SD03029S/04/EN/03.25-00
71694012
2025-01-13

Special Documentation
Security Manual FieldEdge SGC500

Industrial edge device for connecting field devices to the Netilion Cloud

Endress+Hauser
People for Process Automation

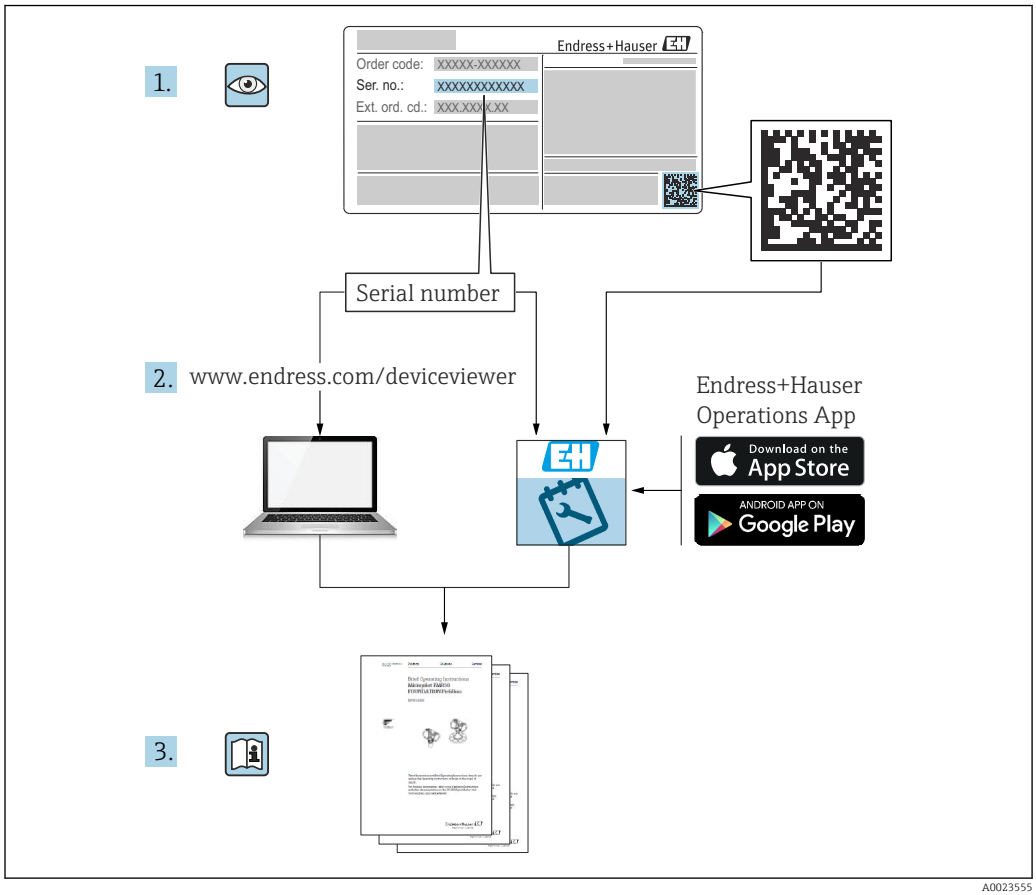

1.
Endress+Hauser
Order code: XXXXX-XXXXXX
Ser. no.: XXXXXXXXXXX
Ext. ord. cd.: XXX XXX XX
Serial number
2. www.endress.com/deviceviewer
Endress+Hauser
Operations App
Download on the App Store
ANDROID APP ON Google Play
3.
A0023555

Table of contents

1 Notification of security vulnerabilities and advisories

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

The web page includes the following information, for example:
- Current security alerts affecting Endress+Hauser products
- Contact information for reporting security vulnerabilities of Endress+Hauser products. PGP provides the option for confidential communication. You can download the public key from the website.
- 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

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 FieldEdge SGC500

- Technical Information TI01525S
- Operating Instructions BA02035S
- 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

This security manual describes the FieldEdge SGC500, the interface to the field device and the interface for the Endress+Hauser Netilion Cloud. It does not cover other components such as connected field devices, fieldbus gateways, the Endress+Hauser Netilion Cloud and operating tools. The system boundaries are marked in blue in the following diagrams.

Outbound calls to the Netilion Cloud are encrypted end-to-end in accordance with TLS 1.2. Netilion Cloud calls are authenticated - (OAuth 2.0).

Field of application

The FieldEdge SGC500 comprises an edge device and the Endress+Hauser software installed on it.

The FieldEdge reads information from the field devices, interprets the data and transmits the data to the Netilion Cloud via an Internet connection. The FieldEdge is intended for use in a cabinet in an access-controlled control room. Ideally, the FieldEdge is connected to the fieldbus network (OT) and the company network (IT) via two separate Ethernet cables.

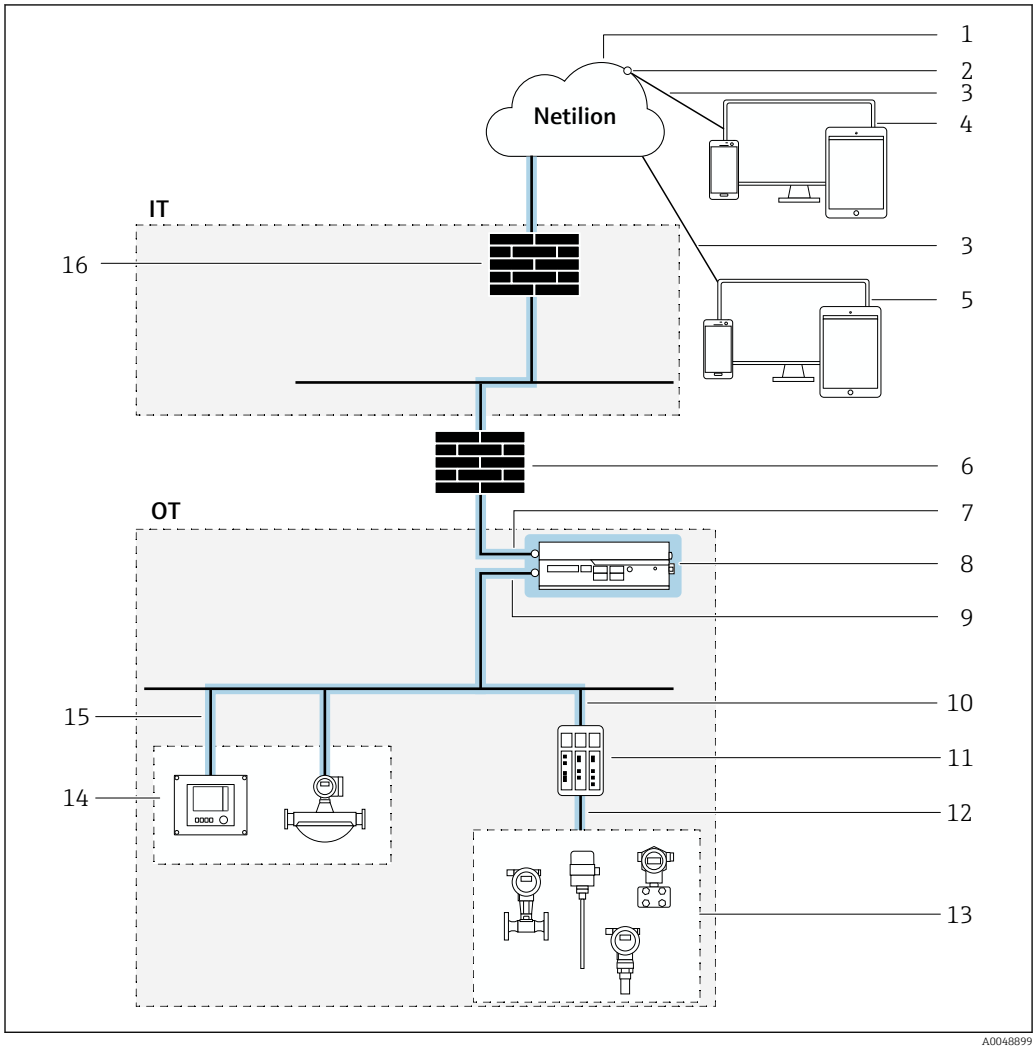
The Endress+Hauser software offers the following:
- Read-only connection to field devices via a variety of fieldbus protocols and field gateways.
  Optional field device write accesses are documented in Netilion Services and require user confirmation.
- Data processing and encrypted transmission of data exclusively to the Netilion Cloud.
- Specific data acquisition for the digital services the user has subscribed to in Netilion.
- Automatic updates run in the background: security updates, software modifications and functional enhancements.

No provisions are made for incoming communication from the Internet and it must be blocked in the firewall. Routing to the field network is not possible.

Information on settings for the firewall: → 20

3.2.2 Connection of the SGC500 via separate interfaces for Internet and fieldbus network

Connection of a fieldbus network



1 *Connecting the FieldEdge SGC500 via separate interfaces for Internet and fieldbus network (blue marking shows the system boundaries for this manual)*

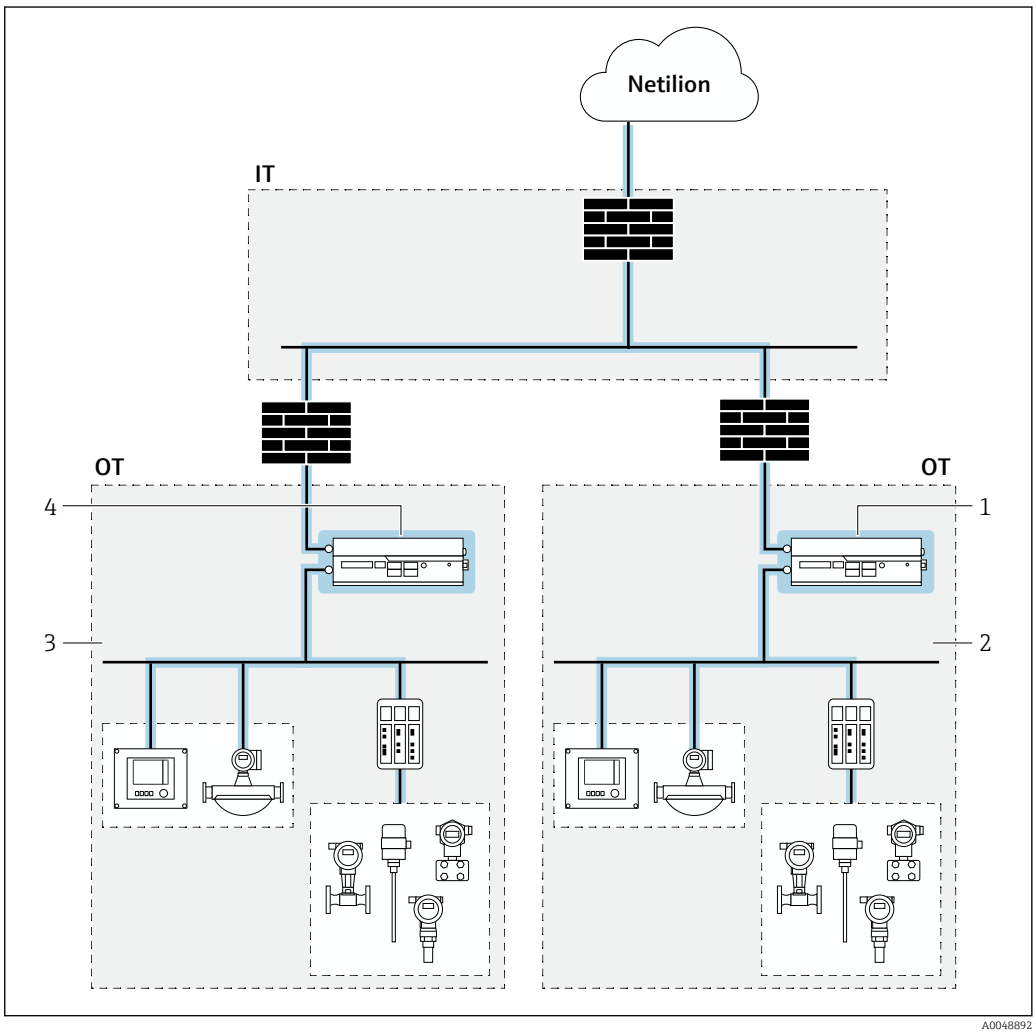
IT Information Technology (here): Company network for information processing, with Internet connection
OT Operational technology (here): Network for process automation
1 Netilion Cloud
2 Netilion Connect: Application Programming Interface (API)
3 https Internet connection
4 User system with user application
5 Netilion Services: browser-based Netilion Service app
6 System firewall
7 WAN Internet connection – https, plant-side connection
8 FieldEdge SGC500 reads field device data and transmits the data safely to the Netilion Cloud
9 Field network
10 Ethernet communication
11 Supported fieldbus gateways for conversion from a fieldbus protocol to an IP protocol
12 Fieldbus communication
13 Plant components such as Endress+Hauser field devices and field devices from other manufacturers
14 Ethernet protocol-based field devices
15 Industrial Ethernet
16 Company network firewall

The figure shows the FieldEdge SGC500 and all components involved in the flow of information that are necessary to record device status information and transmit the information to the Endress+Hauser Netilion Cloud.

The FieldEdge SGC500 is an edge device. Communication between the FieldEdge SGC500 and the plant components is based on Industrial Ethernet protocols such as HART/IP or proprietary protocols. The FieldEdge SGC500 only forwards the dedicated information requested by the FieldEdge from the subordinate plant components to the Netilion Cloud via the web address netilion.endress.com .

There is no general forwarding of data from the fieldbus network (OT) to the company network (IT). The operator must provide a firewall.

Connecting multiple fieldbus network segments



2 *Recommended segmentation for multiple fieldbus networks with multiple FieldEdge SGC500 (blue marking shows the system boundaries for this manual)*

1 *FieldEdge SGC500 for fieldbus network 1*
2 *Fieldbus network 1*
3 *Fieldbus network 2*
4 *FieldEdge SGC500 for fieldbus network 2*

The figure shows the recommended segmentation of a fieldbus network when two FieldEdge SGC500s are used. In this variant, two subordinate fieldbus networks are connected to the Netilion Cloud. Each fieldbus network (OT) is connected to the higher-level company network (OT) via its own FieldEdge SGC500. This wiring ensures that the two fieldbus network segments are isolated.

3.2.3 Segmented fieldbus networks

Network segmentation on the field side with VLANs, for example, is not supported.

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

Analysis of the operating environment for the product should give information on the security requirements that must be provided by the environment. For example, you may observe a denial-of-service attack.

Example of a typical operating environment of the product:
- 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.
- Personnel have been trained in how to use the product and the related 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 to authorized persons.
- Only authorized persons can access the product via the corresponding Human Machine Interface (HMI).

As the processing power of the product under observation is limited, the product can only defend against certain attacks to a limited extent.

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.

The FieldEdge is intended for use in an access-controlled control room in a building.

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 FieldEdge is an edge device that is used in 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.

Please note the following:
- The connection of the FieldEdge to the Internet must at least be via a firewall.
- The fieldbus network (OT) and company network (IT) must be strictly separated.
- Endress+Hauser recommends the segmentation of the fieldbus networks according to DIN IEC 62443-3-3. This can be achieved through the use of several FieldEdge units → 9.

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

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.

Please note the following:
- Only install FieldEdge in an access-controlled control room in a building
- Only grant employees the access rights they require to carry out their tasks
- If local configuration is required during commissioning, log in as described in the Operating Instructions → 6

3.7.4 Monitoring device data and device status

The FieldEdge is part of a network in a process automation system. Network monitoring on the field side is the responsibility of the plant operator.

The online status of the FieldEdge is shown in Netilion. You can access information on the availability of the Netilion Services via https://status.netilion.endress.com/.

3.7.5 Updating product software

Endress+Hauser automatically updates the software for the FieldEdge.

Update management: → 16

3.7.6 Protecting apps/applications

To safeguard the customer system, the customer data, the apps and the Web portal, it is also necessary to ensure the protection of FieldEdge access data that have access to the IIoT ecosystem. This can be accomplished by securely storing the access data and certificates.

During commissioning it may be necessary to configure the FieldEdge locally. The FieldEdge is protected via a login. The local configuration must be made temporarily via a directly connected Ethernet cable in the access-controlled control room.

For more information on "Login (manual connection)", see the Operating Instructions → 6

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.

FieldEdge SGC500 system overview: → 7

4.4.2 Required security steps during commissioning

Endress+Hauser products are delivered in packages that are sealed with an Endress+Hauser adhesive tape. A delivery note and a receipt with the Endress+Hauser logo are enclosed. A seal seals the housing and serves as a safety feature if the housing has been opened.

With regard to security, pay attention to the following during commissioning:
Integrate the product in the operating environment in accordance with the specified requirements → 10.

4.4.3 Configuring the firewall

No firewall is integrated in the FieldEdge. A firewall to the Internet must be provided on the customer side → 7.

For the FieldEdge, we recommend connecting to the Internet and the fieldbus network via separate interfaces → 8.

Configure the firewall as follows:
- Enable port 443 for the https service for outbound calls from the FieldEdge to the Netilion Cloud https://*.netilion.endress.com. Alternatively, enable the following URLs for a detailed firewall rule: https://api.netilion.endress.com and https://downloads.netilion.endress.com
- The Netilion Services are hosted on AWS Heroku. Note: You can block calls from the FieldEdge to other URLs in the firewall.
- You can check the firewall configuration in a Web browser via the URL https://api.netilion.endress.com. It must be possible to call this website when the firewall is active.
- All inbound calls to the FieldEdge must be blocked.

4.4.4 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 FieldEdge. The FieldEdge only uses services that are required for the function.

4.4.5 Configuring user data

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

Account for the Netilion Cloud

To connect the FieldEdge to the Netilion Cloud, an account is saved in encrypted format in the FieldEdge during configuration at the factory.

This account is used to authenticate the FieldEdge in the Netilion Cloud. Therefore, the information of the field devices that is saved in the Netilion Cloud is only available for the authenticated Netilion Account of the FieldEdge customer or an account authorized by the customer.

Information regarding accounts / access data

The following accounts are required for FieldEdge operation:
- Account for connecting the FieldEdge to the Netilion Cloud. Endress+Hauser saves this account in the FieldEdge in encrypted format during the factory configuration.
  This account cannot be changed.
- Account for the local configuration of the FieldEdge. A user name and a password are required for access via this account. (Access data: user name = "admin" and password = "FieldEdge serial number".)
  You cannot change the access data.
- Account for Netilion
  The users define the access data themselves and can also change this data.

For more information on "Login (manual connection)", see the Operating Instructions → 6

4.4.6 Security-related product settings

All security-related settings required for the FieldEdge have been implemented on the FieldEdge in the factory. No changes are required.

4.4.7 User management and impact on security

The FieldEdge implements the following user management to connect to the Netilion Cloud:

- User management for the FieldEdge provides for a user that is permanently configured ex works → 14
- Access to the local configuration is via a device-specific and pre-defined password → 14
- More advanced user management is not provided in the FieldEdge

For more information on Netilion Cloud user management, see the "Netilion – Terms of Service" document → 6

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 FieldEdge does not require any intervention during operation.

To be able to update the FieldEdge firmware, a permanent power supply to the FieldEdge and a permanent Internet connection to the Netilion Cloud must be ensured.

Update management: → 16

5.4 Security factors during operation

The following points must be noted during operation:
- The certificates saved in the FieldEdge have a limited life.
- Before they expire, Endress+Hauser renews the certificates automatically and remotely in the background via operating system updates → 16.
  Manual intervention on the part of the user is not required.

5.5 Update management

Endress+Hauser makes remote updates available via the Netilion Cloud. The timing of the update is set by Endress+Hauser. This cannot be influenced by the user. Some updates require the FieldEdge to be restarted. The restart is performed automatically.

As the FieldEdge does not interfere directly with the automation of the system, Endress +Hauser does not recommend any specific test routines for the application for the new software versions.

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.

You can determine the software version of the FieldEdge as follows: the software version currently loaded in the FieldEdge is shown in the Netilion Account under the SGC500 details for the SGC500 in question.

5.6 Functional enhancements

Once available, Endress+Hauser supplies functional enhancements to the FieldEdge unannounced. The timing of the function enhancement is set by Endress+Hauser. This cannot be influenced or blocked by the user.

Functional enhancements can include the following:
- Improvement to existing services
- Support for new bookable services

5.7 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.

5.8 Repair and disposal

5.8.1 Troubleshooting and repair

Troubleshooting

Proceed as follows if a fault occurs in the FieldEdge:

1. Sign in to Netilion.
2. Create a support ticket via Netilion. Netilion > Select a Service > Netilion > Main Menu > Support Create a ticket
   ↳ The support ticket is sent to Endress+Hauser Service.
   Endress+Hauser Service analyzes the problem and identifies the measures that need to be taken.
   If Endress+Hauser Service finds that the FieldEdge is defective, follow the instructions outlined below → 17.

FieldEdge is defective

Endress+Hauser Service found that the FieldEdge is defective and needs to be replaced. Endress+Hauser Service will send you a preconfigured replacement device.

Furthermore, you are requested to return the defective FieldEdge to Endress+Hauser or to destroy and dispose of the defective FieldEdge.

Proceed as follows if the FieldEdge is defective:

1. After being instructed by Endress+Hauser Service, delete the access data from the FieldEdge to the Netilion Cloud from the defective FieldEdge.
2. In Netilion, delete or reset the data on the following pages: "Network Interface Details", "Field Gateways" and / or "EtherNet/IP Activation Status"
3. Depending on the instructions of Endress+Hauser Service: return the defective FieldEdge immediately to Endress+Hauser or destroy the defective FieldEdge and dispose of it.

4. Connect, configure and commission the new FieldEdge as specified in the Operating Instructions.

We recommend you delete your access data / user data from the FieldEdge if you have to take the FieldEdge out of service due to a defect. By deleting your data, you are preventing any improper use of your data.

5.8.2 Disposal

Proceed as follows if you have to dispose of the FieldEdge:

1. After being instructed by Endress+Hauser Service, delete the access data from the FieldEdge to the Netilion Cloud from the defective FieldEdge.
2. In Netilion, delete or reset the data on the following pages: "Network Interface Details", "Field Gateways" and / or "EtherNet/IP Activation Status"
3. Destroy the defective FieldEdge and dispose of it. Observe the following instructions.

- We recommend you delete your access data / user data from the FieldEdge if you have to dispose of the FieldEdge. By deleting your data, you are preventing any improper use of your data.
- Before you dispose of, or scrap, the FieldEdge, we recommend that you proceed in accordance with the following guideline: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

As required by the Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), Endress+Hauser products are marked with the depicted symbol in order to minimize the disposal of WEEE as unsorted municipal waste. Such products may not be disposed of as unsorted municipal waste and can be returned to Endress+Hauser for disposal under the conditions stipulated in the General Terms and Conditions or as individually agreed by Endress+Hauser.

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 should be removed from the subscription.	1. Delete the customer-specific network data for the FieldEdge on the "Network Interface Details" page in Netilion. 2. Select the FieldEdge on the "Field Gateways / Devices" page in Netilion. 3. Tap on "Delete" on the "Edge Device Details" page. ↳ A dialog opens. 4. Confirm deletion of the FieldEdge.
The product is not being used for a prolonged period of time.	No measures required.
The product has a fault that you are unable to rectify.	Contact Endress+Hauser Service and follow the instructions of Endress+Hauser Service→ 🖹 17.
The product is defective and must therefore be disposed of. The defect has been identified by Endress+Hauser Service → 🖹 17.	Information on product disposal: → 🖹 18
The product is to be disposed of. You want to dispose of the product.	Information on product disposal: → 🖹 18
The Netilion Service Subscription has terminated.	To protect your data and/or your system from access, we recommend you scrap the FieldEdge. To do this, we recommend you proceed in accordance with the following guidelines: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization If you do not want to scrap the FieldEdge, we recommend you delete the software from the FieldEdge immediately. Contact Endress+Hauser Service for further information. After consultation with Endress+Hauser Service, you can return the FieldEdge.

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. → 🖹 10 Where necessary, alternative measures have been taken into account. → 🖹 10	❑
	Planning activities taken into account in engineering phase. Risk analysis and risk assessment completed.→ 🖹 10	❑
	Where possible, risk minimization measures have been taken into account. → 🖹 11	❑
Incoming goods/ transportation	Packaging checked to ensure it is unopened and seal is intact. → 🖹 13	❑
Commissioning	Product hardened for specific application. → 🖹 14	Not applicable
Operation	Update management requirements observed. → 🖹 16	❑
	Recurring risk analysis planning completed. → 🖹 17	❑
Decommissioning	Product taken out of service. → 🖹 19 Depending on reason for decommissioning, disable or destroy the product.	❑

7.2 Version history

Document version	Firmware version	Hardware version	Changes
SD03029S/04/EN/01.22-00	As of 3.00.02	Dev. Rev. 1	First version
SD03029S/04/EN/02.23-00	As of 3.00.02	Dev. Rev. 1	Modbus TCP added. "Appendix" section added.
SD03029S/04/EN/03.25-00	As of 3.04.01	Dev. Rev. 1	PROFINET added. Tankvision Tank Scanner NXA820 added.

7.3 Information for security audits

7.3.1 Services required for operation

The services listed in this section are required for FieldEdge operation.

Services for connection to the Endress+Hauser Netilion Cloud

The services listed in the following table must be available or enabled in the firewall, depending on the network structure.

Service	Port	Comment
https	443	Transmission of the field information to the Netilion Cloud
DNS	53/853	It must be possible to reach a TCP-DNS server with the current address resolution.
UDP DHCP (IPv4)	67	Bootstrap Protocol (BOOTP) server, also used by DHCP
TCP/UDP (IPv6)	547	DHCPv6 server

Services for connection to the fieldbus network

To support future fieldbus gateways or Industrial Ethernet networks, you may have to enable additional services on the field device side.

Service	Port	Comment
TCP/IP http	80	Temporary use during initial commissioning
SSH	22 SSH	This service is only used for forensic analysis in the event of a defective FieldEdge. SSH is secured by a private key. The private key is only available on Endress+Hauser development PCs. Endress+Hauser does not provide for access via SSH during operation. We recommend you block this service in the company firewall.
TCP/UDP	–	Specific communication via fieldbus gateway ▪ Service for communication via PROFIBUS Fieldgate SFG500: → 🖹 22 ▪ Service for communication via HART Fieldgate SFG250: → 🖹 21 ▪ Service for communication with the WirelessHART Fieldgate SWG70: → 🖹 22 ▪ Specific communication for Ethernet-based protocols: → 🖹 21
UDP DHCP	67	Bootstrap Protocol (BOOTP) server, also used by DHCP
TCP/UDP (IPv6)	547	DHCPv6 server

Service for remote updates via the LAN1 network

In the case of remote updates, Endress+Hauser makes sure that only services required for the service are executed.

Service	Port	Comment
https	443	The updates of the FieldEdge SGC500 are transmitted to the FieldEdge in a response to a request via https (port 443).

7.3.2 Services that depend on the application

Service for communication via EtherNet/IP network

The connection is always established from the FieldEdge SGC500 to the EtherNet/IP field devices.

Service	Port	Comment
TCP/UDP	44818	Recommended manufacturer default settings: see ODVA specification 5-4.3.2.13.1 CIP Security Considerations The necessary manufacturer default settings for products that support EtherNet/IP over (D)TLS.
TCP/UDP	2221	

Service for communication via HART Fieldgate SFG250

The connection is always established from the FieldEdge SGC500 to the Fieldgate SFG250.

Service	Port	Comment
TCP/UDP	5094	Default HART/IP port

Service for communication via Modbus TCP

The connection is always established from the FieldEdge SGC500 to the Modbus TCP field device.

Service	Port	Comment
TCP	512	Default Modbus TCP port

Service for communication via PROFIBUS Fieldgate SFG500

The connection is always established from the FieldEdge SGC500 to the Fieldgate SFG500.

Service	Port	Comment
TCP	80	Use for requests from the Fieldgate
TCP/IP	60010	Use for requests from the Fieldgate

Service for communication via PROFINET

The connection is always established from the FieldEdge SGC500 to the PROFINET field devices.

Service	Port	Comment
UDP	34964	PROFINET RPC Context Manager
UDP	53247	PROFINET RPC client/server

Service for communication via Tankvision Tank Scanner NXA820

The connection is always established from the FieldEdge SGC500 to the Tankvision Tank Scanner NXA820.

Service	Port	Comment
TCP	80	Identification and designation of the tank names used
TCP/IP	3000	Default HART tunnel for access to connected HART field devices

Service for communication with the WirelessHARTFieldgate SWG50 and SWG70

The connection is always established from the FieldEdge SGC500 to the Fieldgate SWGxx.

Service	Port	Comment
TCP/UDP	5094	Default HART/IP port

www.addresses.endress.com

Endress+Hauser

People for Process Automation