Special Documentation
Security Manual
FieldPort SWA50

Intelligent Bluetooth® and/or WirelessHART adapter for all HART field devices

Endress+Hauser

People for Process Automation

A0023555

Table of contents

1 Reporting security gaps and advisories

Endress+Hauser provides information on cybersecurity and security on the following web page: https://www.endress.com/cybersecurity

The page contains the following information, for example:
- Up-to-date security warnings (security alerts) that affect Endress+Hauser products
- Contact e-mail address to report security gaps in Endress+Hauser products. PGP encryption enables confidential communication. You can download the public key from the web page.
- Subscription option to e-mail service for new advisories on Endress+Hauser products
- Endress+Hauser contact information: PSIRT@endress.com

2 Document information

2.1 Document function

This supplementary Security Manual applies in addition to the product documentation such as Operating Instructions, Technical Information and ATEX Safety Instructions. The supplementary product documentation must be followed throughout the entire life cycle of the product. The additional requirements in relation to security are described in this Security Manual.

2.2 Symbols used

2.2.1 Safety symbols

⚠ DANGER
This symbol alerts you to a dangerous situation. Failure to avoid this situation will result in serious or fatal injury.

⚠ WARNING
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in serious or fatal injury.

⚠ CAUTION
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or medium injury.

NOTICE
This symbol contains information on procedures and other facts which do not result in personal injury.

2.2.2 Symbols for certain types of information and graphics
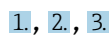
🛈 **Tip**
Indicates additional information

📖
Reference to documentation

🖾
Reference to graphic

▶
Notice or individual step to be observed

1. , 2. , 3.
Series of steps

↳
Result of a step

1, 2, 3, …
Item numbers

A, B, C, …
Views

2.3   Documentation

2.3.1   Further applicable documents

An overview of the associated documentation is provided in the following:
- *W@M Device Viewer* (www.endress.com/deviceviewer): Enter the serial number from the nameplate
- The download area of the Endress+Hauser web site (www.endress.com/download)

Further applicable documents for the FieldPort SWA50

- Technical Information TI01468S (Bluetooth and WirelessHART)
- Operating Instructions BA01987S (Bluetooth)
- Brief Operating Instructions KA01436S (WirelessHART)
- Operating Instructions BA02046S (WirelessHART)
- Bluetooth access data: 71499893
- Netilion – Terms of Service
  https://netilion.endress.com/legal/terms-of-service
- Netilion – Privacy Policy
  https://netilion.endress.com/legal/privacy-policy
- Netilion – Security Policy
  https://netilion.endress.com/legal/security-policy
- Netilion – Service Level Agreement
  https://netilion.endress.com/legal/service-level-agreement

2.3.2   Purpose and content of the document types

Technical Information (TI)

Planning aid
This document contains all the technical data on the product and provides an overview of everything that can be ordered with the product.

Brief Operating Instructions (KA)

Guide that takes you quickly to the 1st measured value
The Brief Operating Instructions contain all the essential information from incoming acceptance to initial commissioning.

Operating Instructions (BA)

Your comprehensive reference
The Operating Instructions contain all the information that is required in various phases of the life cycle of the product: from product identification, incoming acceptance and storage, to mounting, electrical connection, operation and commissioning through to troubleshooting, maintenance and disposal.

Safety Instructions (XA)

Safety Instructions (XA) are supplied with the product depending on the approval. They are an integral part of the Operating Instructions.

The nameplate indicates the Safety Instructions (XA) that are relevant to the product.

Special Documentation (SD)

Additional information
Special Documentation provides additional information on the product. Additional information can include graphical representation of commissioning, for example, or information on an app.

3　System design

3.1　Target group

This section is aimed at planners and system integrators.

3.2　System overview

3.2.1　General information

You can configure and operate the FieldPort SWA50 via the following digital applications:
- Endress+Hauser SmartBlue app
- Endress+Hauser Field Xpert SMTxx (Bluetooth via MSD, HART via DTM)

The WirlelessHART version can additionally be operated as follows:
Remote configuration with FieldCare SFE500 via WirelessHART-Fieldgate SWGxx and DTMs

The FieldPort SWA50 is equipped with the following interfaces:
- Bluetooth®
- HART (wired)
- WirelessHART version additionally: WirelessHART

HART field devices can be connected to the Netilion Cloud via the FieldPort SWA50 and a FieldEdge device.
- Netilion: https://netilion.endress.com
- Netilion Value: https://Netilion.endress.com/app/value

The Endress+Hauser Netilion Cloud is equipped with the following interfaces:
- https Internet connection
- Netilion Connect: Application Programming Interface (API)

The Bluetooth connection between the FieldPort SWA50 and mobile terminals such as smartphones, tablets or edge devices is protected by CPace. For further information, refer to the following link:

https://www.endress.com/cybersecurity > Section on secure Bluetooth® connection from Endress+Hauser

The WirlessHART connection between the FieldPort SWA50 and WirlessHART gateway provides end-to-end 128-bit AES encryption in accordance with the WirelessHART standard. For further information, refer to the following link:

https://fieldcommgroup.org/wirelesshart-security

3.2.2　System design and system boundaries

This Security Manual takes into account the FieldPort SWA50, the interface to the wired field device, the Bluetooth connection and the WirelessHART connection. The other components such as connected field devices, gateways, edge devices, the Endress+Hauser Netilion Cloud and operating tools are not part of this Security Manual. The system boundaries are highlighted in color in the following diagrams.

System design of the FieldPort SWA50 Bluetooth version
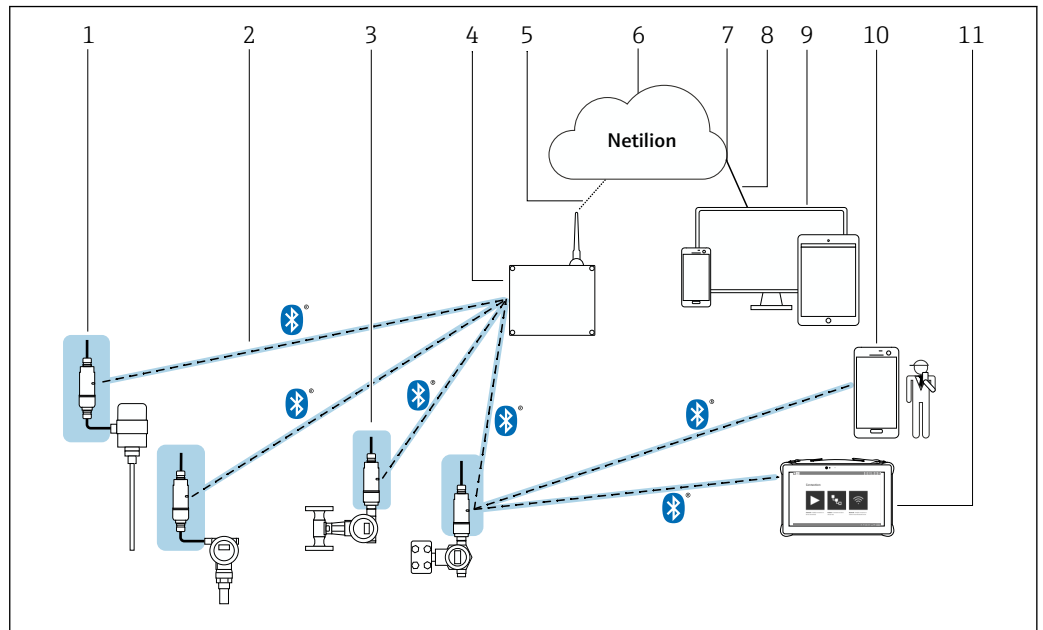
A0049179

🖼 *1   System design of the SWA50 Bluetooth version (color highlighting shows the system boundaries for this manual)*

1   HART field device with FieldPort SWA50, remote mounting
2   Encrypted wireless connection via Bluetooth®
3   HART field device with FieldPort SWA50, direct mounting
4   FieldEdge SGC200
5   LTE connection
6   Netilion Cloud
7   Application Programming Interface (API)
8   https Internet connection
9   Internet browser-based Netilion Service app or user application
10   Endress+Hauser SmartBlue app
11   Endress+Hauser Field Xpert, e.g. SMTxx

ℹ️ The FieldPort SWA50 is referred to as a product or terminal in general text in this document depending on the context.

System design of the FieldPort SWA50 WirelessHART version
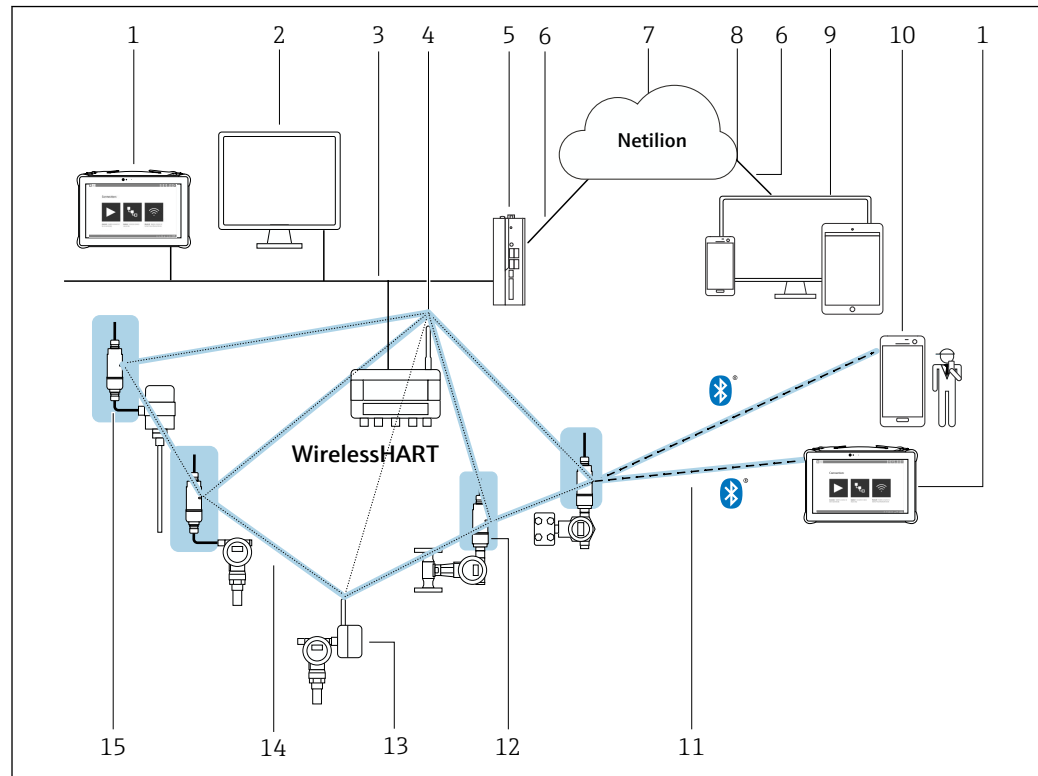
⊡ *2* *System design of the SWA50 WirelessHART version (color highlighting shows the system boundaries for this manual)*

1   Endress+Hauser Field Xpert, e.g. SMTxx
2   Host application/FieldCare SFE500
3   Ethernet communication
4   WirelessHART-Fieldgate, e.g. SWG70
5   FieldEdge SGC500
6   https Internet connection
7   Netilion Cloud
8   Application Programming Interface (API)
9   Internet browser-based Netilion Service app or user application
10   Endress+Hauser SmartBlue app
11   Encrypted wireless connection via Bluetooth®
12   HART field device with FieldPort SWA50, direct mounting
13   HART field device with WirelessHART adapter, e.g., SWA70
14   Encrypted wireless connection via WirelessHART
15   HART field device with FieldPort SWA50, remote mounting

> The FieldPort SWA50 is referred to as a product or terminal in general text in this document depending on the context.

3.3   Defining the security level

Both the system and the products installed in the system must meet different levels of requirements depending on the required security level. You must first define the required **security level** from SL1 to SL4 for the system. Depending on the security level, you define the requirements for the system in accordance with DIN IEC 62443-3-3 and the requirements for the product in accordance with DIN EN 62443-4-2.

3.4　　Typical operating environment of the product

We recommend that you define the typical operating environment of the product in order to draw up the security-related properties.

The requirements of the environment should be determined by assessing the operating environment. For example, you can factor in a denial-of-service attack.

The following considerations may apply for a typical operating environment for example:
- The product is a system component.
- The product is equipped with at least one interface. See the system overview section for information on interfaces.
- The product is operated in an industrial environment.
- Access to the system is regulated. Only authorized staff have access to the system.
- The personnel are trained and instructed on the use of the product and on the security risks.
- The product is operated in an Ethernet network that is intended for industrial purposes only. The network is either fully separated from the rest of the company's network or protected by firewalls.
- The product has at least one data connection that leaves the production area.
- The automation network is protected against attacks from the outside, such as a denial-of-service attack, by means of perimeter protection.
- The product is installed in an environment that is protected in accordance with the defense in depth principle.
- Passwords for the product are only known by authorized personnel.
- Only authorized personnel can access the product via the associated Human Machine Interface (HMI).

The product can only defend against attacks to a limited extent because the processing power of the product in question is limited.

3.5　　Measures required if necessary operating environment cannot be provided

If the specified requirements for the operating environment cannot be met, alternative measures may have to be arranged. This may involve, for example, mechanical protection of the product against tampering, mechanical protection of the cabling, or organizational measures.

For example, you can use the FieldPort SWA50 in free space. Measures to combat physical tampering of the FieldPort SWA50 must be arranged by the customer.

3.6　　Carrying out risk analysis and risk assessment

When planning a system, you must carry out a risk assessment for the entire system taking a holistic approach. You can follow the guidelines in the VDI 2182 standard when carrying out a risk assessment on systems.

You carry out a risk/threat analysis during the course of the risk assessment.

Take the following aspects into account for the risk analysis:
- Interfaces of the product that allow communication with the product or enable access to the product
- Product data flows within the system
  - Incoming data to the product
  - Outgoing data from the product
- Product data flows that leave the area of the system and go through firewalls if necessary

You can define risk minimization measures based on the risk analysis.

In addition to the risk assessment, the planning process should also include specifications on how the product is to be configured during commissioning. This includes, for example, switching off interfaces and/or services that are not required or changing default passwords etc. These measures are explained in the following sections.

3.7   Recommended risk minimization measures

3.7.1   Taking the entire system into account

The FieldPort SWA50 is a terminal that is used in what is referred to as a closed IIoT ecosystem.

Due to its decentralized and modular structure, an IIoT ecosystem can quickly become a patchwork of different terminals. Due to the heterogeneous nature of these overall solutions, each divergent product represents a new source of danger that compromises security at the interfaces and can result in insecure data transmission paths.

This manual covers integration into the Netilion IIoT ecosystem from Endress+Hauser. Additional analysis is required if the FieldPort SWA50 is integrated into a different system.

3.7.2   Training the users

Depending on the application scenario, users who are not specialized in this area may come in contact with the IIoT ecosystem. We recommend that these users be trained in the safe use of the relevant terminals and/or interfaces and be made aware of security issues.

3.7.3   Optimizing access management

Bluetooth

You will require appropriate access data such as user name and password to access the FieldPort SWA50 via Bluetooth. You must use the password set at the factory when logging in for the first time. We recommend that you change the password after the first time you log in and keep the password in a safe place. The initial password is specified on the nameplate and on the Bluetooth access data sheet provided.

> For further information, refer to Operating Instructions BA01987S (Bluetooth) and Bluetooth access data → 🖺 6

WirelessHART

To operate the FieldPort SWA50 in a WirelessHART network, you need the network ID (Network Identification) and network password (Join Key) of the relevant WirelessHART network. We recommend that you treat these access data confidentially and keep them safe.

> For further information, refer to Brief Operating Instructions KA01436S (WirelessHART) and Operating Instructions BA02046S (WirelessHART) → 🖺 6

IIoT ecosystem

We recommend that you apply the same identity and access management rules for access to the IIoT ecosystem as for other areas of the company.

- Only grant access rights to employees who require access to carry out their tasks
- Only allocate user accounts (Accounts) with strong passwords
- Generate, back up and manage passwords with a password manager

3.7.4 Monitoring device data and device status

Since real-time monitoring is not an option for most users, this process needs to be automated. We recommend using monitoring software that monitors specific parameters and the condition of the product and reports any deviations.

Monitoring via HART

The FieldPort SWA50 can be connected to a control system via HART. Detection and correction of anomalies is then the responsibility of the control system operator.

Monitoring via WirelessHART

The FieldPort SWA50 can be a user in a WirelessHART network. Detection and correction of anomalies is then the responsibility of the WirelssHART network operator.

Monitoring via the IIoT ecosystem

The FieldPort SWA50 can be a terminal in an IIoT ecosystem and the detection of anomalies is a function of the higher-level system.

3.7.5 Updating product software

Terminals for an IIoT ecosystem must be developed in such a way that the number of enhancements required subsequently via updates is kept to a minimum. Given the dynamic nature of IT and increasing requirements in networking, updates are always required in real life.

We recommend that you regularly check if new updates are available and install them. Missed updates are a serious security risk as potential attackers could also be aware of the vulnerabilities to be fixed.

3.7.6 Protecting apps/applications

Software and, in particular, a heterogeneous software landscape represent a further security risk, such as the use of Android apps on a tablet and Windows solutions on a PC.

In order to secure the applications, apps and cloud servers, protection should also be provided for the mobile and stationary terminals that have access to the IIoT ecosystem.

Protection of the access data of the terminals should also be ensured in order to protect the customer system and customer data. Access data and certificates must be kept in a safe place.

4 Commissioning (installation and configuration)

4.1 Target group

This section is aimed at operating personnel.

4.2 Requirements of the personnel

Personnel must fulfill the following requirements:
▸ Must have a relevant qualification for this specific function and task.
▸ Authorized by the rig owner/operator.
▸ Be familiar with federal/national regulations.
▸ Before starting work: personnel must read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application).
▸ Personnel must follow instructions and comply with general policies.

4.3 Installation

Install and connect the product in accordance with the relevant Brief Operating Instructions/Operating Instructions.

4.4 Configuration

4.4.1 Commissioning and configuring the product

Commission and configure the product in accordance with the associated Brief Operating Instructions/Operating Instructions. With regard to security, please also refer to this section and the following sections.

🛈 FieldPort SWA50 system overview: → 🖺 8

4.4.2 Required security steps during commissioning

Endress+Hauser uses the principles of the "known consignor" system for shipping. As recipient, you can assume that the product will reach you in a defined condition. It is not necessary to check the hardware for tampering.

With regard to security, pay attention to the following during commissioning:
Integrate the product in the operating environment in accordance with the specified requirements→ 🖺 11.

4.4.3 Hardening the product

In the field of security, the term "hardening" means that the only services enabled are those that are required for the correct operation of the product in the application in question.

Hardening of the FieldPort SWA50 is only possible for the WirelessHART version. If you are no longer using the Bluetooth connection after commissioning, you can disable the "Bluetooth communication" function via DIP switch 1.

🛈 For further information on the "DIP switch", refer to Brief Operating Instructions KA01436S (WirelessHART) → 🖺 6

4.4.4   Configuring user data

User data include, for example, login data, users, device tags (TAG), passwords, IDs, etc.

You can configure the user data.

ℹ️ For further information, refer to the FieldPort SWA50 documentation → 🗎 6

4.4.5   Security-related product settings

All required security-related settings were carried out on the FieldPort SWA50 in the factory. No adjustments are required.

4.4.6   User management and impact on security

The FieldPort SWA50 has only one user level (admin).

5 Operation

5.1 Target group

This section is aimed at operating personnel.

5.2 Requirements of the personnel

Personnel must fulfill the following requirements:
▶ Must have a relevant qualification for this specific function and task.
▶ Authorized by the rig owner/operator.
▶ Be familiar with federal/national regulations.
▶ Before starting work: personnel must read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application).
▶ Personnel must follow instructions and comply with general policies.

5.3 Tasks during operation

Operate the product in accordance with the associated Operating Instructions. With regard to security, please also refer to this section.

The FieldPort SWA50 does not require any intervention during operation.

5.4 Update management

You can perform a firmware update for the FieldPort SWA50 via the Endress+Hauser SmartBlue app if necessary. DIP-switch 2 with the "Firmware update" function must be set to ON. The function is disabled when in the OFF position.

For further information on the DIP switch and updates, refer to Operating Instructions BA01987S (Bluetooth) and Brief Operating Instructions KA01436S (WirelessHART) → 🖺 6

5.5 Repeating the risk analysis

External events can change the risk situation that systems are exposed to; unknown attack patterns can occur for example. According to Section 4.4 of the VDI/VDE 2182-1-2011 guidelines, risk analysis must be repeated and updated at regular intervals or in the event of changes to the system that could influence the risk analysis.

5.6 Repair and disposal

Repair or dispose of the product in accordance with the Operating Instructions.

6 Decommissioning

6.1 Target group

This section is aimed at operating personnel.

6.2 Requirements of the personnel

Personnel must fulfill the following requirements:
▶ Must have a relevant qualification for this specific function and task.
▶ Authorized by the rig owner/operator.
▶ Be familiar with federal/national regulations.
▶ Before starting work: personnel must read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application).
▶ Personnel must follow instructions and comply with general policies.

6.3 Decommissioning the product

There are various reasons why the product may need to be decommissioned. Depending on the reason for decommissioning, certain actions are required.

Reason for decommissioning	Actions required
The product is not being used for a longer period of time.	We recommend that you reset the password to the password configured at the factory. The initial password is specified on the nameplate and on the Bluetooth access data sheet provided. • For further information, refer to Operating Instructions BA01987S (Bluetooth) and Bluetooth access data → 📖 6 • For further information on WirelessHART, refer to Brief Operating Instructions KA01436S and Operating Instructions BA02046S → 📖 6
The product has a fault that you are unable to rectify.	▶ Contact Endress+Hauser. ↳ Endress+Hauser will either ask you to send the product to them or to dispose of it.
The product is defective and must therefore be disposed of.	Before you dispose of, or scrap, the FieldPort SWA50, we recommend that you proceed in accordance with the following guideline: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization
The product is to be disposed of.	Before you dispose of, or scrap, the FieldPort SWA50, we recommend that you proceed in accordance with the following guideline: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

7   Appendix

7.1   Security checklist for the product life cycle

Life cycle	Task	Checked
Planning	Typical operating environment of the product has been defined and taken into account in planning. → 🕮 11 Where necessary, alternative measures have been taken into account. → 🕮 11	❑
	Planning activities taken into account in engineering phase. Risk analysis and risk assessment completed.→ 🕮 11	❑
	Where possible, risk minimization measures have been taken into account. → 🕮 12	❑
Incoming goods/ transportation	Packaging checked to ensure it is unopened and seal is intact.	❑
Commissioning	Product hardened for specific application. → 🕮 14	❑
Operation	Update management requirements observed. → 🕮 16	❑
	Recurring risk analysis planning completed. → 🕮 16	❑
Decommissioning	Product taken out of service. → 🕮 17	❑

7.2   Version history

Document version	Firmware version	Hardware version	Changes
01.21	From 01.00.xx	Dev. rev. 0	First version

Endress+Hauser

71574843

www.addresses.endress.com

Endress+Hauser

People for Process Automation