



**Intesis**<sup>®</sup>  
BY HMS NETWORKS

# KNX Secure: Enhancing Building Automation Security

---



## Contents

Introduction	03
The KNX Standard	04
The Need for Security an HVAC System Approach	05
KNX Secure Against the Main Security Threats	08
KNX Secure: Present Status and Future Prospects	10
KNX Secure Now	11
The Importance of Tendering Processes	12
KNX Secure in the Immediate Future: a Prognosis	13
Intesis Bet for KNX Secure	14
Summary	15
References	16

---

Cover: AI-generated image using Microsoft Copilot



## Introduction



The rapid proliferation of smart devices and the Internet of Things (IoT) has transformed the landscape of building automation. On the one hand, building management systems (BMS) play a crucial role in managing lighting, HVAC, security, and energy efficiency. On the other hand, the increasing interconnectivity of devices exposes them to cyber threats. In summary, as buildings become smarter, ensuring robust security becomes paramount.

KNX Secure, an extension of the KNX standard, emerges as a solution to protect against unauthorized access, data breaches, and tampering. Nonetheless, the impact of this new KNX version is moderate (at least at the time this paper was published in April 2024).

This paper explores the principles, features, and benefits of KNX Secure, the possible reasons behind the current lack of impact, and a prognostication of its future spreading.

## The KNX Standard

Since the foundation of the KNX Association<sup>1</sup> in May 1999, the KNX standard has become a fundamental framework for building automation and control systems. It provides a uniform, manufacturer-independent communication protocol that intelligently networks various home and building system technologies.

Here are the key aspects of KNX:

- **Open standard:** KNX is not tied to any specific hardware platform or proprietary technology, ensuring interoperability and seamless integration of diverse devices, regardless of the manufacturer.
- **Scalability:** KNX is a decentralized system, so devices can talk directly to each other without needing a central controller or server. This allows KNX systems to easily expand to accommodate future growth or changing needs.
- **Scope of KNX devices:** KNX devices cover a wide range of functionalities, such as lighting control, blinds and shutters, HVAC (Heating, Ventilation, and Air Conditioning), security systems, energy management, audio and video, white goods, and displays.
- **Scope of physical communication media:** KNX installations can use several physical communication media:
  - **Twisted Pair Wiring (TP1 Cable):** The most common medium for KNX communication.
  - **Power-Line Networking:** Devices communicate over existing electrical wiring.
  - **Radio (KNX-RF):** Wireless communication.
  - **IP (EIBnet/IP or KNXnet/IP):** Internet Protocol-based communication.
- **Global recognition and administration:** KNX is an approved standard recognized by international bodies:
  - **ISO/IEC 14543-3:** International standard.
  - **CENELEC EN 50090 and CEN EN 13321-1:** European standards.
  - **ANSI/ASHRAE 135:** U.S. standard.
  - **China Guobiao (GB/T 20965):** Chinese standard.

<sup>1</sup>The KNX Association is a non-profit organization governed by Belgian law that administers KNX.

## The Need for Security: an HVAC System Approach

As buildings become smarter and more interconnected, the security of automation systems becomes a critical concern. As exposed in an article by Mary Kate McGowan published on ASHRAE:

“Building automation systems are part of the infrastructure of buildings, and malicious users that get access to the building automation system’s communication may interfere with the system and produce unwanted behavior or damage to HVAC and other equipment.”

One could think that heating, ventilating, and air conditioning systems (HVAC) are not so extremely relevant. An attack on an HVAC system may cause a failure of that system and could make you uncomfortable, as much. That’s what happened in this case, explained in the previously cited article:





# KNX Secure: Enhancing Building Automation Security



“An attack on a building automation system in two apartment buildings in Finland left residents in the cold during the winter of 2016. A distributed denial-of-service (DDoS) attack hit the Domain Name System service and disabled remote connection access, forcing building management to inspect the homes on-site. The automation system that controlled the homes’ heating, hot water, and ventilation systems continuously rebooted until it stopped working entirely.”

However, HVAC systems play a critical role in other cases, such as keeping the temperature and humidity in data centers. Data centers house large computer

systems that support business storage solutions, operational systems, website hosting, data processing, and more. Basically, data centers allow our modern way of life, where the Internet and all the information circulating from here to there are at the core.

Those computer systems work 24/7, consuming tons of energy and generating a significant amount of heat. Maintaining the optimal temperature and humidity levels within a data center is essential for ensuring the efficient operation and longevity of the equipment; that’s why the data center’s HVAC system goes well beyond mere climate control.

# KNX Secure: Enhancing Building Automation Security

According to an article published in Bleeping Computers:

“Investigators at Cyble have found over 20,000 instances of publicly exposed DCIM<sup>2</sup> systems, including thermal and cooling management dashboards, humidity controllers, UPS controllers, rack monitors, and transfer switches. [...] Exposing these systems without adequate protection means that anyone could change the temperature and humidity thresholds, configure

voltage parameters to dangerous levels, deactivate cooling units, turn consoles off, put UPS devices to sleep, create false alarms, or change backup time intervals.”

The economic impact of a cyber attack on one of these data center’s HVAC systems could be devastating. A 2016 research report by the Ponemon Institute stated that the average cost of a data center outage is nearly \$9,000 per minute.



<sup>2</sup>DCIM goes for Data Center Infrastructure Management. DCIM tools and software are used to visualize, manage, and control the core information technology components within the data center, like routers, switches, and servers, as well as the facility infrastructure components, such as HVAC systems.

See <https://cyble.com/blog/data-centers-facing-risk-of-cyberattacks/>

## KNX Secure Against the Main Security Threats

KNX Secure has been designed with the security challenges faced by BMS systems in mind:

■ **Unauthorized Access Prevention:** In a connected building, various devices communicate over the KNX network. Unauthorized access to these devices can lead to severe consequences.

- KNX Secure uses strong authentication mechanisms, ensuring that only authenticated devices can participate in the network and verifying each device's identity.

■ **Data Confidentiality and Integrity:** BMS systems exchange sensitive data, including control commands, sensor readings, and user preferences. Ensuring the confidentiality and integrity of this data is crucial.

- KNX Secure employs encryption techniques to protect data in transit. It ensures that eavesdroppers cannot intercept or tamper with the information exchanged between devices.

■ **Tampering Prevention:** Unauthorized tampering with devices can compromise safety, comfort, and energy efficiency.

- KNX Secure verifies the integrity of messages exchanged between devices. If any data alteration occurs during transmission, the receiving device detects it and takes appropriate action. For example, if an attacker tries to manipulate a temperature setpoint, KNX Secure ensures that the change is either rejected or flagged for investigation.







■ **Protection Against Replay Attacks:** Replay attacks involve capturing legitimate messages and replaying them later to gain unauthorized access.

- KNX Secure uses timestamps and sequence numbers to prevent replay attacks, ensuring that messages are fresh and not reused and maintaining the integrity of communication channels.

■ **Secure Device Configuration:** Unauthorized configuration changes can disrupt BMS functionality or compromise security.

- KNX Secure devices are configured securely during installation. This prevents unauthorized modifications to device settings.

■ **Group Address Protection:** Group addresses are fundamental to KNX communication. They allow devices to exchange information within specific groups (e.g., lighting control, HVAC).

- KNX Secure restricts access to group addresses. Only authorized devices can send or receive data for specific groups.

## KNX Secure: Present Status and Future Prospects

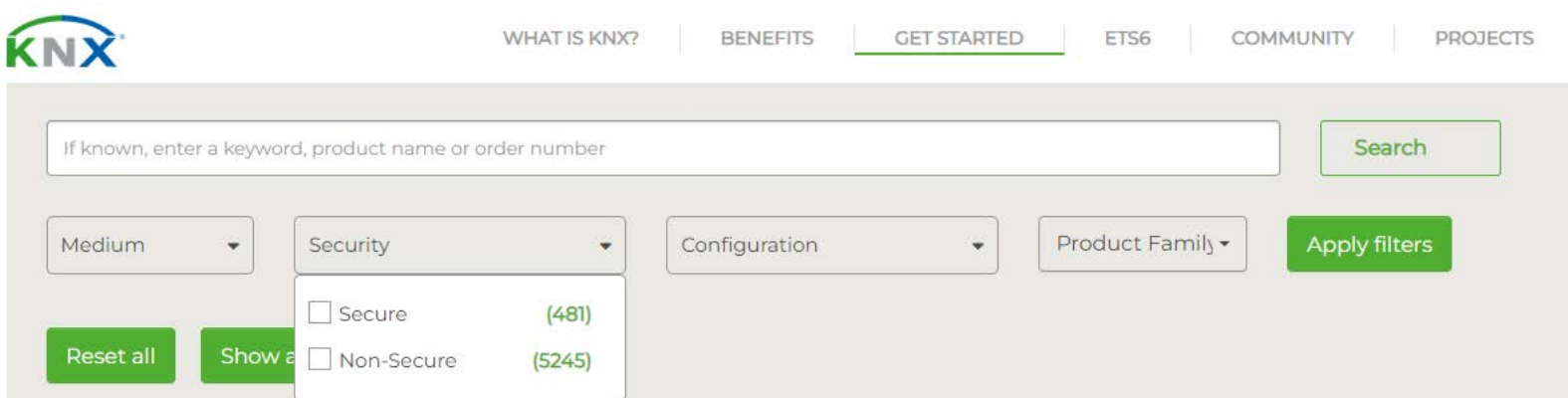


Figure 1: AI-generated image (Microsoft Copilot)

According to the information exposed until now, it looks like KNX Secure should already be widely used in installations and adopted by makers, but that's not the case, actually. In this section, we'll explore possible reasons for that and try to predict its future.

## KNX Secure Now

Searching on the KNX website, we get these numbers:



The screenshot shows the KNX website's search interface. At the top, there is a navigation bar with links: WHAT IS KNX?, BENEFITS, GET STARTED (highlighted), ETS6, COMMUNITY, and PROJECTS. Below the navigation bar is a search bar with the placeholder text "If known, enter a keyword, product name or order number" and a green "Search" button. Below the search bar are four filter dropdowns: "Medium" (set to Medium), "Security" (expanded), "Configuration", and "Product Family". The "Security" dropdown is open, showing two options: "Secure (481)" and "Non-Secure (5245)". There are also "Reset all" and "Show all" buttons. A green "Apply filters" button is located to the right of the filter dropdowns.

Figure 2: Secure and non-secure KNX products listed on the KNX website.

The number of certified products supporting KNX Secure is 481, while the number for the plain version is 5245. This means there are 5726 KNX-certified products, of which only 8.4% are KNX Secure products.

Some reasons could explain the low impact KNX Secure is having today:

- **It's young:** It takes some time for new technologies to be adopted, and even if KNX Secure became a reality in 2019 when the KNX Association decided it was stable enough, it was not until 2022 that it received the certification from the Association for Electrical, Electronic & Information Technologies (VDE), making this version more official and “objectively” approved.
- **KNX was not super secure, but it was already secure:** The plain version of KNX already implements a series of security measures, like password use.
- **Cost and price:** KNX Secure products require more memory and computing power. This increase in technical capacities usually implies an increase in the cost of manufacturing and the price of the product.
- **No presence in tendering processes:** For now, tender managers are not asking for KNX Secure products in their tendering processes. This may be the most crucial point and a keystone for the future spreading of KNS Secure.



## The Importance of Tendering Processes

A tendering process, also known as bidding process, request for quotation, invitation to bid, or invitation to tender, is a formal procedure that companies use to order products or services for their projects, inviting vendors to provide their best prices and payment terms. The company provides bidders with a document including all the requirements, such as:

- Definition of the products or services required with detailed specifications
- Delivery requirements.
- Quantities
- Payment terms
- The proposed method of evaluation
- Decision timeline and review process
- Contract terms and conditions
- Submission requirements

Tendering processes are often used for big projects involving high-volume orders. An example could be a contractor who will build a hotel, an office building, or a residential complex, even though they are not limited to such big projects.

Right now, projects needing KNX products don't specify in their tendering processes that these products must be KNX Secure, so manufacturers don't see the need to make KNX Secure products, so the offer of KNX Secure products in the market is quite small, so projects needing KNX products don't specify in their tendering processes that these products must be KNX Secure, so... It's like a dog chasing its own tail.



## KNX Secure in the Immediate Future: a Prognosis

Despite the current situation, there are good reasons to think that KNX Secure will be a must soon.

On the one hand, we should not forget what we have previously exposed about the need for security: As technology evolves, so do threats. Fortunately, all the entities involved in the building automation sector, from makers to system integrators, are increasingly aware of the importance of security and the benefit of prevention. In the end, spending money on modern control systems is worthless if those systems have evident vulnerabilities that make them suitable prey for cyber attacks.

On the other hand, the makers under the KNX Association have spent a lot of money and effort to create this KNX Secure version, and they know the market tendencies quite well. Also, they are not alone:

- **BACnet Secure Connect (BACnet/SC):** After several years of work and attempts, in the summer of 2021<sup>3</sup>, BACnet launched its secure version for BACnet/IP, the so-called BACnet Secure Connect.

- **Modbus/TCP Security:** Also known as Modbus TLS, this is a security-focused variant of the Modbus/TCP protocol utilizing Transport Layer Security (TLS). Modbus officially announced it on 29 October 2018.

One thing is for sure: there must be good reasons for the organizations behind the main open-source protocols to put this extra effort into making them more secure. Bit by bit, more KNX Secure products are being launched, feeding a growing market. Sooner than later, projects based on KNX demanding the highest levels of security will appear, and tender processes will ask for KNX Secure products. When the real demand starts, makers will have to pull their socks up.

---

<sup>3</sup> The official publication date was the 1st of December 2019, but BACnet did not offer the open-source software repository for BACnet/SC until August 2021.

## Intesis Bet for KNX Secure

While this paper is being written, Intesis is already migrating some of its KNX gateways to the new KNX Secure version. The prevision for the first phase of the project is to upgrade most of the current portfolio's one-to-one KNX gateways for HVAC.

This decision is based on the fact that these gateways are physically integrated using the twisted pair (they don't support IP connection through Ethernet), so the process is simpler at the firmware development level.

Among the most essential hardware improvements to allow KNX Secure, we find the replacement of the old microchip with a new, more powerful one. Also, since this new version of KNX implies the need to store encryption keys, new dedicated memories have been included in the hardware.

Nonetheless, due to the large number of gateways, only a limited number are being upgraded at a time; slowly but surely, as the saying goes.

In summary, incorporating the KNX Secure version into Intesis gateways is challenging, but here at Intesis, we firmly believe that the time, effort, and money you spend on security are valuable investments.





## Summary

KNX is one of the most robust and widely used open-source communication protocols for home automation worldwide. Understanding the new security challenges emerging from this hyperconnected world, in 2019, the KNX Association launched the KNX Secure version of its standard, which incorporates solid security mechanisms, like the use of keys to commission KNX Secure products and the encryption of messages.

The impact this new version is having is lower than expected. One of the main reasons behind this may be that tendering processes are not asking for KNX Secure products—not yet, at least. Since security is becoming a must, everything indicates that this new version will prevail in the market.

In Intesis, we're already upgrading our KNX gateways to this KNX Secure version because, as the saying goes, it's better to prevent than cure.



## References

### **The legacy of KNX**

<https://www.knx.org/knx-en/for-professionals/What-is-KNX/KNX-History/>

### **KNX - The secure solution for your smart building**

<https://www.knx.org/knx-en/for-professionals/benefits/knx-secure/index.php>

### **Building automation systems: Addressing the cybersecurity threat**

<https://www.ashrae.org/technical-resources/ashrae-journal/featured-articles/building-automation-systems-addressing-the-cybersecurity-threat>

### **Data Centers facing the risk of cyberattacks**

<https://cyble.com/blog/data-centers-facing-risk-of-cyberattacks/>

### **Over 20,000 data center management systems exposed to hackers**

<https://www.bleepingcomputer.com/news/security/over-20-000-data-center-management-systems-exposed-to-hackers/>

### **Cost of Data Center Outages**

[https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11\\_51190\\_1.pdf](https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf)

### **KNX Secure: protecting installations from inside and outside**

<https://www.knx.org/knx-en/for-professionals/newsroom/en/news/KNX-Secure-protecting-installations-from-inside-and-outside/>

### **The Request for Quotation (RFQ) process in six steps**

<https://sievo.com/blog/the-simple-request-for-quotation-rfq-process-for-procurement>

### **BACnet Secure Connect**

[https://bacnet.org/wp-content/uploads/sites/4/2022/06/B-SC-Whitepaper-v15\\_Final\\_20190521.pdf](https://bacnet.org/wp-content/uploads/sites/4/2022/06/B-SC-Whitepaper-v15_Final_20190521.pdf)

### **Modbus Security – New protocol to improve control system security**

<https://modbus.org/docs/Modbus-SecurityPR-10-2018.pdf>

# To find out more...



This whitepaper aims to address the different options available for HVAC system integration and discusses the merits and drawbacks of each.

**Download it here**



This whitepaper aims to exhibit how the AC Cloud Control solutions can help gain efficiency in existing AC systems, improve comfort for the end-user, and save energy within buildings.

**Download it here**