WHITEPAPER

Security by design: secure wireless communication in low-voltage power distribution

SIEMENS

Content

1. Introduction

In light of the technological progress, the digitalization of electric power distribution is more important than ever. By means of networked systems, operators gain transparency on energy flows and components, and networks can be closely monitored and proactively maintained. Wireless connections are increasingly in demand for data transmission. However, operators often hesitate to use them as they have concerns regarding Cybersecurity.

This white paper explains how damage from cyberattacks can be averted when using wireless communication. This includes highlighting security features of the communication standards Bluetooth Low Energy and Zigbee-PRO as well as complementary actions at the device level.

Why use wireless communication in power distribution?

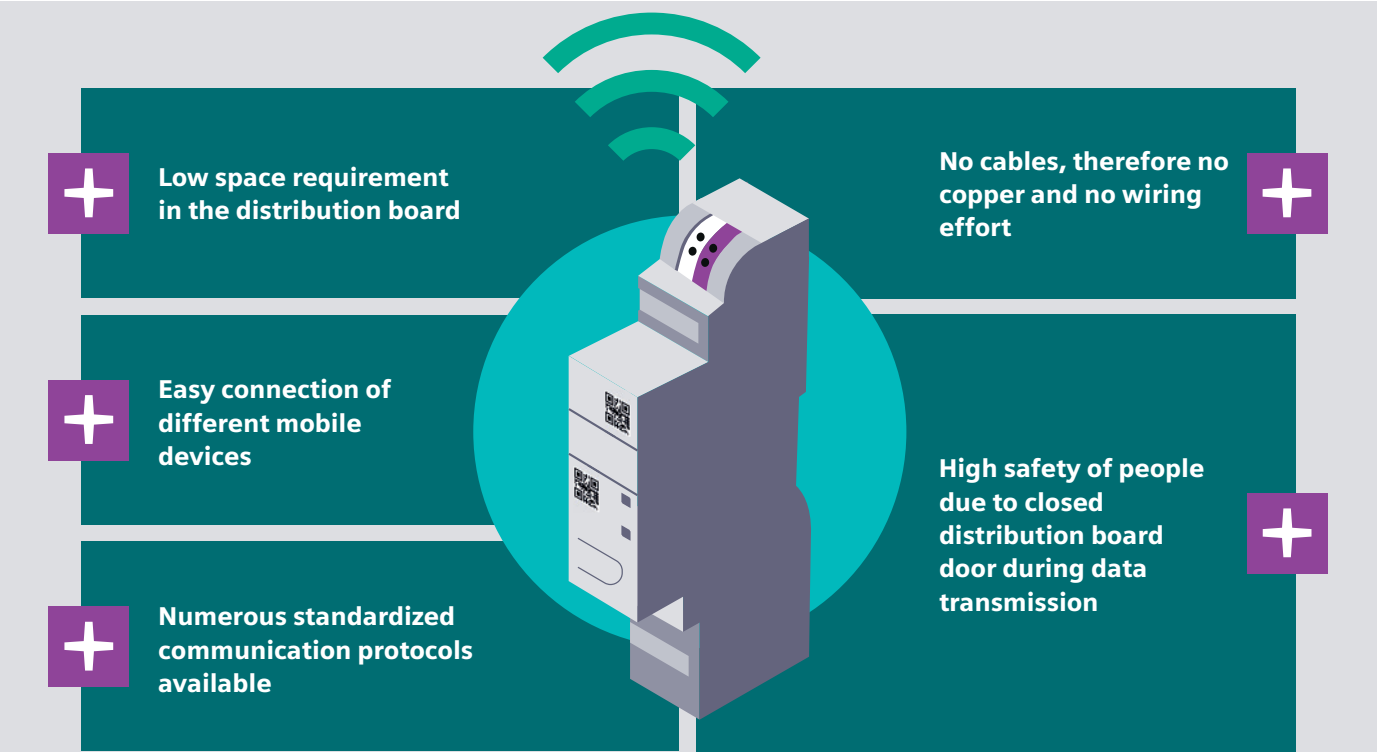

Figure 1: Advantages of wireless communication in low-voltage power distribution

Wireless data transmission offers many advantages (see figure 1). In some applications, wireless connections are the only possibility of linking low-voltage components to one another. They do, however, harbor risks. Wireless signals can be disrupted by an interfering signal or, in case of a cyberattack, the wireless traffic can be recorded. But, if component manufacturers and operators are aware of these risks, they can take targeted measures against them.

2. Cybersecurity starts with the communication standard: Zigbee-PRO and Bluetooth Low Energy

Communication standards comprise rules for data exchange between different devices. They define, at what point which data is exchanged and how it must be structured. The strict adherence of standards ensures a secure and efficient communication. Two standards for applications in the Industrial Internet of Things (IIoT) are looked at more closely in the following: Zigbee-PRO and Bluetooth Low Energy.

2.1 Zigbee-PRO

Zigbee is a versatile communication protocol specifically designed for the transmission of small amounts of data at minimal power consumption. It is therefore one of the preferred standards for the development of wireless sensor networks. It is not just known in the industry, but also in the public realm of home automation. The set of features for Zigbee-PRO was developed with regard to its application in the industry and infrastructure.

Zigbee-PRO offers the following security features [1] [2] [3]:

- Data transmission between all participants of a network is encrypted using the AES-CCM algorithm with 128 bits
- Authentication of network participants by means of secure processes during which network keys are never transmitted unencrypted over the air
- Use of two different session keys for communication: network key for messages to the entire network, link key for communication between two network participants
- Periodic update of the network key
- Protection against interfering signals and interferences: choice from 16 different channels within a 2.4 GHz frequency band possible

Zigbee-PRO: a practical standard for practical use

Zigbee is provided and maintained by the Connectivity Standards Alliance (CSA). The international community consists of almost 600 companies that campaign for open standards in the Internet of Things. As a member of the CSA, Siemens also takes part in the advancement of such standards.

Infobox: Secure encryption with AES-CCM (128 bits)
The Advanced Encryption Standard (AES) is a widespread procedure for the encryption of sensitive data. The algorithm splits the message to be transmitted into blocks with a predefined length. By means of a secret key, several repetitions of complex mathematical operations are performed for each block. The result is an encrypted text that cannot be deciphered without knowing the key. AES was standardized by the National Institute of Standards and Technology (NIST) in the USA and has undergone extensive testing by cryptographic experts from all around the world. To date there is no knowledge of practically relevant attacks [4]. The operating mode CCM (Counter with CBC-MAC) ensures that messages are additionally equipped with an authentication tag. This tag allows checking if the message was altered during transmission [5].

2.2 Bluetooth Low Energy

Bluetooth Low Energy (BLE) is among the most common wireless transmission protocols. Its different security modes and levels intentionally give developers a high degree of freedom, making it universally applicable. In case an application requires it, it is possible to establish an encrypted, integrity-protected and authenticated connection. For this, it is especially important that the pairing process for the initial key exchange for establishing an encrypted channel is designed secure [6].

As of version 4.2, BLE offers among others the following security features [7]:

- Encrypted and authenticated data transmission by means of the AES-CCM algorithm with 128 bits
- LE Secure Connections Pairing: the FIPS*-certified algorithm Elliptic Curve Diffie-Hellmann (ECDH) is used for creating the cryptographic key. This increases the security of the wireless connection during the initial pairing.

Infobox: Tap-proof pairing with Elliptic Curve Diffie-Hellmann (ECDH)
Elliptic Curve Diffie-Hellmann (ECDH) is an algorithm with which two parties can exchange data securely via an unsecure channel. Each party generates a public/private key pair, but only the public keys are transmitted. By means of the public and private keys, a joint secret key is calculated that can be used for communication. The cryptographic key is hence at no time transmitted unprotected.

*FIPS (Federal Information Processing Standards) is a series of American standards that are developed and maintained by the National Institute of Standards and Technology (NIST). They determine requirements for computer security and interoperability of computer systems of non-military American governmental institutions and contractors.

In combination with LE Secure Connections Pairing, BLE offers various authentication methods:

- Just Works: no additional authentication (e.g., at the touch of a button)
- Out of Band: authentication via a Bluetooth-independent channel (e.g., NFC, QR code)
- Numeric Comparison: The user is shown a 6-digit code on both devices and he must confirm that the codes shown on both devices are identical.
- Passkey Entry: The user is either shown a 6-digit code (passkey) on both devices or alternatively on one device and the code must then be entered on the other one. The passkey is not used as an input for the encryption algorithm. It is hence of no value for an attacker as it is not used to decrypt the data transmitted between the devices.

In earlier Bluetooth versions (Legacy Pairing), the authentication methods have identical designations. However, during Legacy Pairing the ECDH algorithm is not used for generating the key, and the initial pairing is not tap-proof. The authentication method is chosen based on the specification during pairing depending on the device capabilities. But, manufacturers can configure components in a way that they only allow connections with devices that support Secure Connections Pairing. A specific procedure for authentication can also be enforced [6][7].

2.3 Conclusion on communication standards

To ensure a secure wireless communication, manufacturers of communicating devices must take Cybersecurity into account already during the early phases of product development (security by design). Both Zigbee-PRO and Bluetooth allow establishing cybersecure solutions. However, each specification leaves room that can lead to weak points in the implementation. Specifications that are implemented incompletely or not at all can lead to security holes [8]. Furthermore, processing power and strategies for cyberattacks continuously evolve. When selecting a device for wireless communication, operators should hence look out for their adherence to protocol specifications and their application of secure methods. Future security gaps in the protocol should be eliminated by permanent updates.

3. Secure wireless connections through complementary actions

Figures 2 and 3 highlight how the SENTRON product family enables secure wireless communication. The protocol specifications described above are consequently implemented and complemented by actions on the device level. Regardless of the application and the applied standard, the following security measures are implemented:

- Range limitation: the transmission path is limited, meaning a connection can only be established between devices in close proximity of one another.
- Updateable: identified weaknesses in the protocol can be remedied by firmware updates.
- Management of weak points: Siemens checks products for weak points. In case a gap is identified, Siemens offers support with countermeasures such as patches and security updates and proactively communicates these to the customer. This check also includes third-party components or open source software applications that are part of Siemens products.

3.1 Wireless commissioning and service

Comfort and speed are arguments that speak for wireless communication for configuration purposes (fig. 2). Service engineers should be able to quickly establish a secure connection to the devices that need to be configured by means of mobile devices. BLE is suitable for these applications as it is supported by common mobile devices.

The low-voltage components from the SIRIUS and SENTRON families only support the above mentioned tap-proof Secure Connections Pairing as of BLE version 4.2 with passkey entry authentication. The Bluetooth interface is only activated when it is needed.

Practical tip: Change the passkey for long-term security
For devices without a display (e.g., SENTRON 7KN Powercenter 1000), the passkey is imprinted as data matrix code ex works. This code can be changed using SENTRON powerconfig – a possibility operators should take advantage of. The Bluetooth specification recommends changing the passkey for every pairing to increase the security of the connection. Devices with a display (e.g., SENTRON 3WA air circuit breakers) automatically show an individual code for each pairing.

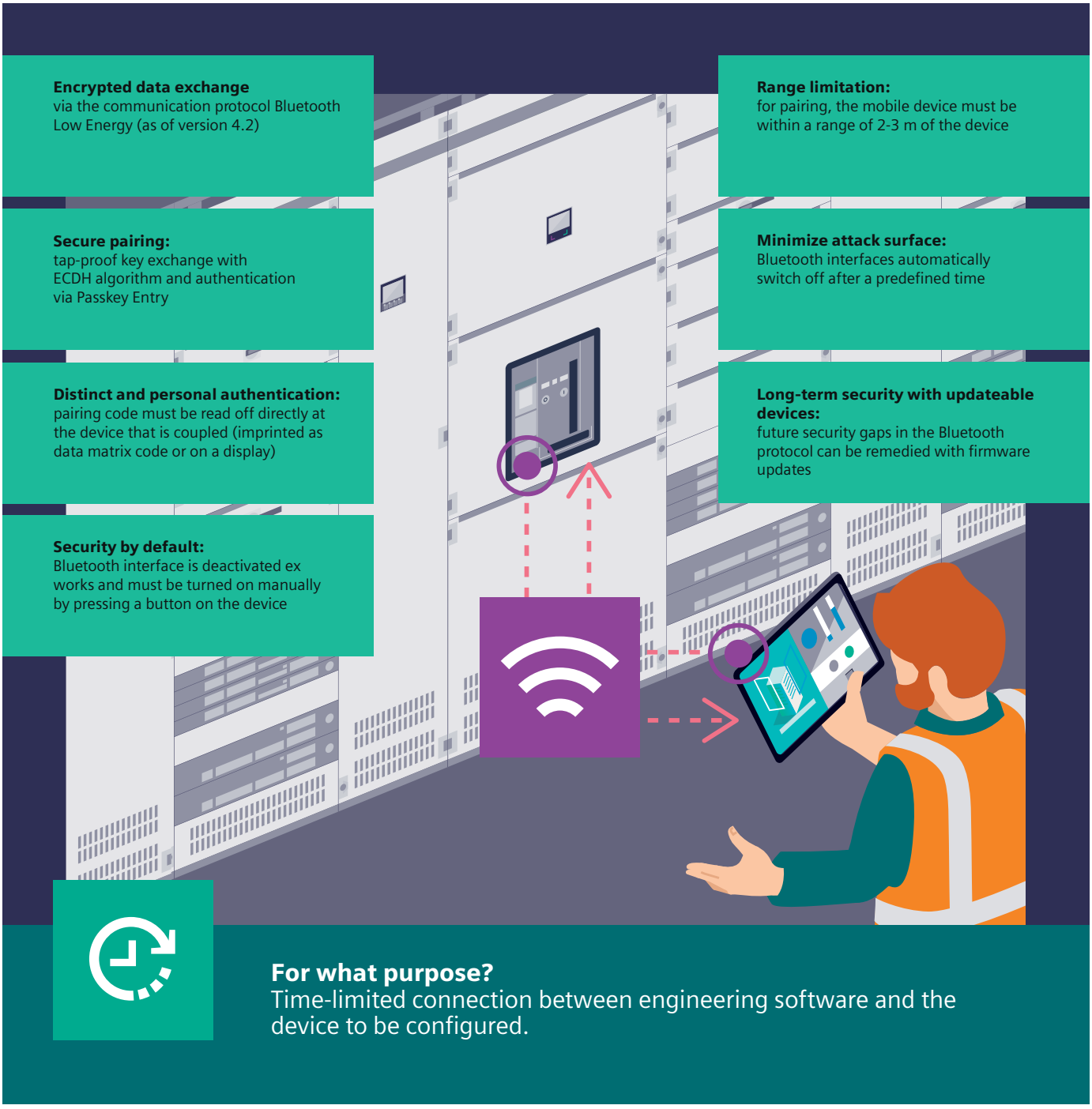

Figure 2: Quick and easy data exchange via Bluetooth Low Energy between the engineering software (SENTRON powerconfig) and the device to be configured (e.g., SENTRON 3WA air circuit breaker)

3.2 Permanent wireless connection

Having little space available is driver for wireless communication when data is transmitted from distribution boards to higher-level systems (fig. 3). Ideally, components in these applications run maintenance-free for a long time, which is why a low power consumption is of high value. The communication between rail-mounted devices and fuses by means of the data transceiver 7KN Powercenter 1000 hence takes place based on the specification Zigbee-PRO.

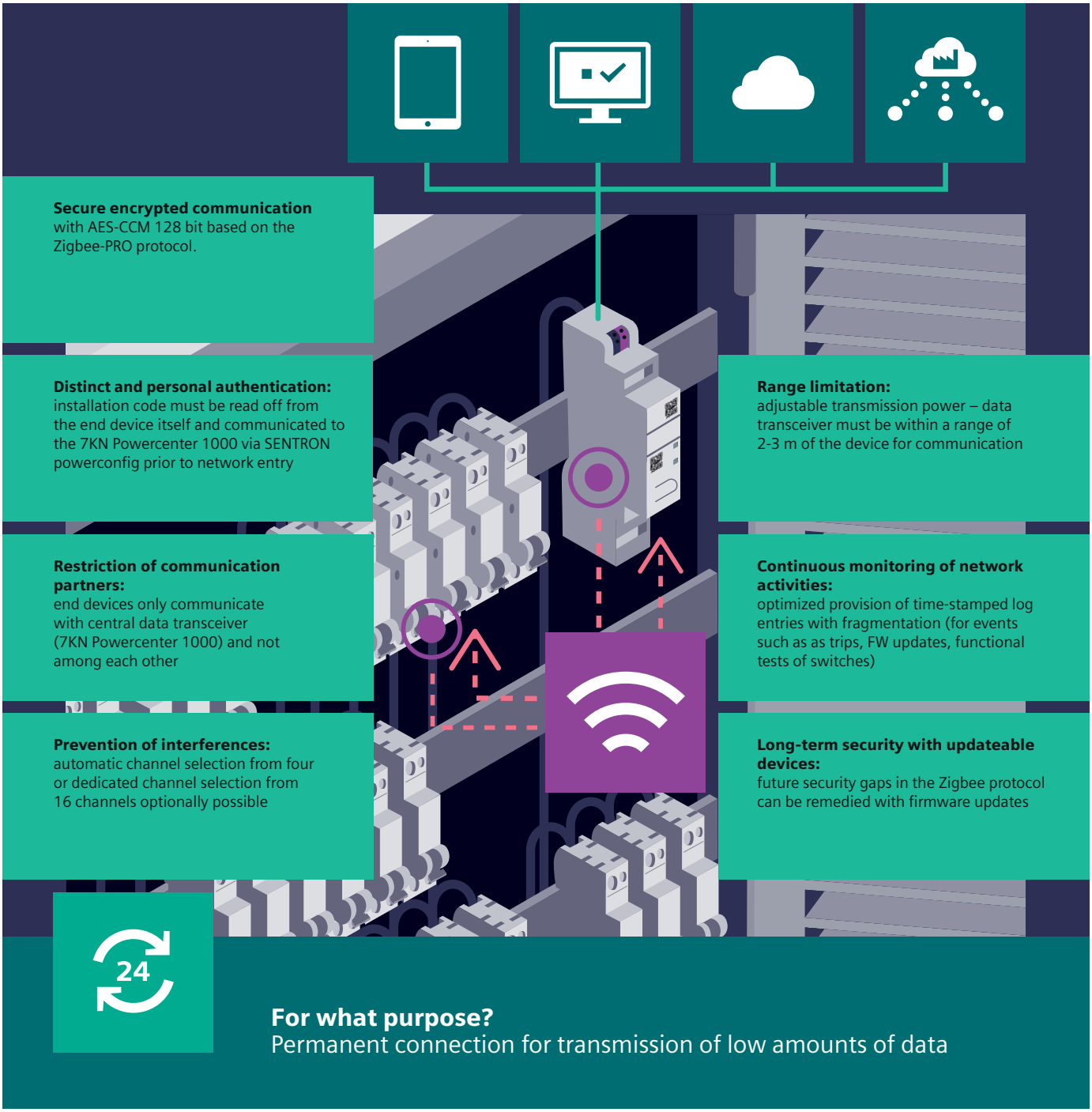

Figure 3: Secure communication between the data transceiver 7KN Powercenter 1000 and measurement- and communication-capable SENTRON protective devices on the basis of Zigbee-PRO.

The data transceiver functions as central Trust Center. Components can only be added to the Zigbee network, if the installation code imprinted on the device as well as the MAC address of the device were entered in the 7KN Powercenter 1000 via SENTRON powerconfig beforehand. On the basis of the installation code, an initial connection code for the device is generated, which is then replaced with a new key by the 7KN Powercenter 1000.

4. Conclusion and recommendations

Wireless communication is a secure way of transmitting data in low-voltage power distribution. This does, however, require holistic measures. Operators should take the following points into account, if they want to use wireless technology:

- Only use components that communicate via secure protocols
- Specification-based and secure implementation of protocols and complementary actions by manufacturers
- Updateability of components and security patches ensured by the manufacturer
- Deactivation of interfaces that are not required (ideally automatically after a defined time period)
- Several levels of Cybersecurity for networked components (e.g., firewalls, network segmentation, ...)
- Best practices for Cybersecurity (e.g., patch management, task separation, ...)
- Multi-level authentication and access control: physical access to devices only as necessary and regular checks of access rights
- Validity of hardware and software: observe updates and security patches

5. Sources

[1] M. D. Prieto, A. Talevski, J. et al, „Zigbee/Zigbee-PRO Security Assessment Based on Compromised Cryptographic Keys," in International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010.

[2] P. Baronti, P. Pillai, et al, „Wireless sensor networks: A survey on the state of the art and the 802.15.4 and Zigbee standards," Computer Communications, p. 1655–1695, 2007.

[3] Zigbee Alliance, „Zigbee Specification, Zigbee Alliance document 05-3474," 2015.

[4] Studyflix.de, „Studyflix: AES Verschlüsselung," [Online]. Available: https://studyflix.de/informatik/aes-verschlusselung-1611. [Accessed on February 15th, 2023].

[5] M. Dworin, „Recommendation for Block Cipher Modes of Oeration: The CCM Mode for Authentication and Confidentiality," May 2004. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38c.pdf.

[6] M. von Tschirschnitz, L. Peuckert, et al, „Method Confusion Attack on Bluetooth Pairing," in IEEE Symposium on Security and Privacy (Oakland), 2021.

[7] Bluetooth Special Interest Group, „Bluetooth Core Specification v4.2," 2014, p. 85 ff.

[8] Fraunhofer Academy, Lernlabor Cybersicherheit, „Blog der Fraunhofer Academy," September 2022. [Online]. Available: https://blog.academy.fraunhofer.de/cybersicherheit/bluetooth-lowenergy/. [Accessed on February 28th, 2023].

Published by:

Siemens AG
Smart Infrastructure
Electrical Products

Siemenspromenade 10
91058 Erlangen, Germany

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under:
https://www.siemens.com/cert/advisories