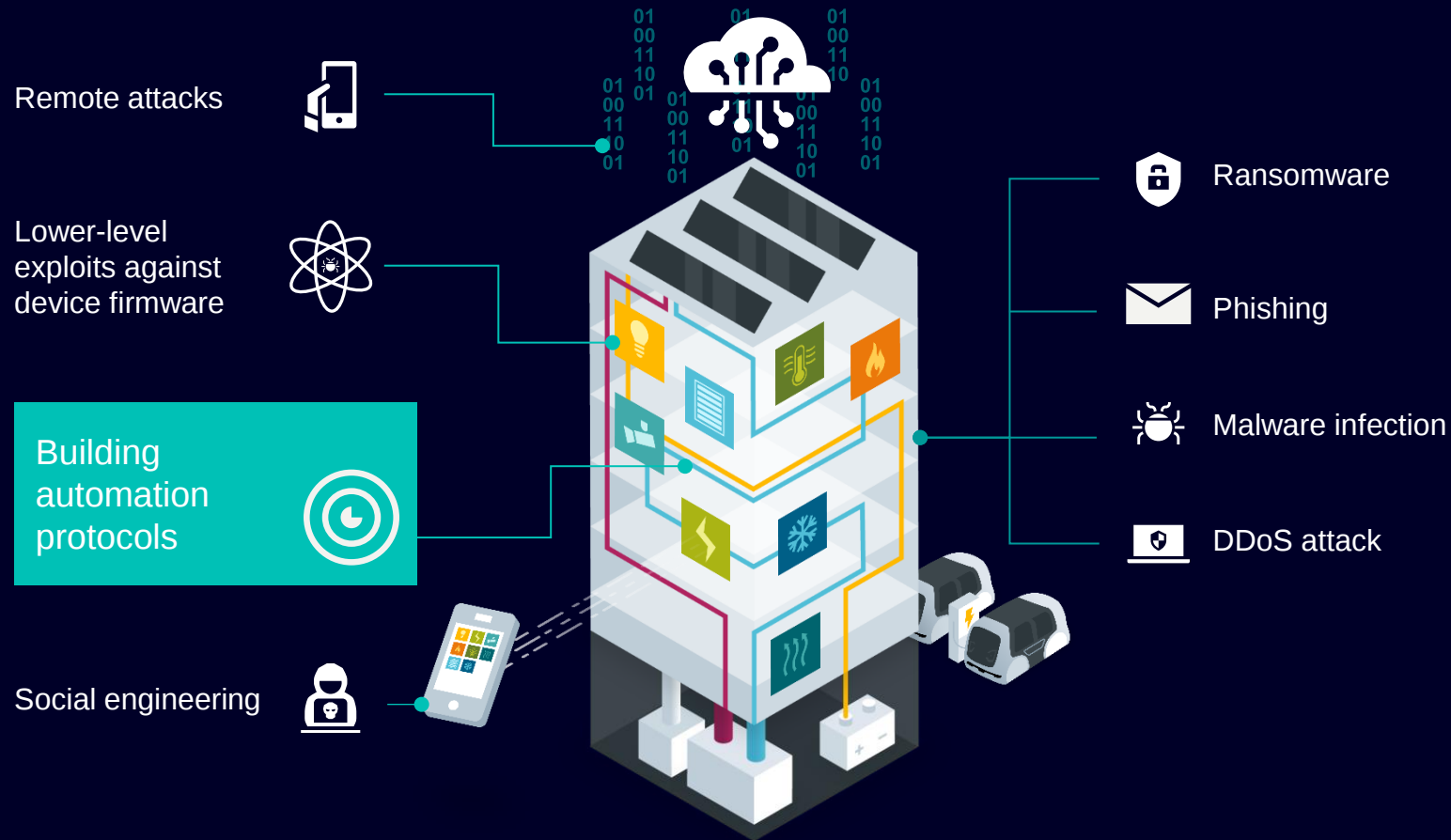




BACnet Secure Connect – A Cyber Resilience Foundation for Building Automation

Industry-leading cybersecurity with Desigo building automation

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



Increased number
of **IP-connected** devices

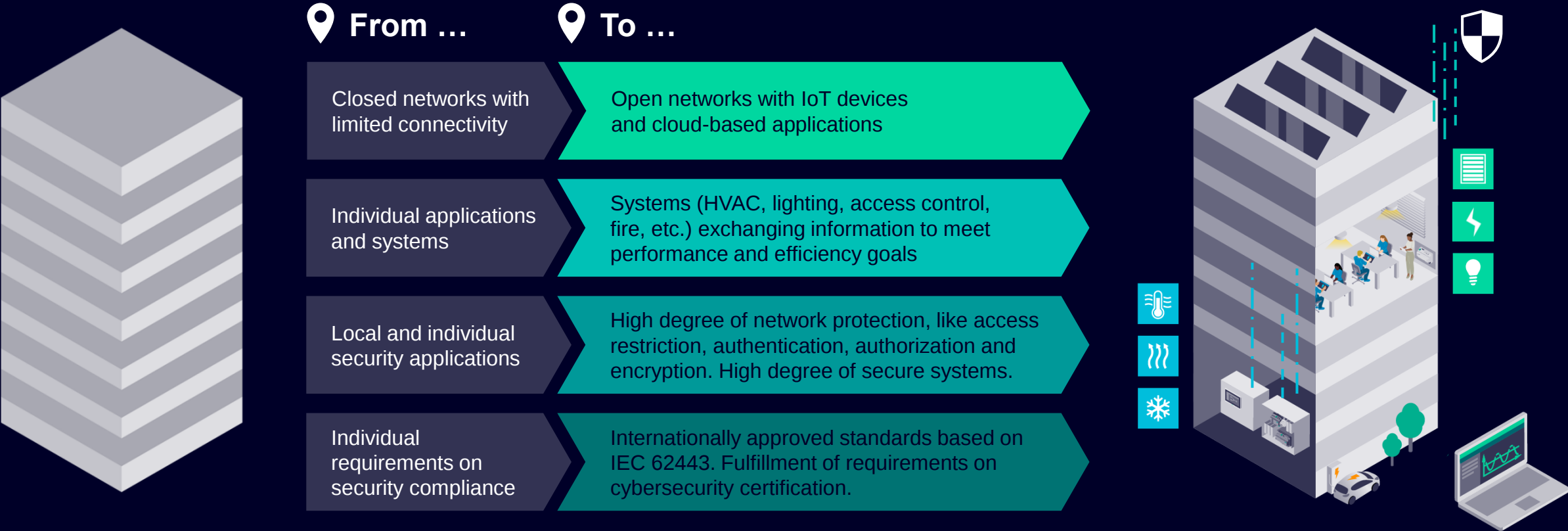
More devices are remotely
accessible

Interconnectivity
of **different systems**

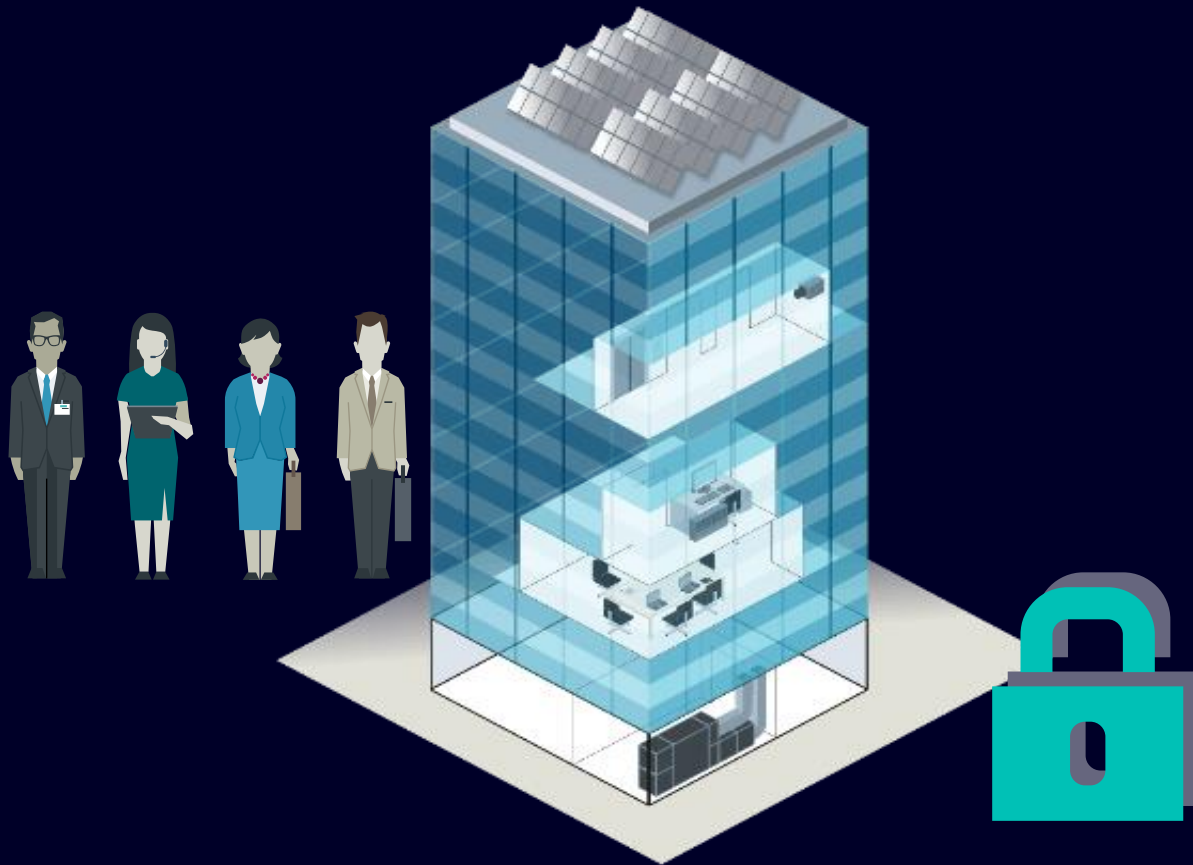
Growing number of **cyberattacks on
operational technology (OT) systems**:
incidents expected to occur every two
seconds by 2031¹

Source: 1 [Cybersecurity Ventures](#)

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



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

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?

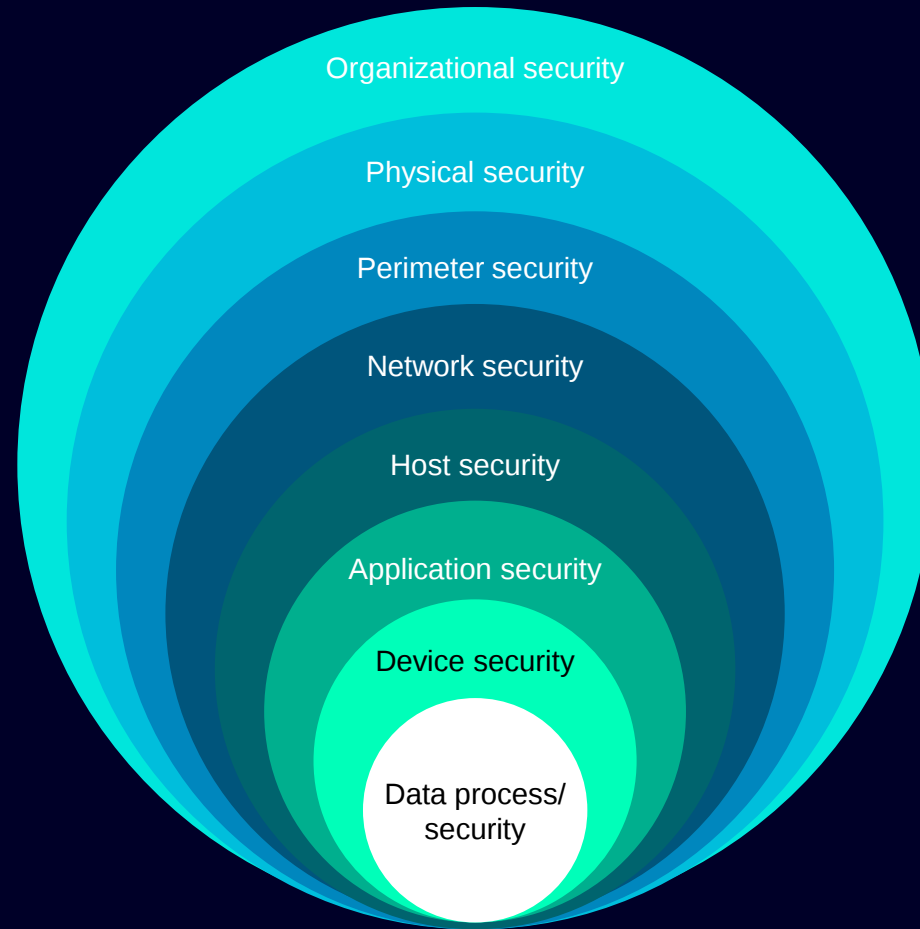
- Strengthen your security resilience on customer site
- Demonstrate security responsibility in front of your customers
- Ensure your cybersecurity compliance with laws and regulations
- Reduce vulnerabilities
- Reduce possible threats exposure
- Safe time and cost on further IEC certifications

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 \(tuvsud.com\)](#)

Strong cybersecurity requires a holistic approach



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



Used in around ~70% of all commercial systems today

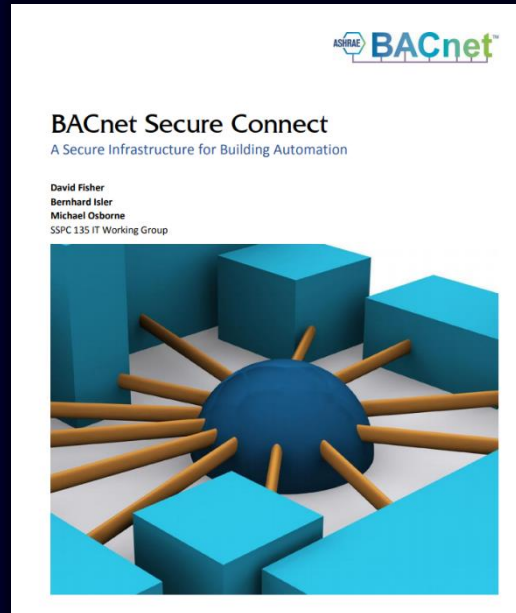
Huge installed base – step-wise upgrade option is needed

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.

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

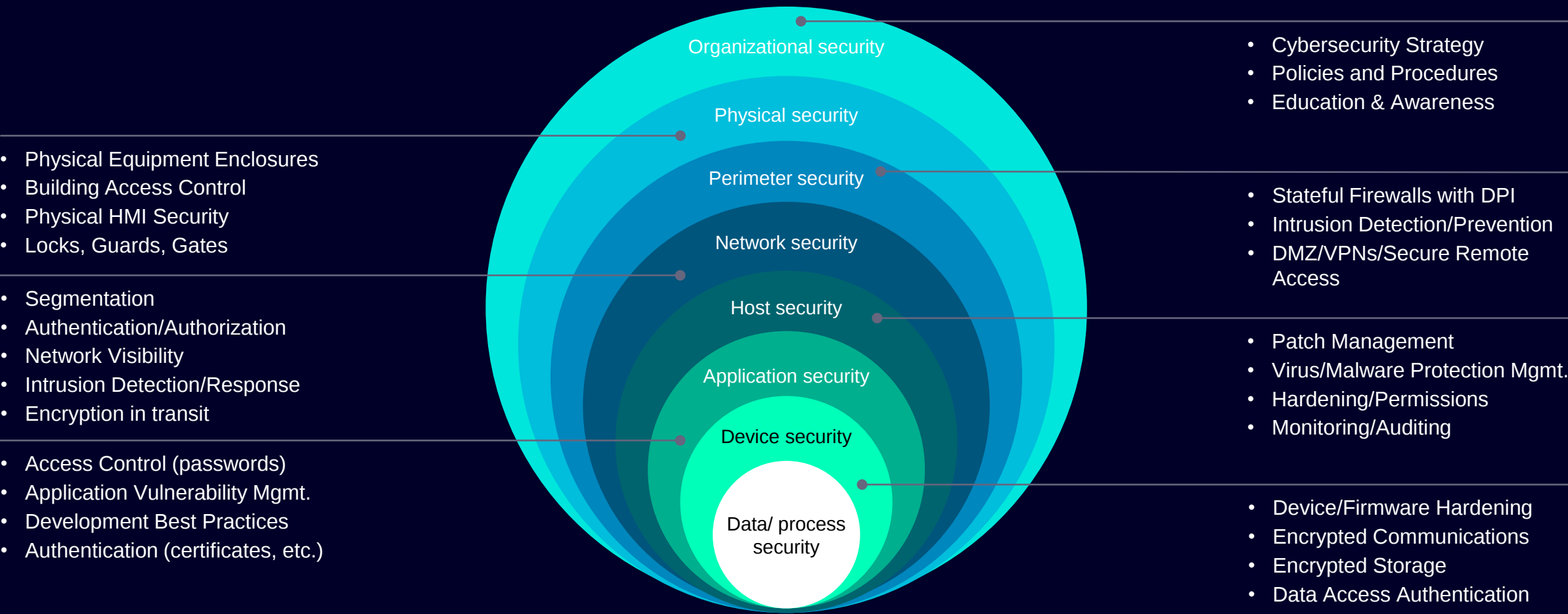
Encrypted traffic

Authenticated devices

IT-friendly

Compatible, flexible, scalable,
and interoperable

Defense-in-depth



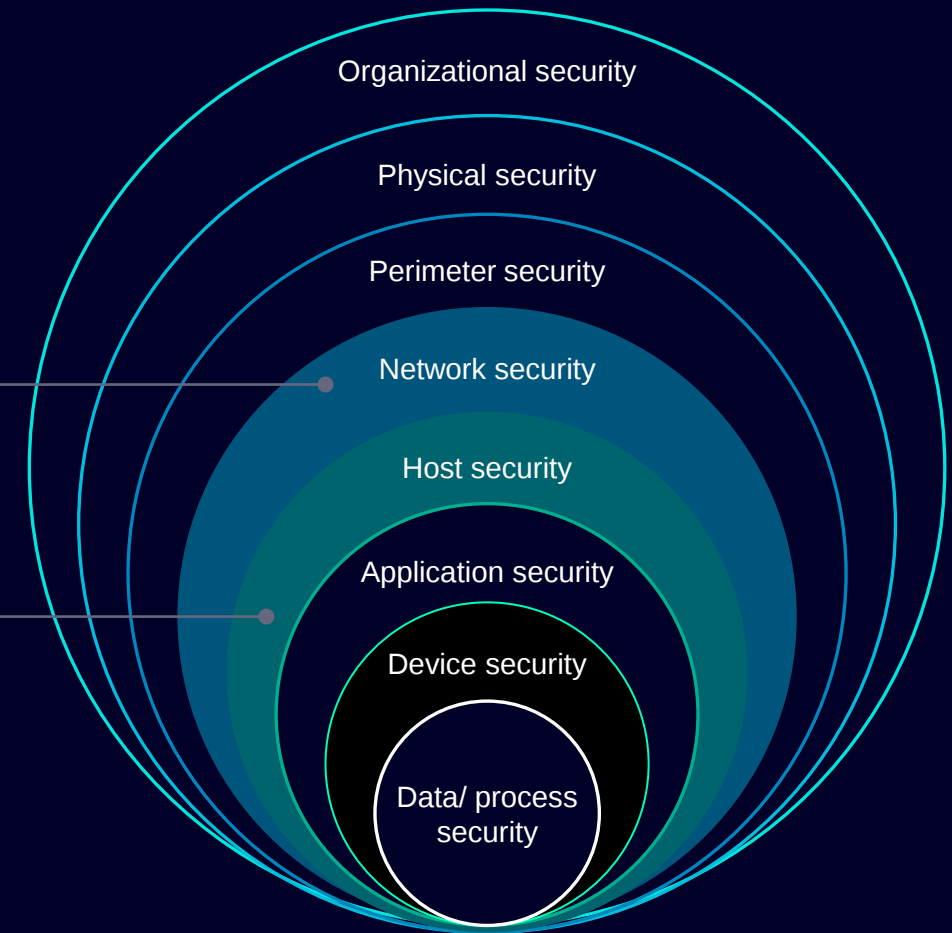
BACnet/SC impact on defense-in-depth model

Network security

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

Device security

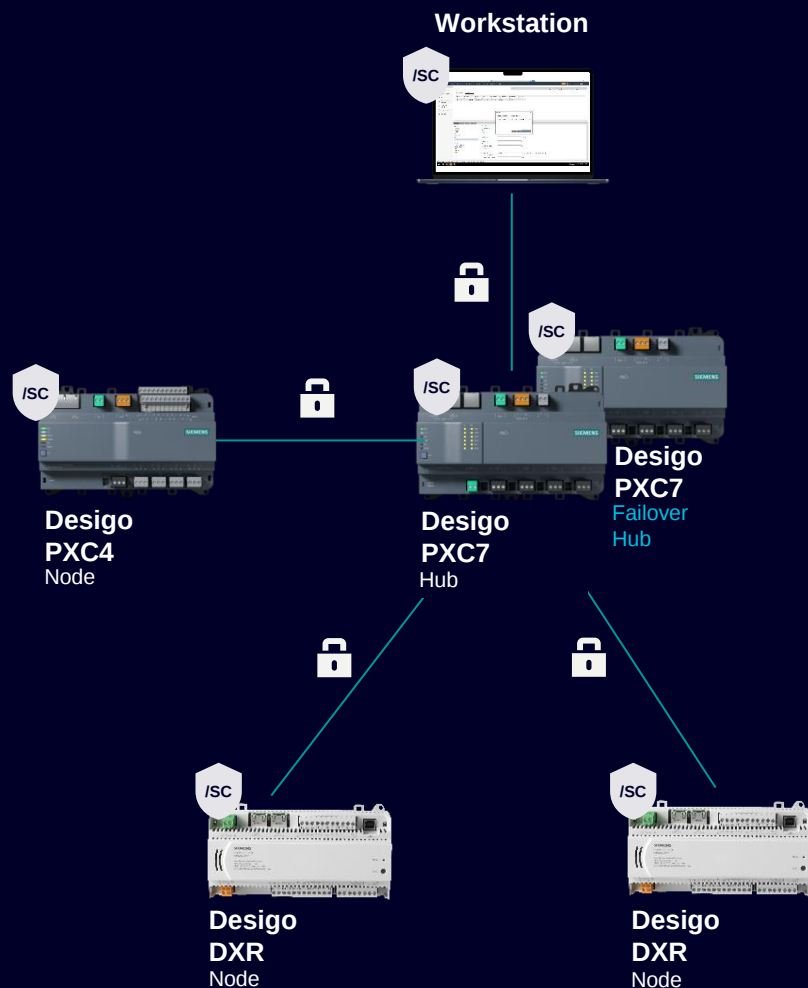
- Firmware hardening
- Device authentication



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		●

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

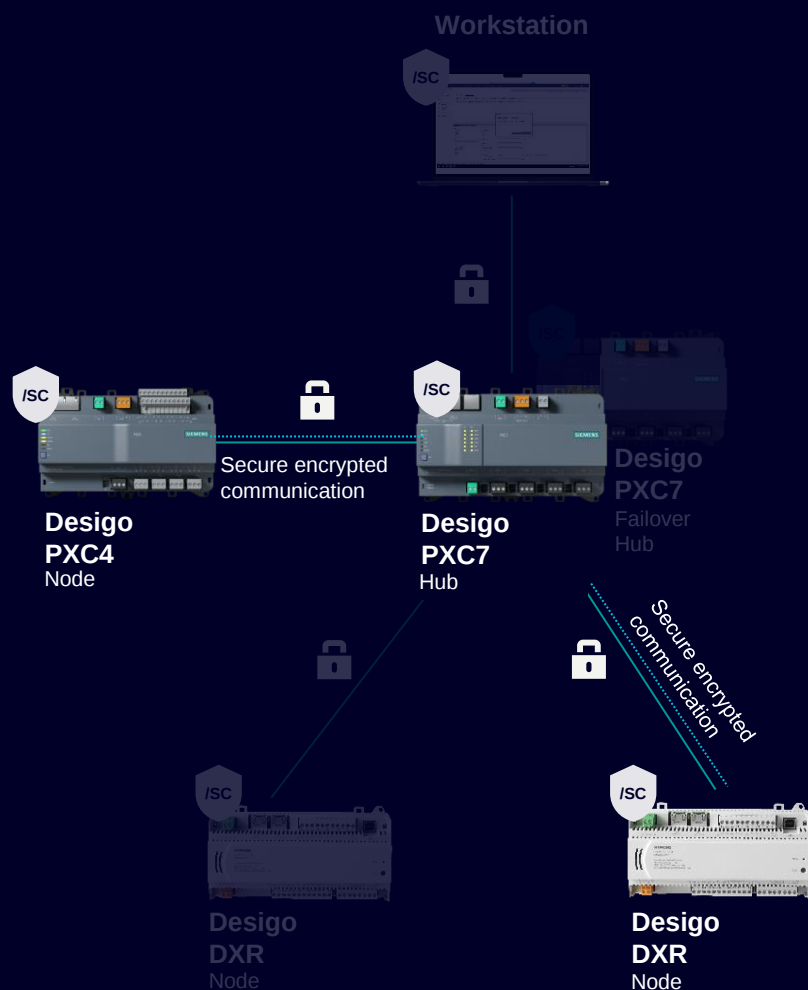
Hub is a BACnet/SC function

- 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

BACnet Secure Connect communication



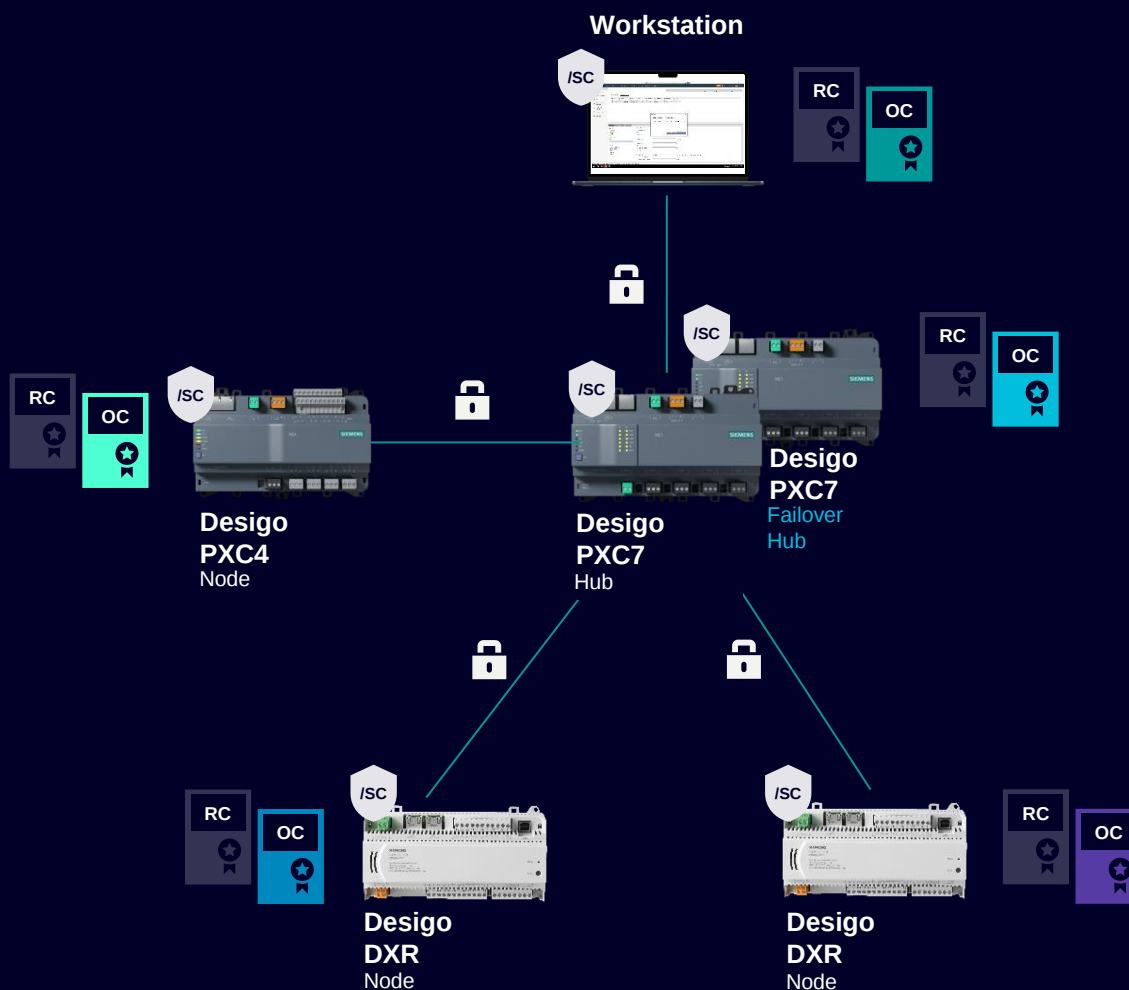
Node must go through the hub to authenticate and communicate

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)

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

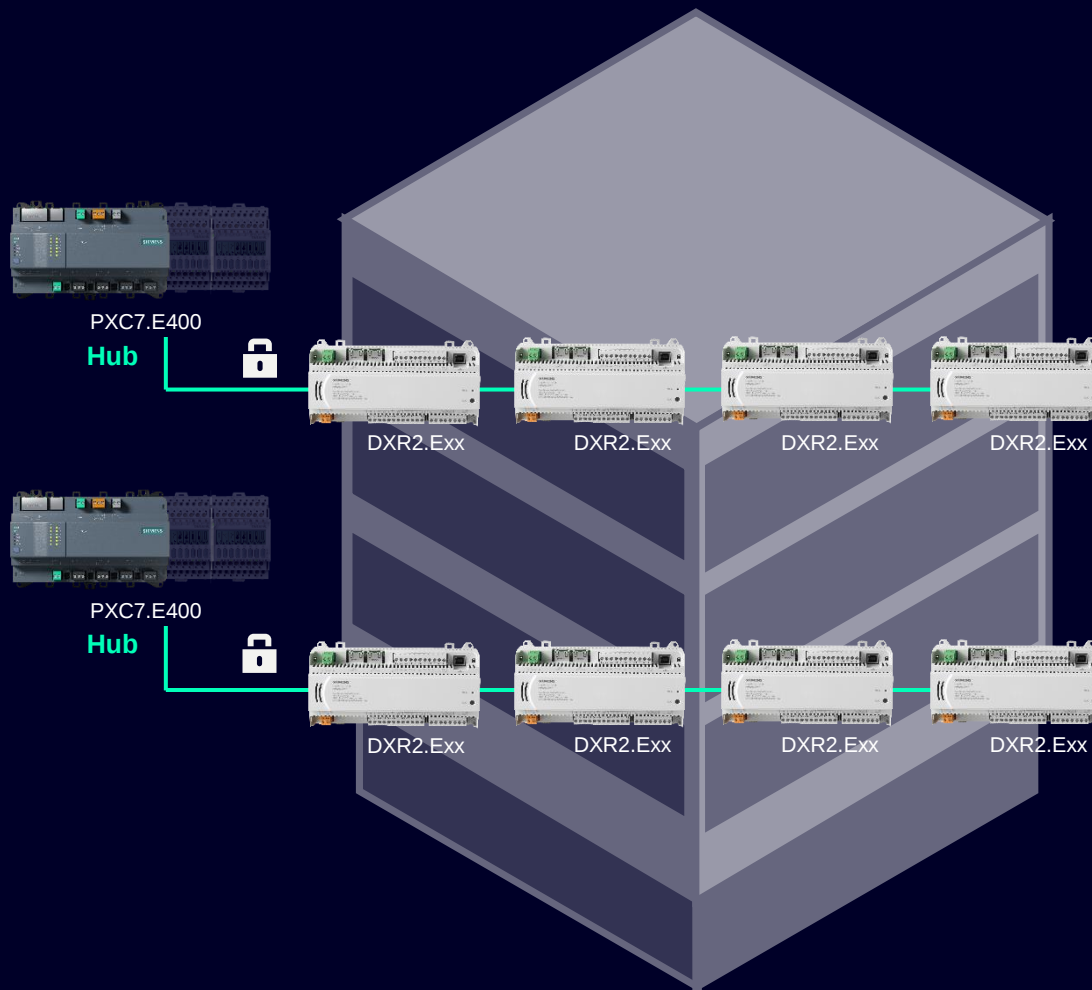
BACnet/SC requires that a single certificate authority (CA) signs the certificates for all devices in the project

We support all three types of certificate management:

- ABT Site
- 3rd Party Vendor tool
- Customer IT

Larger BACnet/SC networks

Example



Room Automation Controllers acting as nodes

One Hub per floor (or segment), depending on size

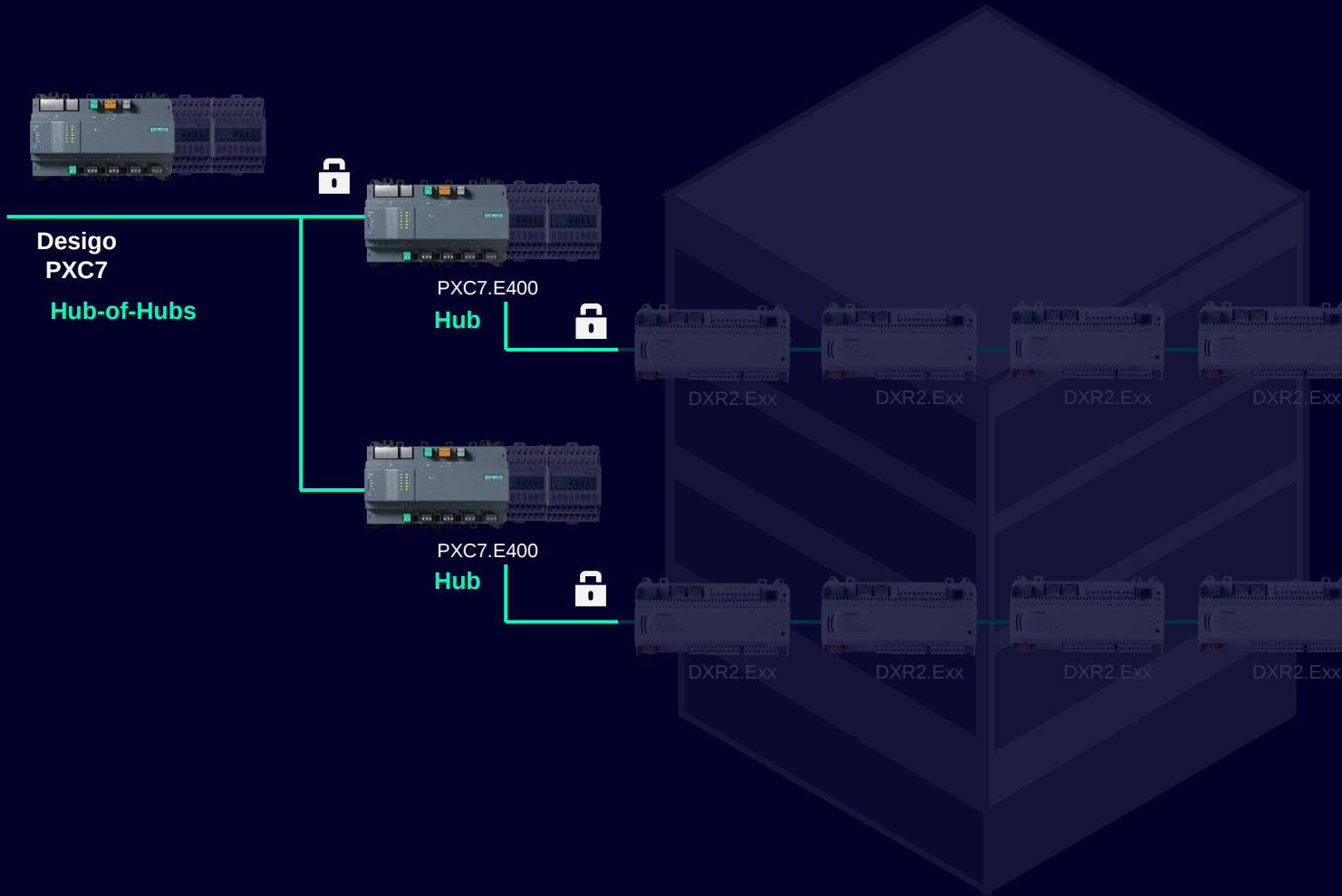


Larger total amount of BACnet/SC devices supported (for sites larger than a single hub capacity)

Mass efficient engineering and commissioning of BACnet/SC devices

Larger BACnet/SC networks

Hub-of-Hubs implementation



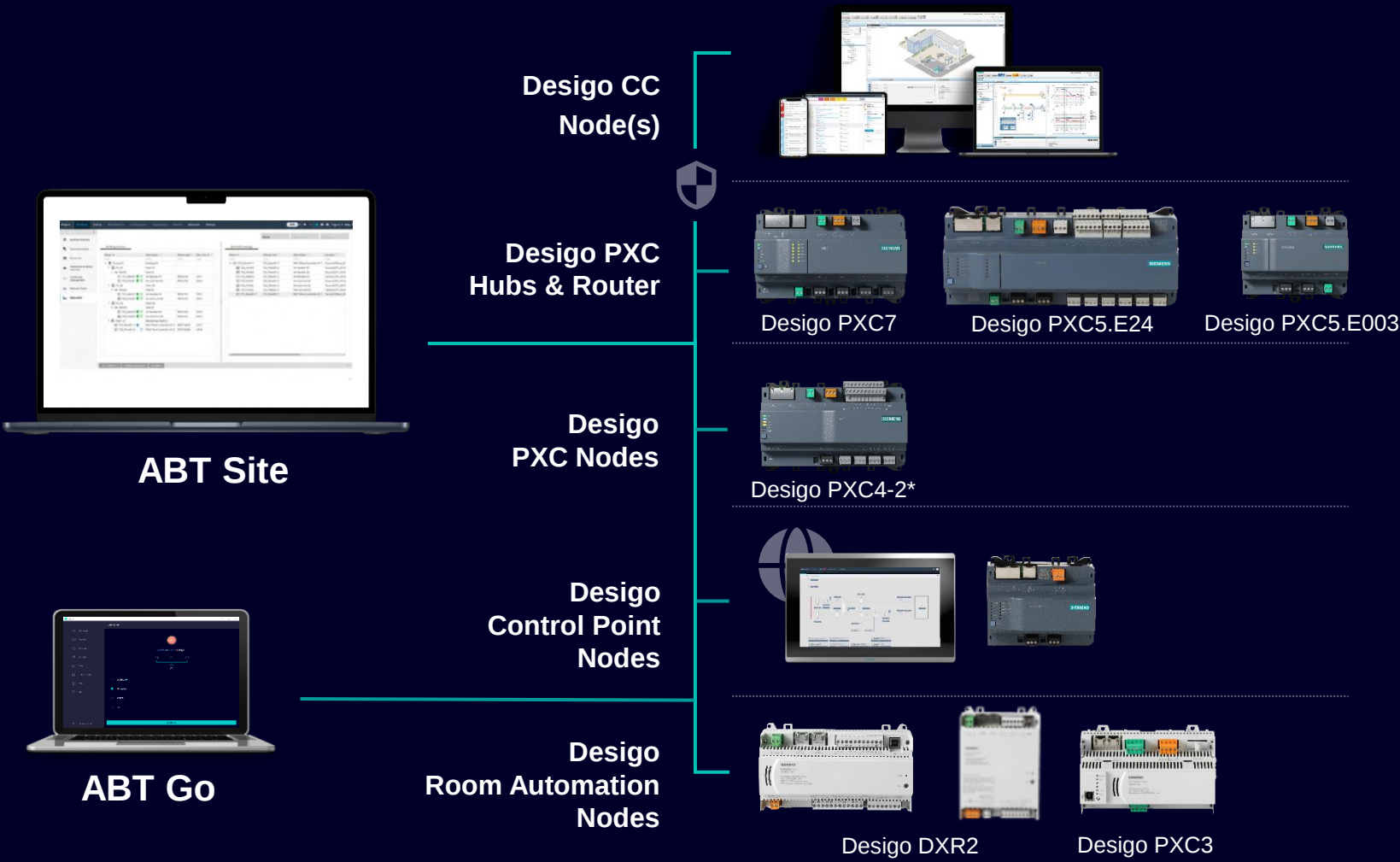
Hierarchical multi-hub topology (Hub-of-Hubs)

Former Hubs per floor/ segment are Nodes of the new superordinate Hub on building scope

Mass efficient engineering and commissioning of BACnet/SC devices to support planning

Compatibility to existing and future BACnet systems

Our complete Designo BACnet/SC offering



Designo CC BMS with BACnet/SC support

ABT Site for BACnet/SC configuration, Certificate Authority, and certificate management

ABT Go for secure commissioning

Designo PXC5/7: Powerful system controller, with built-in routing- and hub functionality to manage both secure- and classic BACnet communication automation stations

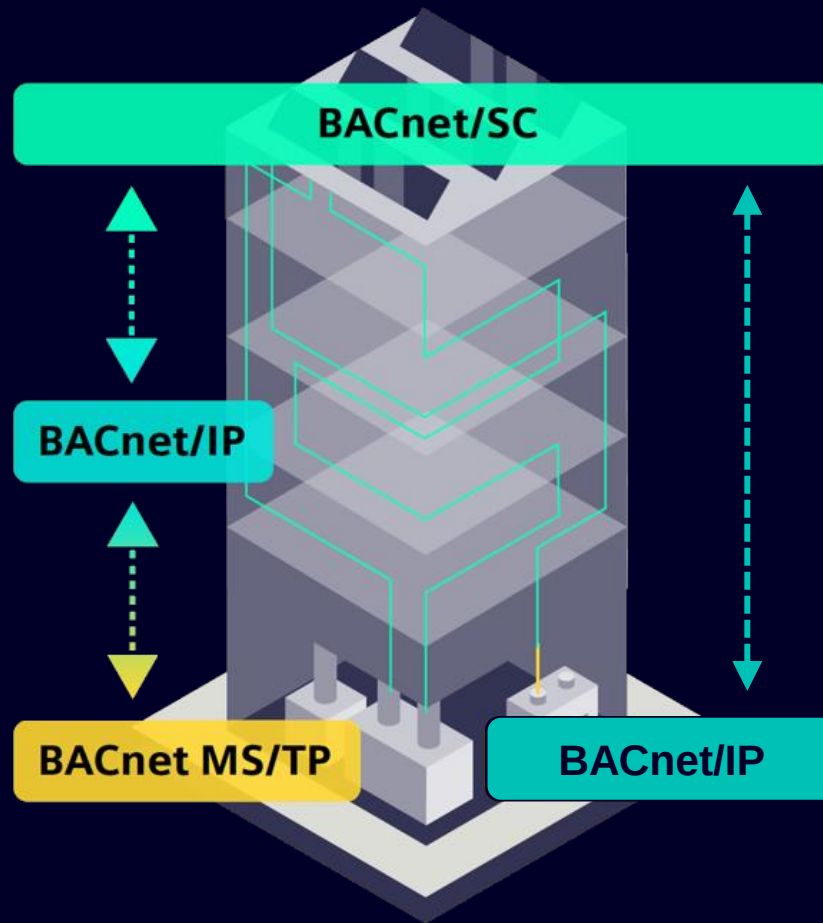
Designo PXC4-2, PXG3 Webserver and Designo Control Point operation panels with BACnet/SC support

Designo DXR2.E and PXC3 room controllers act as BACnet/SC nodes

DXR2.E17 room pressurization and fume hood controller with BACnet/SC support for critical environment control

System limits exist at all levels, please refer to the technical documentation
Designo CC and Designo PXC4/5/7 supporting IEC62443 4-2 SL2 compliant deployments
* PXC4 got succeeded by PXC4-2, both can act as nodes.

Opportunities with BACnet/SC



Can be used in new construction (greenfield) or upgrade (brownfield) projects both for extension and step-wise migration of existing projects

Compatible to existing BACnet systems by using BACnet routing

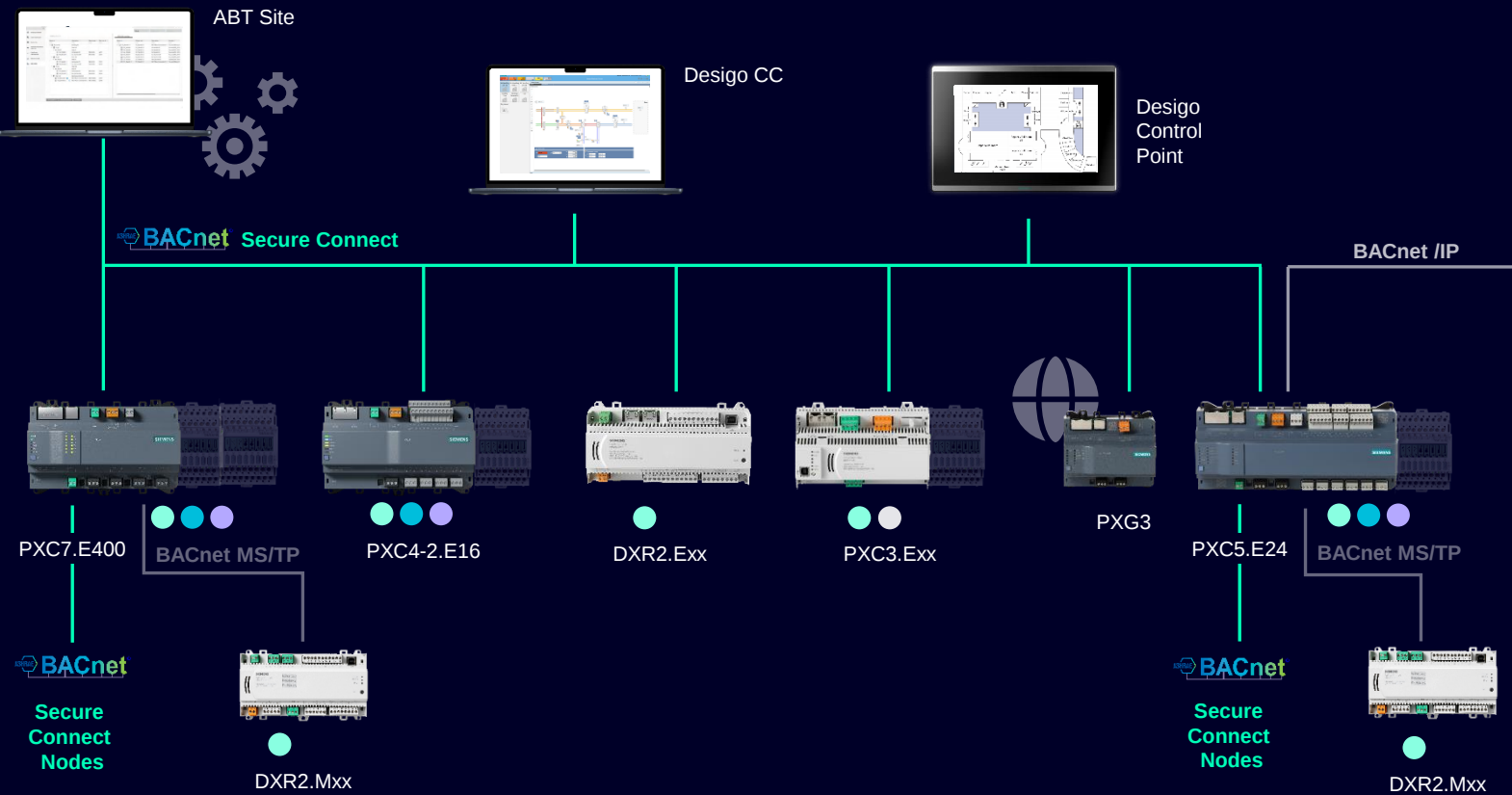
Augments overall cybersecurity

Future proof investment for digitalization

System hardening guidelines for installation

BACnet/SC ready means: Upgrade to BACnet/SC by firmware upgrade

Realize your Designo projects with BACnet Secure Connect native on device level



Legend: ● = PL-Link ● = Modbus ● = M-Bus ● = DALI

Designo CC and Designo PXC4/5/7 supporting IEC62443 4-2 SL2 compliant deployments

Highlights

A **scalable and tailored** solution for your needs

Strong cybersecurity with **BACnet Secure Connect** embedded natively on device level

License-free and intuitive engineering with **Designo Engineering Framework**

Easy **on-board integration** possibilities with consistent workflows

IEC62443 4-1 ML3 **certified** product development process

System limits exist at all levels, please refer to the technical documentation



Köszönöm a figyelmet!