Cybersecurity in Healthcare Building Automation Systems

ALASHE SPRING CONFERENCE

May 15, 2025

Presented by: Bill Coyle

SIEMENS

1

Siemens Building Technologies, Inc. is a Registered Provider with The American Institute of Architects Continuing Education Systems. Credit earned on completion of this program will be reported to CES Records for AIA members.

Certificates of Completion for non-AIA members are available on request.

This program is registered with the AIA/CES for continuing professional education. As such, it does not include content that may be deemed or constructed to be an approval or endorsement by the AIA of any material of construction or any method or manner of handling, using, distributing, or dealing in any material or product.

Questions related to specific materials, methods, and services will be addressed at the conclusion of this presentation.

AIA/CES

SIEMENS

2

Course Description

Cybersecurity in Healthcare (BAS315)

Smart building technology in the healthcare building environment is changing the way we work and perform day-to-day functions. Along with these changes comes new challenges, such as protecting the buildings, organizations, and people from cyber attacks. In this educational session we will cover some of those challenges and discuss some methods to help maintain a cyber secure environment.

Learning Objectives

1. Understand how Building Automation Systems (BAS) in healthcare facilities have become targets for cyber threats.
2. Learn about the challenges of cybersecurity in healthcare facilities.
3. Provide an overview of IT/OT convergence in healthcare facilities and why it is important.
4. Review some recommended steps to strengthen building automation cybersecurity in healthcare building environments.

SIEMENS

3

Course Outline

- Why is Cybersecurity so important?
- Challenges
- IT/OT Convergence
- Recommended Steps

4

Why is Cybersecurity such an important topic?

5

Quick Definitions ….

- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

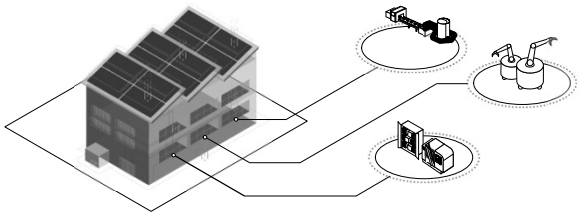
6

Quick Definitions ….

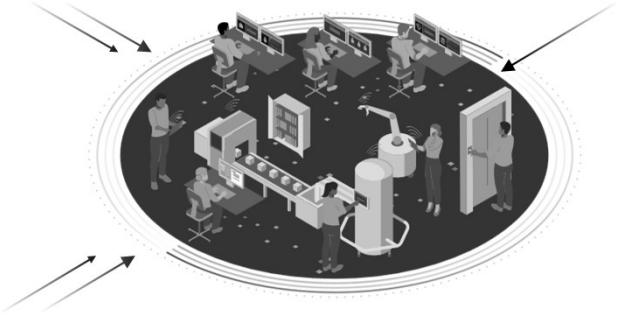
- Information Technology (IT) refers to digital information
- Operational Technology (OT) refers to the operational technology of physical processes (BAS)

7

Why Cybersecurity is even more important now than before!



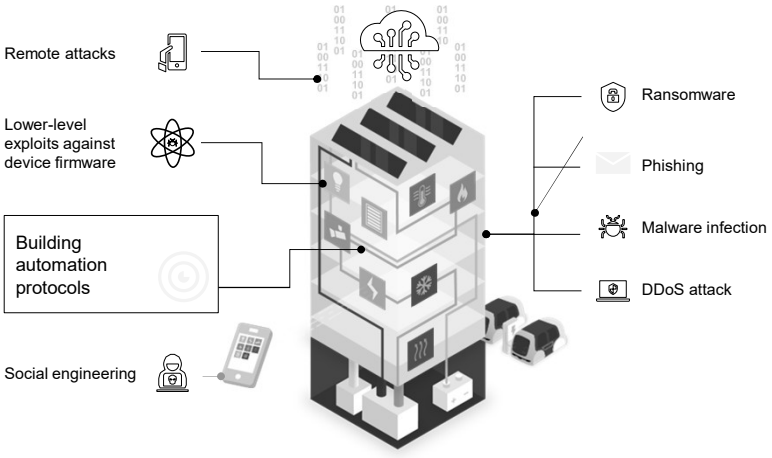
Yesterday we had islands of **communication**.



Today everything is **connected** and the risks **are growing …**

8

Buildings are getting smarter and more connected. Therefore, the attack surface is growing



Increased number of IP-connected devices

More devices are remotely accessible

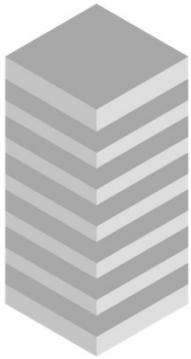
Interconnectivity of different systems

Growing number of cyberattacks on operational technology (OT) systems: incidents expected to occur every two seconds by 2031[1]

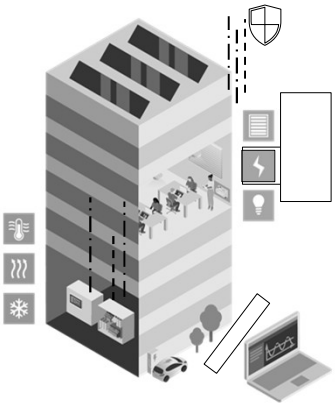
Source: 1 Cybersecurity Ventures

9

Increased connectivity and digitalization in building automation systems brings new cybersecurity requirements

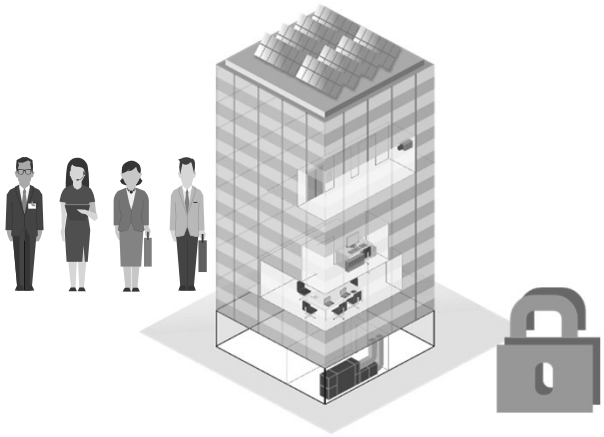


From …	To …
Closed networks with limited connectivity	Open networks with IoT devices and cloud-based applications
Individual applications and systems	Systems (HVAC, lighting, access control, fire, etc.) exchanging information to meet performance and efficiency goals
Local and individual security applications	High degree of network protection, like access restriction, authentication, authorization and encryption. High degree of secure systems.
Individual requirements on security compliance	Internationally approved standards based on IEC 62443. Fulfillment of requirements on cybersecurity certification.



10

Organizations small or large –
have a lot at stake if faced with a cyber attack



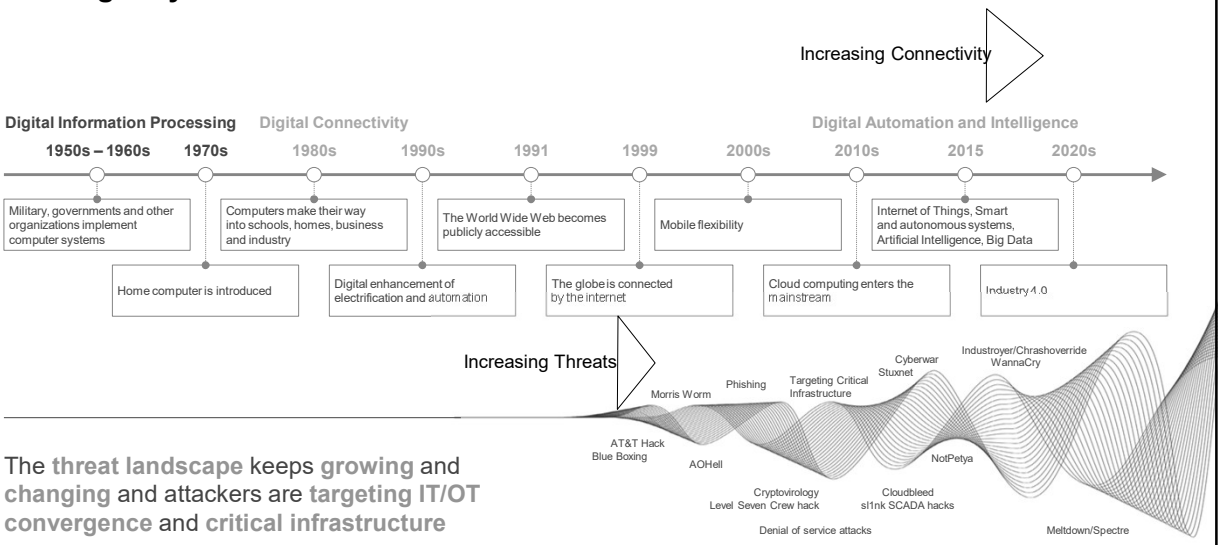
- Financial impact
- Loss of intellectual property
- Loss of valuable data
- Critical operations halted
- Compromised reputation
- Customers lose confidence

11

Challenges

12

Nothing Stays the Same



The **threat landscape** keeps **growing** and **changing** and attackers are **targeting IT/OT convergence** and **critical infrastructure**

13

Recent Cybersecurity Trends in Healthcare

- AI-Driven Attacks: Cybercriminals are leveraging AI to create more sophisticated phishing and ransomware attacks. These AI-driven threats can bypass traditional security measures and target healthcare systems more effectively
- Phishing and Ransomware: Phishing remains a primary method for initiating ransomware attacks. Healthcare organizations are particularly vulnerable due to the high value of patient data
- Cloud Vulnerabilities: As healthcare providers increasingly use cloud services to store patient data, misconfigurations and vulnerabilities in these services are becoming major targets for cyberattacks
- IoT Device Exploits: The proliferation of Internet of Things (IoT) devices in healthcare, such as wearable health monitors and implantable devices, introduces new security risks.

Source: HealthTech; January 2025

14

Cyberattack Impact on Healthcare

- Operational Disruption: Cyberattacks can shut down critical systems, affecting patient care and clinical outcomes
- Financial Strain: The cost of breaches, including fines for HIPAA violations and remediation efforts, can be substantial
- Patient Privacy: Protecting sensitive patient data is crucial, and breaches can lead to loss of trust and legal consequences
- A recent report found 92% of healthcare organizations reported experiencing a cyberattack in 2024, up from 88% in 2023, while the average cost of the most expensive attack was $4.7 million

Source: HealthTech; January 2025

15

Evolving Threats
Require Different Approaches

Median Dwell Time

416 ➤ 24

DAYS IN 2011 DAYS IN 2020

GLOBAL MEDIAN DWELL TIME, 2011-2020

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
All	416	243	229	205	146	99	101	78	56	24
External Notification	–	–	–	–	320	107	186	184	141	73
Internal Detection	–	–	–	–	56	80	57.5	50.5	30	12

Dwell time is calculated as the number of days an attacker is present in a victim environment before they are detected. The median represents a value at the midpoint of a data set sorted by magnitude.

Source: FireEye – M-TRENDS Report, 2021

16

The Right Standard can Help

17

Cybersecurity – Who is involved?

ISA Setting the Standard for Automation™

U.S. DEPARTMENT OF ENERGY

Homeland Security

IEC

DOE-CIRC

ASHRAE

FEMA

NIST National Institute of Standards and Technology U.S. Department of Commerce

ISA Security Compliance Institute

ICS-CERT INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Key Involvement

- International Society of Automation (ISA)
- International Electrotechnical Commission (IEC)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- US Dept. of Energy (USDOE)
- Department of Homeland Security (DHS)
- Other Federal, states and private authorities.

18

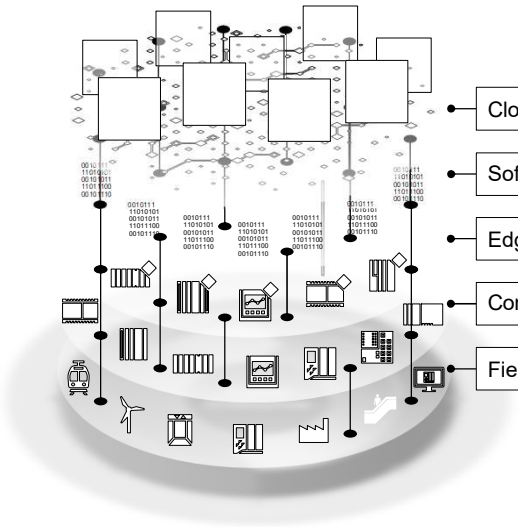
IT/OT Convergence

19

IT/OT integration across all areas and layers
Cybersecurity is a must have in IT **and** OT

Information Technology **(IT)**

Operational Technology **(OT)**



- Cloud
- Software for vertical integration
- Edge
- Controller/Automation platforms
- Field devices

20

Recommended Steps to Strengthen BAS Cybersecurity

21

IEC 62443 4-1 ML3 / 4-2 SL2 certification by an independent 3rd party institution

What is certified?

- IEC 62443 4-1 ML3 certification: The development of the product complies with the security requirements for a Secure Development Lifecycle.
- IEC 62443 4-2 SL2 certification: The product complies with the security technical requirements for an industrial automation and control system with a security level 2

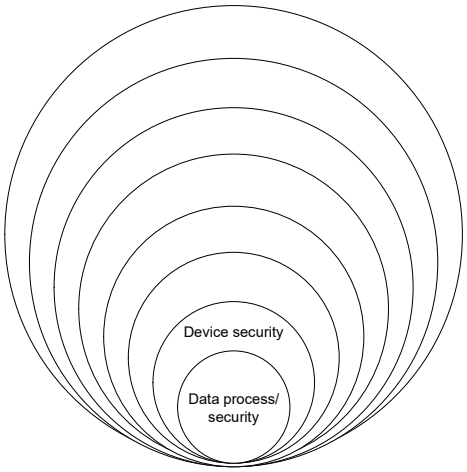
How do you benefit?

- Strengthen your security resilience on customer site
- Demonstrate security responsibility in front of your customers
- Ensure your cybersecurity compliance with laws and regulations
- Reduce vulnerabilities
- Reduce possible threats exposure
- Safe time and cost on further IEC certifications

Learn more: https://sie.ag/5iVoS1
Learn more about IEC: https://www.iec.ch/blog/understanding-iec-62443
Access the latest certificates on the Siemens website or in the Certificate Explorer | TüV SüD (tuvsud.com)

22

Strong cybersecurity requires a holistic approach



23

Building automation systems using BACnet are not inherently secure ... yet

ASHRAE BACnet™

Used in around ~70% of all commercial systems today

Huge installed base – step-wise upgrade option is needed

Lacks security features inherent in the protocol:

- No encryption – no data privacy
- No authentication – not tamper-proof
- Not “IT-friendly” – uses UDP, heavy broadcasts

Today’s BACnet systems are secured using external methods such as VLANs, VPNs, Firewall, DMZ, etc.

24

BACnet Secure Connect brings security to the BACnet protocol

What BACnet/SC is not

- A silver bullet against all kinds of cybersecurity risks
- A fine-granular authorization mechanism (as it is authenticating devices)
- Something that provides IT security “free of charge” …

New BACnet data link option

Encrypted traffic

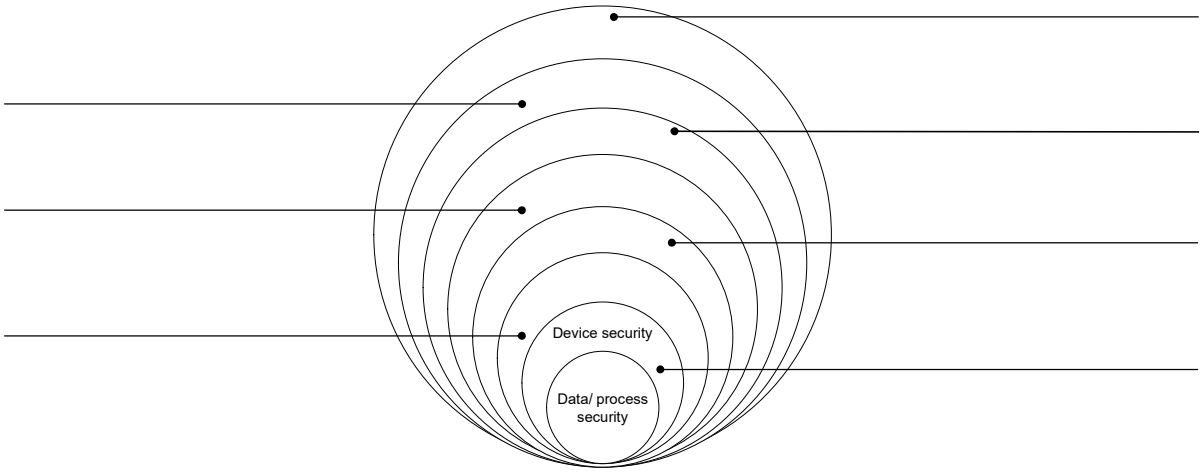
Authenticated devices

IT-friendly

Compatible, flexible, scalable, and interoperable

25

Defense-in-depth

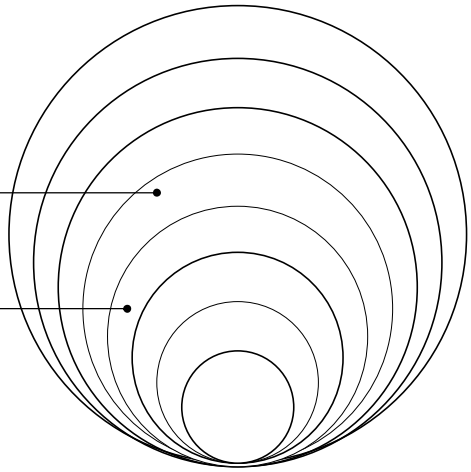


26

BACnet/SC impact on defense-in-depth model

Network security
- Encryption in transit for BACnet/SC compliant devices
- Restricted access to network (IEEE802.1X)

Device security
- Firmware hardening
- Device authentication



27

With BACnet/SC your Desigo system provides…

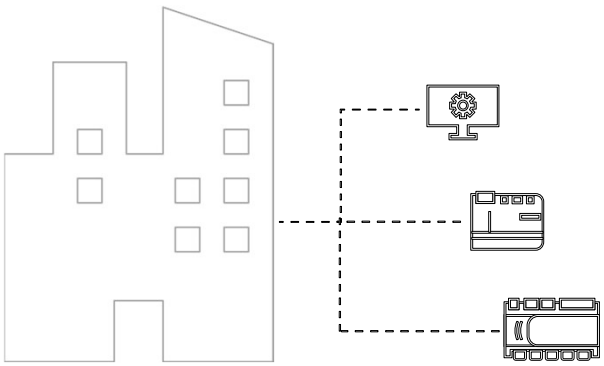
Industry-leading cybersecurity

Scalability

IT- friendliness

28

Industry-leading cybersecurity
in every aspect of building automation



High level of cybersecurity in all aspects of building automation

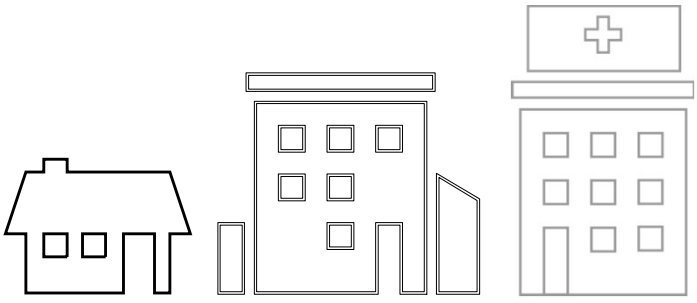
Rule out rogue devices

Prevent Man in the Middle (MitM) attack

Traffic encryption to prevent machine-2-machine (M2M) communication against tampering

29

Scalability
Secure communication from small to large projects



Hub-of-hub topologies to scale up for large projects

Step-wise integration and backward compatibility

Secure & non-secure communication (Router)

Integration of 3rd BACnet/SC devices (as Hub)

For every size of new or existing project

30

IT-Friendly
Leveraging existing IT technology and established IT protocols for easy deployment

Authentication mechanism to protect access to project

Secure end-to-end device communication via insecure IP networks

Independent from underlying LAN infrastructure

Firewall-friendly use of WebSockets

Thought-through workflow and debugging processes

The ABT Site tool

- provides all the necessary functionality to manage certificates on Siemens devices or
- can import/export BACnet/SC certificates to exchange with other vendors' tools for interoperability or
- act as an intermediary to a trusted certificate authority of the customer's choice

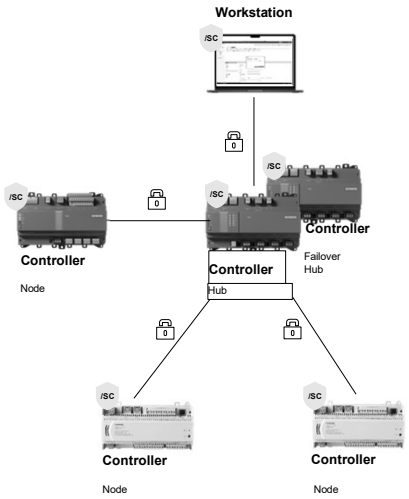
31

Features of BACnet/IP and BACnet/SC

	BACnet/IP	BACnet/SC
Standardized data model for communication	◯	◯
Interoperability between vendors with BTL listings and matching BIBBs in PICS	◯	◯
Compatibility with existing and future versions of BACnet	◯	◯
BACnet routing between different BACnet Data links (BACnet/IP, BACnet MS/TP, BACnet/SC)	◯	◯
Device instance number and Object instance numbers for device object identification	◯	◯
System scalability and flexibility	◯	◯
Connectionless UDP protocol	◯	
Connection-oriented TCP protocol		◯
Traffic is end-to-end encrypted using TLS v1.3 secured WebSockets		◯
All devices authenticated using X.509 certificates before joining the network		◯
Does not require BACnet Broadcast Management Device (BBMD) to get across IP subnets		◯
Works well with IP firewalls or Network Address Translation (NAT)		◯
No static IP Addresses required		◯

32

BACnet Secure Connect communication



Hub and Node are functions in the products comprising the system and define how they behave on the BACnet/SC network

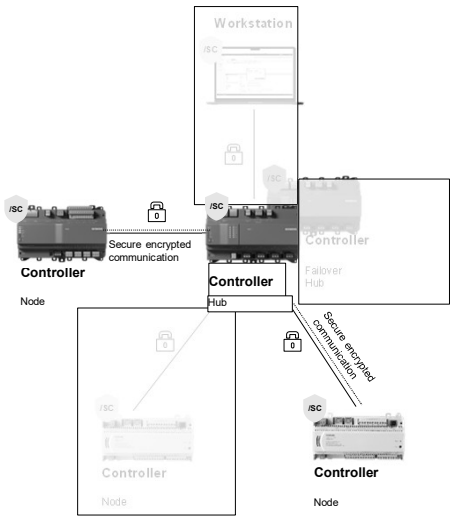
Hub is a BACnet/SC function
- A Primary Hub must be assigned
- A Failover Hub is strongly recommended (hot-standby redundancy)

Node must go through the hub to authenticate and communicate

ABT Site tool – configure BACnet/SC and manage certificates with easy and intuitive workflows

33

BACnet Secure Connect communication



Node must go through the hub to authenticate and communicate

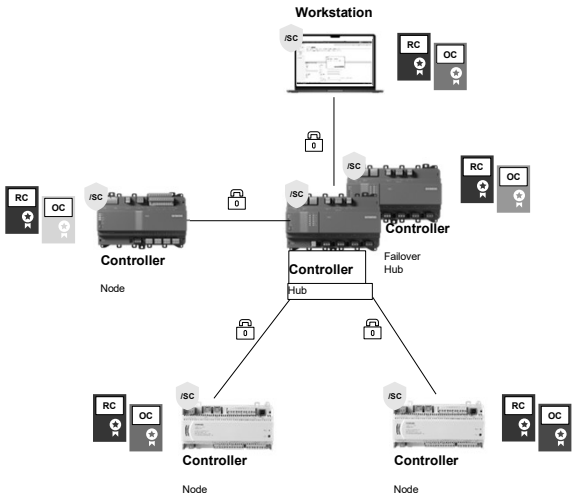
TCP (Transmission Control Protocol) and WebSocket – two reliable mechanisms based on the internet protocol (IP) widely used in IT – are used for secure data transmission

TLS is used to ensure bug-proof and tamper-proof communications TLS (Transport Layer Security). All BACnet/SC communication is **encrypted** WSS (TLS v1.3)

Every BACnet/SC device is **authenticated by** X.509 certificates via a dedicated certificate authority (CA)

34

BACnet Secure Connect certificate management and tools



In BACnet/SC, device authentication relies on proper certificates

Each device requires two certificates to participate on the BACnet/SC network

The first certificate is a common root certificate (RC), which is identical on all devices in a project regardless of device manufacturer

The second is the individual operational certificates (OC), 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

We support all three types of certificate management:
- ABT Site
- 3rd Party Vendor tool
- Customer IT

35

Recommended Steps

- Network protection starts with a cybersecurity assessment
- A cybersecurity assessment can provide insights and identify potential vulnerabilities that could invite hackers

36

Recommended Steps

- A cybersecurity assessment provides a solid foundation for understanding a buildings BAS communication protocol and a BACnet/SC fit
- Specifying Engineers incorporate BACnet Secure Connect into project specifications

37

Recommended Steps

- Everyone connected to an organization should be accountable for keeping it secure
- Create a culture of security awareness

38

Recommended Steps

- The best defense is a good offense
- Approach threat and risk assessment from a hacker's perspective

39

Recommended Steps

- Consider critical security controls for BAS
- Network segmentation
- Role Based Access Control (RBAC)
- Documentation from Integrators and 3rd Party demonstrating proper security configuration

40

Recommended Steps

- BAS operators are the first line of defense
- Proper use and operation of BAS

41

Recommended Steps

- Require a strong backup process to mitigate damage from cyberattacks
- Specify Recovery Time and Recovery Point Objectives

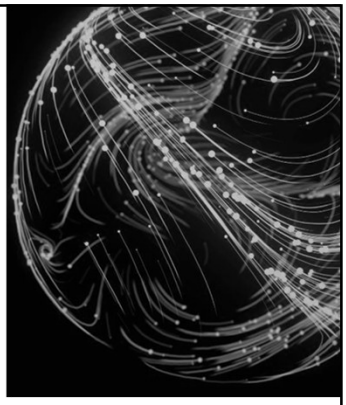
42

Thank you for attending!

SIEMENS

43

Contact



Phillip Brooker
Sr. Sales Executive - Automation
Siemens Infrastructure Buildings, USA
E-mail robert.brooker@siemens.com

Bill Coyle
National Business Manager, US, CAN
Siemens Infrastructure Buildings, USA
E-mail william.coyle@siemens.com

SIEMENS

44