

Special Documentation

Security Manual

Micropilot FWR30

Free space radar





A0023555

Table of contents

1	Reporting security gaps and advisories	4	5	Operation	13
			5.1	Target group	13
2	About this document	5	5.2	Requirements of the personnel	13
2.1	Document function	5	5.3	Tasks during operation	13
2.2	Symbols used	5	5.4	Security factors during operation	13
2.2.1	Safety symbols	5	5.5	Update management	13
2.2.2	Symbols for certain types of information and graphics	5	5.6	Repeating the risk analysis	13
2.3	Documentation	6	5.7	Repair and disposal	14
2.3.1	Further applicable documents	6	6	Decommissioning	15
2.3.2	Purpose and content of the document types	6	6.1	Target group	15
3	System design	7	6.2	Requirements of the personnel	15
3.1	Target group	7	6.3	Decommissioning the product	15
3.2	System overview	7	7	Appendix	16
3.2.1	General information	7	7.1	Security checklist for the product life cycle ...	16
3.2.2	System design and system boundaries	7	7.2	Version history	16
3.3	Defining the security level	8			
3.4	Typical operating environment of the product	8			
3.5	Measures required if necessary operating environment cannot be provided	9			
3.6	Carrying out risk analysis and risk assessment	9			
3.7	Recommended risk minimization measures ...	9			
3.7.1	Taking the entire system into account	9			
3.7.2	Training the users	10			
3.7.3	Optimizing access management	10			
3.7.4	Monitoring device data and device status	10			
3.7.5	Updating product software	10			
3.7.6	Protecting apps/applications	10			
4	Commissioning (installation and configuration)	11			
4.1	Target group	11			
4.2	Requirements of the personnel	11			
4.3	Installation	11			
4.4	Configuration	11			
4.4.1	Commissioning and configuring the product	11			
4.4.2	Required security steps during commissioning	11			
4.4.3	Hardening the product	11			
4.4.4	Configuring user data	12			
4.4.5	Security-related product settings ...	12			

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 About this document

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



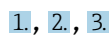
Reference to documentation



Reference to graphic



Notice or individual step to be observed



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 Micropilot FWR30

- Technical Information TI01499F
- Operating Instructions BA01991F
- Special Documentation SD02474F (Free space radar)
- Special Documentation SD02672S (Netilion Value)
- 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 operate the Micropilot FWR30 with the following digital applications:

- Netilion Value: <https://Netilion.endress.com/app/value>
- Netilion Inventory: <https://Netilion.endress.com/app/inventory>
- SupplyCare Hosting: <https://portal.endress.com>

SupplyCare Hosting is commissioned by the Endress+Hauser Service team.

The Micropilot FWR30 is equipped with the following interfaces:


https cellular radio connection

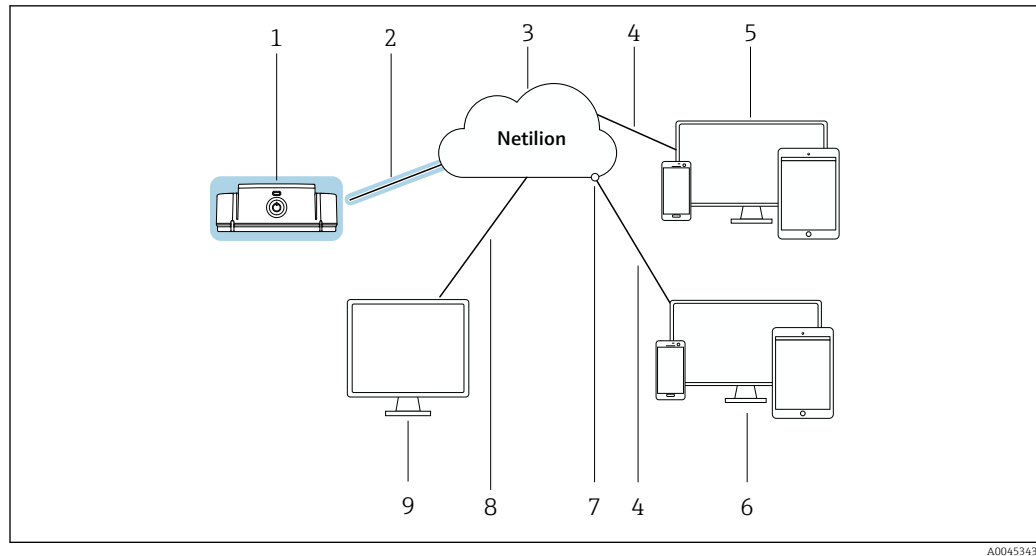
The Endress+Hauser Netilion Cloud is equipped with the following interfaces:

- https Internet connection
- Netilion Connect: Application Programming Interface (API)

The connections between the Micropilot FWR30 and Netilion Cloud are encrypted end to end with 2048-bit RSA in accordance with TLS 1.2. The connection is authenticated by means of a client certificate and a server certificate.

3.2.2 System design and system boundaries

 This Security Manual covers the Micropilot FWR30 and the cellular radio connection to the Netilion Cloud. Other components, such as the Endress+Hauser Netilion Cloud and operating tools, are not included in this Security Manual. The system boundaries are highlighted in color in the following diagram.



1 *Micropilot FWR30 system overview (color highlighting shows the system boundaries for this manual)*

- 1 *Micropilot FWR30*
- 2 *https cellular radio connection*
- 3 *Netilion Cloud*
- 4 *https Internet connection*
- 5 *Netilion Services: browser-based Netilion Service app*
- 6 *User application*
- 7 *Netilion Connect: Application Programming Interface (API)*
- 8 *https Internet connection*
- 9 *SupplyCare Hosting*

i The Micropilot FWR30 is generally referred to in this document as a product or terminal, 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 observed, 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 Micropilot FWR30 in free space, e.g. on a tank on a truck. Measures to combat physical tampering 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 Micropilot FWR30 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 Micropilot FWR30 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

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

The occurrence of multiple attacks on a product in an IIoT ecosystem causes anomalies in the data. If a product suddenly starts producing unrealistic values, this may indicate the occurrence of an attack.

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.

The Micropilot FWR30 is a terminal in the 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 other sections.

The commissioning of SupplyCare Hosting for the Micropilot FWR30 is carried out by the Endress+Hauser Service team.

 System overview of the Micropilot FWR30: →  7

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 →  8.

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.

It is not possible or necessary to harden the Micropilot FWR30. The Micropilot FWR30 uses only services required for the function.

4.4.4 Configuring user data

User data include, for example, login data, users, device tags (TAG), passwords, IDs, etc. No user data is stored in the Micropilot FWR30.

4.4.5 Security-related product settings

All security-related settings required for the Micropilot FWR30 were performed on the Micropilot FWR30 in the factory. No adjustments are required.

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 and the following sections.

The Micropilot FWR30 does not require any intervention during operation.

5.4 Security factors during operation

The validity period of the certificates stored in the Micropilot FWR30 is limited to five years.

Approximately one year before the certificates expire, Endress+Hauser renews the certificates for the Micropilot FWR30 via the Netilion Cloud. Log the Micropilot FWR30 into the Netilion Cloud at least once a year.

5.5 Update management

Endress+Hauser provides remote updates via the Netilion Cloud. The user must activate the update via the Netilion Cloud. The timing of the update is configurable. It is necessary to restart the Micropilot FWR30 following some of the updates. The restart is performed automatically.

Endress+Hauser provides remote updates in the following cases:

- security updates
- bug fixes: fixes for existing functions
- functional enhancements to the product
- renewal of certificates

Endress+Hauser uses checksums and signatures in the firmware to safeguard the integrity and authenticity of the updates. The user does not need to carry out integrity and authenticity checks on the updates.

5.6 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.

5.7 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.	▶ Disable the product by pressing and holding the button.
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 Endress+Hauser or destroy it.
The product requires a service from Endress+Hauser, e.g. calibration.	<ol style="list-style-type: none"> 1. Disable the product by pressing and holding the button. 2. Send the product to Endress+Hauser.
The product is defective and must therefore be disposed of.	▶ Disable the product by pressing and holding the button.
The product is to be disposed of.	▶ Disable the product by pressing and holding the button.

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. → 8 Where necessary, alternative measures have been taken into account. → 9	<input type="checkbox"/>
	Planning activities taken into account in engineering phase. Risk analysis and risk assessment completed. → 9	<input type="checkbox"/>
	Where possible, risk minimization measures have been taken into account. → 9	<input type="checkbox"/>
Incoming goods / transportation	Packaging checked to ensure it is unopened and seal is intact.	<input type="checkbox"/>
Commissioning	Product hardened for specific application. → 11	Not applicable
Operation	Update management requirements observed. → 13	<input type="checkbox"/>
	Recurring risk analysis planning completed. → 13	<input type="checkbox"/>
Decommissioning	Product taken out of service. → 15 Depending on reason for decommissioning, disable or destroy the product.	<input type="checkbox"/>

7.2 Version history

Document version	Firmware version	Hardware version	Changes
01.21	as of 01.00.01	Dev. Rev. 1 Dev. Rev. 2	First version



71574844

www.addresses.endress.com
