Hardening BACnet Networks: Practical Security Guidelines for OT Installers

Securing BAS White Paper Series 3 of 6

CONTACT INFORMATION

877.444.5622

info@kmccontrols.com

www.kmccontrols.com

19476 Industrial Drive, New Paris, IN 46553

Table of Contents

Executive Summary 1

Introduction 1

Why BACnet Needs Hardening 2

Best Practices for Network Hardening 3

Hardening BACnet Devices Themselves 4

Conclusion 6

Minimum Handover Items for a Hardened BACnet Installation 6

Executive Summary

This paper provides Operational Technology (OT) installers with actionable best practices to secure BACnet-based building automation networks. While BACnet was not designed with cybersecurity in mind, it remains a foundational protocol in building systems. The paper outlines practical network hardening strategies, device-level protections, and anomaly detection techniques that improve integrity and availability without compromising uptime.

BACnet hardening should be implemented as part of a documented OT security baseline that protects safety and availability while also defining approved remote access, account ownership, network boundaries, monitoring, backup expectations, and change control for BAS environments.

Before the system is commissioned, installers, service providers, and owners should agree in writing on who maintains network diagrams, device inventories, remote connections, privileged credentials, log review, and incident escalation.

Introduction

OT networks running building automation systems (BAS) often rely on the BACnet protocol, a widely adopted communication standard designed to enable interoperability among devices such as HVAC controllers, lighting systems, and access control equipment. However, it was originally developed without security in mind. As cyber threats become more frequent and targeted, OT installers play a key role in securing the networks they deploy.

OT installers play a key role in securing the networks they deploy, but BACnet hardening is only effective when the resulting design is supportable by the owner and service provider over the full system life cycle.

This paper provides practical guidance on hardening BACnet networks while maintaining the operational flexibility and uptime that building systems require. It builds on the S/AIC framework introduced in White Paper 2 and focuses on actionable steps installers can take with the equipment they already use.

Where site conditions allow, these steps should be reflected in a simple cyber design package that includes a network diagram, list of BACnet segments, approved service paths, critical devices, and compensating controls for legacy or unpatchable equipment.

Why BACnet Needs Hardening

BACnet/IP and BACnet MS/TP are widely used in BAS for HVAC, lighting, access control, and more. However, BACnet's original design assumed a trusted network. It lacks built-in encryption, authentication, and access control. Common vulnerabilities include:

- Rogue devices broadcasting misleading data.
- Spoofed devices impersonating legitimate ones.
- Lack of visibility into traffic or anomalies.
- Open ports and unsecured network segments.
- Undocumented connections, shared vendor credentials, and unmanaged remote paths that bypass otherwise sound network design.

These risks are amplified by legacy devices with limited processing power and environments where patching is difficult or impossible.

BACnet hardening should combine technical controls with procedural controls such as approval of changes, review of third-party access, and clear responsibility for monitoring and response.

Best Practices for Network Hardening

Segment the Network with VLANs

Create logical separation between building systems, tenants, management workstations, and internet-connected devices. Each should be in its own VLAN to help contain potential breaches, simplify traffic management, and limit the spread of unauthorized activity between segments from infected devices.

Where practical, define BACnet segments as zones or trust boundaries and document only the conduits required for operations, alarms, integrations, engineering access, and maintenance.

Keep a current drawing showing controller networks, supervisory controllers, operator workstations, jump hosts, wireless bridges, and cloud-dependent paths so troubleshooting does not require broad emergency access.

Use Switch Port Security

- Disable unused ports.
- Restrict ports to specific MAC addresses where supportable.
- Limit the number of allowed devices per port.
- Enable shutdown or alerting modes on violations.
- Label ports and panels so unauthorized field changes can be detected quickly.

Apply Access Control Lists (ACLs)

Restrict traffic between VLANs to only what is needed. For example, prevent lighting systems from initiating connections to HVAC controllers unless the integration requires it.

Document approved source, destination, service, and purpose for each cross-segment rule and review exceptions whenever systems are expanded or integrated.

Configure Firewalls and NAT

Restrict external access. Use outbound-only rules where possible. Avoid direct inbound internet access to BACnet devices. Do not install devices within an organization's DMZ with a publicly accessible IP address.

Remote service should terminate on an approved VPN or jump host with multifactor authentication, named user access, session logging, and owner visibility into who connected, when, and why.

Deploy Network Intrusion Detection and Logging

While many IDS solutions are IT-focused, some can be tuned for OT traffic patterns. Use logging to detect unexpected activity and track device behavior over time.

At minimum, preserve logs for remote access sessions, firewall denies, device additions, and major configuration changes, and be sure to define who reviews alerts and how incidents are escalated.

Hardening BACnet Devices Themselves

Disable Unused Services

Some BACnet devices ship with unnecessary services enabled by default. Disable anything not needed immediately. Record any required legacy service that cannot be disabled and note the compensating control being relied upon.

Change Default Passwords

Although commonly recommended, it is often overlooked. Use unique, strong credentials. Do not share one vendor or installer password across customers, buildings, or job sites, and assign ownership for privileged credentials.

Implement Authorization Where Supported

BACnet devices themselves do not implement role-based access control, but BAS operator workstations and front-end software often do support user permissions and role-based access. Use these controls to restrict which users can issue commands, change setpoints, or modify configurations. Disable or remove dormant accounts promptly and review administrator permissions whenever staff, vendors, or contracts change.

Special Considerations for MS/TP

Standard BACnet devices, including MS/TP, BACnet/IP, and BACnet 8802 do not natively support IP-based encryption like TLS. Because neither physical-layer encryption nor device-level authentication are available on MS/TP networks, security for these segments must rely heavily on physical access controls and network segmentation, such as:

- Physical security: lock panels and secure wiring closets.
- Controlled access to RS-485 networks and field trunks.
- Identify critical trunks and document how the site is to detect unauthorized splices, replacements, or temporary service connections.

Anomaly Detection, Recovery, and Change Control

BACnet networks typically generate predictable, low-volume traffic compared to IT networks, making them good candidates for anomaly detection:

- Look for new or unexpected device announcements.
- Monitor for changes in message frequency or type.
- Set thresholds for normal traffic volumes.
- Back up controller databases, workstation configurations, graphics, and integration settings before major changes and test restoration on a defined schedule.
- Record significant network and controller changes so unusual behavior can be tied quickly to recent maintenance, firmware updates, or integrations.

Conclusion

Hardening a BACnet network does not always require a complete system overhaul. Many improvements can be implemented with existing hardware and thoughtful configuration. The S/AIC framework — focusing on Safety/Availability, Integrity, and Confidentiality — helps prioritize actions that strengthen resilience while keeping building systems running smoothly.

The strongest BACnet deployments pair these technical measures with documented responsibilities for inventories, remote access, logging, backup, incident escalation, and periodic review so the system remains supportable after commissioning.

When owners, installers, and service providers align on these minimum practices, BACnet environments become easier to defend, troubleshoot, recover, and expand without sacrificing operational uptime.

Minimum Handover Items for a Hardened BACnet Installation

Before turnover, confirm that the following items are available to the owner or designated service provider:

- Current network diagram and BACnet segment list.
- Approved remote access method and support contacts.
- Record of default credential changes and privileged account ownership.
- Backup location for databases, workstation configurations, graphics, and integrations.
- List of legacy constraints and compensating controls.
- Escalation path for suspected cyber events or unexplained device behavior.