SIEMENS

Building Automation System Security with BACnet Secure Connect

Augment your organization's cybersecurity by including building automation systems into a holistic security approach

Index

The necessity for enhanced security in building automation systems

Building automation systems (BAS) have seen numerous advancements in technology in recent years. Increased building connectivity and a drive toward accomplishing smart building applications has led to a convergence of operational technology (OT) and IT networks.

Cyber threats now extend beyond the typical purview of IT. If not managed properly, the convergence of IT networks with less secure OT networks — such as heating, ventilation, air conditioning (HVAC), lighting, energy metering, security, and access control — can increase security risks and leave smart buildings vulnerable to cyberattacks. Increased connectivity means a growing attack surface, which has brought the focus of IT and cybersecurity professionals to OT systems security. The value of connected building systems is clear; however, managing and decreasing the attack surface is more challenging than ever as a result.

One building can have numerous systems and IoT-enabled devices. The increasing number of connections makes the attack surface larger and organizations are more vulnerable than ever.

If not properly protected, connected systems could expose an organization's critical data or digital processes and increase the chance of a security breach. About half of the IP-connected devices in a building today are non-traditional devices like IP cameras, IoT devices, and OT devices. This increases the attack surface and makes it very hard for security teams to patch and manage networks, which is why it is important that devices have built-in security. BACnet Secure Connect (BACnet/SC) brings security on the device level right into the communication protocol. If a hacker found their way into the BACnet system, BACnet/SC could be the last line of defense.

BACnet/SC reduces risk and enhances BAS security by adopting well known and accepted IP application protocols and IT-industry-standard techniques that IT professionals use today.

If not properly protected, connected systems could expose an organization's critical data or digital processes and increase the chance of a security breach.

Closing the IT-OT **cybersecurity gap**

There is compounded growth of cyberattacks as building automation systems become increasingly connected, requiring organizations to respond with more layered defense mechanisms. However, OT networks are often ignored when it comes to holistic security.

Operational technology is the backbone of a functioning building. Enhancing security of OT systems means providing protection for the availability, integrity, reliability, and safety of the physical devices that make essential building functions possible. In addition to protecting operational infrastructure, incorporating OT systems security into a holistic security approach can close attack vectors and drastically decrease the possibility of cyber threats originating in the OT space.

Cyberattacks can be costly, but the risks are not limited to financial impact. The reality of a cyberattack is also the loss of valuable data and intellectual property. Cyberattacks can bring critical processes to a halt and compromise an organization's reputation and ultimately diminish their brand. It is a myth that only large organizations who have a lot at stake are concerned with cybersecurity. Most organizations, whether small or large, have data and processes that are critical and valuable to their business and could be crippled in the event of a cybersecurity breach.

The desire for increased cyber protection is not limited to government, healthcare, critical environments, big pharma, data centers, or financial institutions. Organizations have a lot at stake, but also require the benefits of smart building applications to meet targets of efficiency, space flexibility, occupant comfort, and compliance to government regulations. Cyberattacks are on the rise, and attempts to exploit newly connected systems to access sensitive data or sabotage operations are constantly being covered in the media. Cybersecurity in OT networks is no longer an option. An enhanced security solution for OT networks is needed to protect smart buildings. Thankfully, the building automation industry is actively addressing cybersecurity risks by implementing advanced security features.

BACnet/SC brings security and IT acceptance to OT systems

It is never too early for organizations to prepare for phasing in new technologies that strengthen building automation system security. BACnet/SC is the next step on the continuum to interoperable and secure BAS.

The new BACnet/SC data link layer option is a significant update to the BACnet standard which brings enhanced cybersecurity and IT acceptance to BACnet systems. By investing in BACnet/SC upgrades, customers are not only investing in cybersecurity and a peace of mind, but also enabling their BAS to be prepared for future requirements as new innovations in smart building technology become available.

What is BACnet/SC	BACnet/SC Value Proposition
It is still BACnet and is a new BACnet data link option like MSTP or IP	**Investment protection**: Compatibility to existing and future BACnet networks and stepwise extension/upgrade path
BACnet traffic **encryption** to protect BAS communications from tampering	**Privacy**: Secure end-to-end communication even in unsecure network environments
An **authentication** mechanism to restrict access to a project	**Protection**: Rule out rogue devices on the network and man-in-the-middle attacks
An **IT-friendly** way to do secure building automation communication	**Practical and cost efficient:** Blends nicely into existing mainstream IT landscape

Easy deployment and device detection

BACnet/SC adds an encryption layer to BACnet communication and requires device authentication using certificates, which makes OT networks less vulnerable to cyberattacks. It uses standard and trusted technologies such as the WebSocket protocol over HTTPS, secured by TLS v1.3 (mutual handshake) and X.509 certificates, which IT professionals are comfortable with. It no longer uses the UDP protocol, which has been replaced by the TCP protocol. BACnet/SC also works easily with IP firewalls and Network Address Translation (NAT), and there are no more heavy broadcasts on the IP network.

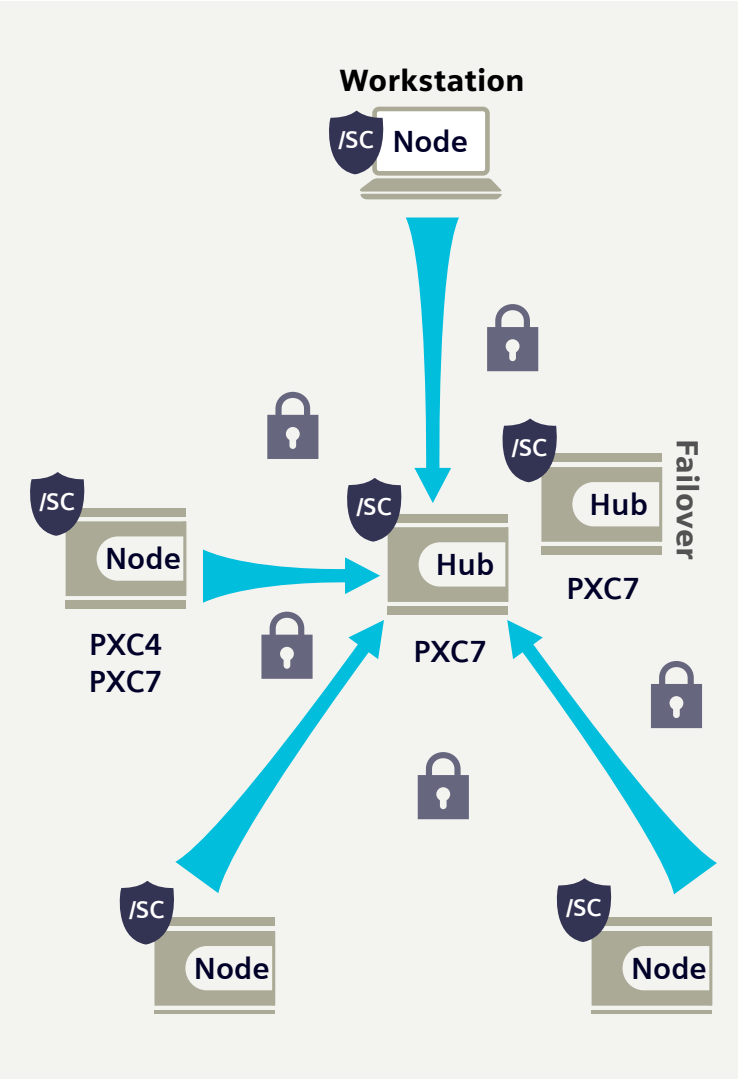
Trusted by IT professionals, WebSocket protocol is used over HTTPS, replacing UDP with TCP.

Feature Contrast	BACnet/IP	BACnet/SC	
Standardized data model for communication	●	●	STILL BACNET
System scalability and flexibility	●	●	
Interoperability between vendors with BACnet Testing Laboratory (BTL) listings and matching BACnet Interoperability Building Blocks (BIBBs) in Protocol Implementation Conformance Statement (PICS)	●	●	
Compatibility with existing and future versions of BACnet	●	●	
BACnet routing between different BACnet data links (BACnet MS/TP, BACnet/IP, BACnet/SC) to form a BACnet internetwork	●	●	
Device instance number and object instance number method of device and object identification	●	●	
Upgrading BACnet/SC compatible systems from BACnet/IP to BACnet/SC is seamless. There is no re-engineering of Trends, Alarms, Graphics, Schedules, or other database components required. It is only a BACnet driver configuration change and certificate loading	●	●	
Same physical (Ethernet) topologies possible - no need to rewire	●	●	
Identical user-side application workflows during runtime	●	●	
All BACnet Services remain the same	●	●	
Connectionless, less reliable, no congestion control UDP protocol	●		
Connection-oriented, reliable message delivery, scalable TCP protocol		●	MORE IT FRIENDLY AND SECURE
Certificate-based mutual device authentication and network access restriction using X.509 v3 certificates		●	
Certificate authority options for self-signed CA or trusted CA of organization's preference		●	
End-to-end traffic encryption using TLS v1.3 secured WebSockets		●	
No heavy network broadcasting on IP network		●	
Independent of underlying IP network infrastructure, micro-segmentation friendly		●	
Agnostic to changes in IP network topology		●	
IPv6 ready (currently supported on IPv4)		●	
Passes across IPv4-IPv6 borders		●	
No BACnet Broadcast Management Device (BBMD) required to get across IP subnets		●	
Firewall and Network Address Translation (NAT) friendly (works well with micro-segmentation)		●	
No static IP addresses required (static IP address recommended for hub device unless FQDN used)		●	
No additional licensing cost to use BACnet/SC in a system		●	
Secure BACnet communication even in unsecure environments		●	
Allows using shared IP networks without VPN setup		●	
No special networks required to be installed - allows for IT/OT network convergence		●	
BACnet essentially becomes a web application on the network like many others		●	
Fits well into a holistic information security approach (Defense-in-Depth)		●	

Since BACnet/SC is just another data link option, it can take advantage of BACnet routing to connect to existing BACnet data links, such as BACnet/IP and BACnet MS/TP. BACnet/SC still uses the same method of device/object identification (the device instance and object instance numbers). There is no need to rediscover devices and their objects or recreate trends, schedules, and graphics when switching network configuration from BACnet/IP to BACnet/SC or when routing from existing data links to BACnet/SC which saves time on upgrade projects. Just as importantly, BACnet/SC maintains the well-known and desired BACnet features of system scalability and flexibility, as well as interoperability between different vendors who are BACnet-compliant with BTL listings and matching BIBBs in the PICS of the devices comprising the system.

BACnet/SC logical network architecture

Hub and node are logical functions in the firmware of BACnet/SC devices. BACnet/SC's hub and node architecture requires that at least one BACnet/SC hub device resides on the network.



The **hub** is the centralized point of device authentication. All other devices on the BACnet/SC network are **nodes**. Nodes authenticate to the hub and node traffic must go through the hub.

- Hubs are embedded devices such as system controllers which are designed to be resilient to failure and are powerful enough to support many simultaneous node connections as well as BACnet routing between different data links, all while also performing their task as a building equipment controller.
- The hub could become a single point of failure, so a second hub (a failover hub) is strongly recommended for network resiliency — which can be another system controller on the network with BACnet/SC hub functionality.
- If the primary hub fails, nodes are configured to look for the failover hub and communication continues without interruption.
- Any device with hub functionality is also inherently a node and can be used as needed in the project.

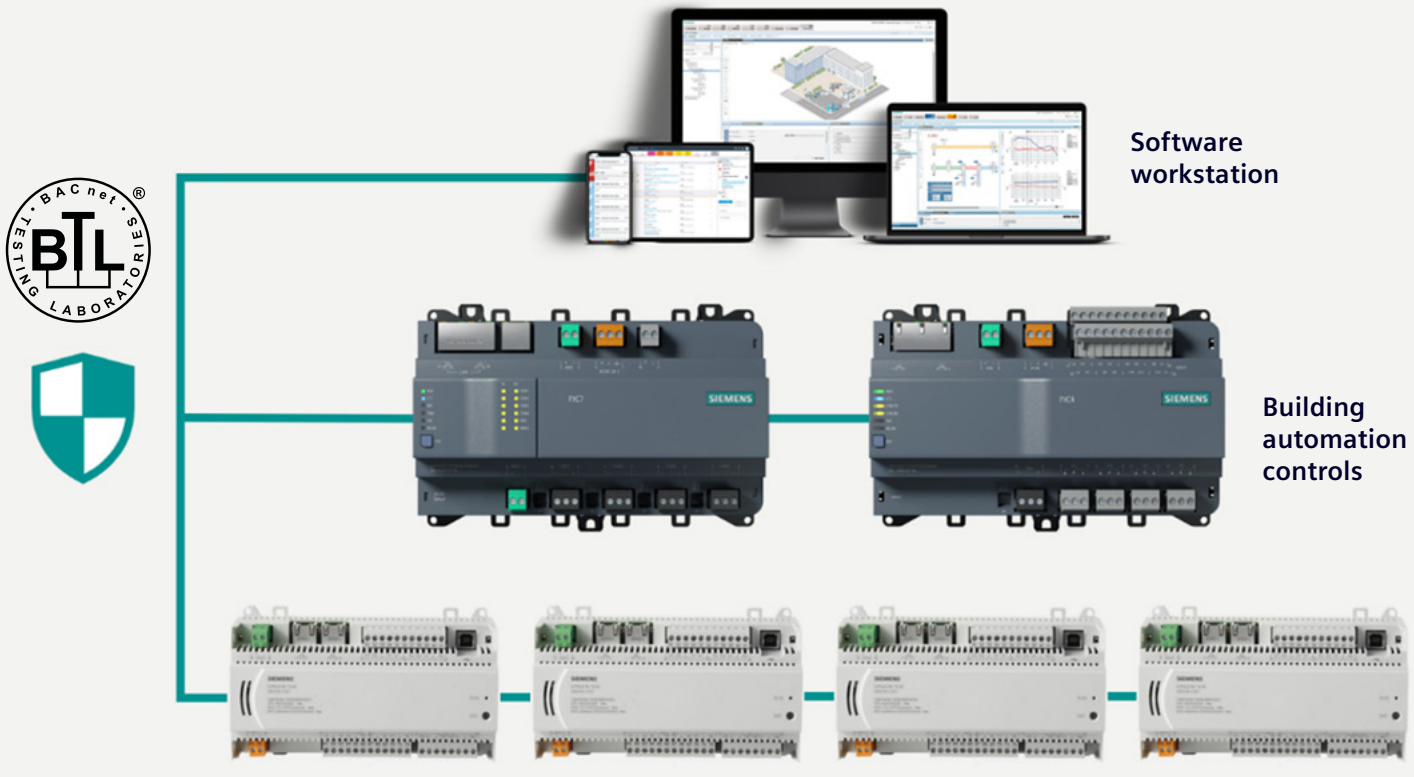
Siemens industry-first BACnet/SC system

Siemens PXC series of system controllers and the Desigo CC workstation with BACnet/SC support is an industry-first complete primary system solution.

The PXC7 has both BACnet/SC hub and node functionality, so it can be used as either, depending on the need. The PXC7 also has BACnet routing functionality. It can route between BACnet/SC and BACnet/IP networks, as well as BACnet MS/TP thanks to its four EIA-485 ports. The PXC4 controller, the DXR.E room controllers, and the Desigo CC workstation have the BACnet/SC node functionality. These products allow you to get on the path to a more secure building automation infrastructure, starting with the most important system components.

Industry-first complete solution, bringing building automation and cybersecurity together

Siemens BACnet/SC solution

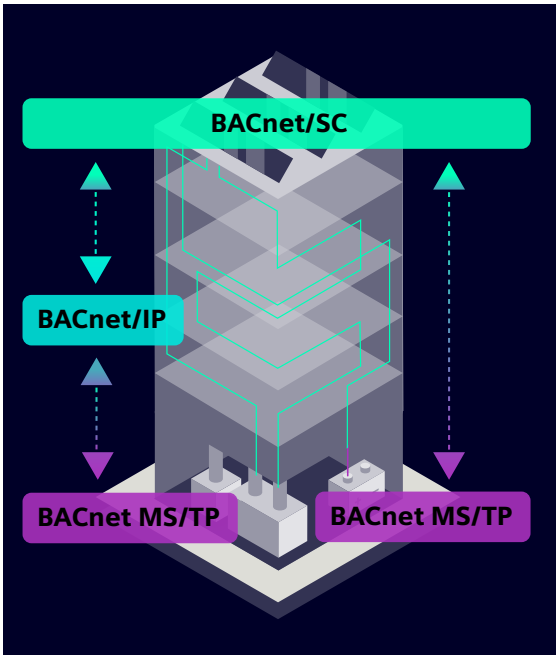


For reference, please see this page with our topology and the descriptions:
https://new.siemens.com/us/en/products/buildingtechnologies/automation.html

BACnet/SC in new construction or existing BACnet system upgrades

It is never too early to get on the path to a more secure building infrastructure with products that support BACnet/SC. In new construction projects, BACnet/SC systems should be designed with available products which support BACnet/SC natively, as well as BACnet/SC-ready products which are powerful enough to support future firmware upgrades to BACnet/SC.

Protect your investments with a flexible, stepwise transition to BACnet/SC



The most important components to start with are at the top of the system — the workstation and the system controllers — because they are most likely to be accessible on networks with public access such as enterprise IT networks, or cloud-connected networks, and there is less pressure to secure networks deep inside the building for now. Another reason to start BACnet/SC systems with the system controllers is that they are powerful enough to support the vital function of BACnet/SC hub and BACnet routing between different BACnet data links. Thanks to BACnet routing, existing BACnet/IP and BACnet MS/TP products that do not support BACnet/SC can also be used in projects when their specific functionality is required.

In existing BACnet system upgrades or extension projects, a stepwise approach should be taken to ensure a smooth transition and protect building owners' current automation system and security investments.

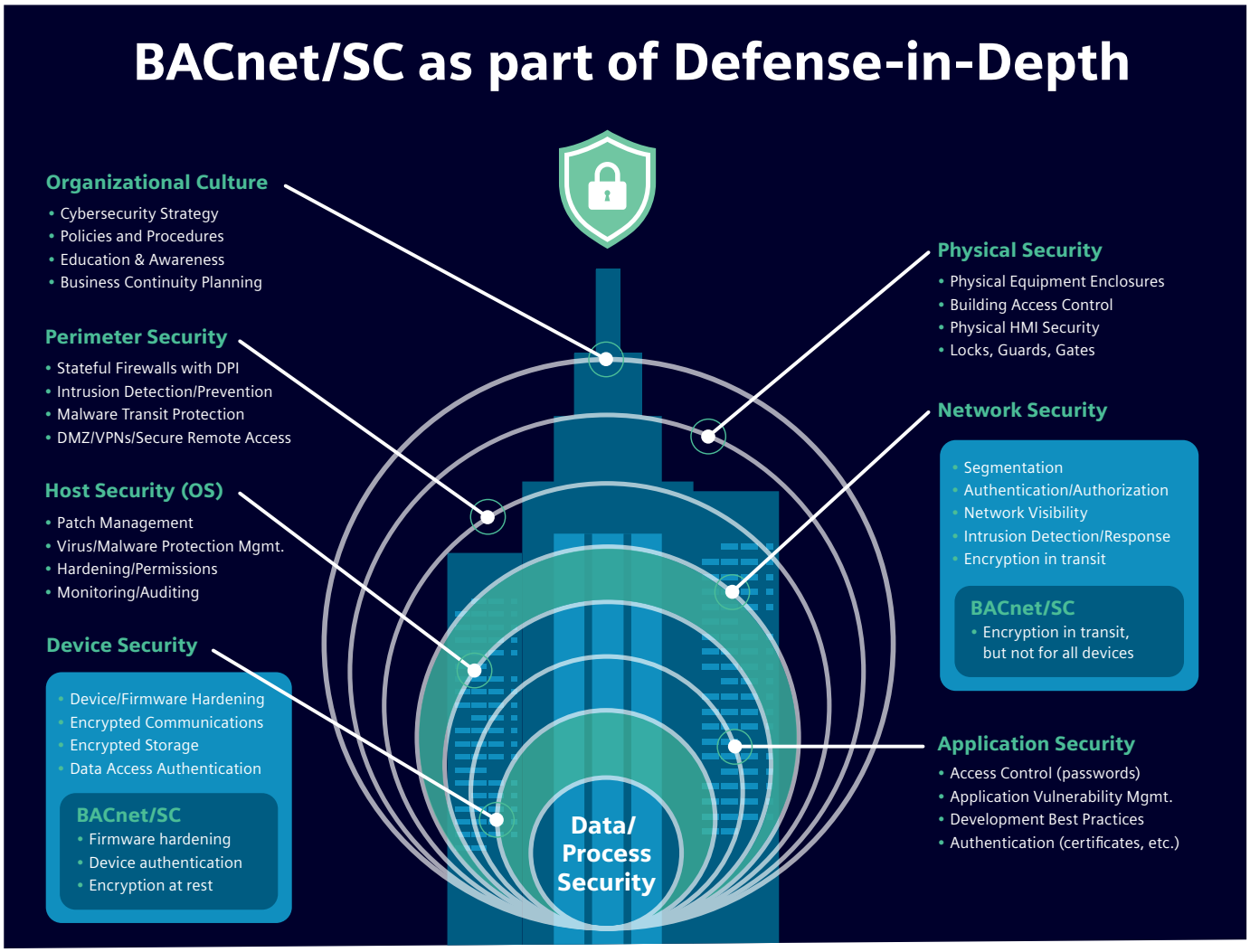
- BACnet/SC can be connected to existing BACnet/IP and BACnet MS/TP networks/systems using BACnet routing (available in PXC7), allowing existing systems to be upgraded incrementally and flexibly as needed.
- To begin upgrades, BACnet networks/systems can be partitioned into individual BACnet logical networks of different data link types, with BACnet/SC logical network "islands" being connected using BACnet routing.
- The remaining unsecure networks can be upgraded as the devices on those networks become obsolete and replacements become available.
- Since BACnet/SC communication is only secure between the BACnet/SC hub and node devices (the BACnet/SC logical network), non-BACnet/SC network segments need to be connected and protected with consideration for the overall system security.

Holistic security approach for buildings

There are many layers to a good defense system. Defense-in-depth is the simple principle that while no single security feature is perfect on its own, adding many independent layers of defenses will make it difficult for an attacker to breach the system, and slow them down to the point where an attack is not worth the expense to initiate it.

BACnet/SC gives IT professionals the methods they are familiar with to incorporate OT systems into a holistic security approach and have peace of mind when it comes to their organization's security. A carefully designed and properly deployed OT network with BACnet/SC supports a proactive, multi-layered defense-in-depth approach and could become a smart building's last line of defense in the event of a cyberattack.

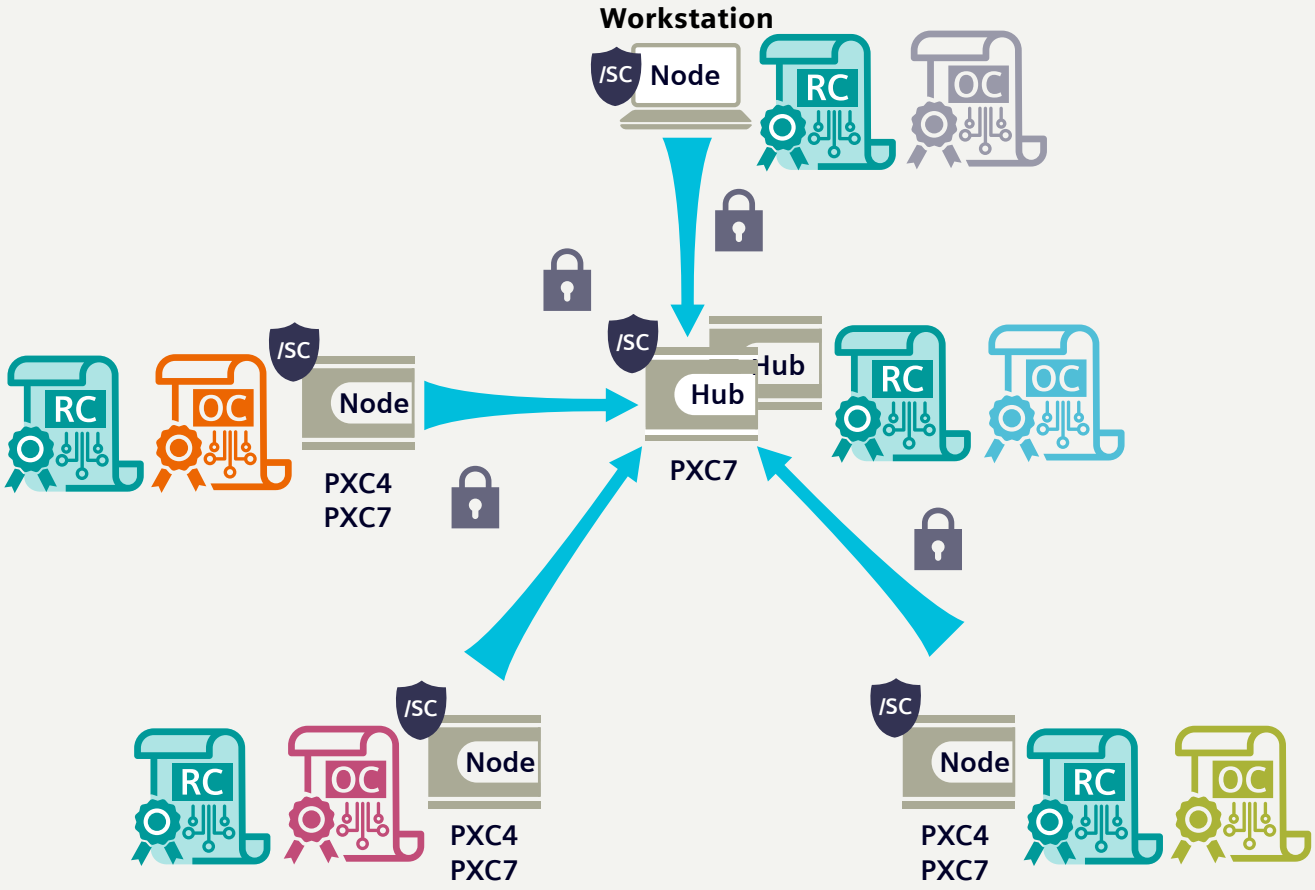
BACnet/SC provides the methods and technology for IT best practices which can now be applied to OT/BAS networks.



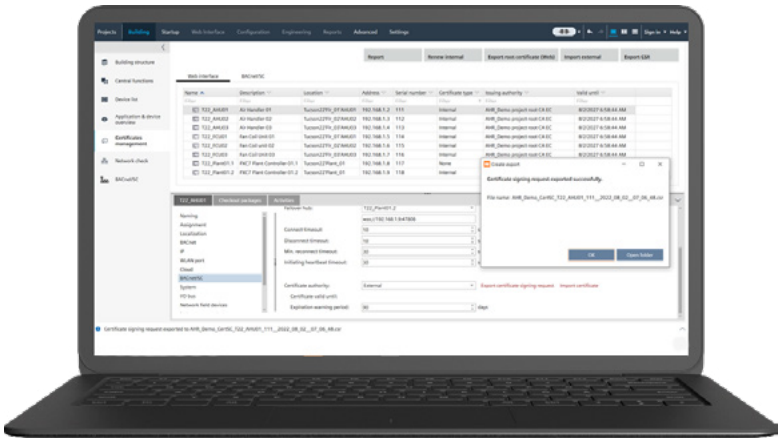
BACnet/SC **certificate management and tools**

In BACnet/SC, device authentication relies on having the proper certificates. Each device requires two certificates to participate on the BACnet/SC network.

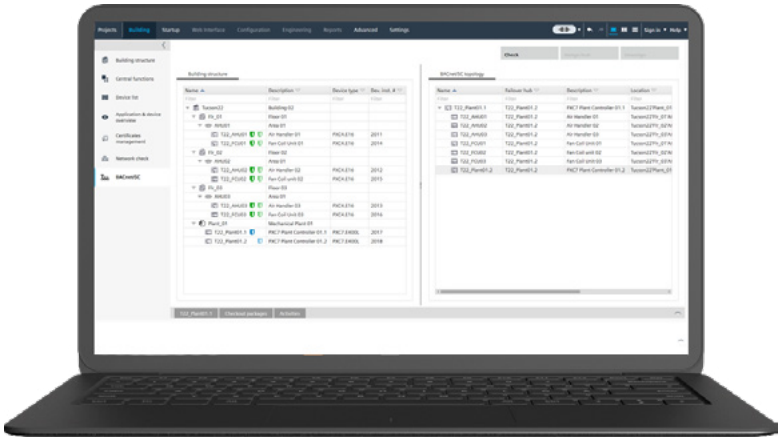
The first is a common root certificate, which is identical on all devices in a project regardless of device manufacturer. The second is the individual operational certificates, which are unique per device and used for authentication of devices and encryption/decryption of traffic. BACnet/SC requires that a single certificate authority (CA) signs the certificates for all devices in the project. Siemens offers the ABT Site application with easy and intuitive workflows to customers for free to meet all of their BACnet/SC network management needs. ABT Site provides all the necessary functionality to generate, sign, provision and renew certificates on Siemens devices, as well as import/export BACnet/SC certificates on the file level to exchange with other vendors' tools for interoperability or act as an intermediary to a trusted certificate authority of the customer's choice.



Easy certificate management with ABT Site



BACnet/SC certificate signing request (CSR)



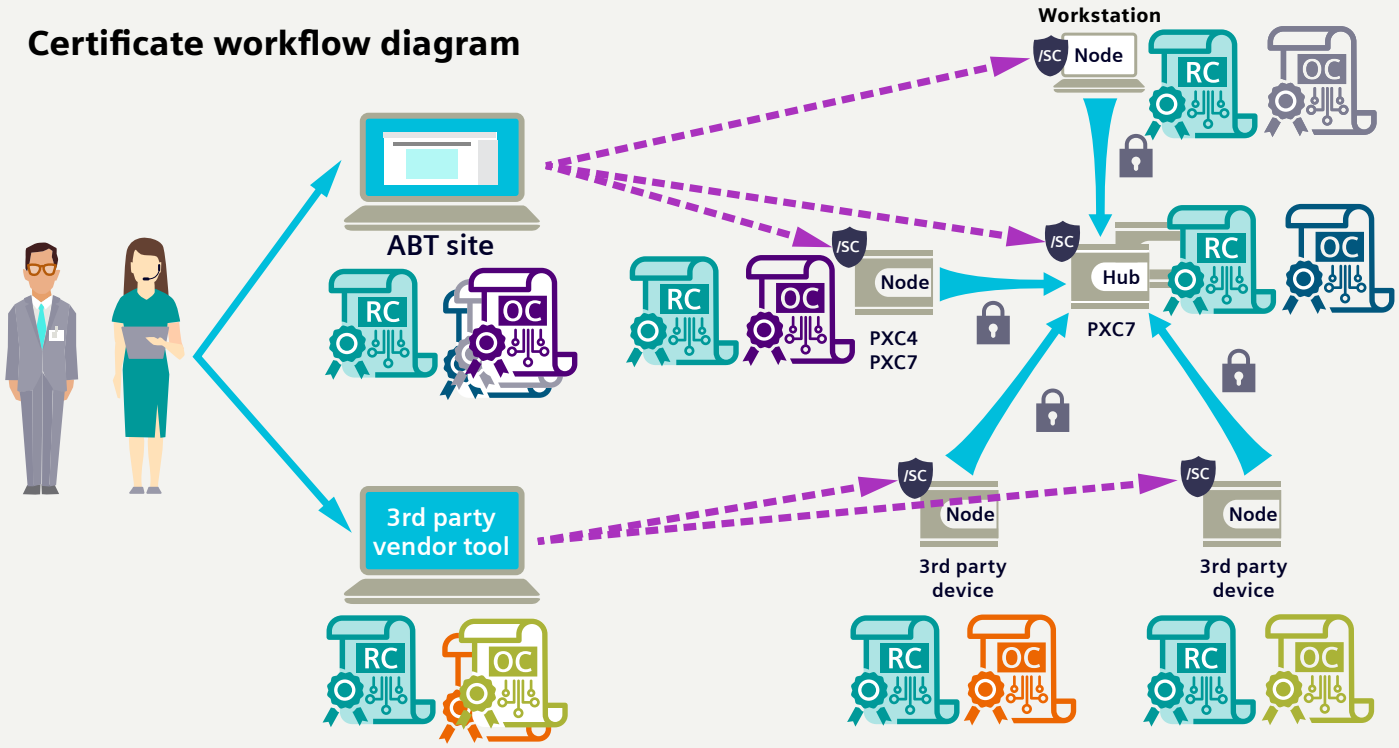
BACnet/SC logical network topology configuration

Organizations may find it easier to use Siemens ABT Site application as a certificate authority. In this case, ABT Site is used entirely on its own to generate, self-sign, provision and renew certificates. This allows customers to take advantage of encrypted communication and device authentication without the complexity of an external certificate authority or chain of trust management.

Some customers prefer to use their own trusted CA. This method requires additional workflows for certificate exchange where a certificate signing request (CSR) is exported from ABT Site and the certificates are signed by the trusted CA of the customer's choice. Once signed by the trusted CA, the certificates are imported back into ABT Site and provisioned onto Siemens devices. (Automated certificate management solution for the system will be delivered with a future market release.)

In either case, the IT team or building operations team charged with certificate management should map out the use cases and procedures they need to efficiently secure the network. Properly secured networks require security-conscious organizational culture and dedicated personnel responsible for device monitoring, certificate renewal, and coordination of different OT vendors on the site. This role also comes with a higher level of responsibility as the team responsible holds the key to this secure OT network. IT and OT professionals must collaborate closely to ensure the OT network is properly monitored and managed.

Certificate workflow diagram



A higher risk factor for cyber threats is caused by increasing BAS digitalization, which means threats could potentially originate in the OT space. As a result, cybersecurity for OT systems is no longer an option. BACnet/SC provides secure communications and authentication between building automation devices to bring cybersecurity and IT acceptance to OT networks.

BACnet/SC can be easily leveraged in projects because it is compatible with any BACnet system, and it maintains the flexibility, scalability, and interoperability that BACnet is known for.

Siemens is at the forefront of building cybersecurity and is proud to announce a complete system for your building. We are committed to bringing more BACnet/SC products for various building automation needs to market. As your trusted cybersecurity partner, we take cyber threats seriously, and our holistic cybersecurity approach will help you master the challenges of an increasingly digitalized world.

Learn more about Siemens building automation solutions **here**.

Let us help you increase cybersecurity across your systems.

- Cybersecurity services to assess your current situation and develop a plan to close gaps in cybersecurity, while protecting your investment
- Products and systems designed with cybersecurity in mind from the very beginning using the latest technologies and validating them through extensive penetration testing
- Information transparency related to vulnerabilities and incidents with timely response updates
- Automation, digitalization, and cybersecurity domain knowledge in compliance with international standards and providing long-term security as technology, products, and systems evolve

Siemens Industry, Inc.

Smart Infrastructure

1000 Deerfield Parkway

Buffalo Grove, IL 60089

Tel: (847) 215-1000

Siemens Canada Limited Headquarters

1577 North Service Road

East Oakville, ON L6H OH6 Canada

Tel: (905) 465-8000

Part #: 153-SBT-1414 (08.2022)