Collaboration for Secure, Future-Ready Buildings



Hans Symanczik
Founding Member
BACnet Interest Group Europe



Iain Gordon
President KNX UK



Graham Martin
Chairman & CEO EnOcean Alliance

Collaboration for Secure,

Future-Ready Buildings

As building technology becomes more connected, the challenge is no longer simply choosing the right system. It is ensuring that different technologies can work together securely, flexibly and in a way that supports the building throughout its life.

This central theme brings together perspectives from BACnet Interest Group Europe, KNX UK and the EnOcean Alliance.

This report considers three closely connected areas: interoperability and collaboration, cybersecurity and data protection, and the need to create buildings that can adapt to future demands including work/lifestyle changes and emerging technologies.

Who this report is for

Developers, consultants, specifiers, building owners, facilities teams and systems integrators considering how to make new and existing buildings more adaptable.

A handy recap of the seminar's key points to help you continue the conversation and share insights with colleagues who were unable to attend.



See further reading and contact information at the end of this report.

Interoperability:
Designing around the building, not the technology

Modern buildings increasingly incorporate technologies from different manufacturers and disciplines. Lighting, HVAC, energy management, access, sensors and other building services may all need to exchange information, making the ability of systems to work together increasingly important.

Ethical choice, adaptable spaces, occupant wellbeing and benefits for developers and contractors are all key but often competing ideals. Designers, integrators and building owners need greater freedom to select solutions according to the needs of each unique mix of priorities rather than being constrained to a single technology ecosystem.

Buildings change: spaces are repurposed, equipment is replaced, occupants have different requirements and new technologies emerge. Systems need to accommodate change rather than becoming a barrier to it.

This highlights the need for modular interoperable systems that can be adapted over time without the need to scrap whole systems. The immediate need for better energy efficiency and pressure on resources, are exacerbated in many parts of the world by ageing building stock, heritage and protected sites. Adding technology that will be out of date in a few years, really isn't an option any longer.

There are as many solutions as there are disparate and constantly changing needs. These solutions need to be capable of being updated in a way that doesn't require demolition of cherished sites or wasting precious resources.

Systems need to be designed as bespoke, multi-source solutions, allowing individual components to be adapted, upgraded or replaced modularly as requirements and legislation evolve.



Cybersecurity:
control systems must be secure

Greater connectivity inevitably brings greater responsibility for cybersecurity. Building automation systems can directly influence real operations including heating, cooling, ventilation, lighting, access and energy. Unprotected communications may expose both data and control commands, while remote access and maintenance connections have the potential to create additional routes into the building network.

Encryption, authentication and integrity.

Open protocols by definition benefit from broad industry collaboration, with multiple organisations investing in their security, resilience and long-term credibility because they share a commercial interest in protecting the ecosystems built around them.

However, cybersecurity cannot be considered at protocol level alone. Assets and connections need to be identified, remote access controlled, communication between different network zones managed, devices maintained and recovery considered throughout the building's operational life.

UK and EU cybersecurity requirements, including the UK NIS Regulations, GDPR and Data Protection Act, the PSTI product security regime, NIS2 and the EU Cyber Resilience Act. Legislation does not and should not prescribe one particular building protocol; applicability depends on the organisation, product and use case.

Secure systems require long-term management - certificates need to be issued, protected, monitored, renewed and replaced, raising an important practical question: who retains responsibility after project handover.



Requirements for long term responsibility are being addressed by manufacturers, technology developers and legislators, a challenge that will continue to be prominent in current and future property construction, maintenance and repurposing.

Cyber risk in building operations

Connected building systems influence real operations

Heating, cooling, ventilation, lighting, access, energy

Unprotected traffic can expose data and control commands

Readable with network access – and easier to alter without authentication

Remote access and maintenance connections increase exposure

Every external path needs to be controlled

Three different protections

Encryption
keeps traffic private

Authentication
proves who is communicating

Integrity
detects changed messages

Building automation controls real things: heating, cooling, ventilation, lighting, access and energy. So cyber security in buildings is about operations, not just data.

Unprotected BACnet traffic can be read by anyone with network access, and without authentication and integrity checks, messages may be easier to inject or change. A purely hypothetical example: altered temperature values or unauthorised setpoint changes could waste energy or disrupt a process, perhaps unnoticed for a while. Remote access and maintenance connections add further ways in.

Three protections are worth keeping apart. Encryption keeps traffic private. Authentication proves who is communicating. Integrity shows that a message has not been changed.

NOTE: The setpoint scenario is a hypothetical illustration, not a documented incident

SOURCE: NCSC – Operational Technology collection (ncsc.gov.uk/collection/operational-technology).

UK and EU cybersecurity requirements

United Kingdom	
NIS Regulations 2018	Operators of essential services and relevant digital service providers
UK GDPR / Data Protection Act 2018	Wherever personal data is processed
PSTI product security regime	Consumer connectable products – not every commercial BMS component
Cyber Security and Resilience Bill	*Still before Parliament – not yet law*

Legal status: 5 October 2026

European Union – relevant for UK businesses	
NIS2 Directive	In-scope entities under national laws; reaches UK firms through EU activities and supply chains
Cyber Resilience Act	Products with digital elements on the EU market – including those of UK suppliers. Reporting duties apply now; most obligations from Dec 2027

Laws only – standards and guidance (e.g. IEC 62443, NCSC) are not legal obligations. None of these texts prescribes a specific protocol.

Applicability depends on the organisation, product and use case

Regulation adds pressure, but it is not one rule for everyone. In the UK, the NIS Regulations 2018 apply to operators of essential services and certain digital service providers.

UK GDPR and the Data Protection Act apply whenever personal data is processed, and occupancy or access data can be personal data. The PSTI regime covers consumer connectable products, not every commercial building controller.

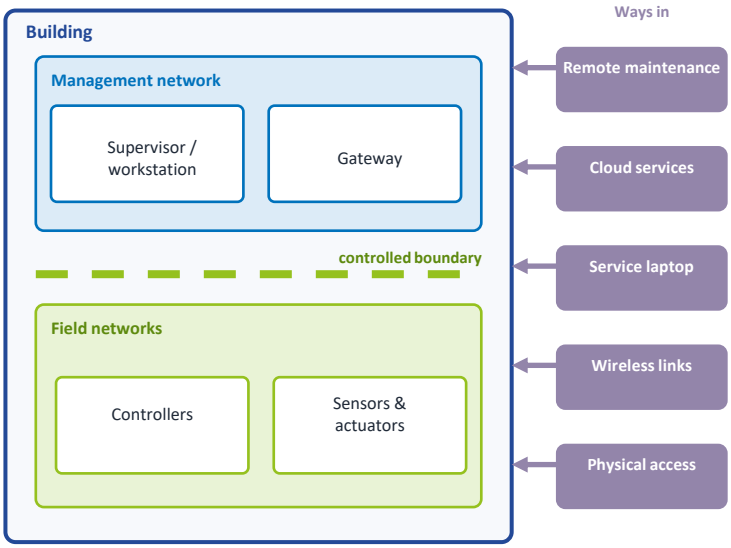
Looking at the EU, NIS2 applies to in-scope entities through national law and often reaches UK suppliers through contracts. The Cyber Resilience Act covers products with digital elements sold in the EU. Its reporting duties have applied since 11 September, and most other obligations follow in December 2027.

The UK Cyber Security and Resilience Bill is still before Parliament. So applicability depends on the organisation, the product and the use case, and none of these texts mandates a particular protocol.

ASHRAE BACnet INTEREST GROUP EUROPE · KNX NATIONAL · enocean alliance

Security across the whole building

- Identify assets, connections and responsibilities
- Control remote access and communication between zones
- Maintain devices, monitor changes and prepare recovery



The protocol is one part of the security concept.

Whatever the regulation says, the protocol is only one part of the answer.

Start by knowing what you have: devices, connections and who is responsible for them. Then look at the ways in: remote maintenance, cloud links, operator workstations, service laptops, gateways, wireless and physical access.

A locked plant room helps, but it does not secure a maintenance connection or a compromised laptop. And secure communication cannot protect you from a device that is authorised but already compromised.

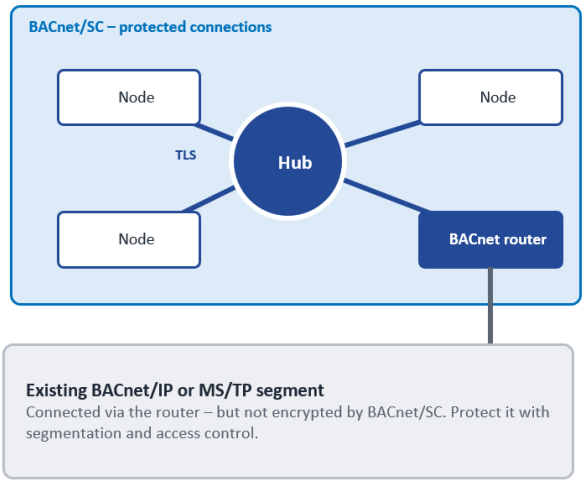
Updates, access rights, monitoring and recovery belong in the operating concept.

ASHRAE BACnet INTEREST GROUP EUROPE
KNX NATIONAL U.K.
enocean alliance

BACnet Secure Connect

- Encrypted communication using established TLS technology
- Certificate-based authentication of communication peers
- Protection against undetected changes in transit
- Integration with existing BACnet networks through suitable routers

Runs on site – no cloud service required.



Where BACnet communication itself needs protection, BACnet Secure Connect, or BACnet/SC, is the answer from within the BACnet standard.

It uses established IT technology: TLS-encrypted WebSocket connections and X.509 certificates, so both ends of a connection can prove who they are, and changes in transit are detected. BACnet/SC can run entirely on site; it does not need a cloud service. Suitable BACnet routers connect it to existing BACnet/IP or MS/TP networks, so you can introduce it step by step.

Two limits are important. The protection applies to the BACnet/SC connections. A classic segment behind a router is not encrypted just because it is connected. And BACnet/SC does not replace device hardening, user permissions or the other measures I have just mentioned.

BACnet/SC was introduced by Addendum 135-2016bj and is part of current editions of ANSI/ASHRAE Standard 135. It uses a hub-and-spoke topology (primary and failover hub) with optional direct connections.

SOURCES: bacnetinternational.org/bacnetsc · BACnet/SC white paper (2019 – background only, not for current implementation details).

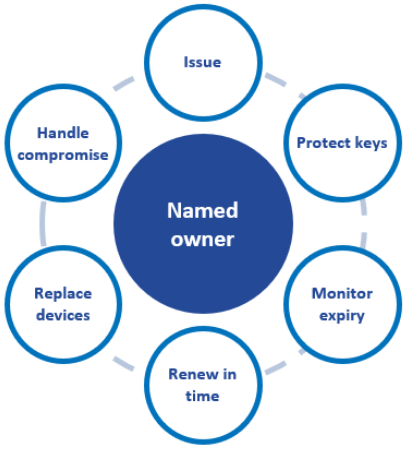
ASHRAE BACnet INTEREST GROUP EUROPE
KNX NATIONAL
enocean alliance

Certificate management brings IT and OT together

- Familiar security methods, new operational responsibilities
- Certificates need managed issuance, renewal and replacement
- Ownership must continue throughout the building's life

IT brings
identities, trust structures, certificate management

OT brings
availability, long lifetimes, maintenance windows



Who renews the certificates after the installer has left?

For me, the key topic is certificates. In IT, certificates and public key infrastructure, PKI, have been familiar for many years. For many building automation teams, they are a newer operational task.

IT brings experience with identities and trust; OT brings knowledge of availability, long lifetimes and maintenance windows. The challenge is to organise this together.

Certificates must be issued, private keys protected, expiry dates monitored, certificates renewed in time, devices replaced and compromised credentials handled. A well-managed local PKI can be a good fit; not every project needs a large enterprise PKI. But even a small solution needs named owners and documented procedures.

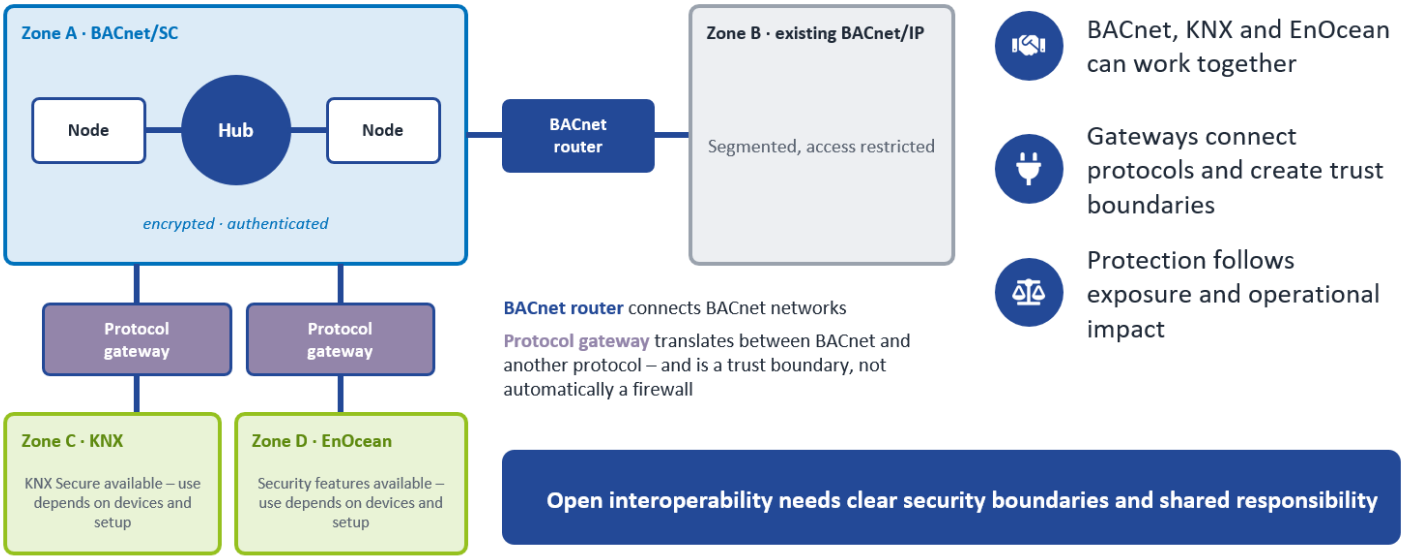
Default certificates from the manufacturer are not a basis for years of unattended operation.

So the question I would put to every project is: who renews the certificates after the installer has left?

SOURCES: BACnet/SC white paper (certificate concept); NCSC OT guidance (ownership and lifecycle).

ASHRAE BACnet INTEREST GROUP EUROPE
KNX NATIONAL U.K.
enocean alliance

Interoperability across security zones



Finally, interoperability, which is why the three of us are on this stage. BACnet, KNX and EnOcean already work together in many buildings.

A BACnet router connects BACnet networks; a protocol gateway translates between BACnet and another protocol.

KNX and EnOcean have their own security mechanisms, but whether they are used depends on devices, gateways and configuration. Secure links on both sides of a gateway are not end-to-end encryption, and a gateway is not a firewall just because of its name.

So protection should follow exposure and impact. Does the last few metres to a light switch need encryption?

That is a risk decision: who can reach it, what happens if it is manipulated, how far the radio reaches. Open interoperability needs clear security boundaries and shared responsibility.

SOURCES: bacnet.org/faq (router vs gateway) · KNX Secure: support.knx.org · EnOcean Alliance: Security of EnOcean Radio Networks (v3.02).

ASHRAE BACnet INTEREST GROUP EUROPE
KNX NATIONAL
enocean alliance

Future-ready means adaptable, not simply "smart"

Future-ready buildings must respond to sustainability and resource-management pressures, changes in use, an ageing population, ageing building stock, evolving cybersecurity requirements and emerging technologies.

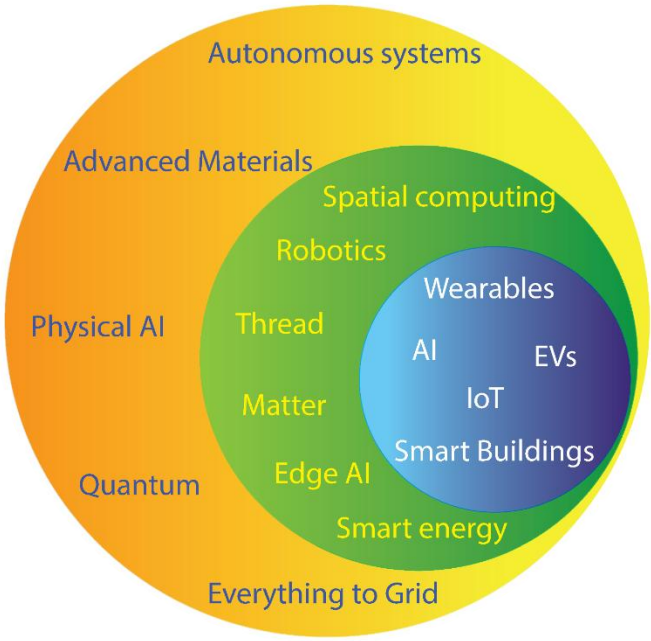
They also need to work across both retrofit and new-build environments. That makes compatibility and adaptability increasingly important.

A building designed around open, interoperable technologies has greater potential to evolve as requirements change.

Components can be upgraded, additional technologies incorporated and spaces adapted without necessarily requiring wholesale replacement of the underlying building-control infrastructure.

This is particularly relevant as smart buildings begin to interact with a much wider technology landscape, from IoT and smart energy to AI and emerging connected systems.

The objective is not to predict exactly which technologies will dominate in the future, but to ensure today's buildings are capable of accommodating tomorrow's requirements.

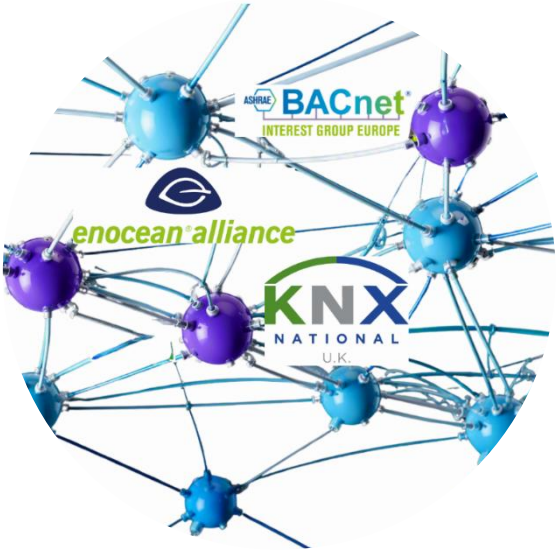


Collaboration and adaptation are the common threads

Perhaps the strongest message is that interoperability, cybersecurity and resilience cannot be considered in isolation.

It is hoped that the collaborative approach between BACnet, KNX and EnOcean in this instance, demonstrates that these three protocols cannot only operate alongside one another, but stand together ethically and commercially to promote a single shared goal.

The aim is therefore not to promote one protocol over another. It is to create buildings in which appropriate technologies can work together, with clearly defined responsibilities, sensible security boundaries and an understanding of how any building can be optimally managed throughout its life.



"Future-ready buildings will not be defined simply by how much technology they contain – but by how successfully that technology can collaborate, adapt and remain secure over time." Iain Gordon

Collaborating for Secure Future-Ready Buildings

BACnet INTEREST GROUP EUROPE

KNX NATIONAL U.K.

enocean alliance

www.big-eu.org
www.knxuk.org
www.enocean-alliance.org

References & Further Reading:

NIS Regulations 2018: operators of essential services (e.g. energy, transport, health, drinking water, digital infrastructure) and relevant digital service providers.

UK GDPR / DPA 2018: security of processing applies to personal data, e.g. access control logs, occupancy or presence data linked to people.

PSTI: in force since 29 April 2024 for relevant consumer connectable products (default passwords, vulnerability reporting, support period)

NIS2: EU directive, applied through national transposition laws; not UK law, but relevant for EU activities and supply-chain contracts

CRA (Regulation (EU) 2024/2847): Article 14 reporting of actively exploited vulnerabilities and severe incidents applies since 11 September 2026 via ENISA's Single Reporting Platform; most other obligations from 11 December 2027.

UK Cyber Security and Resilience (Network and Information Systems) Bill: status 5 October 2026 = House of Lords, report stage next; NOT yet law. Re-check before the event.

Standards and guidance (e.g. IEC 62443, NCSC guidance) are not laws.

gov.uk NIS collection · ico.org.uk guide to data security · gov.uk PSTI regime · bills.parliament.uk/bills/4035 · digital-strategy.ec.europa.eu (NIS2, CRA).

NCSC OT guidance, secure connectivity Principle 6 "Limit the impact of compromise" (segmentation and controlled boundaries).