KNX SECURITY IN BUILDINGS

KNX System Hardening Guide

Contents

1. Purpose of the Document

This document aims to provide essential insights into the cybersecurity measures necessary for safeguarding KNX building automation systems. It highlights typical cyberattacks that can threaten building automation and offers practical strategies for protecting KNX installations through secure device installation and network management. Additionally, the document addresses important considerations for project handover to ensure ongoing security and resilience in building operations.

2. KNX Secure: Built-In Protection for Smart Homes and Buildings

The KNX Secure technology complies with all relevant security regulations, ensuring robust protection for modern, networked infrastructures. KNX Secure is standardized according to EN 50090-3-4, confirming its effectiveness in defending against cyberattacks targeting the digital infrastructure of smart buildings. This significantly reduces the risk of unauthorized access or digital break-ins. KNX Secure adheres to the highest encryption standards, including ISO 18033-3, and uses AES 128 CCM encryption to safeguard data. This ensures that communication within the KNX system remains confidential and tamper-proof.

Cybersecurity is a shared responsibility. While products play a crucial role, especially in networked smart home and building control systems, other factors, such as proper installation, configuration, and system segmentation, are equally important.

ABB is committed to supporting system integrators and installers in securing their systems. However, the ultimate responsibility for system security lies with the installers, system integrators, planners, technical consultants, and IT specialists involved in the project.

3. Attack Methods on KNX Systems

Attack via the Internet
Potential attackers can gain access to an installation via the internet. These attacks can be carried out largely anonymously, as the attacker does not need to be on-site. Often, attackers have already bypassed IT security barriers to gain access to KNX devices or the system.

Attack with Partial Access to the KNX System or Components
Examples include unprotected bus cables outside the building or a secretly installed Raspberry Pi. These scenarios often cause significant concern and are useful for demonstration purposes. However, they are relatively unrealistic, as the attacker must be physically present.

Systematic and On-Site Attacks in KNX Installations
Systematic or on-site attacks involve the deliberate exploitation of vulnerabilities in devices or communication protocols. These scenarios typically require in-depth knowledge of the KNX system and a comprehensive understanding of the specific installation. As such, they are generally relevant only in large-scale or security-critical environments and often depend on insider knowledge.

4. Approaches to Securing KNX Installations

A fundamental principle of any robust security concept is the strict isolation of the system from unauthorized access. In the context of KNX systems, physical access should be restricted exclusively to authorized individuals such as installers, caretakers, or designated users. This isolation can be achieved through a combination of native KNX technologies, such as KNX Secure, and IT security strategies, including the segmentation of systems into distinct security zones.

During the planning and installation phases, all critical points associated with each KNX medium must be thoroughly secured. The following principles should be observed for any KNX-based building control system:

- Utilize KNX Secure communication wherever feasible to ensure encrypted and authenticated data exchange.
- Implement additional security measures beyond KNX Secure to enhance protection. These measures apply to both KNX Secure and KNX Plain installations.
- Do not treat these measures as substitutes for KNX Secure. Instead, they should complement it to form a layered security approach.
- In KNX Plain or mixed environments, these additional security practices are especially critical, as they play a vital role in physically isolating the system and mitigating potential vulnerabilities.

a) Device Installation

Building control products must be securely installed to prevent easy removal, which could grant unauthorized access to the KNX bus. If theft or dismantling protection is available, it should be utilized.

Enclosures and distribution boxes containing KNX devices must be locked appropriately or installed in rooms accessible only to authorized personnel.

In public areas that are not sufficiently monitored, it is recommended to use conventional installation products in combination with binary inputs or push-button interfaces. This can make access to the building control system more difficult.

The following points should be evaluated: Were the following measures considered during installation?

- **Device Mounting:** Are the devices securely mounted? Has appropriate anti-theft protection been implemented to prevent unauthorized removal? Devices should be mounted in secure panels or protected against theft.
- **Access Control:** Is access to distribution boards containing KNX installations restricted to authorized personnel only (e.g., by ensuring they are always locked or located in secured rooms)?
- **External Accessibility:** Are devices installed in external areas positioned in a way that makes unauthorized access difficult (e.g., mounted at a sufficient height)?
- **Public Area Operation:** If the KNX installation can be operated from publicly accessible and unsupervised areas within a building, has the use of binary inputs (installed within distribution boards) or push-button interfaces been considered?
- **Touch Panel Security:** Are KNX touch panels protected by passwords (e.g., user, group, or guest mode)?

b) Twisted Pair (TP) Communication

The following points should be evaluated:

- **Is the cabling - whether inside or outside the building - sufficiently protected against unauthorized access or tampering?**

  KNX cabling should not be accessible in public areas or from the exterior of the building. Suppose sensors are required in such locations (e.g., weather sensors or push buttons). In that case, it is advisable to use non-KNX devices and connect them to KNX input modules located in secure, restricted-access areas. This approach eliminates the need to route the KNX bus cable through unsecured zones, thereby enhancing system security.

- **If twisted pair cabling is used in areas requiring enhanced protection, have the necessary security measures been implemented?**

  These measures may include designing the network topology to provide dedicated KNX lines or KNX line segments for such areas and applying appropriate filter settings to protect and isolate them. While KNX repeaters offer some level of protection by galvanically isolating line segments, they do not support filtering of KNX bus traffic. Therefore, for better control and security, the topology should be designed using KNX segment couplers or line couplers instead (e.g., ABBs LK/S4.3 Line Coupler Secure).

c) KNX Network Segmentation

Enhanced security can be achieved by enabling filter tables and configuring the appropriate filter settings. KNX line couplers and KNX IP routers support the forwarding, filtering, or blocking of the following types of telegrams:

- Broadcast telegrams (e.g., line scans)
- Individually addressed telegrams (used for KNX device configuration and parameterization)
- Group-addressed telegrams

In standard KNX runtime communication, only group-addressed telegrams are used. By blocking or filtering all other types of telegrams, the overall security of the KNX installation is significantly increased.

Generally, unfiltered communication should be reserved for temporary testing and debugging purposes. In installations that include a visualization system, where most group-addressed telegrams are routed through a central interface, enabling filtering is strongly recommended. This not only enhances system performance but also improves message control and reliability.

d) KNXnet/IP and IT Networks

IP-based building control devices are often deployed on dedicated networks. Historically, these networks were typically unmanaged, designed solely to provide basic IP connectivity for device communication, with little to no consideration for security.

Securing IP-based building control devices (like HVAC, lighting, access control, and surveillance systems) is critical in modern smart buildings.

1. OT Network

An Operational Technology (OT) is a specialized infrastructure designed to host IP devices that control various non-IT operations and functions. These systems encompass building control systems including HVAC (Heating, Ventilation, and Air Conditioning), Lighting, Elevators, Fire alarms and sprinklers, access control and surveillance, and energy management systems. The establishment of an OT Network typically necessitates the collaboration between two trades: the building control trade and the IT trade. Early planning and communication are essential for this endeavour.

What makes OT Networks different from IT Networks?

Feature	OT Network	IT Network
Purpose	Control and automation of physical systems	Data processing and communication

Feature	OT Network	IT Network
Devices	Sensors, controllers, actuators, PLCs	PCs, servers, printers
Protocols	BACnet, Modbus, KNX, …	TCP/IP, HTTP, SMTP
Priorities	Availability, safety, real-time control	Confidentiality, integrity
Update Frequency	Infrequent updates due to uptime needs	Regular patches and updates

Network Segregation / OT Network
IT security can be effectively applied to building control systems by integrating traditional cybersecurity principles. A first step is to introduce Network segmentation and place buildings controls devices on a dedicated OT Network. The OT Network can be a dedicated physical network; however, in many cases, especially in bigger installations, it will be a VLAN (Virtual Local Area Network).

VLAN (Virtual Local Area Network)
A VLAN offers several essential security benefits in a network environment. A VLAN allows you to group devices based on function, department, or application, rather than physical location. Even if devices are plugged into the same switch, they can be isolated from each other using VLANs. Typically, all devices connected to a switch can communicate with one another. With VLANs, the switch is configured to assign ports to different Virtual Local Area Networks (VLANs). Devices in VLAN 10 can't talk to devices in VLAN 20 unless a router or Layer 3 switch is used to connect them.

Key Benefits:

- Isolation of Non-IT Infrastructure: Building systems (like HVAC, elevators, lighting, and access control) are often less secure and more vulnerable to cyberattacks.
- Reduced Risk of Lateral Movement: Cyber attackers often move laterally within a network after gaining initial access. Network separation prevents lateral movement from office systems (e.g., email, file servers) to operational systems that control physical infrastructure.
- Protection of Life-Safety Systems: Systems such as fire alarms, emergency lighting, and access control are mission-critical. Isolating them ensures that a breach in the IT network doesn't affect systems that could endanger human safety.
- Tailored Security Policies: Building control systems often use specialized protocols (e.g., BACnet, Modbus) that are not used in IT environments. A separate network enables custom firewalls, intrusion detection, and access controls tailored to these protocols.
- Improved Monitoring and Incident Response: With a dedicated network, it's easier to monitor traffic, detect anomalies, and respond to incidents without interference from unrelated IT traffic.
- Safe Maintenance and Testing: Updates or changes to building systems can be tested in isolation, reducing the risk of disrupting business operations or exposing sensitive data.
- Regulatory Compliance: Many standards (e.g., IEC 62443, NIST, ISO/IEC 27001) recommend or require network segmentation for critical infrastructure. A separate network helps meet these requirements more easily.

2. IT Security to Protect Building Controls

Once building control devices are on a segregated IT network, targeted IT security practices can enhance the protection of building controls:

Firewalls and Access Control Lists

- Purpose: Control which devices or users can communicate with building systems.
- Benefit: Prevents unauthorized access and lateral movement.
- Example: Only allow specific management stations to access the Building Management System (BMS).

Network Access Control

- Purpose: Authenticate and authorize devices before they connect to the network.
- Benefit: Blocks rogue or unauthorized devices.
- Example: Use MAC address filtering or 802.1X authentication

Monitoring and Logging

- Purpose: Track network activity and detect anomalies.
- Benefit: Early detection of intrusions or misconfigurations.

Vulnerability Management

- Conduct regular vulnerability scans of building control networks and devices to identify potential security risks.
- Prioritize and remediate identified risks according to their severity.

Secure Protocols and Encryption

- Replace non-crypted IP protocols with secure alternatives (e.g., KNX Secure instead of KNXnet/IP and BACnet/SC instead of BACnet/IP).

Security Awareness and Training

- Train facility managers and building engineers on **cyber hygiene** and **incident response**.
- Encourage collaboration between IT and OT teams.
- Many IP-based building control protocols don't natively support network authentication, data encryption, or provide access control. Here, the best method to secure the system is to control and restrict access to the IP network as much as possible, using native IT methods.

MAC Address Filtering

- MAC address filtering is a network security feature used in devices such as routers, switches, and access points to control which devices are permitted to connect to the network. Each network-enabled device (e.g., computer, smartphone, or printer) has a unique identifier known as a MAC address (Media Access Control address), typically formatted as a 12-digit hexadecimal number (e.g., 00:1A:2B:3C:4D:5E).
- Network administrators can configure MAC address filtering in two ways:
    - **Whitelist (Allow List):** Only devices with MAC addresses on this list are allowed to connect.
    - **Blacklist (Deny List):** Devices with MAC addresses on this list are explicitly blocked from connecting.
- Benefits:
    - Provides an additional layer of access control.
    - Particularly effective in small or static networks where devices are known and rarely change.
- Limitations:
    - **Not foolproof:** MAC addresses can be spoofed by attackers.
    - **Manual upkeep:** Adding or removing devices requires manual updates.

- **Limited scalability:** Becomes impractical in large or frequently changing environments.

- In the context of building automation systems such as KNXnet/IP, which, like many building control IP standards, does not support native IT-level authentication, cybersecurity must be reinforced through layered defenses. While MAC address filtering alone cannot guarantee security, it contributes to a defense-in-depth strategy by increasing the effort required for unauthorized access.

What is IGMP?

IGMP (Internet Group Management Protocol) is a network protocol used to manage multicast groups within an IP network. It allows hosts to join and leave multicast groups, enabling efficient delivery of data to multiple recipients simultaneously. IGMP is part of the IP protocol suite and operates at the network layer. It allows devices (such as computers, IP cameras, or smart TVs) to inform a router that they wish to receive specific multicast traffic, such as a live video stream or a KNXnet/IP signal.

Multicast is a method of sending one stream of data to multiple recipients at once, without sending separate copies to each device. It's more efficient than unicast (one-to-one) or broadcast (one-to-all). KNXnet/IP Routing utilizes multicast communication on the IANA-registered multicast IPv4 address 224.0.23.12 (default).

3. MAC Address Filtering and IGMP

Both IGMP Snooping and MAC Address Filtering can be used to filter and control Multicast IP communication. The primary scope of both technologies differs. While the main aim of the IGMP protocol is to ensure effective multicast communication, the focus of MAC Address Filtering is on network access control. Both technologies require close cooperation with IT departments managing the VLAN. The implementation is strongly dependent on the network design and the type of network equipment used.

Feature	MAC Address Filtering	IGMP
Primary Purpose	Access control	Multicast group management
Security Role	Yes	No (unless combined with IGMP snooping)
Ease of Use	Simple	More complex
Use Case	Small networks, Wi-Fi	IPTV, streaming, multicast
Traffic Control	No	Yes (for multicast)

5. Secure Remote Access

Secure remote access enables remote monitoring, management, and maintenance of building control systems, thereby reducing maintenance costs. To ensure secure connectivity, the following best practices should be implemented:

- Use of Encrypted Communication Channels: Utilize secure protocols such as KNX Secure (KNX IP Secure) and VPN tunnels to protect data in transit.
- Authentication and Access Control: Implement strong authentication mechanisms and role-based access to restrict system access to authorized personnel only.

- Firewall and Network Segmentation: Isolate the KNX network from external networks using firewalls and segment it to limit the spread of potential threats.
- Regular Updates and Patching: Keep all devices, routers, and software up to date with the latest security patches to ensure optimal security.
- Monitoring and Logging: Continuously monitor remote access sessions and maintain logs for auditing and incident response.

For remote access purposes, KNX IP Secure devices, such as the KNX IP router (IPR/S3.5.1) and the IP interface (IPS/S3.5.1), are recommended. When utilized in conjunction with a VPN gateway, these devices facilitate secure and efficient system management from any location.

6. Project Handover

The European Union's Cyber Resilience Act (CRA) mandates cybersecurity requirements for all products with digital elements, including KNX products. A fundamental principle of the CRA is that customers should assume the default security of a product; any limitations to this security must be clearly communicated to the customer.

When handing over a KNX project, it is essential to:

- Transfer all security-relevant data, along with the general project data.
- Provide the customer with a clear explanation of the system's security features, including any known or unavoidable risks.
- Document this information and include it in the technical handover package to avoid future liability.

a) ETS Reports

The ETS generates two key reports that contain essential security information:

- Project Security Report
- Project Certificates Report

These reports should be prepared and reviewed with the customer, and they should be included in the project handover documentation.

b) Customer Awareness and Access to Project Data

Customers—especially those without ETS access—must be informed about:

- The central role of the ETS project in maintaining KNX Secure systems.
- The need for ongoing collaboration with the system integrator to maintain the project's security and ensure it remains up to date.

c) Password Management

The ETS project is protected by a password, which is required for planning and maintenance. If the customer has an ETS license, they may assign a new local password, but:

- This change only affects their local copy.
- It does not affect ToolKeys, MAC Keys, or group keys.

- If the system integrator retains a copy of the project, they can still access and modify the system.

It is recommended to:

- Agree on a clear policy for managing ETS project copies and passwords.
- Maintain a list of individuals who have access to the ETS project.

d) Device Certificates

For reusing KNX Secure devices after a master reset or in a new project, the device certificate is required. The method of certificate dsitribution and retrieval varies by manufacturer and product. It is crucial to establish a process for recording, managing, and transferring these certificates between the system integrator and the customer.