SD03377C/07/EN/01.24-00
71700057
2024-12-11

Special Documentation
Liquiline edge module CYY7

Connection to Netilion via cellular radio or Ethernet
Cellular radio/Ethernet version (EMR) and Ethernet version (EME)
Security Manual

Endress+Hauser
People for Process Automation

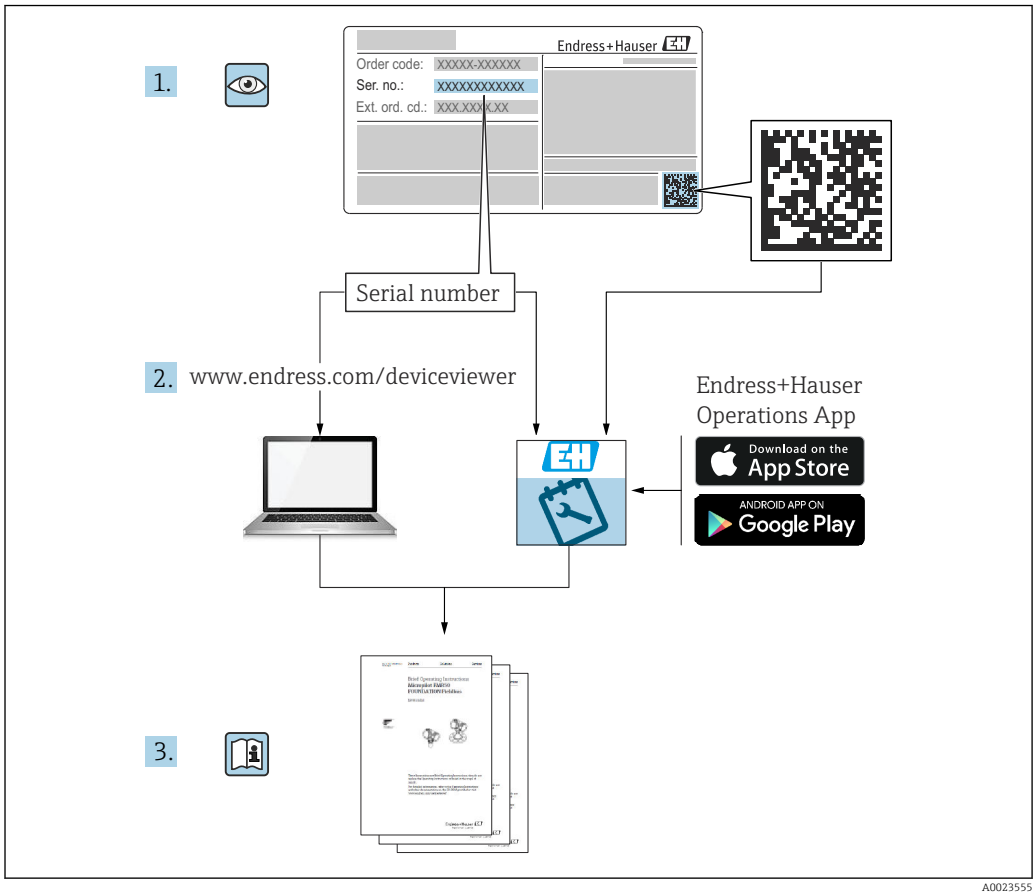

1.
Endress+Hauser
Order code: XXXXX-XXXXXX
Ser. no.: XXXXXXXXXXX
Ext. ord. cd.: XXX XXX XX XX
Serial number
2. www.endress.com/deviceviewer
Endress+Hauser
Operations App
Download on the App Store
ANDROID APP ON Google Play
3.
A0023555

Table of contents

1 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 Notification of security vulnerabilities and safety instructions

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 safety instructions for Endress+Hauser products
- Endress+Hauser contact information: PSIRT@endress.com

3 About this document

3.1 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.

3.2 Warnings

Structure of information	Meaning
⚠ DANGER **Causes (/consequences)** If necessary, Consequences of non-compliance (if applicable) ▶ Corrective action	This symbol alerts you to a dangerous situation. Failure to avoid the dangerous situation **will** result in a fatal or serious injury.
⚠ WARNING **Causes (/consequences)** If necessary, Consequences of non-compliance (if applicable) ▶ Corrective action	This symbol alerts you to a dangerous situation. Failure to avoid the dangerous situation **can** result in a fatal or serious injury.
⚠ CAUTION **Causes (/consequences)** If necessary, Consequences of non-compliance (if applicable) ▶ Corrective action	This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or more serious injuries.
NOTICE **Cause/situation** If necessary, Consequences of non-compliance (if applicable) ▶ Action/note	This symbol alerts you to situations which may result in damage to property.

3.3 Symbols

- Additional information, tips
- Permitted
- Recommended
- Forbidden or not recommended
- Reference to device documentation
- Reference to page
- Reference to graphic
- Result of a step

3.4 Documentation

Observe the Netilion policies:
- 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

4 System design

4.1 Target group

This section is aimed at planners and system integrators.

4.2 General information

This security manual describes the Liquiline edge module CYY7, the interface to the field device and the interface for the Endress+Hauser Netilion cloud platform. Other components, such as control components, the Endress+Hauser Netilion cloud platform and operating tools, are not included in this Security Manual. The system boundaries are marked in blue in the following diagrams. Outgoing connections to the Netilion cloud platform are encrypted end-to-end according to TLS 1.2 and use mutual authentication (mTLS) by means of TLS certificates.

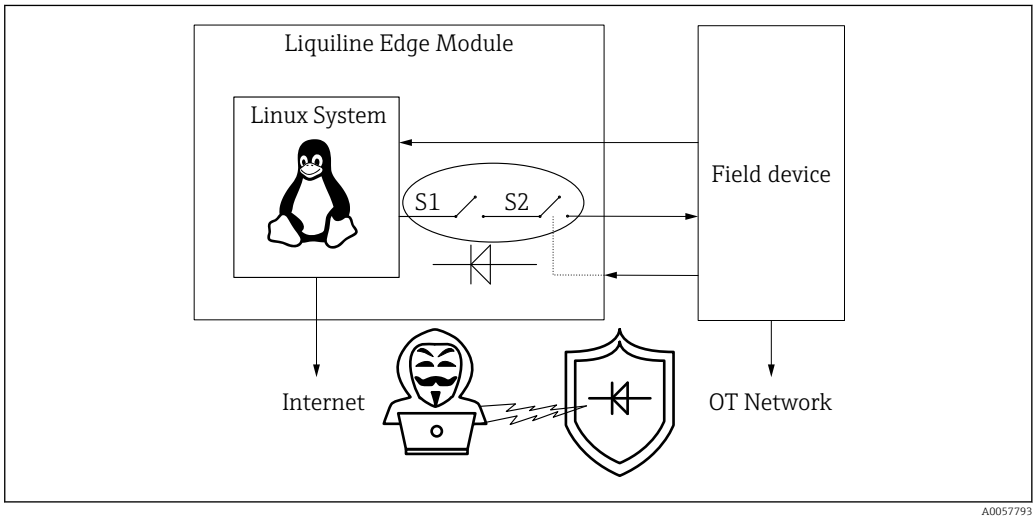
The Liquiline edge module is operated as a plug-in module in a field device and connects this field device to the Netilion cloud platform from Endress+Hauser. This connection requires an Internet connection that is either established via Ethernet or a cellular network. In order to operate the field device safely and without affecting communication with the Internet, various measures are required in addition to the security mechanisms provided by the Liquiline edge module.

The Liquiline edge module uses various mechanisms to achieve a high level of protection:
- Secure Boot
- A/B firmware update
- Encrypted file system
- Secure key storage
- Encrypted HTTPS connection with two-factor authentication (mTLS)
- No back doors or service access

The field device can be affected if, despite these measures, an attacker succeeds in taking over the Liquiline edge module. In order to protect the field device in this case, the data communication from the Liquiline edge module to the field device can be limited or blocked.

The field device can always send data to the Liquiline edge module.

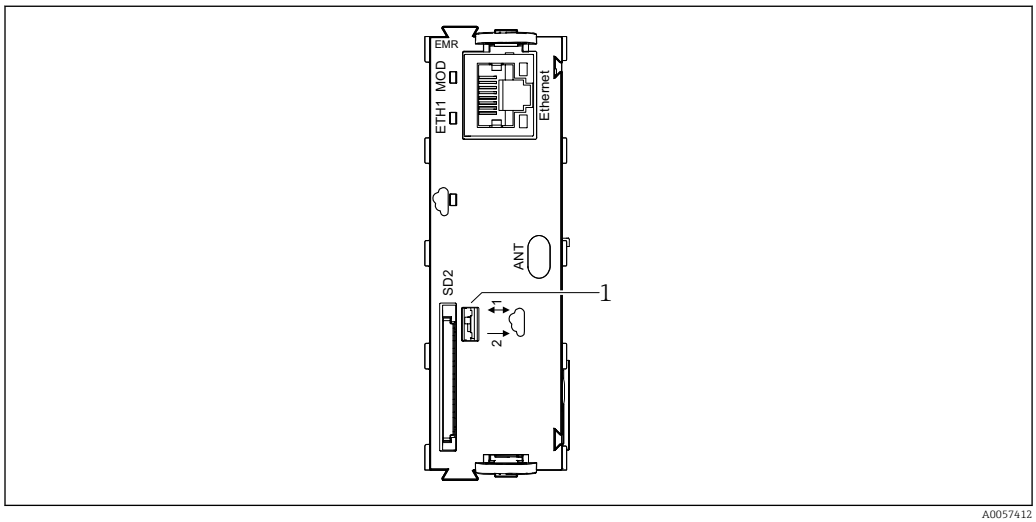
The data direction from the Liquiline edge module can be restricted in several stages. This is done by setting up a series of two S1 and S2 switches in the data signal line from the Liquiline edge module to the field device. The S1 switch is mechanical and can be operated via the module orifice plate. The S2 switch is electronic and is controlled from the field device.



A0057793

When delivered, the S1 and S2 switches are closed to enable bidirectional communication between the field device and the Liquiline edge module.

When the mechanical switch S1 is open, no data communication from the Liquiline edge module to the field device is possible.



1 Edge module

1 S1 mechanical switch: Bidirectional/unidirectional data transmission. Switch position 1: Closed. Switch position 2: Open.

When the S1 mechanical switch is closed, data communication from the Liquiline edge module to the field device can be restricted or blocked via the S2 electronic switch. For configuration options, see the Operating Instructions of the Liquiline edge module.

Path: **Menu/General settings/Extended setup/Edge module/Security/Bidir. data transfer**

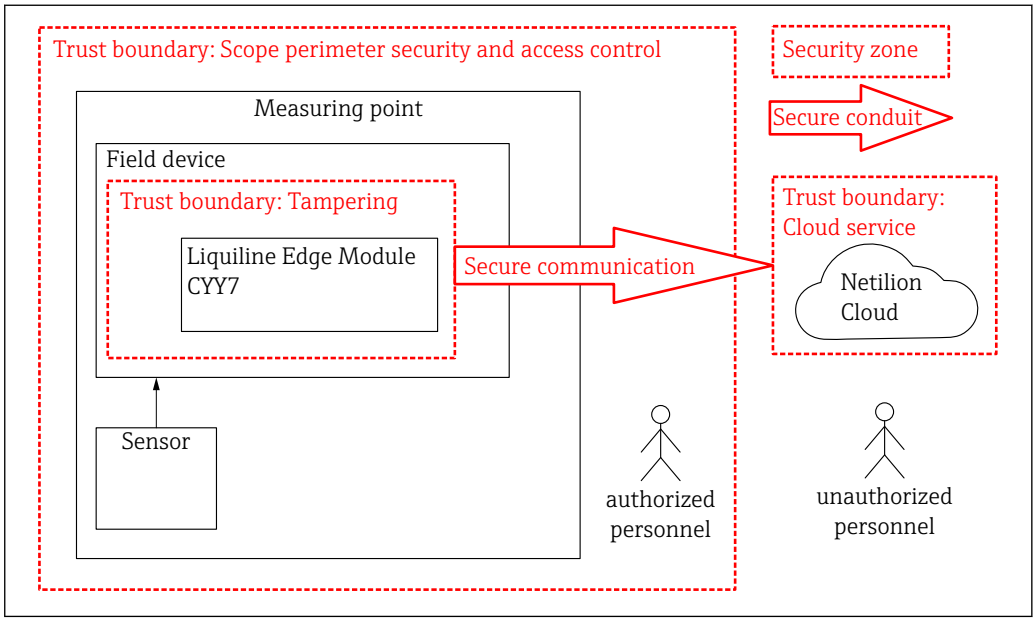
As a user of the Liquiline edge module, you must take the following measures as a minimum: - Access protection to prevent physical attacks (tampering) - Note the requirements from this document

The following measures are required by the customer:

1. Ensure access protection to prevent physical attacks (tampering).
2. Observe the requirements of this document.

4.3 System overview

4.3.1 System design and system boundaries



The system structures and system boundaries (trust zones) necessary for the safety consideration differ depending on whether communication with the Netilion cloud platform is via Ethernet or cellular radio.

Netilion connection via Ethernet

Obtain the IPv4 address of the edge module automatically from the DHCP server (factory setting):

- Navigate to the path: **Menu/General settings/Extended setup/Edge module/ Ethernet ETH1/IP settings/Automatic (DHCP)**

Manually enter the IPv4 address for the edge module:

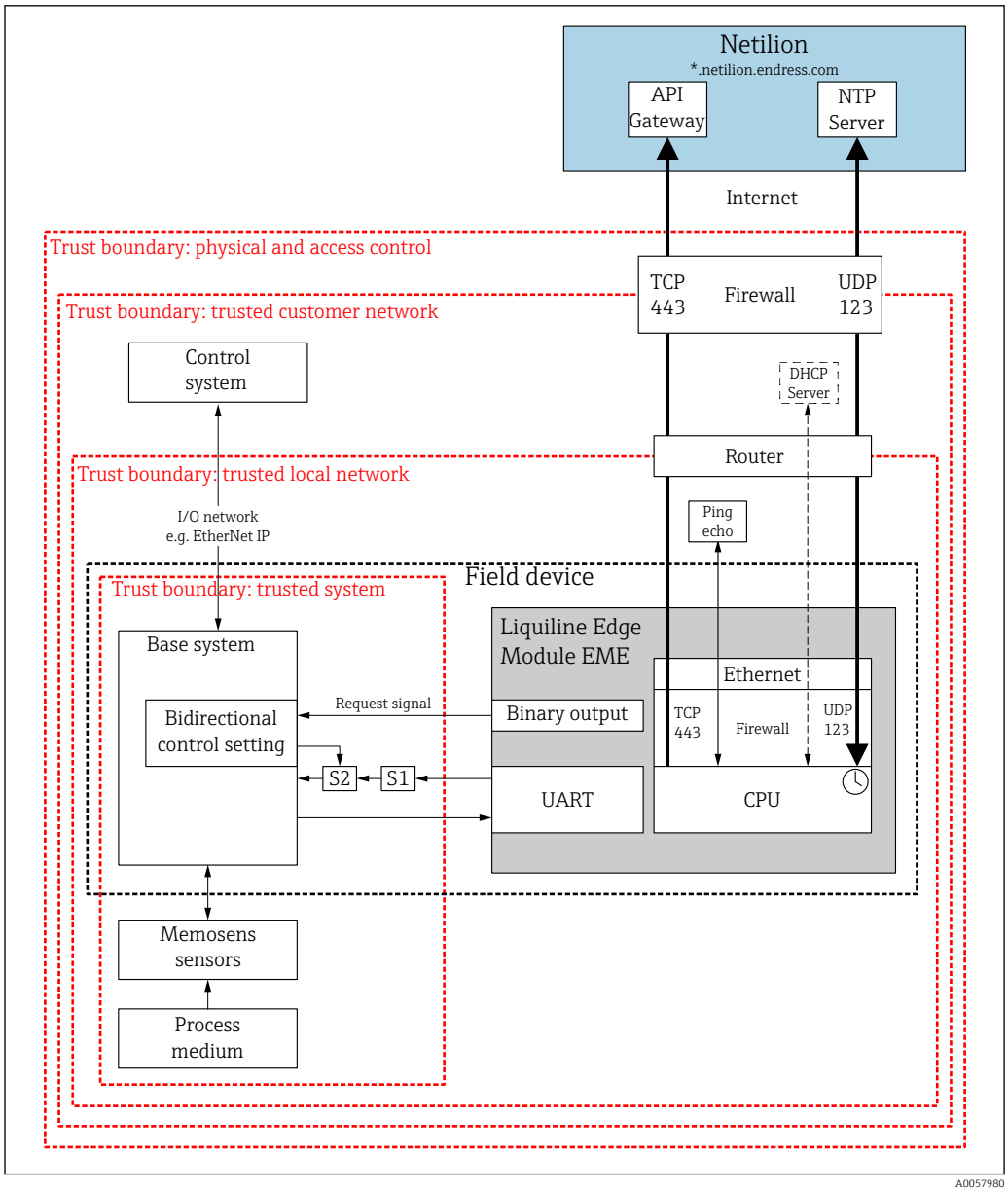
1. Navigate to the path: **Menu/General settings/Extended setup/Edge module/ Ethernet ETH1/IP settings/Manual (static)**
2. Enter the **IP address**, **Netmask**, **Gateway** and **DNS** via the menu.
3. Accept using the softkey **SAVE**.

Firewall configuration:

1. All incoming connections to the edge module must be blocked via a customer firewall.
2. Enable TCP port 443 for outgoing HTTPS connections **dis.lem.netilion.endress.com**.
3. Enable UDP port 123 for **time.netilion.endress.com**.

Check the firewall configuration:

- Call up the URL https://api.netilion.endress.com via a web browser. It must be possible to access this page if the firewall is activated.



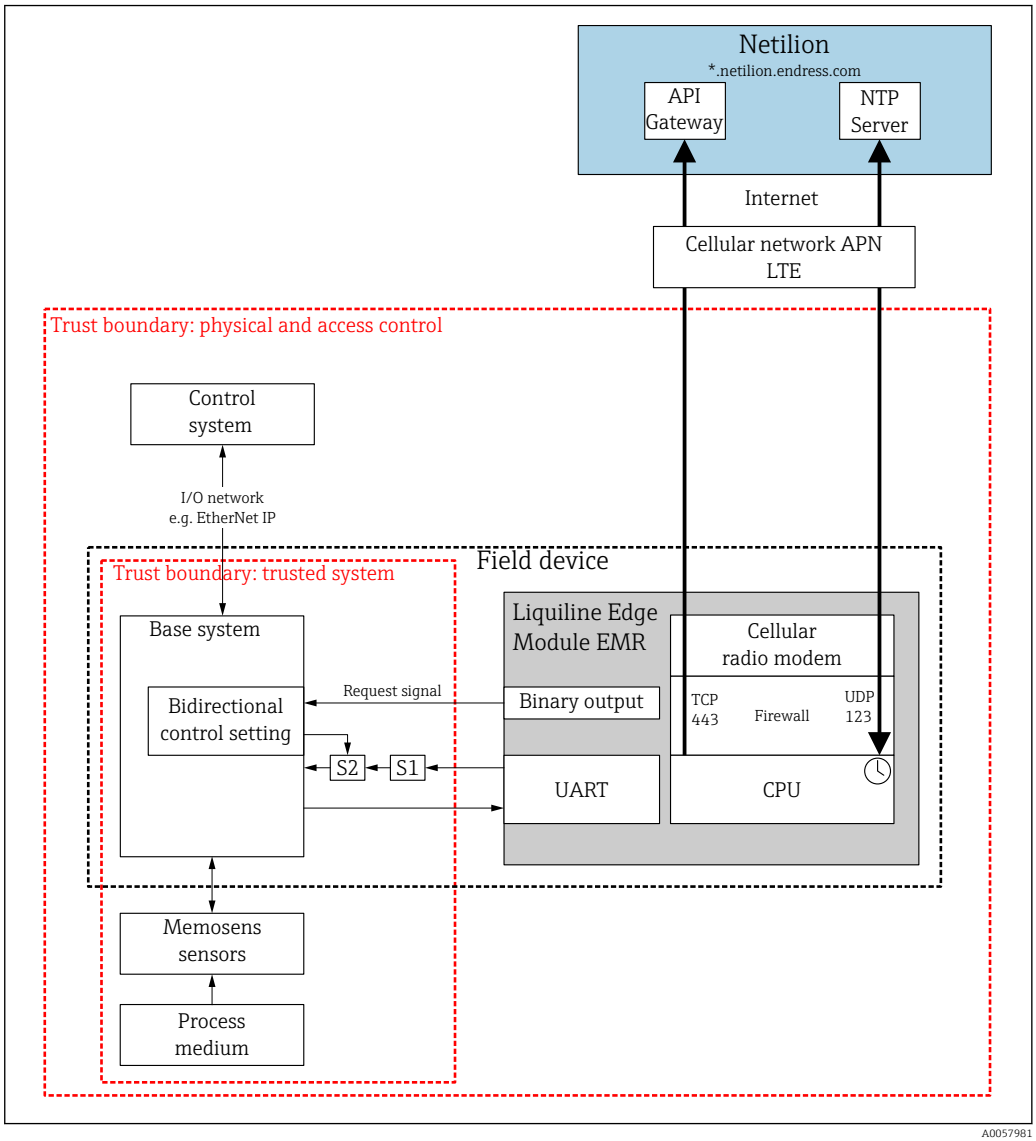
Ping requests are only answered by the edge module if one of the following conditions is met:
- The source IP of the ping is in the IPv4-subnet of the Ethernet interface
- The source IP of the ping comes from the address range for Intranet IPs (RFC 1918)

The Liquiline edge module does not accept incoming connections.

After booting up, the Liquiline edge module synchronizes its time with one of Endress +Hauser's NTP servers. Afterwards, an HTTPS mTLS 1.2 connection to Netilion is set up. The TLS connection uses two-factor authentication. Each edge module uses an individual client certificate that is validated by the Netilion API gateway. The edge module checks the server certificate of the Netilion cloud platform. The client certificates have a duration of five years and are renewed automatically no later than 90 days before the expiry.

If the field device diagnostics indicate a certificate error, contact the Endress+Hauser Service Team.

Netilion connection via cellular radio



After booting up, the edge module establishes an Internet connection via a cellular network (LTE-M or NB-IoT) and synchronizes its time with one of Endress+Hauser's NTP servers. Afterwards, a TLS 1.2 connection to the Netilion cloud platform is established. The TLS connection uses two-factor authentication. Each edge module uses an individual client certificate for this purpose. The Liquiline edge module checks the server certificate of the API gateway for the Netilion cloud platform. The client certificates have a duration of five years and are automatically renewed before the expiry.

If the field device diagnostics indicate a certificate error, contact the Endress+Hauser Service Team.

4.4 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.

4.5 Typical operating environment of the product

The edge module has been designed and optimized for the following operating conditions. If the operating environment differs, take additional protective measures if necessary. In the product security context, the edge module is considered a networking device since it transmits data from one security zone to another.

The edge module is mainly used in water/wastewater treatment plants where unauthorized access is physically restricted. Within the perimeter, there is unlikely to be any additional restrictions on access (no cabinets or designated areas), such that the staff inside the trust zone is usually authorized by the plant operator and responsible for ensuring that the device is not tampered with.

4.6 Measures if the required operating environment cannot be provided

Insofar as the specified requirements for the operating environment cannot be met, put in place alternative measures if necessary. This may involve, for example, mechanical protection of the product against tampering, mechanical protection of the cabling, or organizational measures.

Measures to combat physical tampering must be arranged by the customer.

4.7 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.

4.8 Recommended risk minimization measures

4.8.1 Analyzing the whole system

The edge module is an IIoT gateway 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 components. Every deviating component represents a new potential vulnerability in such heterogeneous integrated solutions and it may be exploited by an attacker.

4.8.2 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.

4.8.3 Optimizing access management

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

- Employees should only be given access authorization that is required for the employee to carry out their work
- User accounts should only be issued with strong passwords
- Generate, save and administer passwords using a password manager

4.8.4 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 checking regularly to see if new updates are available and to install any updates. Missed updates represent an acute security risk as attackers could have information on the vulnerabilities that are being rectified.

Firmware updates can be installed via Netilion or via SD card.

It is not possible to downgrade to legacy firmware versions.

The firmware update can be scheduled in Netilion. Schedule the remote firmware update so that the field device is not disconnected from the network or restarted for at least 30 minutes at the scheduled time. The time from planning to update installation must be at least 24 hours. During this time, the firmware is transferred to the edge module. The firmware update starts at the planned time.

During the firmware update, the edge module restarts and performs self-tests with the new firmware. In the event of an error, the previously installed firmware version is restored. The firmware update can be tried again

4.8.5 Protecting applications and apps

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 control system or the terminal.

Protection of the login details for the terminals should also be ensured in order to protect the customer system and customer data. Keep login details and certificates safe.

5 Commissioning

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 Installation

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

To prevent physical access to the device, we recommend installing the device in a lockable control cabinet or in a room with restricted access.

We also recommend implementing other external measures such as a network segmentation, firewalls, an intrusion detection system and perimeter protection.

5.4 Protecting the product against access by unauthorized persons

5.5 Configuration

5.5.1 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 additional sections.

5.5.2 Required steps during commissioning

Depending on the customer's specifications, configure the security settings during commissioning:

- Via the mechanical "bidirectional/unidirectional data transmission" switch
- Via the security parameters of the edge module

When performing maintenance work, make sure that if the security settings are temporarily changed, they are restored in accordance with the specifications. For further information, see the Operating Instructions of the edge module.

5.5.3 Configuring the firewall

For operation via Ethernet, a firewall to the Internet must be provided by the customer.

Required firewall configurations:
- All incoming calls to the edge module must be blocked.
- Enable TCP port 443 for outgoing HTTPS connections to **dis.lem.netilion.endress.com**.
- Enable UDP port 123 for **time.netilion.endress.com**.

Check the firewall configuration:
Call up the URL https://api.netilion.endress.com via a web browser. It must be possible to access this page if the firewall is activated.

5.5.4 Hardening the product

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

It is not possible or necessary to harden the edge module. The edge module only uses services that are required for the function.

5.5.5 Configuring user data

User data includes login data, for example. No user data is stored in the edge module. Data in the buffer memory of the edge module is automatically deleted if the edge module is plugged into another field device.

5.5.6 Security-related product settings

All security-related settings required for the edge module have been implemented in the factory. No adjustments are required.

For settings relating to the operational safety of the field device, see → 14.

6 Operation

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 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.

Check whether there are updates for the edge module firmware at regular intervals and perform these updates.

6.4 Security aspects during operation

If the edge module is connected to the Netilion cloud platform, its TLS certificate will be renewed automatically 90 days before the expiry.

If the certificate expires while the edge module is offline, the expired certificate is accepted for the issue of a new certificate and automatically replaced. This does not apply if the certificate has been revoked. In this case, you must contact the Endress+Hauser Service Team.

6.5 Update management

Endress+Hauser provides remote updates via the Netilion cloud platform. The user must activate the update via the Netilion cloud platform. The timing of the update can be adjusted. During all updates, the edge module is automatically restarted. The operation of the field device is not affected.

Endress+Hauser provides updates for the following cases:
- Security updates
- Bug fixes: Troubleshooting of existing functions
- Functional product upgrades
- 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.

In addition, updates can be installed using an SD card.

6.6 Functional upgrades

Once available, Endress+Hauser supplies functional upgrades to the Netilion cloud platform unannounced. The timing of the function upgrade is set by Endress+Hauser. This cannot be influenced or blocked by the user.

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

6.7 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.

6.8 Repair and disposal

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

7 Decommissioning

7.1 Target group

This section is aimed at operating personnel.

7.2 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.

7.3 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 prolonged period of time.	▶ No action required.
The product has a fault that you are unable to rectify.	▶ Contact Endress+Hauser.
The product is to be disposed of or sold.	▶ Before disposing of or selling the product, delete the Netilion asset of the edge module. To do so, you will need the login details for the Netilion account.

8 Appendix

8.1 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. Where necessary, alternative measures have been taken into account.	❑
	Planning activities taken into account in engineering phase. Risk analysis and risk assessment completed.→ 🖹 12	❑
	Where possible, risk minimization measures have been taken into account.	❑
Incoming goods / transportation	Packaging checked to ensure it is unopened and seal is intact.	❑
Commissioning	Product hardened for specific application.	Not applicable
Operation	Update management requirements observed.	❑
	Recurring risk analysis planning completed. → 🖹 17	❑
Decommissioning	Product taken out of service. Depending on reason for decommissioning, disable or destroy the product.	❑

8.2 7.2 Requirements of IEC62443-4-2

In accordance with NAMUR recommendation NE177, this product meets the following requirements of IEC 62443-4-2 according to the "NOA Security Gateway Basic" protection profile.

"Status" column legend:
- ✔: Satisfied
- (✔): Not applicable
- ✗: Not satisfied

Requirement	Status	Explanation
CR 1.1 Human user identification and authentication	(✔)	No human user interface present.
CR 1.1 RE (1) Unique identification and authentication	(✔)	See CR1.1
CR1.2 Software process and device identification and authentication	✔	
CR 1.3 Account management	(✔)	See CR1.1
CR 1.4 Identifier management	(✔)	No identifier or identifier management present as there is no interface to the user network. Mutual identification for communication with Netilion using the certificates generated by Endress+Hauser.
CR 1.5 Authenticator management	(✔)	Device-specific key pairs for authentication via asymmetric cryptography are stored and protected and cannot be replaced.
CR 1.5 RE (1) Hardware security for authenticators	(✔)	See CR1.5
NDR 1.6 Wireless access management	(✔)	No wireless interface available to access this product.

Requirement	Status	Explanation
NDR 1.6 RE (1) Unique identification and authentication	(✔)	See NDR1.6
CR 1.7 Strength of password-based authentication	(✔)	See CR1.1
CR 1.10 Authenticator feedback	(✔)	See CR1.1
CR 1.11 Unsuccessful login attempts	(✔)	See CR1.1
CR 1.12 System use notification	(✔)	See CR1.1
NDR 1.13 Access via untrusted networks	✔	
CR 1.14 Strength of symmetric key-based authentication	(✔)	See CR1.5
CR 2.1 Authorization enforcement	(✔)	See CR1.1
CR 2.1 RE (1) Authorization enforcement for all users (humans, software processes and devices)	✔	
CR 2.1 RE (2) Permission mapping to roles	(✔)	See CR1.1
CR 2.1 RE (3) Supervisor override	(✔)	See CR1.1
CR 2.2 Wireless use control	(✔)	See NDR1.6
EDR 2.4 Mobile code	(✔)	There is no way to provide or complete command files, scripts, macros or other code.
EDR 2.4 RE (1) Mobile code authenticity check	(✔)	See EDR2.4
CR 2.5 Session lock	(✔)	Do not use sessions.
CR 2.6 Remote session termination	(✔)	See CR 2.5
CR 2.8 Auditable events	✗	As there is no human user interface present, local logbook functionality is not implemented.
CR 2.9 Audit storage capacity	(✔)	See CR2.8
CR 2.10 Response to audit processing failures	(✔)	See CR2.8
CR 2.11 Timestamps	✔	
CR 2.12 Non-repudiation	(✔)	See CR1.1
EDR 2.13 Use of physical diagnostic and test interfaces	✔	
CR 3.1 Communication integrity	✔	
CR 3.1 RE (1) Communication authentication	✔	
EDR 3.2 Protection from malicious code	(✔)	See EDR 2.4
CR 3.3 Security functionality verification	✗	Security mechanisms are always active and cannot be disabled.
CR 3.4 Software and information integrity	✗	See CR 3.3
CR 3.4 RE (1) Authenticity of software and information	(✔)	See 3.4
CR 3.5 Input validation	✔	
CR 3.6 Deterministic output	✔	
CR 3.7 Error handling	✔	
CR 3.8 Session integrity	(✔)	See CR 2.5
CR 3.9 Protection of audit information	(✔)	See CR 2.8
EDR 3.10 Support for updates	✔	
EDR 3.10 RE (1) Update authenticity and integrity	✔	
EDR 3.12 Provisioning product supplier roots of trust	✔	

Requirement	Status	Explanation
EDR 3.13 Provisioning asset owner roots of trust	(✔)	No operator service available that requires an operator root of trust.
EDR 3.14 Integrity of the boot process	✔	
EDR 3.14 RE(1) Authenticity of the boot process	✔	
CR 4.1 Information confidentiality	✔	
CR 4.2 Information persistence	✔	
CR 4.3 Use of cryptography	✔	Use of TLS1.2 (e.g. RSA3072, P256, AES) for secure connection to the Netilion cloud platform.
CR 5.1 Network segmentation	✔	
NDR 5.2 Zone boundary protection	✔	
NDR 5.2 RE(1) Deny all, permit by exception	✔	
NDR 5.3 General purpose, person to-person communication restrictions	✔	
CR 6.1 Audit log accessibility	(✔)	See CR 2.8
CR 6.2 Continuous monitoring	✘	No continuous monitoring by device.
CR 7.1 Denial of service protection	✔	The load that can be entered is limited.
CR 7.1 RE (1) Manage communication load from component	(✔)	See CR 7.1
CR 7.2 Resource management	✔	
CR 7.3 Control system backup	✔	
CR 7.3 RE (1) Backup integrity verification	✔	
CR 7.4 Control system recovery and reconstitution	✔	
CR 7.6 Network and security configuration settings	(✔)	Only one communication path towards the Netilion cloud platform. Security mechanisms permanently set. See CR1.4 This product does not appear independently in the operator's network, but at most as a feature of a transmitter.
CR 7.7 Least functionality	✔	
CR 7.8 Control system component inventory	(✔)	See CR1.4 This product does not appear independently in the operator's network, but at most as a feature of a transmitter.

8.3 Version history

Date	Edge module firmware version	Changes to firmware	Documentation
02/2025	01.00.00	Release	SD03377C/07/EN/01.24

www.addresses.endress.com

Endress+Hauser

People for Process Automation