athena engineering inc.

BUILDING INTELLIGENCE SERIES

THE BUILDING AUTOMATION CYBERSECURITY CHECKLIST

A PRACTICAL READINESS CHECK FOR BUILDING OWNERS, FACILITY TEAMS, AND SPECIFYING ENGINEERS

What's included

1 Know what you have

2 Segment the network

3 Control who gets in

4 Secure communications

5 Keep it current

6 Watch and log

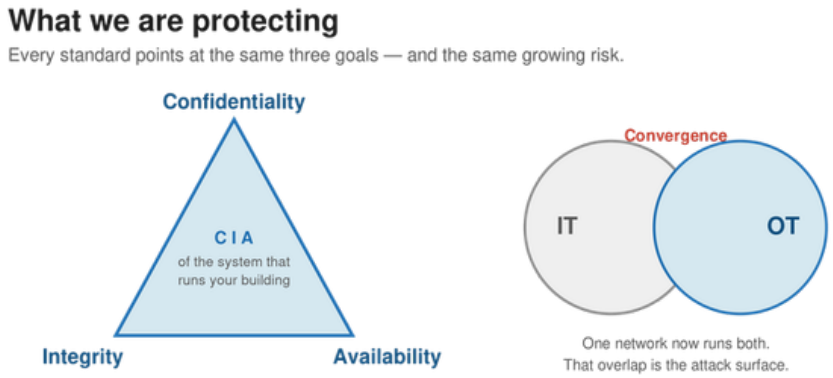
7 Plan for the bad day

8 Lock the doors

9 Build into the spec

Why this matters

Building automation used to live on its own island. That island is gone. The same network that runs your chillers, air handlers, and lighting now touches corporate IT, a handful of vendor laptops, and — more often than anyone would like — the open internet. That convergence is exactly where the risk lives, and it is why building automation systems now show up in the same security guidance as industrial and federal control systems.



This checklist translates the standards that matter — the NIST Guide to Operational Technology Security (SP 800-82 Rev. 3), the ISA/IEC 62443 "zones and conduits" model, and the federal UFC 4-010-06 control-system criteria — into questions you can walk a real building through. Behind all of them sits the same goal: protect the confidentiality, integrity, and availability of the system that keeps your building running.

One theme runs through every one of these standards: security breaks down when it is designed in a silo. The mechanical engineer, the controls integrator, the IT group, and whoever owns cyber-risk all belong in the same conversation, early. We say that plainly because it is where a lot of buildings quietly go wrong — and because self-performing both the mechanical and the controls in-house is how we keep that conversation under one roof.

How to Use it:

Print it, walk your site, and check the boxes. Any box you cannot check is a conversation worth having — with your team, your integrator, or us.

Know what you have

□ Inventory every BAS device — make, model, firmware, and location.

- □ Controllers, automation servers, gateways, switches, and sensors.
- □ Include non-IP field devices: VAV controllers, thermostats, sensors.

□ Keep a current network diagram (BAS to IT, internet, and third parties).

□ Name an owner accountable for BAS security.

□ Document every remote-access path — who, how, and why.

□ Flag end-of-life equipment and put it on a migration roadmap.

Segment the network

□ Isolate BAS traffic on its own VLAN or a physically separate network.

□ Keep controllers and servers off the public internet.

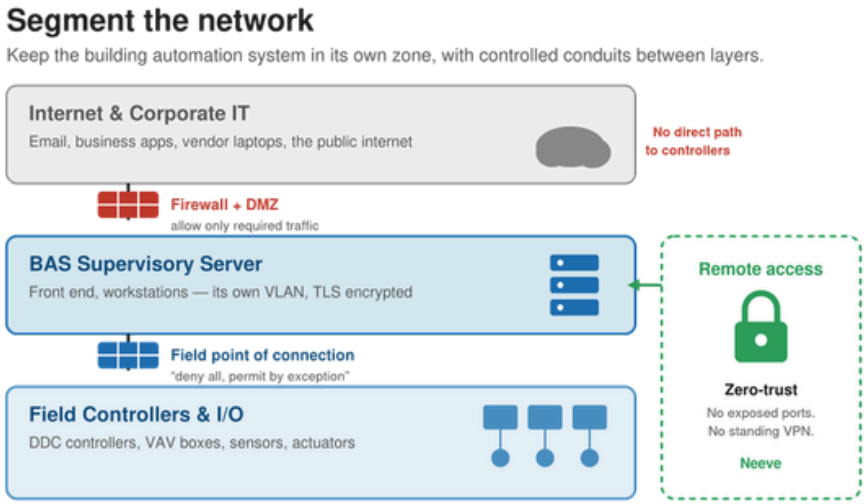
□ Add a DMZ between the BAS front end and outside networks.

□ Set firewall rules that allow only the traffic that must cross.

□ At the field point of connection, apply “deny all, permit by exception.”

□ Use zero-trust, cloud-managed remote access — no exposed ports, no standing VPN. (Neeve, below.)

□ Keep guest, tenant, and vendor networks separate.



Control who gets in

- □ Change every default password.
    - □ Controllers, servers, switches, and web interfaces.
- □ Give each user unique credentials.
- □ Retire shared “engineering” logins.
- □ Set role-based access, down to the point level.
- □ Require MFA on the server and every remote entry point.
- □ Require contractor laptops to run anti-malware, current patches, and a user login.
- □ Disable accounts when staff or contractors leave.
- □ Audit access on a regular schedule.

Secure the communications

- □ Encrypt server-to-workstation traffic (TLS).
    - □ Enable BACnet Secure Connect (BACnet/SC) where devices support it.
- □ Where they don’t, isolate BACnet behind a firewall on a segmented network.
- □ Disable unused protocols, services, and ports.
- □ Encrypt any wireless links and put them on their own segment.

Keep it current

- □ Patch firmware and software on a defined cadence.
- □ Track manufacturer and CISA advisories for your platforms.
- □ Buy from vendors with a secure-development lifecycle (IEC 62443-4-1).
- □ Fund a migration plan for legacy systems before support ends.

Watch and log

□ Turn on logging at the supervisory server.

□ Review the logs on a set cadence.

□ Alert on failed logins, config changes, and dropped devices.

□ Add IDS/IPS and monitoring sized to the system.

□ Baseline normal behavior so abnormal stands out.

Plan for the bad day

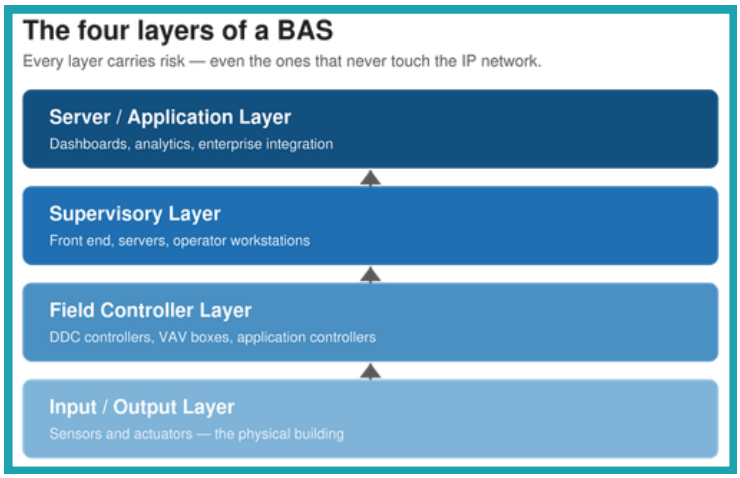
□ Back up controller programs and server configs off the BAS network.

□ Test the restore end to end.

□ Write an incident-response plan with the owner.

□ Name who to call, and in what order, when something looks wrong.

□ Add your integrator's emergency contact to the plan.



Lock the doors

□ Secure panels, server rooms, and closets — and log access.

□ Close unused USB and network ports in shared spaces.

□ Make exposed field devices tamper-resistant.

Build security into the specification

For specifying engineers, the cheapest place to secure a building automation system is on paper, before it is installed.

□ Write the spec collaboratively — owner, IT, MEP, integrator, and cyber.

□ Put cybersecurity requirements in Division 25 (Integrated Automation).

□ Reference IEC 62443, the NIST CSF, or UFC 4-010-06 where they apply.

□ State vendor requirements: secure coding, patching, and proof of compliance.

□ Require a commissioning security handoff.

- □ Clear default credentials, rotate passwords, deliver documentation.

□ Set warranty and service terms that keep the system patched.

A well-built platform does much of this for you

The systems we deploy — Schneider Electric EcoStruxure as our primary line — ship with much of this checklist built in: BACnet Secure Connect, encrypted communications, role-based and point-level access control, forced admin-password changes, imported accounts disabled by default, secure boot, SHA-256 password hashing, and audit logs with synchronized timestamps. Configured correctly, the platform enforces the rules so your team does not have to remember them.

More from Athena Engineering

- Why are BACnet/IP controllers a big deal?
- Cloud-managed BMS, explained
- Expertise: Building Automation

More from our partners

- Neeve — Certified Secure
- Neeve — Trust Center
- Neeve — Product Selector

Standards & guidance

- NIST SP 800-82 Rev. 3 — Guide to Operational Technology (OT) Security
- UFC 4-010-06 — Cybersecurity for Facility-Related Control Systems (federal criteria)
- ASHRAE Journal — Building automation systems: addressing the cybersecurity threat
- IFMA — 6 steps to enhance building cybersecurity
- Schneider Electric — Checklist to help secure your building management systems
- Nozomi Networks — Building automation system cybersecurity
- Veridify — Why building automation systems are the new cybersecurity target

How Athena Engineering helps

We self-perform both the mechanical and the controls work in-house, which means the people who install your building automation system are the same people who secure it. That is unusual in our trade, and it is the whole point: no finger-pointing between the HVAC contractor and the controls house when a network question comes up.

We design and integrate open, standards-based systems on Schneider Electric EcoStruxure (our primary platform, as an EcoXpert-certified partner) and Johnson Controls Facility Explorer, communicating over open protocols — BACnet, LON, and Modbus — so your building is never locked to a single vendor. From building-automation design-assist and Division 25 specifications through installation, integration, and ongoing service, we build security in from the drawing set forward and keep it current afterward.

For remote access, multi-site portfolios, and buildings where IT wants OT off their network entirely, we deploy cloud-managed building automation built on Neeve, our edge-cloud partner. It replaces exposed ports and standing VPNs with zero-trust remote access, and it carries its own security pedigree — ISO/IEC 27001 and SOC 2 Type 2 certification with continuing third-party penetration testing (see the Neeve Trust Center). For the longer version, our Insights on cloud-managed BMS and BACnet/IP controllers walk through how it fits together.

athena engineering inc.®

ATHENA CHIERA
Vice President
amc@athenaengineering.com
Direct: (909) 971-8439
Cell: (949) 395-7972

athenaengineering.com