Presentation to start at 11:00am EDT

ISASecure webinar

BACnet and ISA/IEC 62443 Conformance using BACnet Secure Connect

Presented by Jon Williamson

September 22, 2021

ISASecure®

Agenda

BACnet overview

- BACnet overview
- BACnet Secure Connect
- BACnet device certification - BTL and ISA Secure
- Secure deployment challenges and techniques

ISA Secure gap analysis

- BACnet - Classic vs. Secure Connect

Smart Buildings need cybersecurity across all systems

Power	HVAC	BMS	Security	Fire	Lighting / Other
Substations	Ventilation	Temperature Control	Video	Panels	Lighting
Microgrid	Chillers	Thermostats	Access Control	Detectors	Shade / Blind
Generators	Air Handlers	Analytics	Intrusion	Monitoring	Digital Signage
Power distribution	Purification	Air Quality / Health	Loss Prevention	Suppression	Conference
Arc flash technology			Monitoring	Smoke	Emergency
Metering			Parking	Safety	
			Elevator / Lift		
			Occupant Health		

ASHRAE BACnet®

LoRa™

Microsoft AD

Proprietary

M-Bus

Modbus

SIP

zigbee

OSDP™

ONVIF®

SNMP

MQTT

KNX

http://

DALI

Z-WAVE

DMX

ASHRAE BACnet® evolution

- 1995 – Initial release
- 2010 – Network Security “addendum G”
- 2019 – BACnet/SC “secure connect”

… regardless of protocol

ASHRAE BACnet®

ISASecure®

“BACnet” = Building Automation Control Network

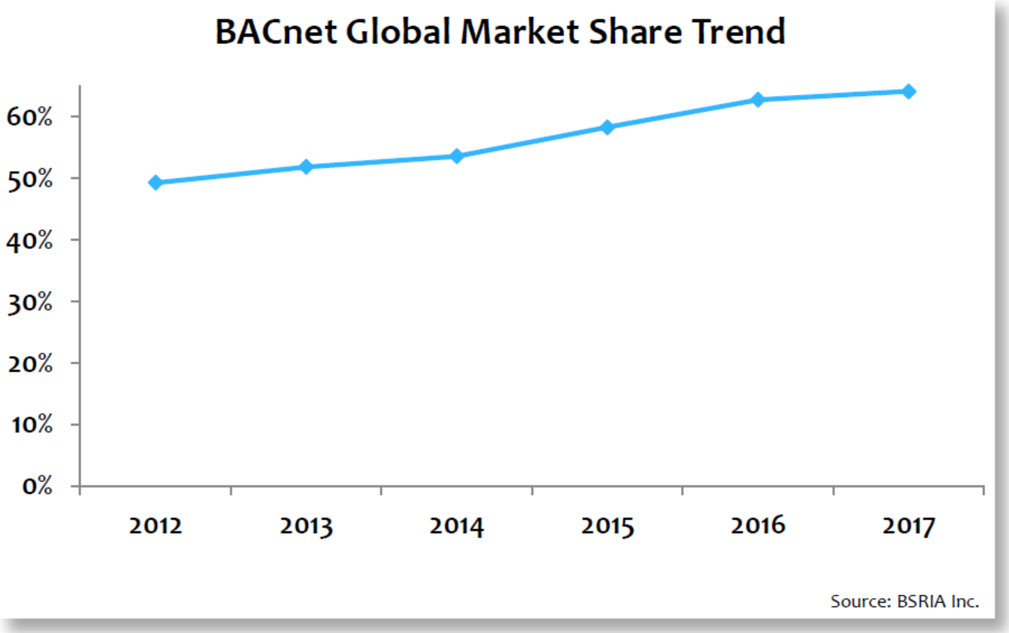
Globally adopted ANSI/ASHRAE standard -

- 1250+ assigned vendor IDs
- Vendors registered in 50+ countries
- ISO 16484

Publications: 135-2020 (BACnet-2020, Ver. 1, Rev. 22)

- 135-2016 (BACnet-2016, Ver. 1, Rev. 19)
- 135-2012 (BACnet-2012, Ver. 1, Rev. 14)
- 135-2010 (BACnet-2010, Ver. 1, Rev. 12)
- 135-2008 (BACnet-2008, Ver. 1, Rev. 7)
- 135-2004 (BACnet-2004, Ver. 1, Rev. 4)
- 135-2001 (BACnet-2001, Ver. 1, Rev. 2)
- 135-1995 (BACnet-1995, Ver. 1, Rev. Not Applicable)

BACnet testing standard: 135.1-2019



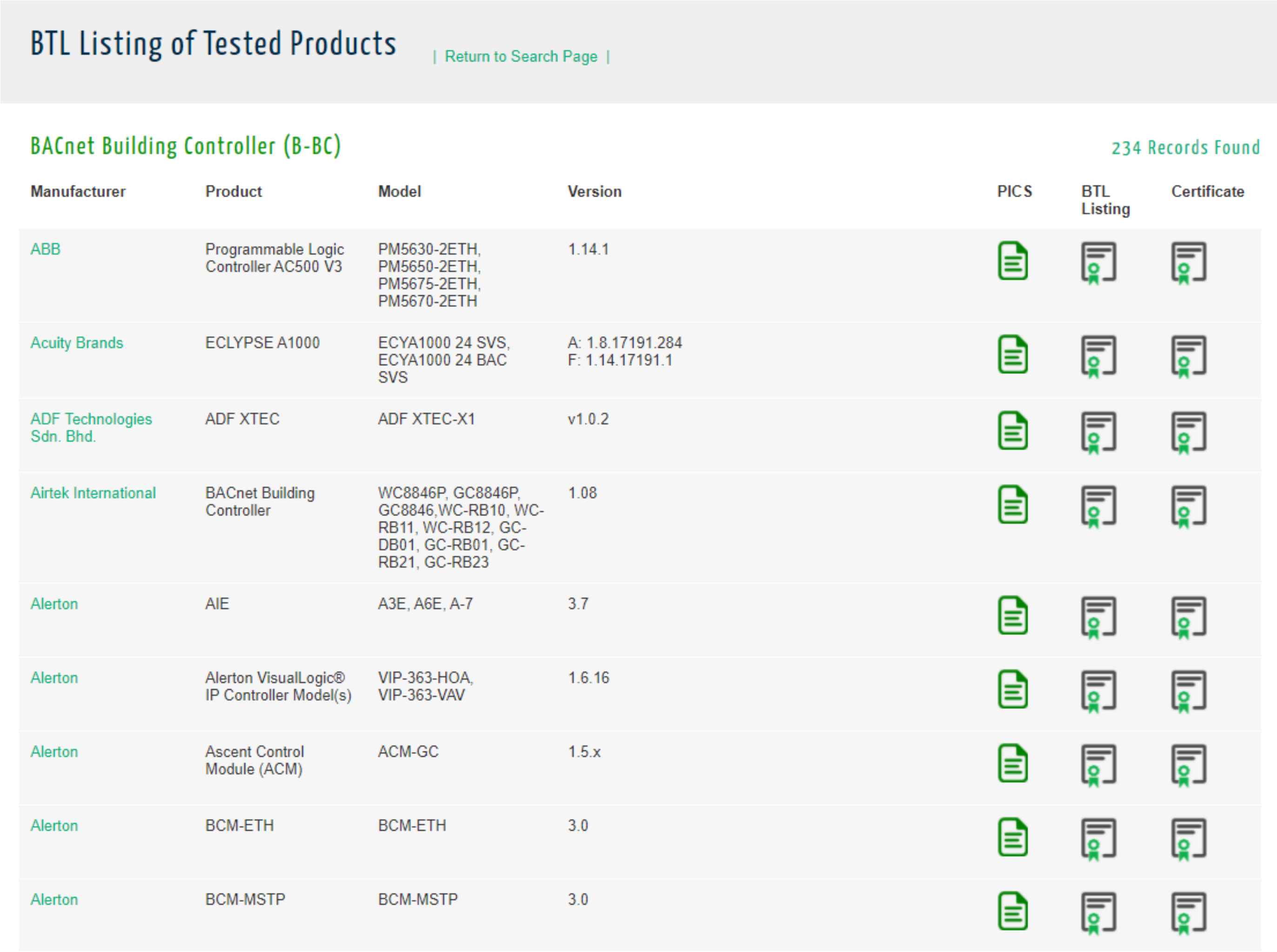
Source: BSRIA Inc.

Building Automation & Control Systems data 2012 to 2017
from BACnet International market report 2018 by BSRIA
“Market Penetration of Communication Protocols”

BACnet device

ISASecure®

A collection of “objects”



BTL Listing of Tested Products | Return to Search Page |

BACnet Building Controller (B-BC)

234 Records Found

Manufacturer	Product	Model	Version	PICS	BTL Listing	Certificate
ABB	Programmable Logic Controller AC500 V3	PM5630-2ETH, PM5650-2ETH, PM5675-2ETH, PM5670-2ETH	1.14.1	📄	📄	📄
Acuity Brands	ECLYPSE A1000	ECYA1000 24 SVS, ECYA1000 24 BAC SVS	A: 1.8.17191.284 F: 1.14.17191.1	📄	📄	📄
ADF Technologies Sdn. Bhd.	ADF XTEC	ADF XTEC-X1	v1.0.2	📄	📄	📄
Airtek International	BACnet Building Controller	WC8846P, GC8846P, GC8846,WC-RB10, WC-RB11, WC-RB12, GC-DB01, GC-RB01, GC-RB21, GC-RB23	1.08	📄	📄	📄
Alerton	AIE	A3E, A6E, A-7	3.7	📄	📄	📄
Alerton	Alerton VisualLogic® IP Controller Model(s)	VIP-363-HOA, VIP-363-VAV	1.6.16	📄	📄	📄
Alerton	Ascent Control Module (ACM)	ACM-GC	1.5.x	📄	📄	📄
Alerton	BCM-ETH	BCM-ETH	3.0	📄	📄	📄
Alerton	BCM-MSTP	BCM-MSTP	3.0	📄	📄	📄

BACnet objects

63 Objects types within 135-2020

Communications
- Device
- Network Port

Inputs
- Analog
- Binary
- Multi-state

Outputs
- Analog
- Binary
- Multi-state

Values
- Analog
- Binary
- Multi-state

Primitive Values
- CharacterString
- Large Analog
- BitString
- OctetString
- Integer
- Positive Integer

Time/Date Values
- Date
- Time
- DateTime

Programming
- Program
- Loop
- Averaging
- Command
- Timer
- Accumulator

Scheduling
- Schedule
- Calendar

Time/Date Patterns
- DateTime Pattern
- Time Pattern
- Date Pattern

Logging
- Trend Log
- Trend Log Multiple
- Event Log
- Audit Reporter
- Audit Log

Alarming
- Event Enrollment
- Notification
- Notification Forwarder
- Alert Enrollment

Life-safety
- Life Safety Point
- Life Safety Zone

Physical Security
- Access Door
- Access Point
- Access Zone
- Access User
- Access Rights
- Access Credential
- Credential Data Input

Elevators
- Lift
- Elevator Group
- Escalator

Electrical
- Pulse Converter
- Load

Lights
- Lighting
- Binary Lighting
- Channel
- Staging

Organization
- Group
- Global Group
- Structured View

Other
- File

BACnet properties

Data contained within an object

Conformance Codes

- Read only (R)
- Writable (W)
- Optional (O)

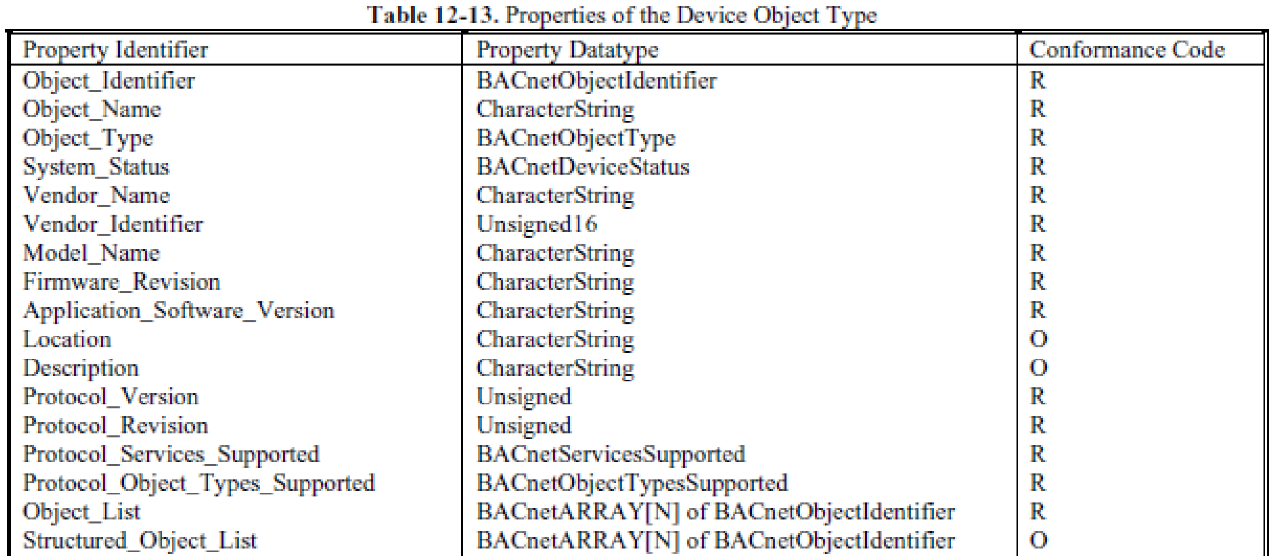


Table 12-13. Properties of the Device Object Type

Property Identifier	Property Datatype	Conformance Code
Object_Identifier	BACnetObjectIdentifier	R
Object_Name	CharacterString	R
Object_Type	BACnetObjectType	R
System_Status	BACnetDeviceStatus	R
Vendor_Name	CharacterString	R
Vendor_Identifier	Unsigned16	R
Model_Name	CharacterString	R
Firmware_Revision	CharacterString	R
Application_Software_Version	CharacterString	R
Location	CharacterString	O
Description	CharacterString	O
Protocol_Version	Unsigned	R
Protocol_Revision	Unsigned	R
Protocol_Services_Supported	BACnetServicesSupported	R
Protocol_Object_Types_Supported	BACnetObjectTypesSupported	R
Object_List	BACnetARRAY[N] of BACnetObjectIdentifier	R
Structured_Object_List	BACnetARRAY[N] of BACnetObjectIdentifier	O

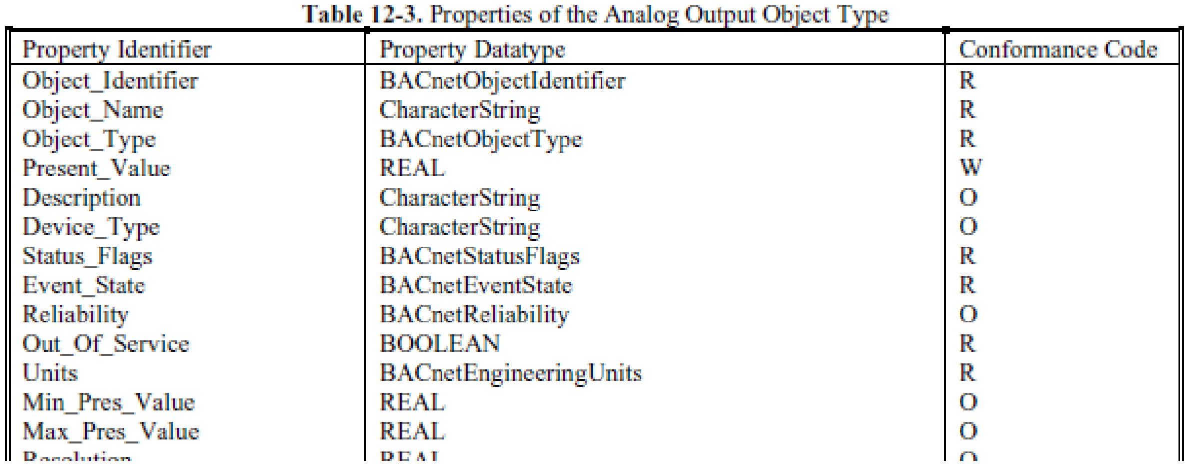


Table 12-3. Properties of the Analog Output Object Type

Property Identifier	Property Datatype	Conformance Code
Object_Identifier	BACnetObjectIdentifier	R
Object_Name	CharacterString	R
Object_Type	BACnetObjectType	R
Present_Value	REAL	W
Description	CharacterString	O
Device_Type	CharacterString	O
Status_Flags	BACnetStatusFlags	R
Event_State	BACnetEventState	R
Reliability	BACnetReliability	O
Out_Of_Service	BOOLEAN	R
Units	BACnetEngineeringUnits	R
Min_Pres_Value	REAL	O
Max_Pres_Value	REAL	O
Resolution	REAL	O

BACnet interoperability

5 Interoperability Areas

Data Sharing	Alarming	Trending	Scheduling	Device Management

Services

Data Sharing

- Read Property
- Read Property Multiple
- Read Property Conditional

Object Modification

- Write Property
- Write Property Multiple
- Add List Element
- Remove List Element
- Create Object
- Delete Object

Alarm and Event

- Acknowledge Alarm
- Confirmed Event Notification
- Get Alarm Summary
- Get Enrollment Summary

COV Notification

- Confirmed COV Notification
- Confirmed Event Notification
- COV Property Notification
- Unconfirmed COV Notification

Device Management

- Device Communication Control
- Confirmed Private Transfer
- Reinitialize Device
- Confirmed Text Message
- Unconfirmed Text Message
- Time Synchronization
- Who Has / I Have
- Who Is / I am

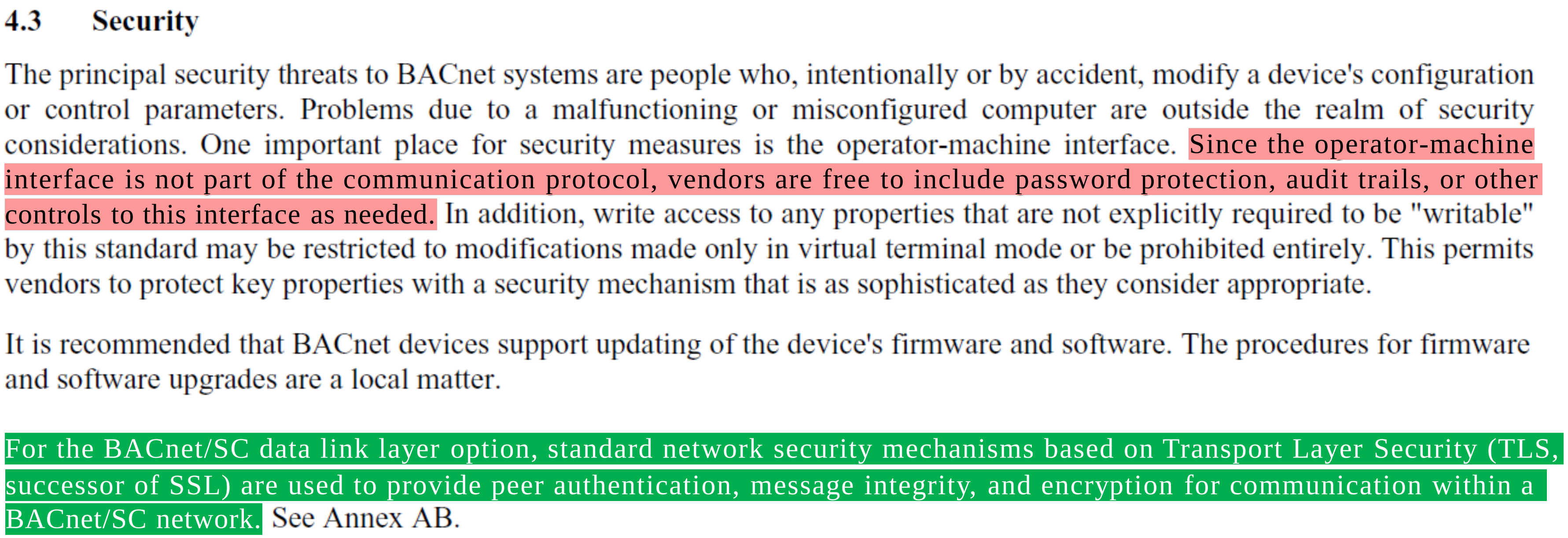
File

- Atomic Read File
- Atomic Write File

BACnet Security – BACnet Secure Connect (SC)

Does not address operator interfaces

BACnet/SC adds TLS encryption and authentication



4.3 Security

The principal security threats to BACnet systems are people who, intentionally or by accident, modify a device's configuration or control parameters. Problems due to a malfunctioning or misconfigured computer are outside the realm of security considerations. One important place for security measures is the operator-machine interface. Since the operator-machine interface is not part of the communication protocol, vendors are free to include password protection, audit trails, or other controls to this interface as needed. In addition, write access to any properties that are not explicitly required to be "writable" by this standard may be restricted to modifications made only in virtual terminal mode or be prohibited entirely. This permits vendors to protect key properties with a security mechanism that is as sophisticated as they consider appropriate.

It is recommended that BACnet devices support updating of the device's firmware and software. The procedures for firmware and software upgrades are a local matter.

For the BACnet/SC data link layer option, standard network security mechanisms based on Transport Layer Security (TLS, successor of SSL) are used to provide peer authentication, message integrity, and encryption for communication within a BACnet/SC network. See Annex AB.

ASHRAE 135-2020 – ANNEX AB

Adds support for:

- Websockets / TLS
- New routing options

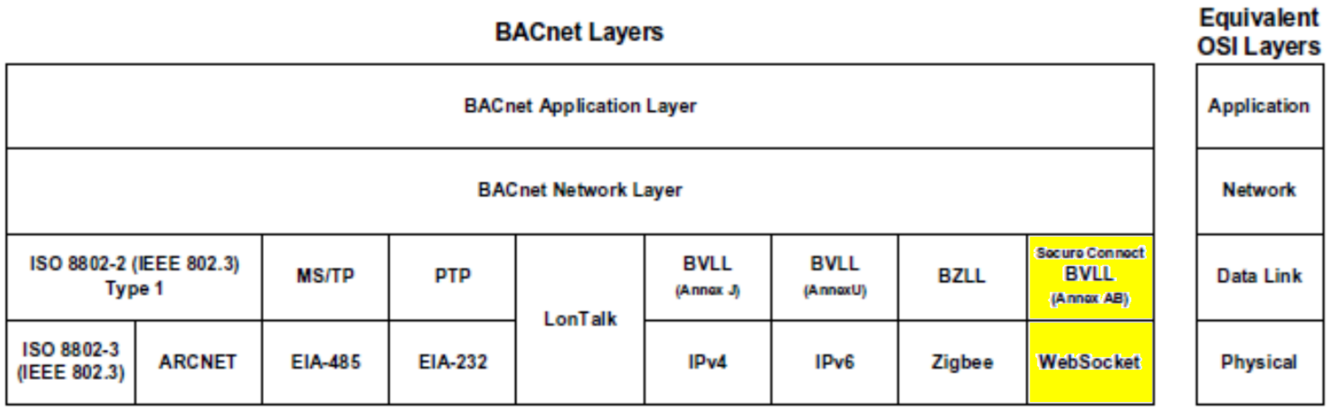
NOTE: BACnet Secure Connect (SC) enable devices are in development but not widely available today

BACnet transports

All BACnet transports deliver the same BACnet messages

135-2020
Adds the Secure Connect transport

- Ethernet (ISO 8802-3)
- ARCNET (ATA 878.1)
- MS/TP
- PTP
- LonTalk (ISO/IEC 14908.1)
- BACnet/IP
- BACnet/IPv6
- ZigBee
- **BACnet/SC**



BACnet Layers									Equivalent OSI Layers
BACnet Application Layer									Application
BACnet Network Layer									Network
ISO 8802-2 (IEEE 802.3) Type 1		MS/TP	PTP	LonTalk	BVLL (Annex J)	BVLL (AnnexU)	BZLL	Secure Connect BVLL (Annex AB)	Data Link
ISO 8802-3 (IEEE 802.3)	ARCNET	EIA-485	EIA-232		IPv4	IPv6	Zigbee	WebSocket	Physical

Figure 4-2. BACnet collapsed architecture.

BACnet topology

BACnet has a “flat” architecture

- no hierarchy
- no prescribed network topology
- all devices have equal permissions

BACnet Segment

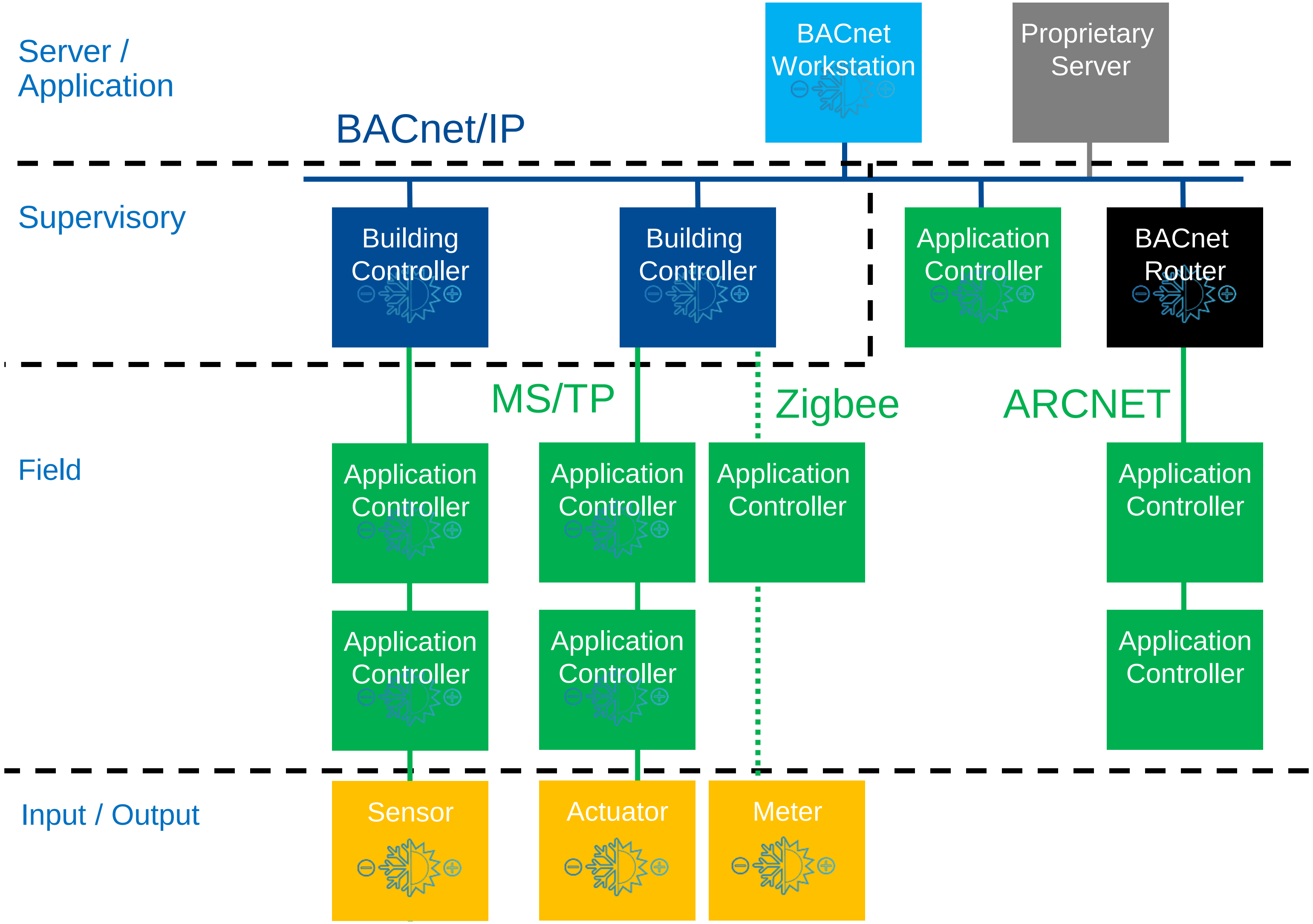
- One or more physical segments connect by Repeaters (R)

BACnet Network

- One or more segments interconnected by Bridges (B)

BACnet Internetwork

- Multiple networks interconnected by BACnet Routers (RT)

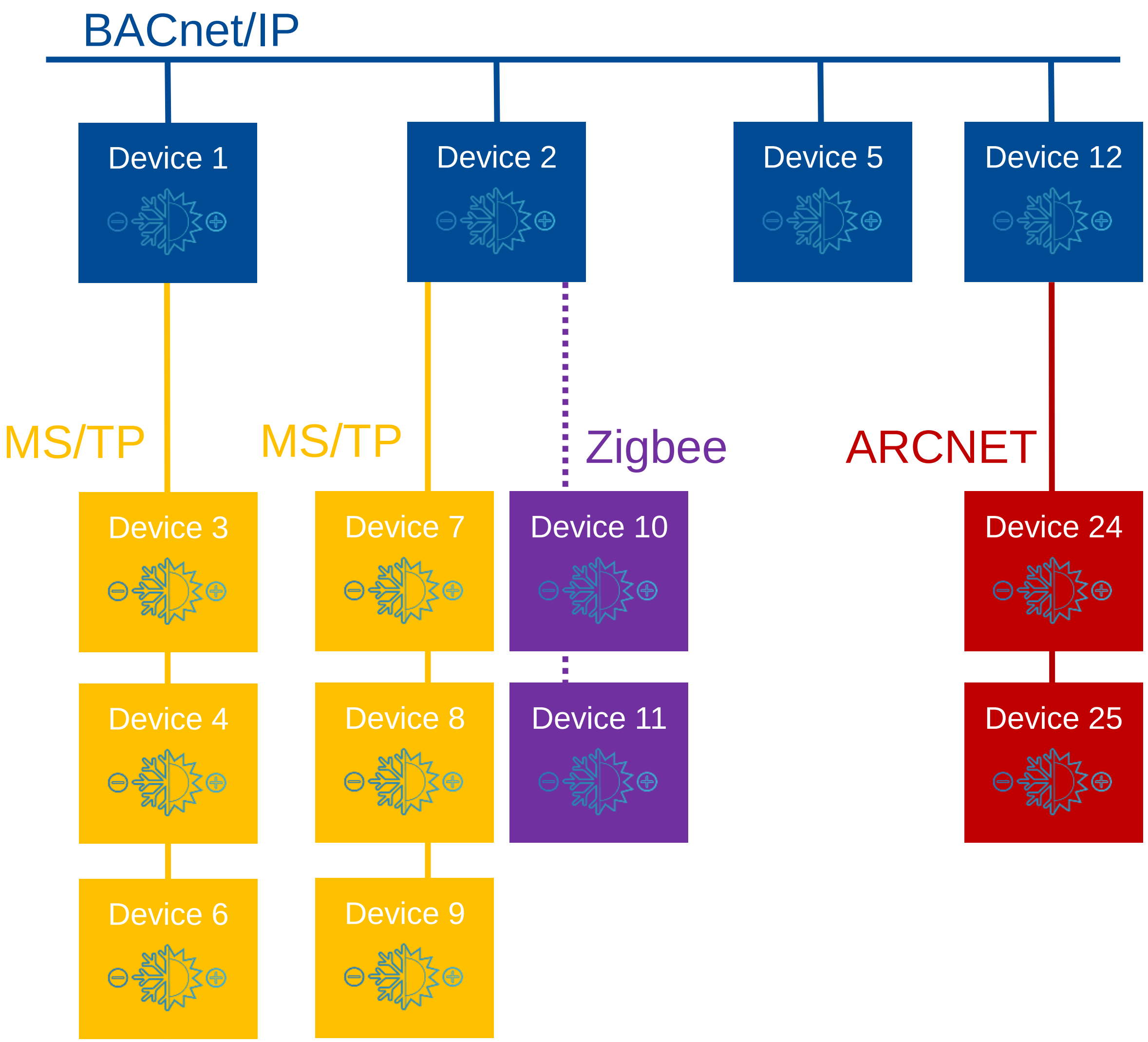


Multi-transport deployment

BACnet devices can route between transports

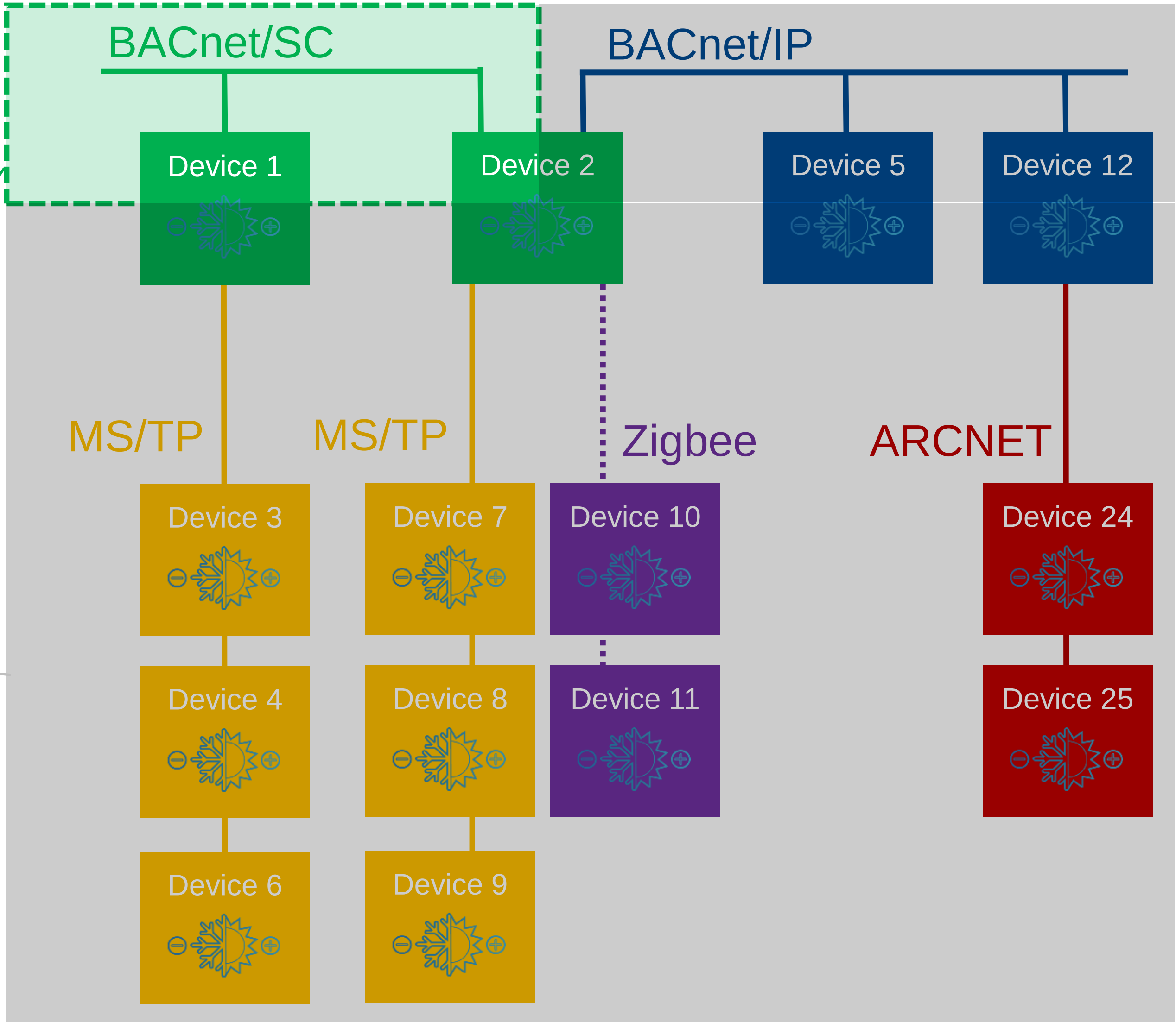
Classic BACnet transport have

- No encryption
- No authentication



Transitioning to BACnet Secure Connect (SC)

BACnet/SC can interoperate with Classic BACnet devices

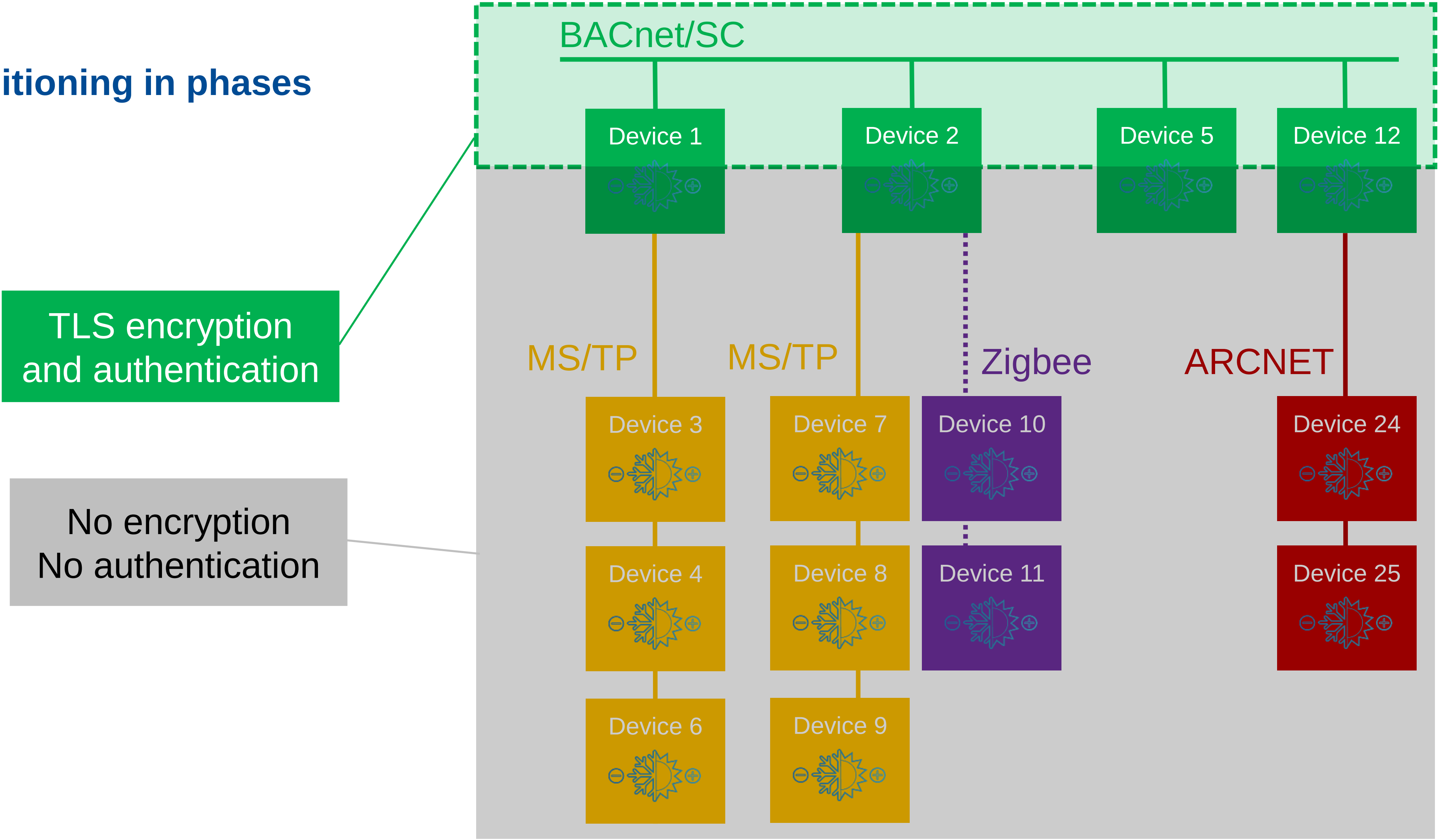


TLS encryption and authentication

No encryption
No authentication

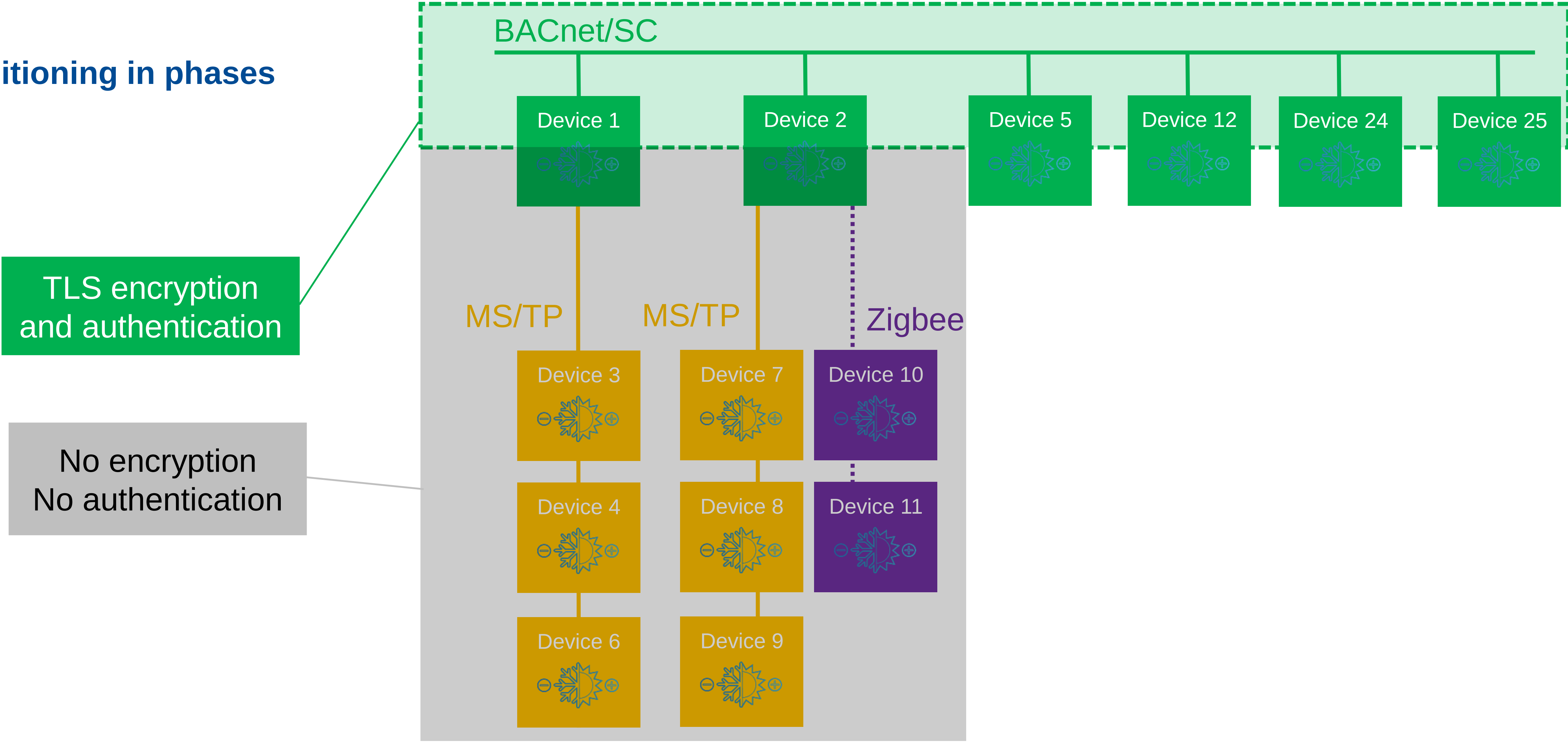
Transitioning to BACnet/SC

Transitioning in phases



BACnet topology

Transitioning in phases



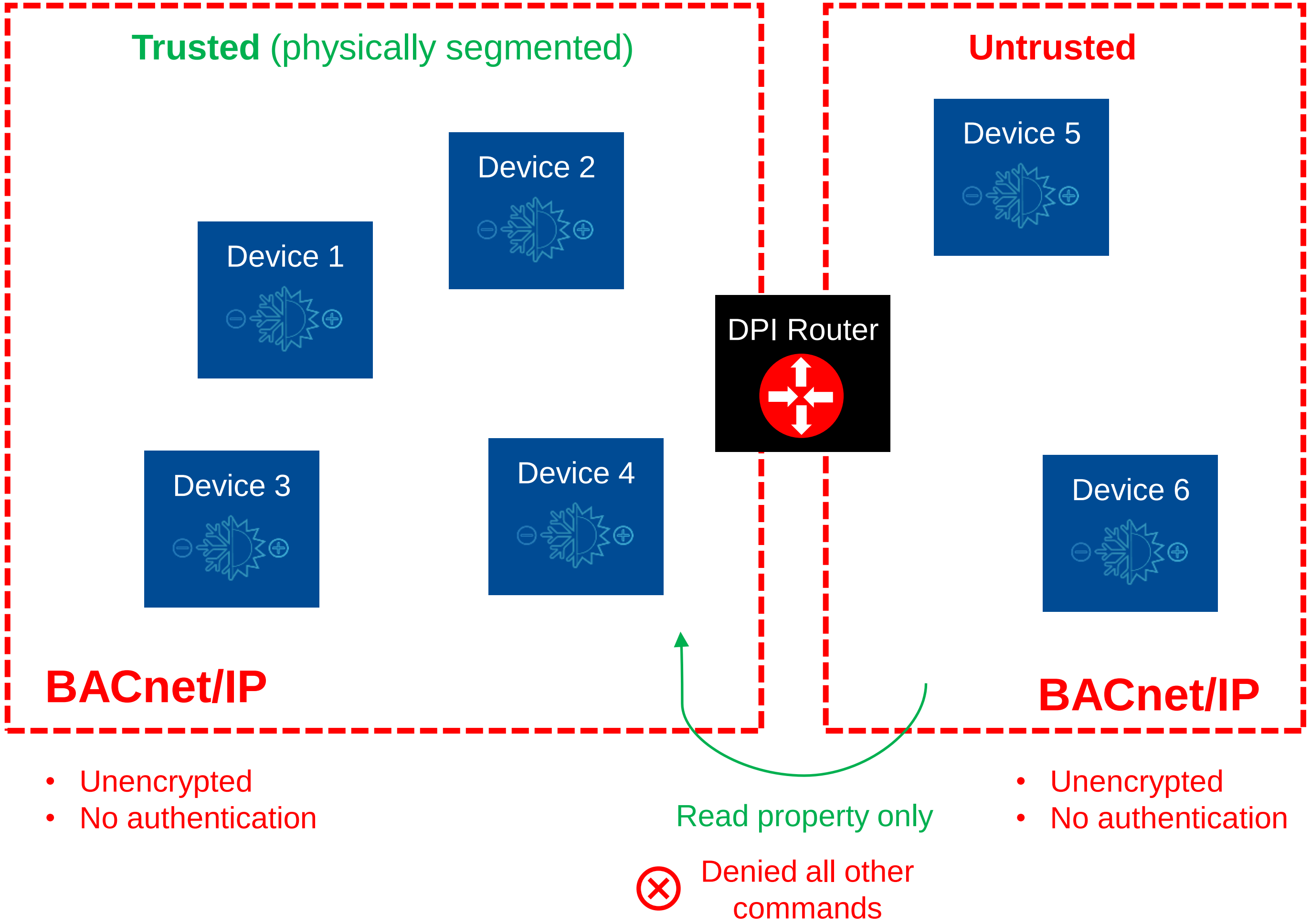
BACnet/IP security management

Apply IEC 62443 security measures

- Zone
- Conduits
- Firewall / DPI* Rules

Deep Packet Inspection (DPI)

- Flow control – limit by BACnet command
- Work with unencrypted packets



- Unencrypted
- No authentication

- Unencrypted
- No authentication

BACnet/SC security management

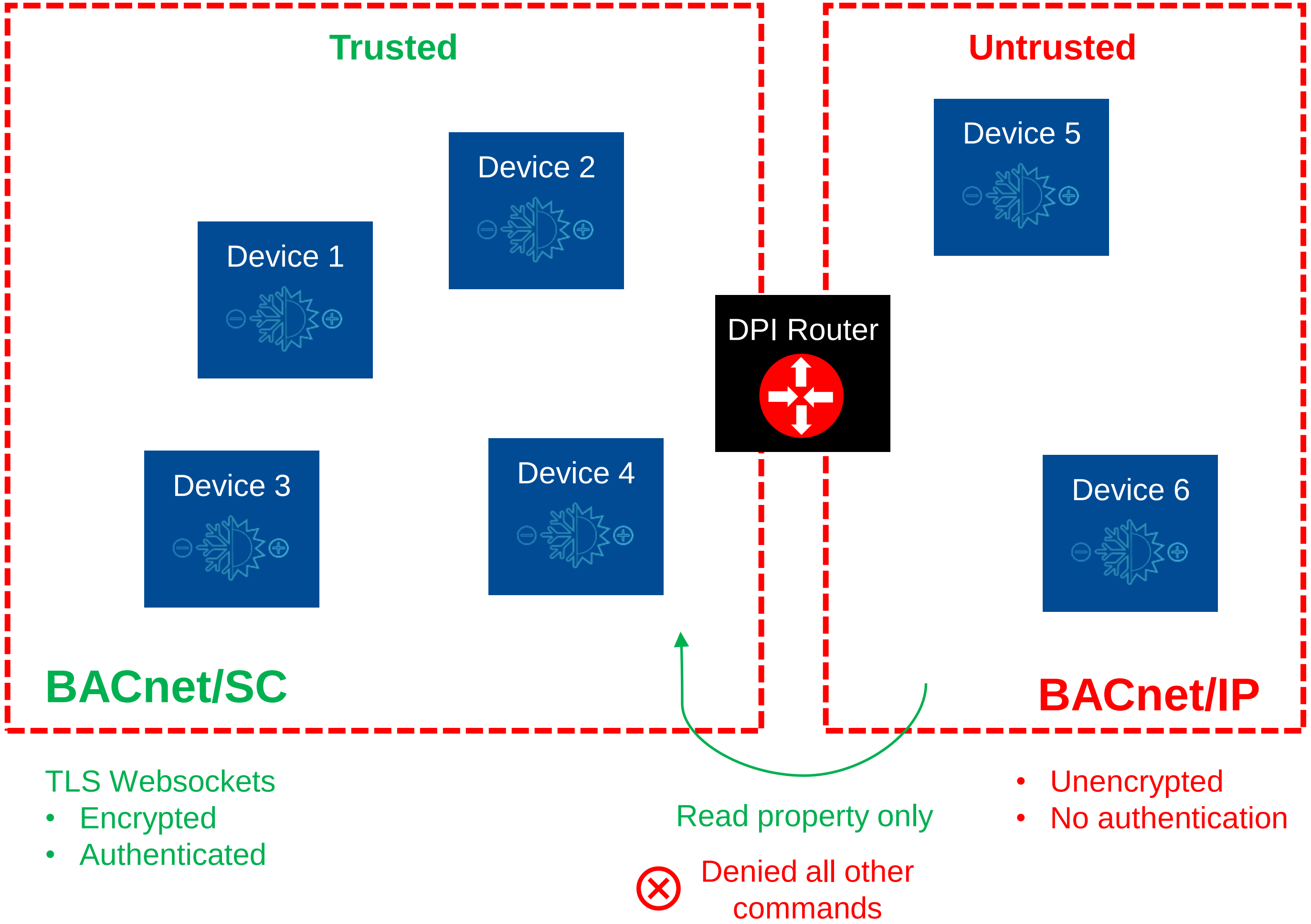
Apply IEC 62443 security measures with BACnet Secure Connect devices

Segment BACnet/IP from BACnet/SC

- **Zone**
- **Conduits**
- **Firewall / DPI Rules**

The BACnet/SC zone

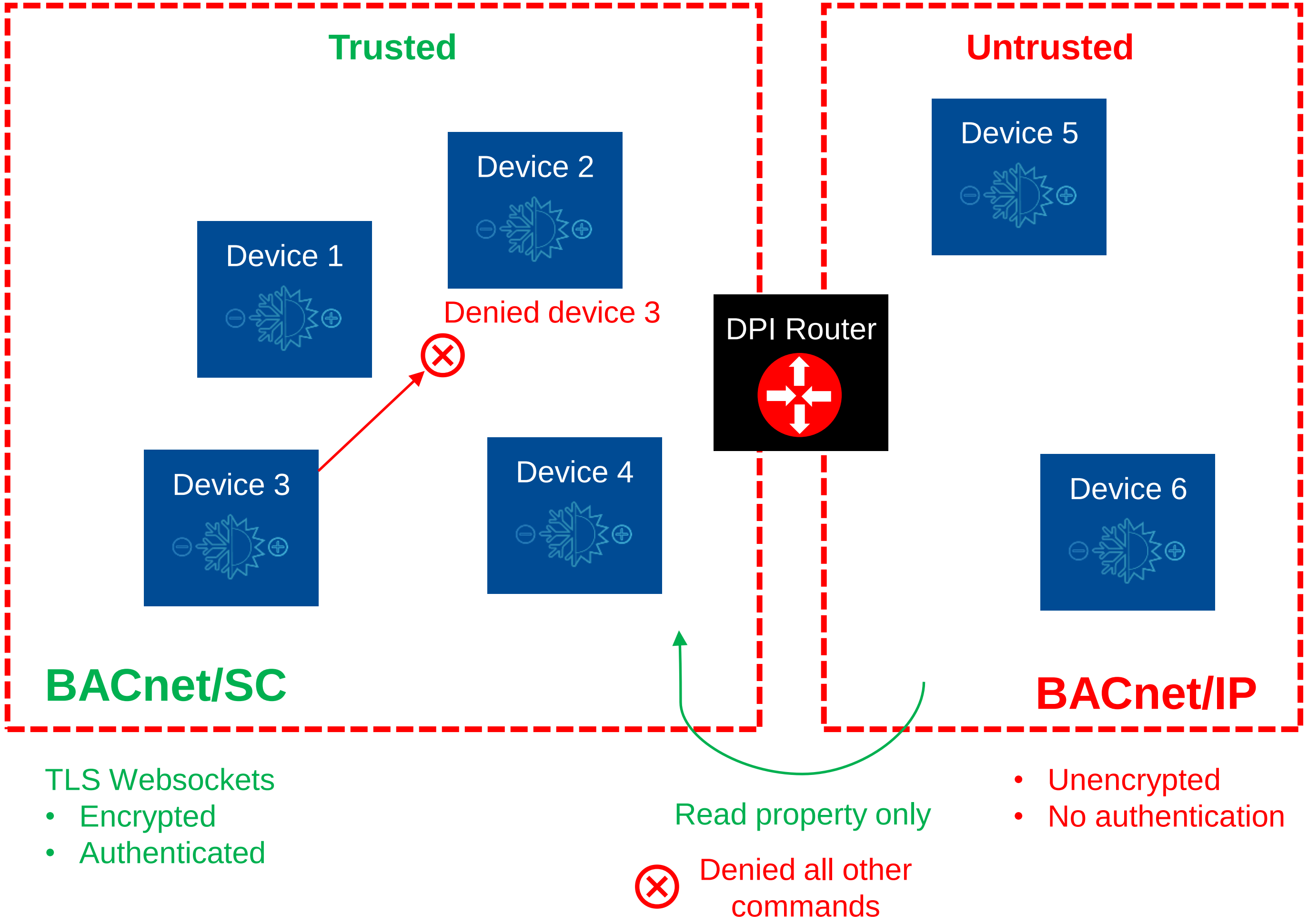
- **Physically segmentation is less critical**
- **TLS certificates protect against impersonation**



BACnet/SC security management

Apply IEC 62443 security measures with BACnet Secure Connect devices

- **More granular control is possible**
  - **Devices can have their own access control list**
  - **Even within same zone**
- **Physically segmentation is less critical**
- **TLS certificates protect against impersonation**



Multi-domain / building deployments

BACnet has a “flat” architecture

- no hierarchy
- no prescribed network topology
- all devices have equal permissions

BACnet Segment

- One or more physical segments connect by Repeaters (R)

BACnet Network

- One or more segments interconnected by Bridges (B)

BACnet Internetwork

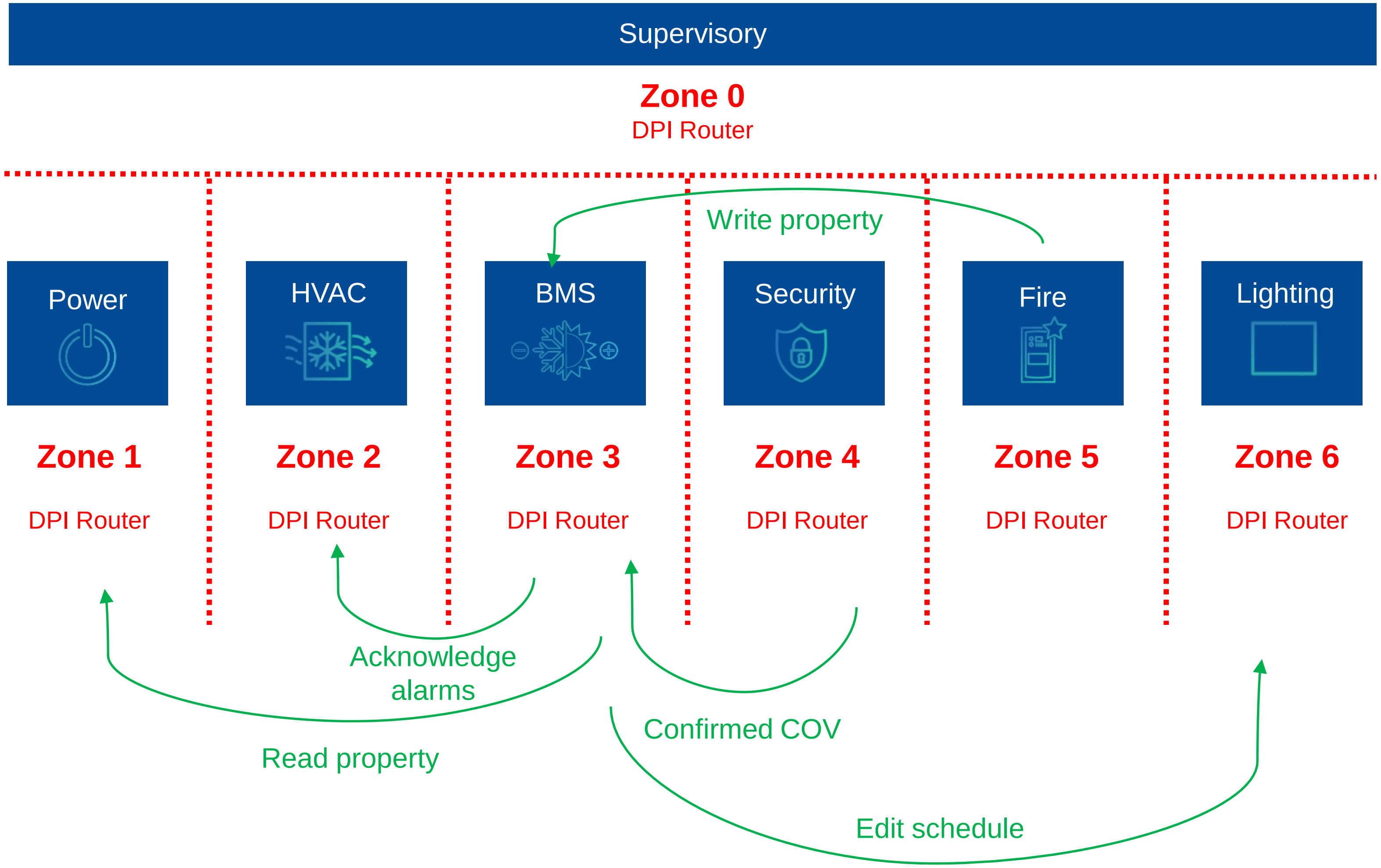
- Multiple networks interconnected by BACnet Routers (RT)

Power
HVAC
BMS
Security
Fire
Lighting

BACnet security management – multi-domain

Apply IEC 62443 security measures

- Zone
- Conduits
- Firewall / DPI Rules



Device Certification

ISASecure®

OT Interoperability focused

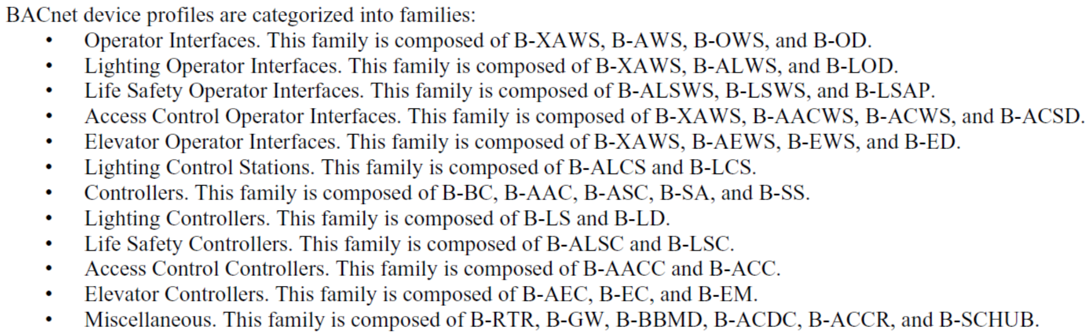
BTL Certification

ASHRAE 135.1

Conformance based on declared support in

Protocol Implementation Conformance Statement (PICS)

BACnet Device Profile



BACnet device profiles are categorized into families:

- Operator Interfaces. This family is composed of B-XAWS, B-AWS, B-OWS, and B-OD.
- Lighting Operator Interfaces. This family is composed of B-XAWS, B-ALWS, and B-LOD.
- Life Safety Operator Interfaces. This family is composed of B-ALSWS, B-LSWS, and B-LSAP.
- Access Control Operator Interfaces. This family is composed of B-XAWS, B-AACWS, B-ACWS, and B-ACSD.
- Elevator Operator Interfaces. This family is composed of B-XAWS, B-AEWS, B-EWS, and B-ED.
- Lighting Control Stations. This family is composed of B-ALCS and B-LCS.
- Controllers. This family is composed of B-BC, B-AAC, B-ASC, B-SA, and B-SS.
- Lighting Controllers. This family is composed of B-LS and B-LD.
- Life Safety Controllers. This family is composed of B-ALSC and B-LSC.
- Access Control Controllers. This family is composed of B-AACC and B-ACC.
- Elevator Controllers. This family is composed of B-AEC, B-EC, and B-EM.
- Miscellaneous. This family is composed of B-RTR, B-GW, B-BBMD, B-ACDC, B-ACCR, and B-SCHUB.

OT Cybersecurity focused

Certified Component ISASecure®

Component Security Assurance (CSA)

ISA/IEC 62443-4-1, **ISA/IEC 62443-4-2**

Vulnerability Identification Test + Communication Robustness Test

ISA/IEC 62443-4-2 Foundational requirements for components

Develop

ISA 62443-4-2

Component requirements

Foundational Requirement Groups

FR1 - Identification and authentication control (IAC)

FR2 - Use control (UC)

FR3 - System integrity (SI)

FR4 - Data confidentiality (DC)

FR5 - Restricted data flow (RDF)

FR6 - Timely response to events (TRE)

FR7 - Resource availability (RA)

Security Levels	Definition	Means	Resources	Skills	Motivation
SL1	Protection against casual or coincidental violation	simple	low	generic	low
SL2	Protection against intentional violation using simple means with low resources, generic skills and low motivation				
SL3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation	sophisticated	moderate	IACS-specific	moderate
SL4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation	sophisticated	extended	IACS-specific	high

ISA/IEC 62443-4-2 Foundational requirements for components

Develop

ISA 62443-4-2

Component requirements

Component Requirement Challenges		BACnet 135-2016 Compliance	Vendor addressable	BACnet 135-2020 w/ Secure Connect Compliance	Vendor addressable
FR 1	**Identification and authentication control**				
	• User account ID and authentication	N/A – No users	Yes, user interfaces	N/A – No users	Yes, device access control
	• Device ID and authentication	ID not authenticated	No workaround	Yes - TLS	BACnet addresses
	• Encryption	NO	No workaround	Yes - TLS	BACnet addresses
	• Key protection	N/A	Dependencies not meet	N/A	Yes
FR 2	**Use control**				
	• User authorizations	N/A – No authorizations	Yes, user interfaces	N/A – No authorizations	Yes, RBAC
	• Device authorizations	N/A – No authorizations	No workaround	N/A – No authorizations	Yes, device access control
	• Time synchronization	Yes – but not secure	Yes – disable BACnet time sync	Yes – manageable	Yes, device access control
	• Audit log	Partial with BACnet audit features	Yes	Partial with BACnet audit features	Yes

ISA/IEC 62443-4-2 Foundational requirements for components

Develop

ISA 62443-4-2

Component requirements

Component Requirement Challenges		BACnet 135-2016 Compliance	Vendor addressable	BACnet 135-2020 w/ Secure Connect Compliance	Vendor addressable
FR 3	**System Integrity**				
	• Communications integrity	NO	No workaround	Yes	BACnet addresses
	• Cryptographic integrity protection	NO	No workaround	Yes - TLS	Compliments
	• Malicious code protection	N/A	Yes	N/A	Yes
	• Security functionality verification	N/A	Yes	N/A	Yes
	• Integrity checks and notification	N/A	Yes	N/A	Yes
	• Input validation	N/A	Yes	N/A	Yes
	• Deterministic outputs	Priority array can support	Yes	Priority array can support	Yes
	• Session integrity and management	NO	Yes	Yes – TLS supports	Yes
	• Protection of audit information	N/A	Yes	N/A	Yes
	• Originality	N/A	Yes	N/A	Yes

ISA/IEC 62443-4-2 Foundational requirements for components

Develop

ISA 62443-4-2

Component requirements

Component Requirement Challenges		BACnet 135-2016 Compliance	Vendor addressable	BACnet 135-2020 w/ Secure Connect Compliance	Vendor addressable
FR 4	**Data Confidentiality**				
	• Information confidentiality	NO encryption	No workaround	In transit - TLS	At rest
	• Decommission information purging	N/A	Yes	N/A	Yes
	• Shared resource memory purging	N/A	Yes	N/A	Yes
	• Recognized cryptography	NO encryption	No workaround	In transit - TLS	At rest
FR 5	**Restricted Data Flow**				
	• Network segmentation (CR 5.1) • Zone boundary protection (CR 5.2)	Supports routers etc.	Deployment of routers, Deep packet inspection	Supports routers etc.	Deployment of routers, Deep packet inspection
	• General purpose person-to-person communication restrictions (CR 5.3)	N/A	Yes	N/A	Yes
	• Application or device partitioning (CR 5.4)	N/A	Yes	N/A	Yes

ISA/IEC 62443-4-2 Foundational requirements for components

Develop

ISA 62443-4-2

Component requirements

Component Requirement Challenges		BACnet 135-2016 Compliance	Vendor addressable	BACnet 135-2020 w/ Secure Connect Compliance	Vendor addressable
FR 6	**Timely Response to Events**				
	• Audit log accessibility	Partial with BACnet audit features	Yes	Partial with BACnet audit features	Yes, RBAC
	• Programmatic access to audit logs	Partial with BACnet audit features	Yes	Partial with BACnet audit features	Yes, device access control
	• Continuous monitoring	N/A	Yes	N/A	Yes, device access control
FR 7	**Resource availability**				
	• Denial of Service Protection	N/A	Yes	N/A	Yes
	• Manage communication load	N/A	Yes	N/A	Yes
	• Resource management	N/A	Yes	N/A	Yes
	• Backup and reconstitution	BACnet backup/restore	Additional as required	BACnet backup/restore	Additional as required
	• Emergency power	N/A	Yes	N/A	Yes
	• Network and security configuration settings	Device and network port	Yes	Device and Network Port	Yes
	• Least functionality	N/A	Yes	N/A	Yes
	• Control system component inventory	Device list	Yes	Device list	Yes

Interoperable & Secure Device Certification

BTL Certification

✓

OT Interoperability Conformance

BACnet® with **BACnet/SC** + ISA/IEC 62443 enhancements

OT Cybersecurity Conformance

Certified Component

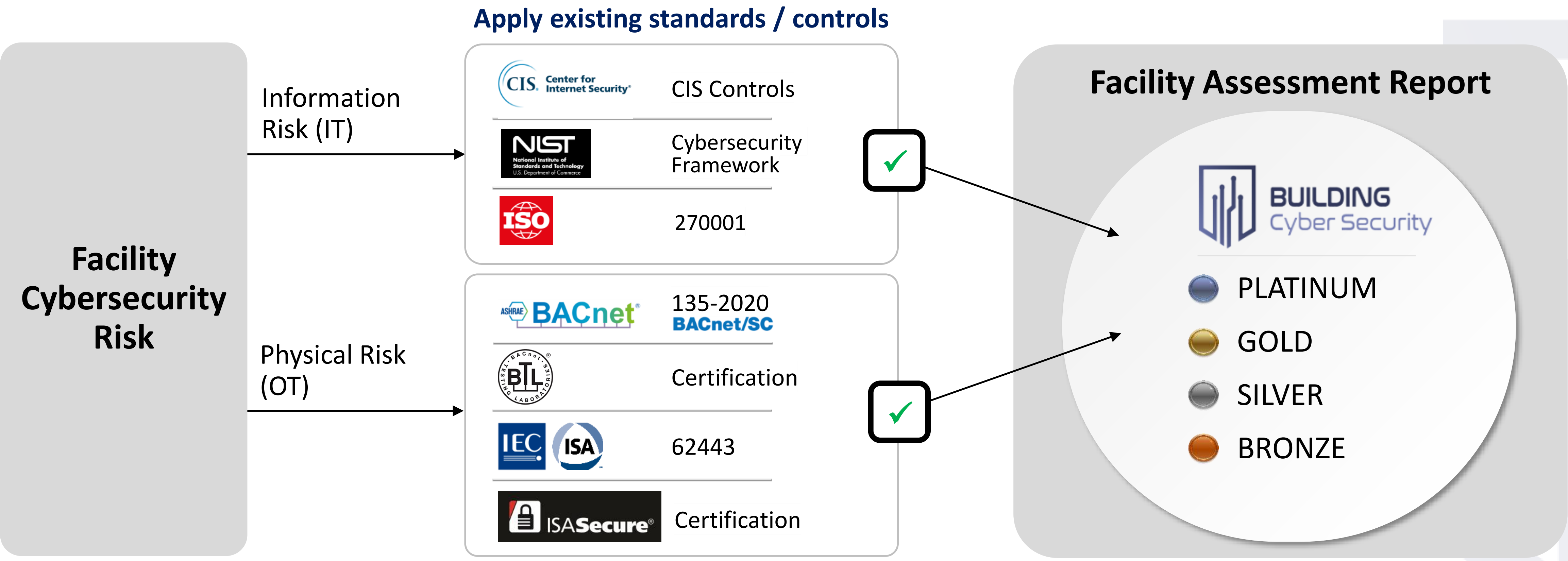
ISASecure®

Component Security Assurance (CSA)

✓

ISA Secure Certification

Interoperable & Secure Facilities



Facility Cybersecurity Risk

Information Risk (IT)

Physical Risk (OT)

Apply existing standards / controls

CIS Center for Internet Security	CIS Controls
NIST National Institute of Standards and Technology U.S. Department of Commerce	Cybersecurity Framework
ISO	270001

✓

ASHRAE BACnet	135-2020 BACnet/SC
BTL BACnet Testing Laboratories	Certification
IEC ISA	62443
ISASecure	Certification

✓

Facility Assessment Report

BUILDING Cyber Security

- PLATINUM
- GOLD
- SILVER
- BRONZE

ISASecure webinar

BACnet and ISA/IEC 62443 Conformance using BACnet Secure Connect

Questions

ISASecure®