lag IT systems in terms of the number, sophistication, and integration of defense layers, leaving it more open to exploitation.

State-of-the-art firewalls protecting network boundaries are still critically important. However, effective protection requires implementing a blended IT/OT defense-in-depth approach, including well-thought-out policies.

BACnet/SC provides an incredibly powerful set of tools to secure OT devices and BACnet protocols and can play a key role in a defense-in-depth plan. For example, Web UI (user interface) should be secured with strong passwords. Secure (HTTPS) embedded web servers encrypt the data exchanged between the user's web browser and the web server and require a password change on initial login—ensuring that no "default" passwords are used on embedded devices. This is a big piece of defense in depth. Also, devices should not have any "open ports"—ports with vulnerabilities or back doors. BACnet/IP was the last unsecure piece and now with secure BACnet/SC, the communications are fully secure.

BACnet/SC implementation: **The hub-and-spoke principle**

Typical BACnet/SC implementation uses a hub-and-spoke architecture to effectively manage the data and provide secure communication between devices. In this case, a hub is employed to centrally manage the communication of BACnet/SC nodes. Connected to the hub are several nodes consisting of automation controllers and a control-system user interface (UI).

The hub relays all messages between the BACnet/SC network nodes. A network may have several hubs that route messages between nodes. The nodes initiate the connection to the hub and once authenticated, node-to-node communication is also possible to reduce the burden of processing lots of messages by the hub which can be useful in large systems to reduce hub traffic and ensure its operational performance and stability. With this architecture, an additional failover hub should be configured to avoid a single point of failure.

A BACnet/SC hub is a software function that can run on a BACnet router or other hardware such as an on-site server, or even in the cloud since the nodes reach out to the hub and not the other way around. It is firewall-proof and no exceptions in the firewall are needed as was the case with BACnet/IP. With BACnet/SC, connections are outbound (LAN to WAN). BACnet/SC routers allow for interoperability and backward compatibility to existing (or new) BACnet/IP and BACnet MS/TP networks. In fact, the BACnet/SC hub-and-spoke architecture can be set up to allow remote and local access, including access to multiple facilities across the internet, and access to a mix of secure and unsecure devices.

It's worth noting that a BACnet router which is routing BACnet/SC-to-BACnet/IP is not making the BACnet/IP network secure, it is simply making it accessible from the BACnet/SC side. The BACnet/IP network itself is still unsecure and should be considered a point of vulnerability for the entire building network. The same is true for BACnet MS/TP networks—a BACnet/SC router does not make these old BACnet networks secure, it simply makes them compatible to BACnet/SC clients which will include Desigo CC and Desigo Optic building management software solutions.

BACnet/SC **use cases**

The following use cases illustrate many possible BACnet/SC implementations, including scenarios illustrating secure access to unsecure systems for compatibility and migration purposes.

Local access with BACnet/SC devices

The BACnet Operator Workstation provides internal access via a hub to BACnet/SC devices. Connections are secure all the way around the network as all devices support certificates and authentication using BACnet/SC. A failover hub for redundancy also provides for direct communication between devices. Currently, this set-up would typically be seen in new construction.

Local access to a mix of secure and unsecure devices

The BACnet Operator Workstation uses BACnet/SC communication to connect to different routers and hubs, with failover hubs also possible. Some hubs may be connected to BACnet/SC devices only, maintaining all-around security. Other hubs may consist of a router connected to BACnet/IP and/or MS/TP devices. The BACnet Operator Workstation manages each network securely. It connects with BACnet/SC devices directly, while maintaining the ability to connect with unsecure devices via a BACnet/SC router. This will be a typical scenario due to the number of devices deployed using BACnet/IP in today's buildings and will become increasingly common everywhere as legacy systems are upgraded with BACnet/SC.

Remote access with BACnet/IP devices

The BACnet Operator Workstation accesses a facility remotely using BACnet/SC secure communications to a BACnet/SC hub and router (with a failover hub available for redundancy). Since the devices accessed are a mix of routed BACnet/IP and BACnet MS/TP devices, the communication is only secure between the BACnet Operator Workstation and the hub with BACnet/SC nodes connected to it — the BACnet/SC side of the network. Though communications inside the facility using BACnet/IP and BACnet MS/TP are not secure, this may be acceptable if it is anticipated that most threats will come from outside the facility.

Access to multiple facilities

The BACnet Operator Workstation uses BACnet/SC communication to access multiple remote hubs and routers, which may each have their own failover hub. Communication is secure from the workstation to the hubs and routers. Communication between any given hub and BACnet/SC devices is secure, as well.

BACnet/IP and BACnet MS/TP devices, which may be connected to the BACnet/SC router inside the facilities, are inherently unsecure, but are secured to the remote workstation connection thanks to BACnet/SC.

Interoperability and certificates with BACnet/SC

An important document used to assure interoperability for each BACnet product and compliance with the BACnet standard is the Protocol Implementation Conformance Statement (PICS). The PICS is critical for systems specifications. BACnet/SC has added key terms to watch for when evaluating BACnet/SC devices. Those terms include BACnet Interoperability Building Blocks (BIBBs) with new hub and direct-connection functions, as well as device profiles for hub and router functions.

Certificates are also important in BACnet/SC implementation. Currently, the BACnet/SC standard does not address the management of certificates or the tools and processes to manage creation, distribution, and renewal. As a result, each vendor's BACnet/SC certificate management may differ.

There are two approaches for certificate management for each BACnet/SC product. Certificates may be managed internally (Internal Certificate Authority) with the vendor tools that manage the BACnet/SC system specifically, or they may be managed with an External Certificate Authority provided by the customer.

Internal certificates will be easiest to manage, at least at first, using vendor-provided tools and methods. However, external certificate management may be implemented in some cases for high-security projects. Vendors and the end customer must work together on the process of authentication and certificate management. The IT department or individuals most familiar with certificate management processes should be the ones to map out use cases and the procedures needed to operate a building securely and efficiently.

Testing by BACnet Testing Laboratories (BTL) ensures that devices with operational certificates signed by the same certificate authority will be able to communicate with one another and support specified BACnet/SC features. Vendors must use encryption and authentication based on common certificates to ensure their products properly share BACnet messages with other vendors' products.

However, BACnet-based incompatibilities may still exist regardless of which link-layer is used (BACnet/SC, BACnet/IP, or BACnet MS/TP). It's important to check the PICS statement of each product to ensure they support matching BACnet functions as well as to confirm that they support BACnet/SC.

Migrating or upgrading to BACnet/SC

Because BACnet/SC supports routing to BACnet/IP and BACnet MS/TP, those with existing BACnet systems have the option to upgrade their existing systems incrementally and flexibly to BACnet/SC as needed. Building owners who are not already using BACnet systems should discuss migration options with the vendor or service team associated with their building management system. There may be ways to migrate cost-effectively without replacing the entire system.

It's important during the transition to consider the security of any non-BACnet/SC network segments. BACnet/IP and MS/TP devices are still subject to attacks as they are today, and access to the entire BACnet network through these older devices is still possible. New processes will also need to be developed for both certificate management and user training as part of extending the defense-in-depth building security model. If all existing BACnet devices need to support BACnet/SC, this requires working with building management system (BMS) vendors or service teams on a plan to upgrade software and firmware and replace older devices.

Key takeaways: BACnet/SC impact on building automation

BACnet/SC will have a significant impact on the building automation industry, including the following:

- Building owners and investors can implement more secure BMS networks. They will be better able to conform to cybersecurity frameworks and regulations such as NIST, ISO 27000 standards, ISO 31000 standards and others.

- IT managers may have BMS networks under their responsibility that conform to IT standards, eliminating some long-standing complaints about BACnet/IP.

- Consultants and specifiers are incorporating designs to support BACnet/SC or asking for "future upgradability."

- System integrators will have options for upgrading their current customers in a stepwise manner, as well as supporting new construction.

- Building operators and facility managers will still have a familiar protocol (BACnet), but without the headaches they had to address with BACnet/IP and ability to secure their unsecure networks.

- BACnet/SC provides the opportunity to completely merge IT and OT networks. This allows for designing and installing a single IP network infrastructure in new construction and avoiding the excess equipment, labor, cost, and complexity of running separate IT and OT network infrastructures.

As with anything new, IT will also need to prepare for new challenges faced with controller access, service costs, troubleshooting, and so on. Incorporating a new level of security protocol will require close partnership with manufacturers to ensure the building automation system is positioned for success.

When it comes to comprehensive security, however, BACnet/SC on its own is not enough. Instead, BACnet/SC should be considered an essential part of a defense-in-depth plan. There are also still more aspects to managing BACnet beyond the Secure Connect link-layer before the full expectations of the different stakeholders for BACnet/SC can be met. ASHRAE has mapped out plans to enable a fully managed and even more secure and IT-friendly BACnet soon.[4]

BACnet/SC does, however, solve the main issue of unsecure OT communication on the network which is a huge step in the right direction. Another advantage that the convergence of IT and OT systems (thanks to secure protocols like BACnet/SC) provides is that it equips IT departments with visibility and the ability to monitor and manage OT devices at the site. For example, IT can now monitor OT (building automation) devices and know when they go offline or fail. Visibility over OT devices also creates an increased sense of security and confidence of the site network. IT departments can now see all network-connected devices in the building, compared to in the past when they could only see IT devices, and the OT network was a "rogue" network which they did not have any visibility into or control over.

In the end, smart building networks must be protected against cyberattacks of all kinds—especially if they are to continue benefitting from digital transformation. BACnet/SC secures building automation, is cost-efficient, and enables easy migration. It also creates opportunities due to the flexibility in installation and certificate management and is well-positioned to impact the whole building automation industry as change is pushed by owners and IT managers.

Siemens and BACnet/SC

Siemens has been in the BACnet business since its inception in 1995 and continuously evolved ever since. Siemens is deeply involved in the development of BACnet/SC and is committed to solving outstanding challenges. Numerous Siemens employees have led BACnet's development, including Bernhard Isler (retired 2021), a principal author for BACnet Secure Connect for ASHRAE SSPC 135 IT-WG. The BACnet/SC standard is being applied to all aspects of Siemens BACnet automation systems and tools. For more information or a consultation on your path to more secure smart buildings, contact us today.

Sources

1. Kumar, Mohit, "DDoS Attack Takes Down Central Heating System Amidst Winter in Finland," The Hacker News, November 9, 2016, https://thehackernews.com/2016/11/heating-system-hacked.html.

2. Wei, Wang, "Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer," The Hacker News, April 16, 2018, https://thehackernews.com/2018/04/iot-hacking-thermometer.html.

3. Reber, Nicole, "5 Real-World Incidents Offer Cybersecurity Lessons for FMs," FacilitiesNet, January 10, 2019, https://www.facilitiesnet.com/security/article/5-Real-World-Incidents-Offer-Cybersecurity-Lessons-for-FMs--18191.

4. "ASHRAE's BACnet Standard Could Increase Cybersecurity," ASHRAE, November 10, 2020, https://www.ashrae.org/news/ashraejournal/ashrae-s-bacnet-standard-could-increase-cybersecurity.

Siemens Industry, Inc.
Smart Infrastructure
1000 Deerfield Parkway
Buffalo Grove, IL60089
Tel: (847)215-1000

Order no.: 153-SBT-1403

This document contains a general description of available technical options only, and its effectiveness will be subject to specific variables including field conditions and project parameters. Siemens does not make representations, warranties, or assurances as to the accuracy or completeness of the content contained herein. Siemens reserves the right to modify the technology and product specifications in its sole discretion without advance notice.