SIEMENS

How to Make Building Technologies as Secure as Internet Banking: BACnet/SC

The new standard for building automation security.

siemens.com/cybersecurity-buildings

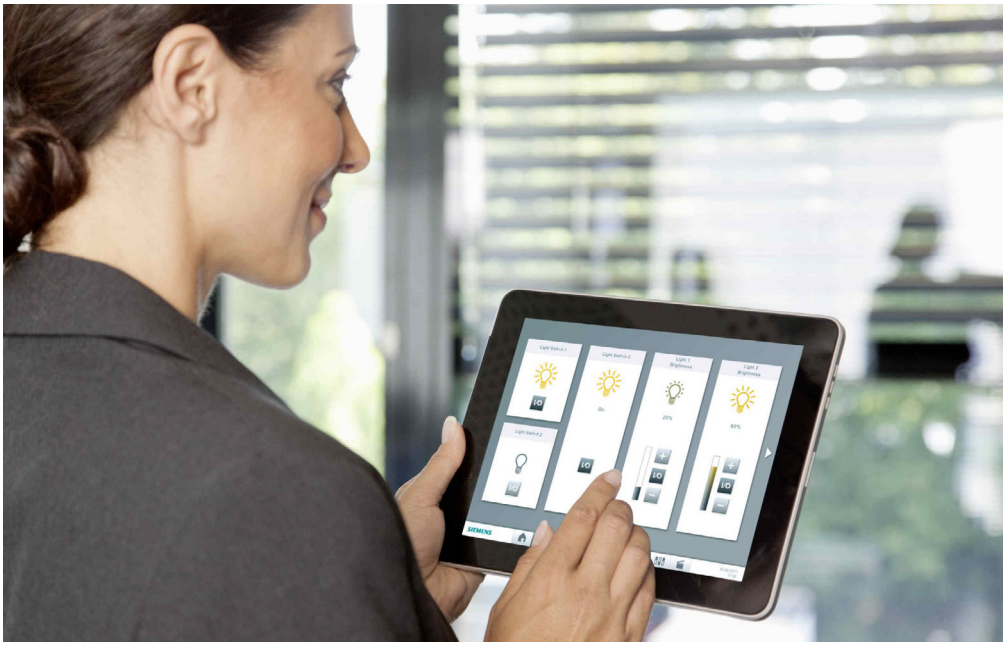
Table of Contents

Executive Overview

Today's increasingly digitalized and interconnected world puts the need for cybersecurity front and center. No longer just the concern of IT professionals, cyber threats can impact anyone in the building automation industry. The question about how to best address cybersecurity is critical. For those who own, operate or design smart buildings, a new technology is being created and standardized. BACnet Secure Connect (BACnet/SC) safeguards communications across building systems and devices to deliver a comprehensive security option. A cost-effective solution for standalone or networked facilities, BACnet/SC is IT-friendly and applies the same technology to secure/encrypt communication between devices as is used on the Internet for online banking connections and other critical applications.

This paper provides a comprehensive look at BACnet/SC. It explores the technological evolution that led us to where we are today, starting with the BACnet standard communication protocol. It examines the effect that Internet-connected devices have had on building automation, making advanced security measures necessary. The paper also provides insight into BACnet/SC and the benefits of incorporating it into the design of building systems. In addition, it addresses changes in the engineering and commissioning workflows and performance requirements for devices.

BACnet: 40+ Years of a Standard Communication Protocol



The industry needed a new technology that would allow various devices and systems to work together seamlessly.

BACnet's story began in the late 1970s and 80s when growing demand for energy efficiency in buildings overlapped a rapid expansion of new building construction. In response, leading manufacturers started producing increasingly sophisticated building automation systems and devices. Most were proprietary, which created new problems for building owners and managers. Namely, competing systems and devices could not communicate with each other. In addition, each system, from HVAC to fire safety and security, came with its own workstation that required separate attention.

The industry needed a new technology that would allow various devices and systems to work together seamlessly. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) decided to solve the problem in 1987. It convened the first meeting of its Standard Project Committee 135P (SPC 135P) that year. The Committee created the Building Automation and Control Networks (BACnet) non-proprietary standardized communication protocol that enabled interoperability between cooperating building automation devices. It was introduced as an ANSI standard in 1995 and became an ISO standard in 2003.

BACnet provides standardized methods for presenting, requesting, interpreting, and transporting information.

Growth of the open standard

Today, more than 1,000 manufacturers use the BACnet communication protocol when developing their products, which cover a broad range of building systems. The protocol provides rules that govern the exchange of data so BACnet-enabled devices can talk to each other easily regardless of the manufacturer. The rules have been applied to a wide variety of building-related products and systems, including HVAC, lighting, access control, elevators, and security devices. This enables an unprecedented level of interoperability across building systems, creating the efficiency sought by building owners, technicians and engineers. It has also helped consolidate multiple workstations into one control center and provided additional opportunities for operational and energy efficiency.

Other BACnet benefits include:

- System scalability and the ability to incorporate a variety of low-cost and advanced devices and workstations
- Backward compatibility with older versions of BACnet
- Flexibility to meet the changing needs of building automation systems, giving end users confidence in making plans for the future

It is no surprise, then, that BACnet adoption has grown dramatically around the world. In 2018, a research study found that BACnet-standardized products had more than 60% share and rising of the global building automation market. The study, conducted by BSRIA, a well-known provider of market intelligence in HVAC and Building Automation and Control Systems (BACS), predicted continued growth in BACnet adoption over the next five years. It anticipated continual improvements to the standard and to its ability to integrate with IT technologies, such as the latest Internet protocols and web services.

The secret behind BACnet's success

BACnet provides standardized methods for presenting, requesting, interpreting, and transporting information. It segments a device's interoperability into three distinct communication needs – how to represent information, how to make requests among each other, and how to transport information. It then defines the methods and standards to meet those needs. This allows BACnet-enabled devices to communicate with each other by creating, sending, and responding to requests over a variety of networks.

IP Subnet

⊤ LAN Segment

○ BACnet Device

BACnet's Unique Ability to Transport Information

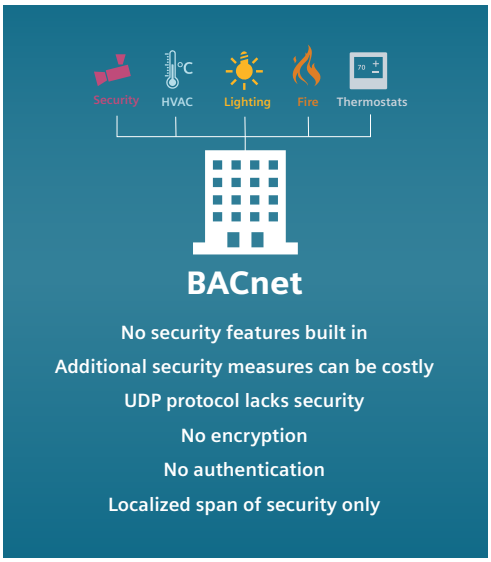
Transporting data is key to device-to-device communication. In the BACnet protocol there is a physical "network" data link layer. It allows BACnet-enabled devices to communicate with each other through an IP, Ethernet, or MS/TP network. This ability to work on multiple networks allows it to be used on a mix of communication networks within a single facility. At the zone (or single room) level, there might be an MS/TP network and BACnet MS/TP devices to send requests and responses among a defined group of devices. However, the building management system (BMS) would not be on an MS/TP network. BACnet-enabled devices can work with Ethernet addresses to communicate among other BACnet-enabled devices on the same subnet through an Ethernet network. And on a higher level using the Internet, BACnet/IP-enabled devices can communicate using a BACnet Broadcast Management Device (BBMD) on each subnet to send messages across the network. BACnet routers are devices that connect two distinct BACnet local networks. BACnet routers are used to route communications among BACnet datalinks.

How Secure is BACnet Today?

BACnet/IP expanded communication among OT systems but it also laid bare potential risks.

The beauty and benefit of BACnet is its interoperability. It allows all BACnet-enabled building automation systems and devices to communicate with each other. Yet, it has had a weakness – security. In the early days, when building automation systems were not connected to IT systems, security was not a significant concern. BACnet-enabled systems were separated physically and virtually from potential wrongdoers; therefore, BACnet messages did not require native encryption or authentication. This changed when the building automation industry embraced digitalization, which brought together IT and operational technology (OT) and created demand for BACnet/IP networks.

BACnet Security Status



BACnet/IP expanded communication among OT systems but it also laid bare potential risks. When BACnet/IP-enabled devices link to the same network as the enterprise, they expose the entire enterprise system to data mining, tampering, or unsanctioned reconfiguration. With the threat of potential damage to building equipment, system security is a necessity and, in more and more cases, a requirement.

Every day, BACnet/IP achieves the goal of expanding communication among OT systems but it lacks the built-in network security functionality that is needed today. Without built-in security, the following can happen:

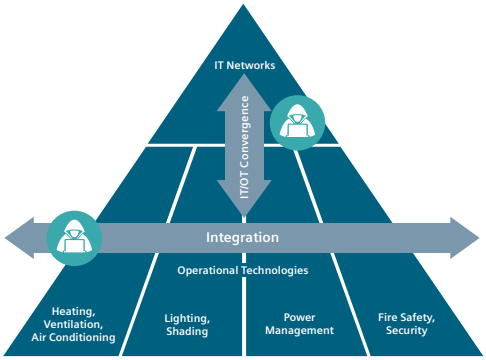
- No native encryption – BACnet messages are visible to anyone with access to the local network segment
- No native authentication or identity validation – any BACnet device can join the network to send or receive messages without proving its identity
- No native authorization – there is no control of BACnet device activity; any device connected to the local network can communicate with any other device
- No native integrity protection – BACnet messages are not protected from interception, modification, or replay
- User datagram protocol (UDP) is susceptible to attacks – the big security problem with UDP is the susceptibility to spoofing and denial-of-service (DOS) attacks. It does not have a handshake mechanism of any type like its more popular alternative the TCP protocol.

The Forces Driving BACnet Security

During the first half of 2019, data breaches exposed over 4.1 billion records.

In addition to BACnet/IP, other forces are driving demand for better BACnet security, from new mobile technology to new legislation. For example, the adoption of the Internet of Things (IoT) across building enterprises was a game changer that accelerated the convergence of IT and OT. IT manages the flow of digital information – or data – while OT manages the operation of physical processes and the machinery used to carry them out, which includes building devices, such as HVAC, surveillance, and access control equipment. Together, IT and OT capture key operational data that end users such as building owners and managers employ to make their facilities more comfortable, safe, and secure.

IoT devices can be easily added to any network, which means building systems are no longer isolated. In fact, Internet-connected devices can be accessed and controlled from anywhere in the world. They can communicate with each other and with an organization's IT systems, making them part of the larger enterprise-wide network.

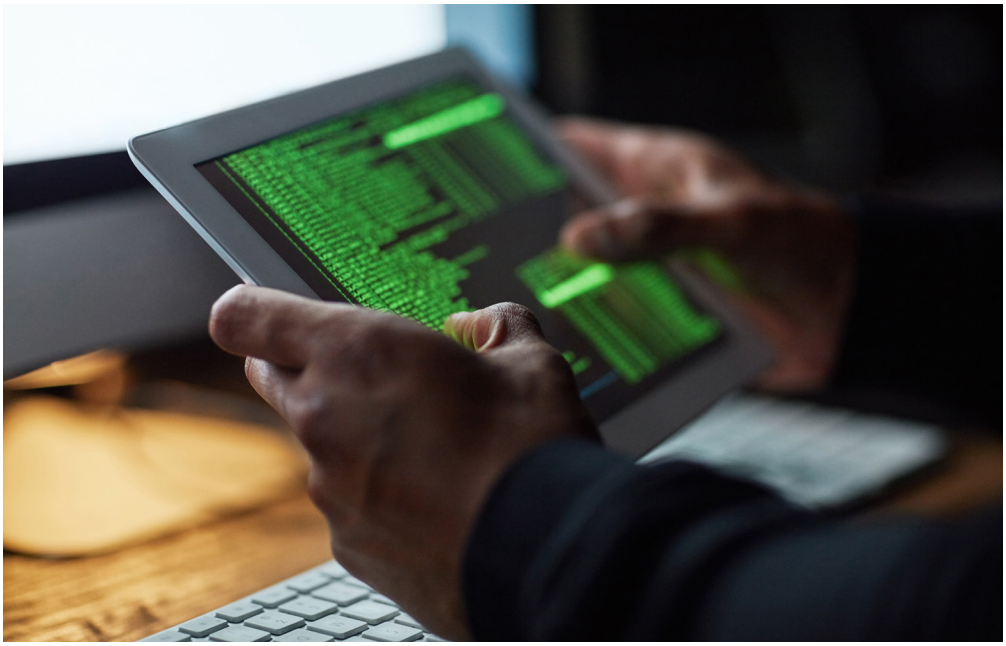


Internet-connected OT systems increase threats of cyber data breaches.

Hastening the convergence of IT and OT are major investments from high-tech global powerhouses. They bring a high level of technological savvy, open ecosystems, system infrastructure, and solutions into the building market. They demand systems and devices that are more intelligent and connected.

In response to these changes, IT departments have grown increasingly concerned. With building devices communicating over the Internet, many IT leaders fear that hackers will attack an organization through its building management systems. And the fear has been justified. In the 2014 attack against a large retail chain, the HVAC system was hacked and used to infiltrate the financial system. Credit card information for over 40 million customers was stolen. Three years later, cybercriminals stole a database of high-roller gamblers from a North American casino. They gained access through an Internet-connected thermostat in an aquarium located in the lobby.

Today, building owners and operators share the concerns of their IT counterparts. During the first half of 2019, data breaches exposed over 4.1 billion records, according to international security consultant Risk Based Security. As happened in the past, spam phishing was leveraged to gain access to OT systems, with hackers using HVAC systems as entry points into corporate IT networks and data centers. While building automation systems can be secured today with additional IT solutions, it requires heavy investment in personnel and financial resources.



Emerging regulations

The damage caused by cyberattacks can often harm large segments of the population. To protect their citizens, local and national governments are taking action by enacting laws and regulations to ensure strong, cybersecurity practices are in place. The laws and regulations are driving change to improve security in building devices and networks. For example, in January 2020, the California IoT Bill came into effect. This new legislation is aimed at regulating the security of IoT devices. It requires that each connected device have a means of communicating authentication. At the same time, the California Consumer Privacy Act (CCPA) came into effect. The CCPA places more repercussions on U.S. companies than the European Union's General Data Protection Regulation (GDPR).

In May 2020, Germany's Federal Ministry of the Interior, Building, and Community (BMI) published a new draft of its IT-security act, called IT-Sicherheitsgesetz 2.0., which broadens and strengthens existing IT security regulations. While its primary focus is securing operators of critical infrastructure, it promises to have a huge impact on all areas of IT security in Germany. It introduces incident notification obligations and mandatory IT security requirements standards. Fines for noncompliance can reach up to EUR 20,000,000 or up to 4% of the total annual corporate turnover achieved in the previous financial year – a massive increase to the previous maximum.

More regulations on the national and local levels are likely to follow. In preparation, organizations should begin following best practices in designing their products, systems, and processes by implementing cybersecurity standards, such as IEC 62443, ISO 27001, and NIST 800-53.

Building owners need to be aware that there will be new national and international laws that will speed up the change from BACnet/IP to BACnet/SC for security purposes.

The Need to Improve Security of BACnet Networks

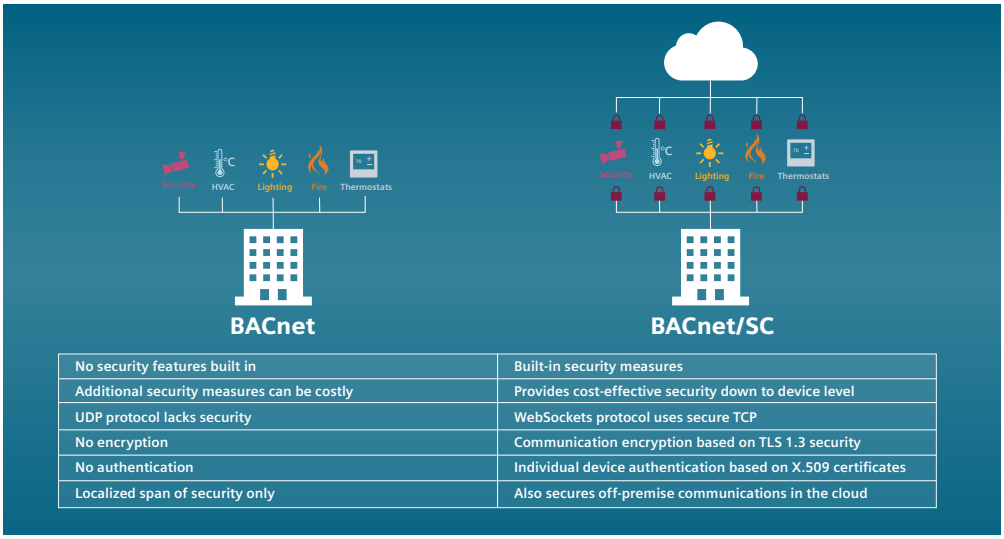
It is clear that BACnet security has become a leading issue. Currently, BACnet security requires a separate system that coordinates with IT to ensure the necessary network segmentation and segregation. Examples of BACnet security measures include using a Virtual Local Area Network (VLAN), a firewall, a Virtual Private Network (VPN), or Media Access Control (MAC)-address filtering with white lists to protect BACnet devices.

Many organizations have chosen VPNs to resolve the BACnet/IP security problem for remote BACnet connections and VLANs for the local separation of BACnet from the IT network. A VPN encrypts data at the sending end and decrypts it at the receiving end. However, widespread adoption of VPNs has not happened because they are complex and costly to create and manage. VLANs are a way to establish several mutually separated logical networks on one shared physical infrastructure. While VLANs are quite common today to separate IT from OT, they are cumbersome to coordinate, require special hardware, and don't solve the core problem that anyone who somehow accesses the (V)LAN also would gain full access to the building automation system. Other organizations use proprietary protocols, a practice that is becoming less accepted daily. As a result, most BACnet networks are not sufficiently protected today.

While current efforts may offer some level of segregation, they do not provide a comprehensive cybersecurity solution. From a building automation perspective, the solution needs to be at the device and building network level, and it needs to provide authentication and encryption. Incorporating better security into the BACnet protocol presents a logical, core solution. If hackers attack an organization through its BACnet systems, a solid BACnet security solution will be the last line of defense.

To solve the security issue, the ASHRAE committee that oversees BACnet developments turned to its IT working group – SSPC 135 WG-IT – to help make BACnet more IT-friendly. As part of its efforts, the IT working group focused on the BACnet security problem. The result is BACnet Secure Connect (BACnet/SC). The new BACnet/SC protocol adds encryption at the device and systems communication level, eliminating many of the concerns building owners, facility managers and IT professionals have had with BACnet.

BACnet/SC Improves BACnet Security Issues



No security features built in	Built-in security measures
Additional security measures can be costly	Provides cost-effective security down to device level
UDP protocol lacks security	WebSockets protocol uses secure TCP
No encryption	Communication encryption based on TLS 1.3 security
No authentication	Individual device authentication based on X.509 certificates
Localized span of security only	Also secures off-premise communications in the cloud

BACnet Secure Connect: What is It?

BACnet/SC is a security addendum to the BACnet protocol that protects BACnet communication from being hacked. Unlike BACnet/IP that lacks built-in security functionality, BACnet/SC is designed to be even more secure than online banking. It uses the same type of communication encryption that banks rely on for financial transactions but it requires a mutual TLS handshake. In online banking, however, the initial authentication step is single-sided only: The bank uses TLS to authenticate its genuineness to the user, but not vice versa. Therefore, bank customers have to use other means to authenticate themselves as legitimate users, such as PINs, TANs, or SmartPhone verification. BACnet/SC elegantly avoids this problem with its use of mutual TLS authentication. It certifies the authenticity of BACnet protocol packets to both ends and thus reduces the possibility of fake communication.

As the BACnet/SC addendum only defines a new, cybersecure datalink, it does not fundamentally change the BACnet application. Therefore, BACnet/SC is compatible with any previous and future versions of BACnet. That means building owners and managers do not need to replace devices, nor will they lose any capabilities from an existing BACnet system. For them, it is just a new TLS-secured datalink for their BACnet-enabled devices.

BACnet/SC's cybersecurity technologies are not new. They come directly from the IT world. The goal of BACnet/SC is to solve many of the challenges of deploying BACnet on IP-based networks. To illustrate how it meets those challenges, on the following page is a high-level view of the BACnet application and the layers that make it work.

Building owners and managers do not need to replace devices, nor will they lose any capabilities from an existing BACnet system.

BACnet Application with BACnet Secure Connect Virtual Datalink	
Application	BACnet Application
	BACnet Application Layer
	BACnet Network Layer
	BACnet/SC
Application Layer	WebSockets / HTTP
Transport Layer	TLS V1.3
	TCP
Internet Layer	IP / Pv6
Link Layer	Any Datalink for IP or IPv6

As illustrated above, BACnet/SC is a virtual datalink that is added directly into the BACnet protocol stack under the BACnet Network Layer in the application.

- The application layer specifies which communications protocols and interface methods the application will use.
  - BACnet/SC uses WebSockets, a communications protocol that operates over HTTP (HyperText Transfer Protocol), the underlying protocol that makes the World Wide Web function. A secured version of the WebSockets protocol is implemented in all current web browsers.
- The transport layer is responsible for end-to-end communication over a network:
  - BACnet/SC is built on TLS 1.3 (Transport Layer Security 1.3), the sophisticated IT encryption standard used for online banking connections and other critical applications. (See “Better BACnet Security” for more details.)
  - BACnet/SC uses TCP (transmission control protocol), which defines how to establish and maintain a network conversation for data exchange. And it is more secure and IT friendly than UDP, which was used initially in BACnet/IP.
- The Internet layer is responsible for the transmission of data packets.
  - BACnet/SC is prepared for IPv6, the latest version of the Internet Protocol, because WebSockets can be used for both IPv4 and IPv6. IPv6 assigns addresses to computers and devices so it can route traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.
- The link layer, also known as the datalink layer, refers to the actual networking architecture, such as the Ethernet, a Wireless Local Area Network (WLAN) or 4G/5G Internet.

Better BACnet Security

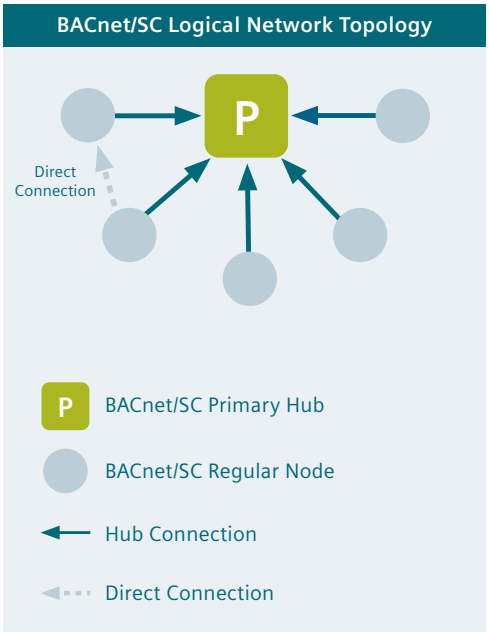
The chart on this page illustrates the core principles of how the BACnet/SC addendum achieves a new level of security without sacrificing backward compatibility. The upper BACnet layers, specifically the application layer and network layer, have not changed at all. However, the way the standard handles end-to-end connections makes it more secure.

The design's architecture, for example, is centered around a hub. It uses a hub-and-spoke principle based on TLS-secured WebSockets to connect devices to a hub and a secured unicast routing mechanism between such hubs. This is an improvement over BACnet/IP, which uses UDP broadcasts and BACnet Broadcast Management Devices (BBMDs). Historically, BBMDs have been a challenge to configure in large systems. Today, BACnet/SC can replace that approach in many applications.

With BACnet/SC, a network may have several hubs that route messages between devices. For security purposes, BACnet/SC hubs will only forward messages between BACnet/SC devices that have the right TLS certification. As for the BACnet language itself, it remains largely untouched, meaning building operations do not have to train for a new protocol. To learn more, it is worth taking a deeper dive into each of these design elements.

Secured messaging: Hub-and-spoke principle

The BACnet/SC hub-and-spoke principle, or topology, delivers messages to devices in a cascading way that prevents the system from overloading. A BACnet/SC hub is a software function that can be on a BACnet router or other hardware, or it can be completely virtual. Regardless, the hub is essential to network communication between devices, so BACnet/SC can be implemented with redundant hubs, avoiding downtime.



Source: ASHRAE BACnet Secure Connect, A Secure Infrastructure for Building Automation Whitepaper

The hub relays all messages to the network devices, as well as between specific devices. All BACnet-enabled devices are required to make a connection to the primary hub. Once the hub authenticates the devices, they can send messages through that hub. For additional security and reliability, BACnet/SC offers the option of peer-to-peer direct connections. In both instances, the hub and node/device in the architecture validate each other in order to have a certificate signed by an accepted Certificate Authority (CA).

In BACnet/SC, hubs take the place of BBMDs, which were not IT-friendly and which presented another unsecured way into the network. Hubs, on the other hand, are an IT-friendly, highly secured method of managing messages to and from machines on the network. Connections are always established from the nodes to their hub, which allows for firewall-friendly topologies with distant hubs.

Certification is a well-known method for keeping malicious users out of a system.

BACnet/SC requires that access to the hubs takes place through encrypted WebSockets. This requirement ensures that communication from the hub to the devices – or nodes – is secured. A node can be as simple as a thermometer or as sophisticated as a device that routes to an existing BACnet system, or even to the facility's main workstation. The hub-and-spoke topology builds redundancy into the system by adding a failover as secondary hub in case the primary hub fails, a mitigation strategy against single point of failure risk. This topology is ideal for networks that span multiple sites.

Secured communication with Transport Layer Security (TLS)

BACnet/SC uses the TLS cybersecurity standard preferred by the IT world. Therefore, an OT system that uses BACnet/SC will be at least as secure as the IT network it resides on and will be able to connect through IT firewalls without any special configuration. TLS is an industry standard being used for securing millions of HTTP transactions over the Internet. While TLS version 1.2 is currently in use in the IT world, BACnet/SC goes even further and demands TLS 1.3. The use of TLS and digital certificates is the basis for the security features of BACnet/SC. TLS is the technology used in "https://" and improves the security of communication between web browsers and web servers.

Secured operation with certification

As mentioned above, another area where BACnet/SC meets IT security standards involves the certification of devices and users. Certification is a well-known method for keeping malicious users out of a system. It requires that a trusted Certificate Authority (CA) digitally signs a certificate for each device and user. The certificate allows devices and users to operate on the network. The server confirms the validity of the digital signature and whether or not the certificate has been issued by a trusted authority. In the case of user authentication, digital certification provides more security than authentication with usernames and passwords, which can be stolen. Once the verification is completed, a successful connection can be made using TLS.

Importantly, BACnet/SC authenticates devices and users using X.509 certificates and public key infrastructure (PKI). PKI serves as the cybersecurity and encryption framework that protects data transmissions. X.509 is a widely accepted international security standard.

Using dynamic IP addresses

An IP address is a numeric or alphanumeric label for every machine that uses the Internet. It both identifies a device and allows it to receive messages, in the manner of a postal address. The two types of IP addresses are static and dynamic. A static address stays the same until the device is decommissioned or the network architecture changes. A dynamic address is assigned by the network when the device connects and which changes over time. BACnet/IP and BACnet/SC allow the use of both types of addresses. Dynamic addresses are particularly useful for the all-important hub in the hub-and-spoke topology.

How BACnet/SC Benefits Building Stakeholders

With its built-in security features, BACnet/SC offers significant benefits for securing an organization's OT network. It is an open and free-to-use standard that applies best practices from the IT world, using state-of-the-art security while working well with existing firewalls. It even improves the security of end-to-end device communication over insecure networks.

The end-to-end encryption in BACnet/SC protects the BACnet data by converting the wrapper that surrounds it into a cipher or code. The effect is like putting the message in an armored car. The encryption creates additional barriers. On top of that, the authentication procedures allow only certified users and devices to be on the network.

But BACnet/SC's value extends beyond securing technology. It provides multiple benefits to stakeholders throughout an organization. BACnet/SC has an impact across the facility, starting at the top, as shown on the next page.

From a management and investment perspective, BACnet/SC offers unexpected efficiencies and opportunities.

How BACnet/SC Can Impact the Building Automation Industry				
Owner / Investor	**Planner / Designer / Consulting Engineer**	**Building Operator**	**IT Operator**	**System Integrator**
• Stronger security landscape and confidence in business continuity • Adhere to regulatory requirements with end-to-end protected communication and privacy • Market-leading identity and branding for assets • Backward compatability to protect new and existing assets	• Creates a user / owner focused solution • Clear path to define security expectations • Industry standard to create compliant integration and cybersecurity specifications • Standard encryption mechanisms guarantee interoperability • Backward compatability	• Improve operation continuity • Clear expectations, auditing and maintenance processes • BACnet language remains untouched – no new protocol to be learned • End-to-end encryption protects communication and privacy even in public environments	• Big step toward addressing overall concerns with OT communications • Reduced complexity • Managed cybersecurity for BACS • NAT and firewall friendly • Leverages IT standards for seamless integration • Fewer special requirements (e.g., static IPs, UDP broadcasts, BBMDs)	• Easy step-wise extension / migration of installed base • BACnet/SC is 100% backward compatible • Service opportunities and extended scope • Deliver with more confidence – manage risk with secured communication

Building Owner and Investor

Many building owners already trust the benefits BACnet offers since it has a 60% and rising share of the global building automation market. BACnet/SC builds on this existing trust and goes a step or two further – it increases confidence in business continuity and helps increase property values. The higher level of security it provides equates to a lower likelihood of business disruption. BACnet/SC is also backward compatible with existing installations, which protects the value of the owner's past investments in BACnet and makes it easy to integrate new versions. This helps maintain the building automation system's value, increasing the facility's worth.

From a management and investment perspective, BACnet/SC offers unexpected efficiencies and opportunities. By protecting digital communication from end to end and applying security best practices common in the IT world, BACnet/SC helps owners and investors comply with current and upcoming laws and regulations about secured communication and privacy. In addition, BACnet/SC not only secures on-premise devices, it also secures off-premise communication via the Internet or cloud, eliminating some financial risk. This opens the door for cloud-based services for organizations interested in selling that service as part of their income stream.

Planner / Designer / Consulting Engineer

For facility planners, designers and consulting engineers, BACnet/SC's interoperability is a significant attribute. Its standardized encryption mechanisms, which guarantee interoperability, provide freedom of choice among devices of different manufacturers. And its backward compatibility with other data link options allows designers to ensure a smooth transition from existing building installations into the new world of BACnet/SC.

Building Operator

BACnet/SC represents a big-picture solution for organizations of any size, supporting a building operator's overall goals. As mentioned, it builds on existing investments in BACnet and takes those investments several steps further. It helps keep the building up and running while simplifying the workload. And since it is an addendum to BACnet/IP, building professionals do not have to learn a new protocol. It is an easy-to-implement solution to secured on-premise devices. And, thanks to its end-to-end encryption, it also makes off-premise communication in public environments via the Internet and the cloud more secure so that it remains private.

BACnet/SC will make it much easier to secure and standardize a building automation infrastructure.

IT Operator

The benefits of BACnet/SC to IT stakeholders cannot be overstated. Its managed cybersecurity for building automation control systems is a big step toward addressing an IT department's overall concerns regarding the cybersecurity of a building's networks. Today, various approaches are used to secure the BACnet infrastructure, but these solutions are complex and can be difficult to implement. BACnet/SC will make it much easier to improve the security of and standardize a building automation infrastructure. It is compatible with existing BACnet deployments and supports IT best practices. For example, BACnet/SC enables a building system to connect through IT firewalls without requiring special configuration. It also supports the infrastructure IT departments have in place for managing their servers and client computers. This includes the previously mentioned PKI and X.509 certificates, which are used in many Internet protocols, including TLS/SSL (secure socket layer), which is the basis for https://, the secured protocol for browsing the web. BACnet/SC integrates easily and seamlessly with existing IT infrastructure.

Systems Integrator

BACnet/SC makes life easier on several fronts for systems integrators. As previously discussed, BACnet/SC is an addendum to BACnet/IP. Its structure enables easy, step-wise extension or migration of an installed base and the mixed use of different topologies. Integrators will also appreciate the fact that BACnet/SC is 100% backward compatible with all existing BACnet deployments and devices. And it is compatible with newer versions of BACnet to easily support new projects. In addition, the effort it takes to incorporate BACnet/SC devices is significantly reduced. For example, BACnet/SC simplifies the IP application.

Systems integrators will be happy to know BACnet/SC eliminates the requirement for user datagram protocol (UDP) broadcast messages, a connectionless communication protocol that is less reliable than BACnet/SC's transmission control protocol (TCP). It also supports the domain name system (DNS) and dynamic host configuration protocol (DHCP) used in the IT world. DNS ensures that servers, devices, and services can be found by their names. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so it can communicate with other IP networks.

Put it all together and BACnet/SC keeps all the features that make BACnet/IP so useful to building owners and facility managers while securing it at a level that meets the highest IT standards.

Challenges and Opportunities Remain for BACnet/SC

While BACnet/SC is setting the stage for a more secure future in building automation, there are a few challenges to overcome before it can be fully adopted across the industry. Five key issues that need to be resolved include:

- Ensuring scalability for large, campus sites
- Developing technical solutions between routers and older data links
- Ensuring full integration to IT enterprise landscapes
- Adapting workflows for engineering and commissioning and operations and maintenance
- Identifying a viable security solution for small facilities with limited IT infrastructure

Another issue that is receiving a lot of attention is the installation and maintenance of digital certificates at both ends of the mutual TLS handshake. A digital certificate provides an additional layer of security. It encrypts and signs messages with a digital signature and allows BACnet-enabled devices to more securely communicate with each other. Each device must have an individual certificate installed and only accept correctly encrypted messages to improve confidentiality and integrity in communication between building devices.

BACnet/SC provides building owners with a lot of flexibility in choosing how to install and maintain certificates. They can select the best option based on the size of the installation site. For small sites, they can choose self-signed certificates, which are signed with a vendor tool. For larger sites and critical infrastructure, the better option is to have certificates signed by a Certificate Authority (CA), a third party that issues and authenticates digital certificates. Today, CAs in IT play a critical role in how the Internet operates and how transparent, trusted transactions can take place online. They issue millions of Digital Certificates each year. If building owners choose CA certificates for their BACnet/SC installation, they have additional options on where to host the certification process – cloud-based certification, gateway-based certification, or certification hosted on each device.

In practice, one of the challenges of BACnet/SC deployment happens in new construction sites, where the IT infrastructure is typically not yet in operation when the building automation installations are commissioned. While this is not much of a problem if self-signed certificates are used for BACnet/SC, it does require more foresight in workflow planning if PKI is being employed.

BACnet/SC has the flexibility to match the size of the project at any site and promises to provide a high level of secured communication among devices.

Small site installations: Self-signed certificates are one of the preferred options for small installations. There are three self-signed solutions. First, the building automation system does it all without IT involvement: it generates and signs the certificates. Second, the building automation system generates the certificates, but IT is involved in the signature. Third, IT generates the certificates, but the building automation system signs them. The certificate is then sent directly to the controllers. It typically remains unchanged over the lifetime of the project.

Large site installations: For large installations or multi-vendor projects or critical infrastructure projects with their high cybersecurity demand such as an airport, a self-signed certificate might not be a feasible option due to the high number of devices from many different manufacturers. As mentioned previously, a better and more efficient solution is to use a CA-signed certificate, which is widely accepted by all manufacturers. CAs form a common "root of trust" among devices. An example of how it works is the client-server communication used on people's personal computers on a daily basis. Everyone can use the encryption and decryption mechanisms because there is a hierarchy of trust among devices. CA-signed certificates do need to be renewed more frequently than self-signed certificates, with required renewals every four to six months, depending on the project and location. However, the broad acceptance of CA-signed certificates makes them a much faster option for large sites, expediting the engineering and commissioning of a project.

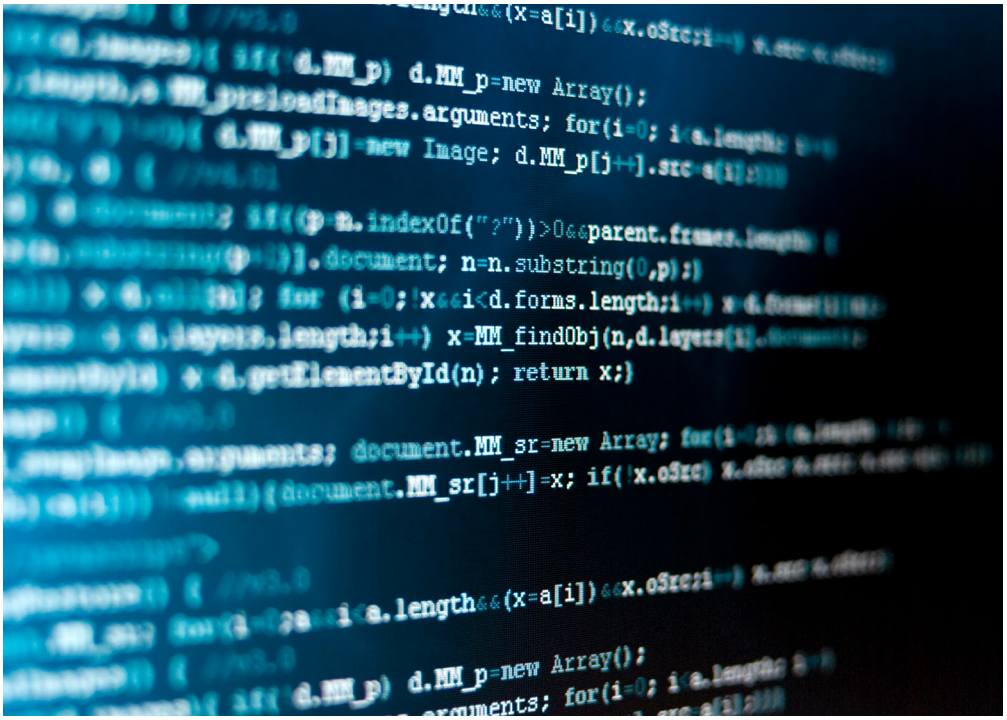
There are several options on how and where to host certification when using BACnet/SC with CA-signed certificates. The first is hosting in the cloud, be it private or public. Advantages of cloud-based certificates include remote access and management, simple renewal, and seamless troubleshooting. Cloud-based hosting is becoming more popular today, and its popularity is expected to accelerate. However, there are markets such as the military and financial industry that will not connect local networks to public cloud-based technology due to security concerns. They rely solely on private cloud networks.

An alternative to cloud-based options is to use a gateway, which acts as a proxy between multiple devices. Users can connect a large number of devices to a single gateway, providing a single hub for external CAs. The gateway offers a virtual handshake to other devices and can utilize public or private keys for rapid encryption, decryption, and tamper detection of digital certificates.

A third option is to have every device maintain its own enrollment for certificates, each being responsible for a direct connection to a CA. But it creates a trade-off between hardware costs and IT-friendliness. It is good for larger installations with fewer devices because the volume of outside connections will scale up linearly to the number of devices. For example, a site with 500 controllers will need to run 500 direct Internet links. This will put a burden on IT professionals to manually enter 500 exception rules into the firewall, which is arguably unreasonable. For sites with hundreds of devices, a gateway would be a better choice.

BACnet/SC has the flexibility to match the size of any project and promises to provide a high level of secured communication among devices. ASHRAE, with the help of manufacturers around the world, is working expediently to improve the ease of using BACnet/SC even further.

Siemens Commitment to BACnet/SC



For Siemens, the BACnet era began with the launch of the Desigo 30 controller in 1995. Since then, the standard has continued to evolve, and Siemens products along with it.

As new technology and regulations continue to drive demand for stronger security measures, Siemens expects BACnet/SC will become a new normal for all kinds of projects: from small facilities like kindergarten to high schools to large critical infrastructures like airports, healthcare systems, and utilities. To help industries adjust to the new normal, Siemens Smart Infrastructure is deeply involved in the development of BACnet/SC and is committed to helping solve its outstanding challenges. Siemens employees have held various leadership roles in BACnet's development, including being a principal author for BACnet Secure Connect for ASHRAE SSPC 135 IT-WG.

Siemens commitment to BACnet/SC goes beyond development and into implementation. The BACnet/SC standard is being applied to all aspects of Siemens BACnet automation systems and tools. This includes making it available via firmware upgrades on relevant devices, starting with new primary controllers (PXC4, PXC5 and PXC7) and Desigo CC. It will be in future releases of Desigo CC, in new Desigo hardware and most actively supported devices, including Desigo Room Automation. In addition, backward compatibility and extension/ migration compatibility will be available where needed. It will also be available for proof-of-concept tests with existing key user groups. Siemens invites investors, building owners, facility operators, and IT managers to engage in discussions about building system security and how BACnet/SC can be applied in their operations. Contact your local Siemens representative or find one at siemens.com/bt/contact.

Summary

The building automation industry has quickly evolved to meet market demand for greater efficiency and control. The last 40 years have seen an incredible expansion of building technology sophisticaton, from the adoption of BACnet, to the Internet of Things, to BACnet/IP, to interoperability and machine-to-machine communications. Once relatively isolated, building technologies are now connected and offer real-time benefits throughout an enterprise. However, greater connectivity increases the threat from cyberattacks. Cybersecurity, an issue once restricted to the IT world is now a pressing problem for building owners, managers and operators.

While a variety of solutions have been developed for protecting building automation assets, most are either too costly or too restrictive for long-term, large-scale use. From a building automation perspective, the solution needs to be at the device and building network level. It needs to require authentication and encryption. To meet the requirements, ASHRAE has developed BACnet Secure Connect (BACnet/SC).

As a security addendum to the BACnet/IP application, BACnet/SC has many benefits. It addresses the risks of sharing data over private and public networks while keeping BACnet systems open, flexible, and affordable. It is compatible with any previous and future versions of BACnet while applying the security techniques used by financial institutions and the IT world. In other words, it keeps all the valuable features of BACnet/IP while providing security levels that meet the highest IT standards. When it is available, today's high cost to improve the security of BACnet networks will be eliminated, providing peace of mind for building owners, facility managers, and IT stakeholders alike.
The time to explore and adopt this emerging technology is now. To learn more about BACnet/SC, please contact your local Siemens representative or find one at siemens.com/bt/contact.

Cybersecurity Disclaimer

Siemens provides a portfolio of products, solutions, systems, and services that includes security functions that support the secure operation of plants, systems, machines, and networks. In the field of building technologies, this includes building automation and control, fire safety, and security management as well as physical security systems.

In order to protect plants, systems, machines, and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines, and networks, which should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g., firewalls and/or network segmentation) are in place. Additionally, Siemens guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html.

Siemens portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under https://new.siemens.com/global/en/products/services/cert.html.

Published by
Siemens Switzerland Ltd.

Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
6300 Zug
Switzerland
Tel +41 58 724 24 24

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Article no. SI_0194_EN (status 12/2020)