CY01002C/07/EN/01.26-00
71785070
2026-08-31

Security Manual
Liquiline CM42B

Two-wire transmitter
Measurement with digital or analog sensors

Endress+Hauser
People for Process Automation

Table of Contents

1 Notification of security vulnerabilities and advisories

Endress+Hauser provides information about cybersecurity at the following web page: https://www.endress.com/cybersecurity . This web page includes the following information, for example:

- Current security alerts affecting Endress+Hauser products
- E-mail address for reporting security vulnerabilities in 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: PSIRT@endress.com

2 About this document

2.1 Document function

This supplementary Security Manual applies in addition to the product documentation, such as the Operating Instructions, Technical Information and Safety Instructions. The applicable product documentation supports secure operation throughout the entire product life cycle. The additional IT security requirements are described in this Security Manual.

2.2 Further applicable documents

An overview of the relevant documents is available at:

- Device Viewer (https://www.endress.com/deviceviewer): Enter the serial number from the nameplate.
- Download section of the Endress+Hauser website (https://www.endress.com/download)
- Operating Instructions BA02380C
- Operating Instructions BA02381C
- Technical Information TI01817C

2.3 Requirements for the personnel

The personnel responsible for installation, commissioning, diagnostics, and maintenance must meet the following conditions:

- They must have a relevant qualification for this specific function and task.
- They must be authorized by the plant owner/operator.
- They must be familiar with federal/national regulations.
- They must follow the instructions in this manual.

The operating personnel must meet the following conditions:

- Personnel must be instructed and authorized according to the requirements of the task by the facility's owner/operator.
- They must follow the instructions in this manual.

3 System design

3.1 System overview

The product can be operated and configured using the following digital applications:

- Endress+Hauser SmartBlue app

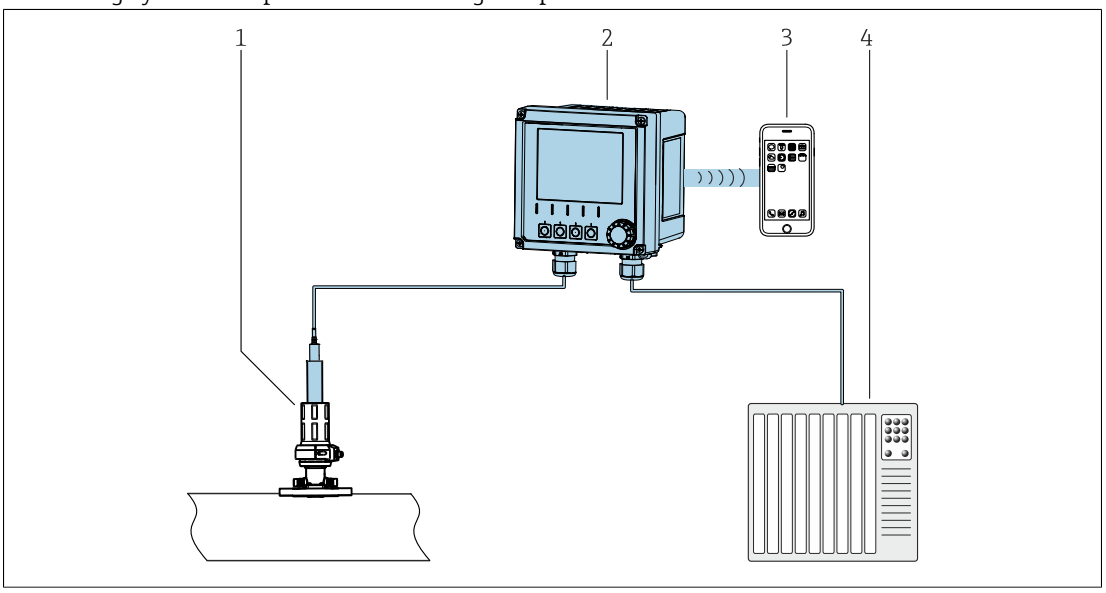
- Endress+Hauser FieldXpert SMTxx (Bluetooth® connection via MSD, HART via FDI)

The device has the following interfaces:
- Bluetooth® Low Energy
- HART

The Bluetooth® connection between the device and mobile devices such as smartphones, tablets or edge devices is protected by CPace. Additional information is available at:

http://www.endress.com/cybersecurity , section on "Secure Bluetooth® connection from Endress +Hauser"

The overview shows examples of measuring systems. Other sensors and assemblies can be ordered for conditions specific to your application (https://www.endress.com/en/field-instruments-overview). These components are collectively referred to below as the IIoT ecosystem. The system boundary (trust zone) is color-coded in the diagram below. A complete measuring system comprises the following components:



1 *Measuring point with sensor and assembly*
2 *Liquiline CM42B*
3 *Mobile device with SmartBlue app, connection via Bluetooth® Low Energy (optional)*
4 *Automation system (e.g., programmable logic controller)*

3.2 Defining the security level

Depending on the required security level, the system and installed products must meet various requirements. First, the required security level (SL1 to SL4) is defined for the system. Depending on the security level, the requirements for the system are derived in accordance with IEC 62443-3-3.

3.3 Product operating environment and security requirements

Endress+Hauser recommends defining the typical operating environment to establish the product's security-relevant characteristics.

An analysis of the operating environment will help determine the requirements for the product functions. For example, a denial-of-service attack might be considered.

The following considerations, for example, may apply to a typical operating environment:
- The product is a system component.
- The product is equipped with at least one interface.
- 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 automation network is protected against external attacks, 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).

Because the product's computing power is limited, it can only defend against attacks to a limited extent.

The product has been designed and optimized for operating conditions in which unauthorized access is physically restricted.

The product is located in a Trust Zone. The operator protects the Trust Zone with a restricted-access perimeter. Sensors, control units and mobile devices can be outside the Trust Zone.

There are no additional access restrictions within the Trust Zone. Authorized personnel ensure device integrity.

Security-related settings can be configured using the Endress+Hauser SmartBlue app via a Bluetooth® connection or via the on-site interface. Configuration changes can also be made via the automation interface using the HART protocol.

If the specified requirements for the operating environment cannot be met, alternative measures may need to be put in place. Alternative measures can include, for example:
- Mechanical protection of the product against tampering
- Mechanical protection of the cabling
- Organizational measures

3.4 Risk analysis and risk assessment

3.4.1 Information on threat analysis

System planning includes a risk assessment of the entire system. The risk assessment is conducted using a holistic approach. The VDI 2182 standard can be used as a guideline.

The operator is responsible for carrying out and documenting the risk analysis or threat assessment. The results will form the basis of the risk assessment.

As part of the planning process, it is necessary to define how the product will be configured during commissioning. This includes, for example:
- Disabling interfaces and/or services that are not required
- Changing default passwords

Take the following into account for the risk analysis:
- Product interfaces that can be used to communicate with or access 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

3.4.2 Analyzing the whole system

The product is a transmitter for industrial process monitoring and control.
- It includes analog and digital inputs and outputs for integrating sensors.
- The product can be operated locally via a display. A four-button control with a navigation function supports configuration.

- The product features a digital communication interface (HART) that enables operation and configuration of the product.
- The product has a Bluetooth interface for advanced functionality. The product can be operated and configured remotely using a mobile device with the SmartBlue app installed.
- A service interface exists locally within the product as an internal interface. This interface is digitally locked upon delivery. No access is possible in operating mode.

3.4.3 Training users

Endress+Hauser recommends training to ensure correct use of terminals and interfaces. Training increases the users' security awareness.

3.5 Defence in Depth Strategy

3.5.1 Defense in depth as a security concept

Defense in depth is a security concept with multiple, independent protective measures. The protective measures reduce the probability and impact of successful cyber attacks. Instead of relying on a single security measure, multiple complementary safeguards are implemented at different system levels.

This section describes how the product contributes to a defense-in-depth strategy by implementing security measures at the device, software, and communication levels. It also describes additional security measures to be implemented in the operating environment.

The defense-in-depth approach described here applies to:

- the product and its software
- supported communication interfaces
- operational and life-cycle-related aspects of the product

System-wide or organizational security concepts are not described in detail. Overall system security depends on the proper integration of the product into a secure environment, as well as on appropriate operating procedures.

The required level of protection requires a secure operating environment and appropriate operating practices.

3.5.2 Defense-in-depth concept for the product

The product is intended for use in industrial automation environments where multiple layers of security are typically implemented. The defense-in-depth concept is based on a combination of the following security levels:

- Physical protection
- Secure system configuration and hardening
- Identity and access control
- Secure communication
- Network and environmental security
- Operational and life-cycle-related security measures

Every level contributes to overall security. If a protective mechanism is weakened or circumvented, additional levels help limit unauthorized access, misuse, or further damage.

3.5.3 Product-level defense-in-depth measures

Secure system configuration and hardening
The product follows a system design approach based on secure design principles that aim to minimize the attack surface. Security measures reduce the device's attack surface and,

consequently, the likelihood of misuse or unintended access. These security measures may include, for example:

- Reducing externally accessible services and interfaces to the absolute minimum
- Disabling or restricting unused functions and interfaces
- Secure default settings after installation
- Separation of user and administrative functions, where applicable

Identity and access control

- The product supports controlled access to its functions and interfaces based on the principle of least privilege. Access to configuration, operating, and maintenance functions is restricted to authorized users or systems.
- Authentication and authorization mechanisms ensure that only authorized entities can access security-related functions. If access control depends on external systems or infrastructure, this dependency must be taken into account during system integration.

Secure communication

The product supports secure communication mechanisms. These mechanisms protect the data exchanged with connected external systems, such as Netilion. Secure communication is an essential layer of defense in depth. This is especially true if the product is connected to external networks or higher-level systems. The security of the communication network within an industrial automation environment depends on the available industrial communication protocols. Depending on the interface and configuration, communication security measures may include the following:

- Protect data against unauthorized access during transfer
- Authentication of communication partners
- Integrity protection to prevent unauthorized modifications to transmitted data

Software integrity and updates

Security is maintained throughout the product life cycle through controlled software management. Security-related aspects may include:

- Use of software from trusted sources.
- Protection against unauthorized changes to the software.
- Controlled update mechanisms for installing fixes or security updates.
- Apply updates according to Operating Instructions and security recommendations. This is the responsibility of the user.

3.5.4 Defense-in-depth measures expected in the environment

A secure operating environment is essential for an effective defense-in-depth strategy. It complements the security measures implemented with the product.

Security zones and trust boundaries

A security zone is a logical or physical grouping of assets with similar security requirements, trust levels and risk profiles.

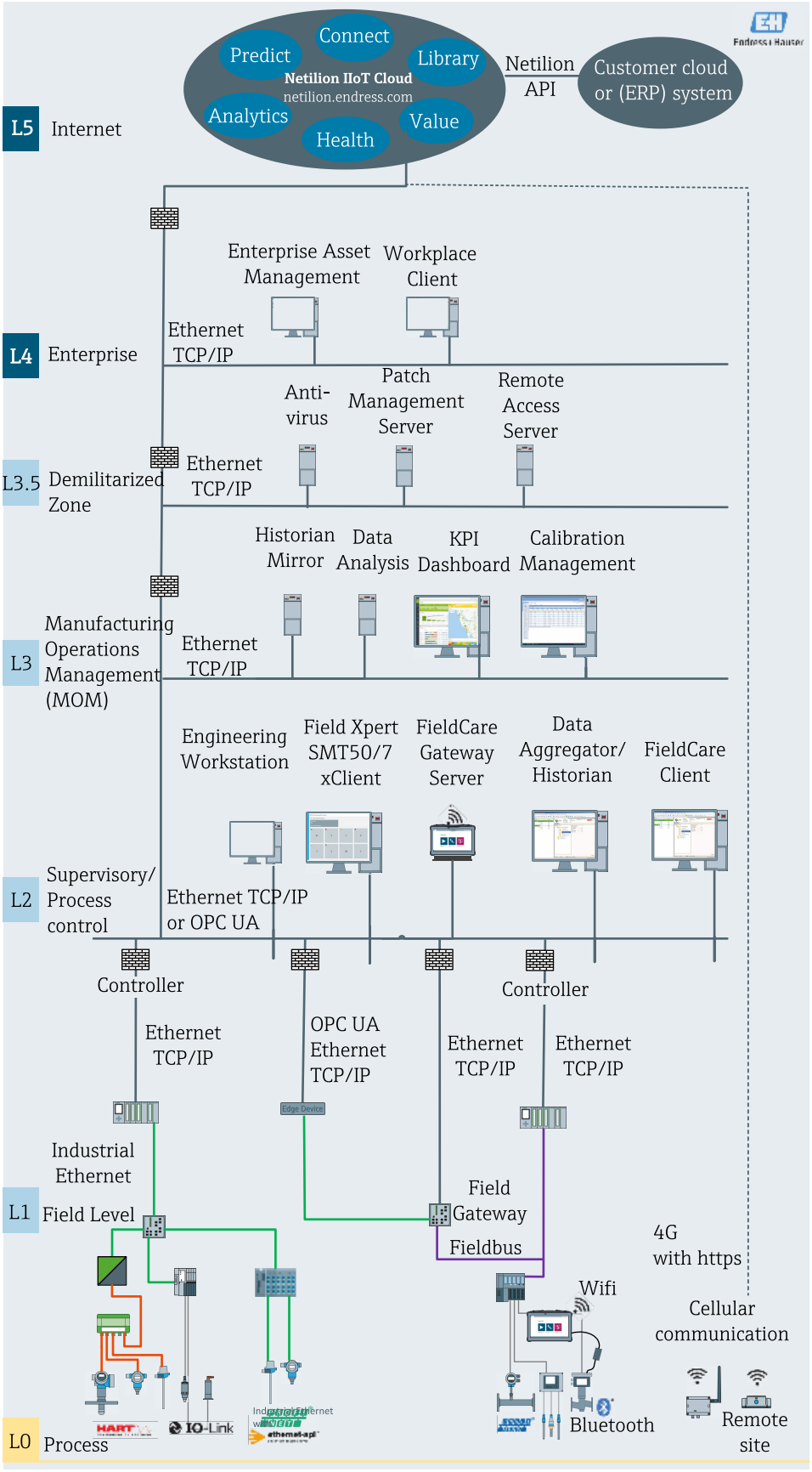
Assets within the same zone trust one another to the extent required for that zone. Communication between zones crosses trust boundaries and must therefore be controlled and protected by technical and organizational measures.

Communication paths between zones are known as conduits. Conduits enforce security policies governing data exchange between zones. This enforcement can be achieved, for example, through the following measures:

- Restricting permitted data traffic
- Access control
- Additional protective measures

Zones and conduits prevent faults and attacks from spreading. They reduce the exposed attack surface and allow security measures to be applied selectively according to risk. The system architect or operator defines the zones and manages them as part of the security concept.

Example of zones with applicable Security Levels in accordance with IEC 62443-4-2. Endress +Hauser recommends operating the product within this type of zone-based architecture.



3.5.5 Network security

Endress+Hauser recommends operating the product in a secure network environment. Operating environment security measures may include:
- Network segmentation (for example, using zones and conduits)
- Firewalls or filtering mechanisms to restrict network traffic
- Protection of remote access paths
- Monitoring of network communication

The specific network security architecture depends on the particular installation and is the responsibility of the system operator or system integrator.

3.5.6 Physical protection

The product is intended for installation in an industrial environment. Possible installation locations include, for example, a control cabinet or a plant room with restricted physical access. Physical protection helps prevent unauthorized tampering, access to hardware interfaces, or removal of the device.

Physical access to the installation location must be restricted to authorized personnel only.

3.5.7 Organizational measures

An effective defense-in-depth strategy requires organizational protective measures that go beyond the product itself, such as:
- Controlled access to installation areas
- Clearly defined user roles and responsibilities
- Personnel training and awareness of IT security and OT security
- Secure processes for the following:
  - Commissioning
  - Maintenance
  - Service

3.5.8 Operational and life-cycle-related security measures

The defense-in-depth concept extends beyond the initial installation and incorporates the entire product life cycle.

Operational security measures include:
- Secure commissioning and configuration
- Use strong authentication, where applicable.
- Check the configuration and access rights regularly.
- Backup and recovery procedures, if required by the application
- Secure storage of the backup with access restricted to authorized personnel
- Install the security updates provided by Endress+Hauser.

Decommissioning and disposal of the product protect data and configuration settings against unauthorized access.

3.6 Residual risk and shared responsibility

Despite the implementation of multiple security measures, residual risk cannot be completely eliminated. Security is a shared responsibility:
- Endress+Hauser provides security functions and security-related information.
- System integrators and operators are responsible for secure system design, integration, and operation.

The effectiveness of defense in depth depends on a combination of the following measures:
- Product-specific measures

- Appropriate environmental and organizational controls

4 Types of communication

4.1 Access management

4.1.1 Access management

4.1.1.1 Access management (4-20 mA / HART)

A connection via the HART interface is established through a fixed user account that is part of the "Maintenance" authorization group. Logging in or authentication is not supported.

The HART interface and the interface to the sensors do not have any security mechanisms. As a result, spoofing, tampering, and information disclosure attacks can easily occur. As a security measure, Endress+Hauser recommends access control or protecting the cables by routing them through conduits or ductwork.

4.1.1.2 Access management (Bluetooth®)

The SmartBlue app supports user accounts with authentication via name and password.
The administrator defines password requirements. The “Operator,” “Maintenance” and “Administrator” authorization groups can be assigned to user accounts.

The Bluetooth® interface can only be enabled or disabled via onsite operation.

The "Administrator" authorization group is only available via the Bluetooth® interface in the SmartBlue app.

Access via Bluetooth® is only possible with login credentials (login and password). Use the initial default password when logging in for the first time. Endress+Hauser recommends changing the password after logging in the first time and store it securely.

The initial password is specified on the nameplate and in the "Bluetooth® access credentials" sheet provided.

4.2 Applications and apps

4.2.1 Applications and mobile apps (Bluetooth®)

Heterogeneous software environments pose a security risk. Examples: ANDROID apps on tablets or Windows solutions on PCs.

Applications/mobile apps, cloud servers and terminals are all relevant to security as they are components that access the control system or the product. These components require suitable protective measures.

To protect the customer's system and data, the security of the terminal's login credentials must also be guaranteed. Secure storage of login credentials and certificates increases system security.

4.3 Device data and device status

4.3.1 Device data and device status

4.3.1.1 Device data and device status (4-20 mA / HART)

Many attacks on a component in an IIoT ecosystem cause anomalies in the data. If a product suddenly delivers unrealistic values, this can be an indication of an attack.

Since real-time monitoring is not a realistic possibility for most users, this process must be automated. Endress+Hauser recommends using monitoring software that monitors specific parameters and the status of the product, and reports any deviations. The device can be connected to a control system via HART for real-time monitoring.

Communication between the HART interface and the control system and connected sensors is unencrypted. The physical protection, as well as detection and correction of anomalies is the responsibility of the control system operator.

4.3.1.2 Device data and device status (Bluetooth®)

Real-time monitoring is not required in every application. The process is therefore automated. Endress+Hauser recommends a monitoring software. The software monitors parameters and the device status. The software reports any deviations.

4.4 Update management

4.4.1 Update management (Bluetooth®)

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 information technology and increasing requirements in networking, updates are always required in real life.

Endress+Hauser recommends that available updates are checked and installed regularly. Failing to install updates is a serious security risk as attackers also have information on the vulnerabilities that are being rectified.

5 Commissioning

5.1 Security steps during commissioning

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

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.

1. During commissioning, observe the security requirements for the product's operating environment.
2. Observe also the measures to be taken in the event of non-compliance with these security requirements.

5.2 Installing the product

- The product is installed within a protected perimeter.
- Only authorized persons have access to the product.
- Endress+Hauser recommends installing the product in such a way as to prevent unauthorized access. Suitable locations include lockable rooms or control cabinets. This prevents physical access.
- The access cables to sensors and the programmable logic controller are protected. This protection is provided by access controls and by routing the cables through conduits.

Install the product in accordance with the applicable Brief Operating Instructions or Operating Instructions and connect it electrically.

5.3 Configuring the product

Commission and configure the product in accordance with the associated Brief Operating Instructions or Operating Instructions.

5.4 Hardening the product

In IT security, "hardening a product" means the following: Only the services required for the specific use case are enabled.

1. Change all default passwords after logging in for the first time.
2. Disable any accounts that are not required, in particular system accounts that are required only for service purposes. Path: **Menu/System/Security/User accounts**
3. Define password requirements for every user group. Path: **Menu/System/Security**
4. Set a password policy through the SmartBlue app menu. Path: **Menu/System/Security/ Advanced settings/Password policy**
5. Disable decommissioning reset and “Reset user accounts and PINs” via the SmartBlue app menu. Path: **Menu/System/Security**
   ↳ This prevents security settings (user groups, passwords) from being reset.
6. Disable the Bluetooth® connection after commissioning. This feature can be disabled in the configuration so that the product does not receive or transmit Bluetooth® signals. Path: **Menu/System/Connectivity/Bluetooth**
7. Endress+Hauser recommends setting passwords or PINs for all user groups.

   The on-site display cannot be disabled for field devices and cabinet devices.

8. Secure the supply line for devices with a HART interface.

   The interface can be disabled for maintenance or installation work, for example. Path: **Menu/Application/HART output**

6 Operation

6.1 Tasks during operation

1. Operate the product according to the accompanying Operating Instructions.
2. Check whether there are firmware updates for the product at regular intervals and perform these updates.
3. Check at regular intervals that only authorized individuals have access to the device.
4. Check at regular intervals that no changes were made to the product or access to the product.
5. Only enter passwords when unobserved.
6. If a password is no longer trustworthy, disable the associated user account immediately or change the password.
7. Automatically lock the product after a user session to prevent unauthorized access.
8. To prevent data loss, regularly download the logbooks from the device and back them up elsewhere. The logbooks have a limited number of entries.

6.2 Security aspects during operation

- The product does not provide lifecycle functions for regular user password changes.

  Endress+Hauser recommends changing user passwords at regular intervals.
- Endress+Hauser recommends checking regularly for firmware updates for the product and installing any available updates.

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

Checksums and signatures in the firmware safeguard the integrity and authenticity of the updates. The user does not need to carry out integrity and authenticity checks on the updates. The firmware updates are installed via the Endress+Hauser SmartBlue app. The Bluetooth® function must be enabled, or temporarily enabled, for this purpose.

Functions from a security perspective

From a security perspective, the following function groups are available to users in the defined authorization groups. Developer and service functions are intended only for Endress+Hauser employees. Disable the associated authorization groups during operation.

Function	Description	Authorization group
Operation	Display of general information (measured value, diagnostics)	Operator Maintenance Admin (via SmartBlue app only)
Configuration and maintenance	Enable and disable settings to configure device response, device updates and device interfaces.	Maintenance Admin (via SmartBlue app only)
Administration	Activate and deactivate user administration, configuration reset, access etc.	Admin (via SmartBlue app only)
Calibration and adjustment functions	Configuration of the available calibration routines. Adjustment of the measurement procedure	Operator Maintenance Admin (via SmartBlue app only)
Enable and disable system access	Enable and disable system access for service and development.	Admin (via SmartBlue app only)
Developer functions	Functions for Endress+Hauser development	Endress+Hauser employees
Service functions	Functions for Endress+Hauser service	Endress+Hauser employees

Login via on-site interface

A user authenticates on the device using a PIN. Users have an access account that makes them a member of one or more authorization groups. The on-site interface supports the fixed access accounts listed in the table. If PINs are not configured for "Operator" and "Maintenance," "Maintenance" access is automatically granted. If a PIN is not configured for "Operator", "Operator" access is automatically granted.

Access account	Authorization group
"Operator"	Operator
"Maintenance"	Maintenance

Connection via the HART interface

A fixed user account is used to establish a connection via the HART interface. The user account is part of the "Maintenance" authorization group. Login or authentication is not supported.

Authorization group
Maintenance

Login via the Bluetooth® interface using the SmartBlue app

The SmartBlue app supports user accounts. Authentication is via name and password. The administrator defines the password requirements. User accounts can have the authorization groups listed in the table. The "Administrator" authorization group is only available via the Bluetooth® interface in the SmartBlue app. The Bluetooth® interface can only be enabled or disabled via the on-site interface.

Authorization group
Operator
Maintenance
Administrator

6.3 Repeating the risk analysis

The risk situation that plants are exposed to can change as a result of external events such as the occurrence of previously unknown attack patterns. In accordance with VDI/VDE 2182-1, Section 4.4, the risk analysis must be repeated and updated at regular intervals. The risk analysis also needs to be updated if the plant is modified in a way that could affect the risk analysis.

7 Repair

7.1 Repair instructions

The repair and conversion concept provides for the following:

- The product has a modular design.
- Spare parts are grouped into kits which include the associated kit instructions.
- Carry out the repair according to the kit instructions.
- Only use original spare parts from the manufacturer.
- Repairs are carried out by the manufacturer's Service Department or by trained users.
- Certified devices can only be converted to other certified device versions by the manufacturer's Service Department or at the factory.
- Observe applicable standards, national regulations, safety instructions for explosion-protected areas (XA), and certificates.
- Document the repair and conversion and enter, or have entered, in the Life Cycle Management tool.

7.2 Spare parts

For currently available spare parts, see: https://www.endress.com/onlinetools

7.3 Return

The requirements for safe device return can vary depending on the device type and national legislation.

Information on this topic can be found on the website: https://www.endress.com

If returning the device, pack it in such a way that it is reliably protected against impact and external influences. The original packaging offers the best protection.

8 Decommissioning

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

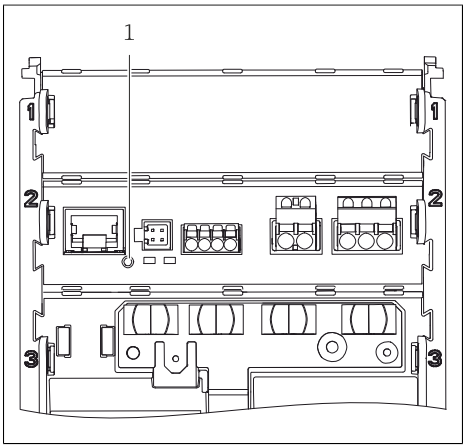
The product is not being used for a prolonged period of time.

1. No action required.

The product has a malfunction that the customer cannot remedy.

2. Contact Endress+Hauser.

The product will be disposed of.

3. 

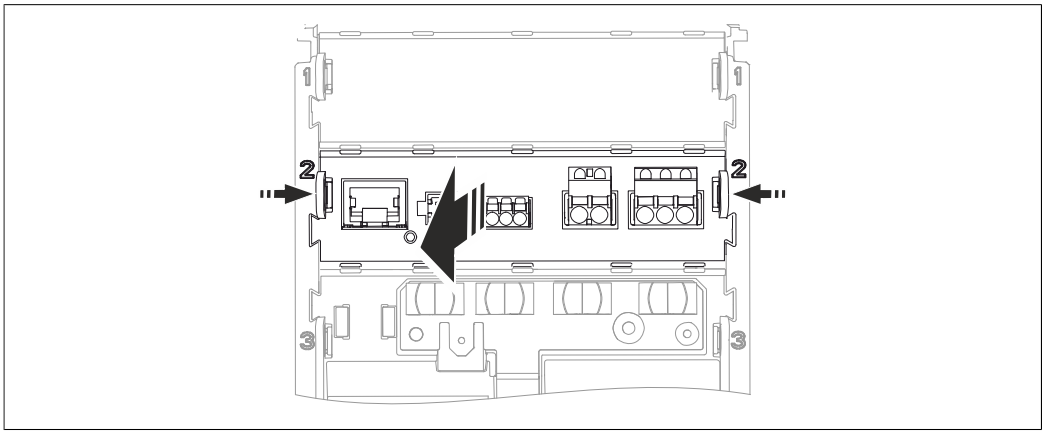
1 Reset button

Reset device. To do this, press the reset button to position 1 for 12 seconds.

↳ The device configuration and user accounts are deleted.

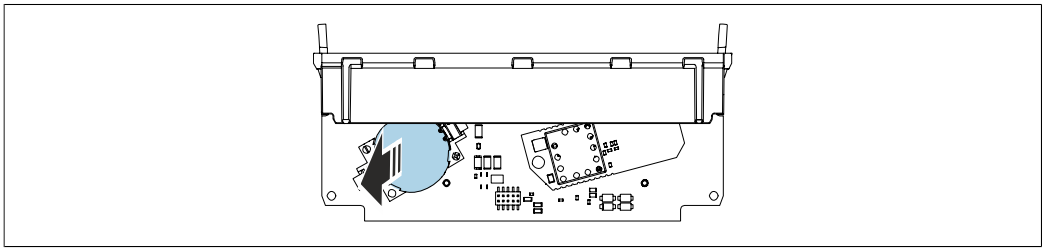
4. Disconnect all the cables that are connected to slot 2 of the plug-in module.

↳ The product is now de-energized.

5. 

Remove the base module from slot 2. To do this, press the locking clips on the sides together.

6.



Remove the battery at the bottom of the base module.

9 Disposal

9.1 Disposal

If required by the Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), the product is marked with the depicted symbol in order to minimize the disposal of WEEE as unsorted municipal waste. Do not dispose of products bearing this marking as unsorted municipal waste. Instead, return them to the manufacturer for disposal under the applicable conditions.

10 Appendix

10.1 Security checklist for the product life cycle

Security checklist for the product life cycle

Life cycle	Task	Tested
Planning	The typical operating environment of the product is defined and taken into account for planning.	☐
	Engineering-phase planning work considered. Threat analysis and risk assessment carried out.	☐
	Where possible, measures to reduce risks considered.	☐
Incoming goods and transportation	Packaging checked to ensure it is unopened, from Endress +Hauser, and the seal is intact.	☐
Commissioning	Product hardened for specific application.	☐
	User data configured.	☐
Operation	Update management requirements observed.	☐
	Recurring threat analysis scheduled.	☐
Decommissioning	Product decommissioned. Depending on reason for decommissioning, disable or destroy the product.	☐

10.2 Security Level according to IEC 62443-4-2

The product meets the requirements of Security Level SL 1.

The device has been developed in accordance with the requirements for embedded devices (EDR = Embedded Device Requirements). The following table evaluates the requirements in accordance with IEC 62443-4-2. Together with the measures implemented by the operator, the device achieves Security Level 1 (SL-C).

The Endress+Hauser ProtectBlue Essential protection profile is implemented for the device.

See https://www.endress.com/field-instruments-overview/measurement-technologies/ProtectBlue

"Status" column legend

✔	The requirement was implemented.
(✔)	The requirement either does not apply to the product or is not required for the security level specified in IEC 62443-4-2 and ProtectBlue Essential.

IEC 62443-4-2 requirements fulfilled

Requirement	Status	Explanation
CR 1.1 Human user identification and authentication	✔	Identification and authentication for on-site operation and Bluetooth®, not for communication via HART
CR1.2 Software process and device identification and authentication	(✔)	No application exists that requires authentication of the device. Required from Security Level 2 onward.
CR 1.3 Account management	✔	Fulfilled for SmartBlue app.
CR 1.4 Identifier management	✔	Fulfilled for SmartBlue app.
CR 1.5 Authenticator management	✔	Fulfilled for SmartBlue app.
CR 1.6 – Wireless access management	✔	Fulfilled for SmartBlue app.
CR 1.7 Strength of password-based authentication	✔	Fulfilled for SmartBlue app.
CR 1.8 – Public key infrastructure certificates	(✔)	Required from Security Level 2 onward.
CR 1.9 – Strength of public key-based authentication	(✔)	Required from Security Level 2 onward.
CR 1.10 Authenticator feedback	✔	Fulfilled for SmartBlue app.
CR 1.11 Unsuccessful login attempts	✔	Fulfilled for SmartBlue app. If the incorrect password is entered 3 times, the user must wait at least Y seconds. This counter is maintained separately for each user account. Y = 'Number of incorrect entries' * 10 s Y_{max} = 15 min
CR 1.12 System use notification	✔	Fulfilled for SmartBlue app.
CR 1.14 Strength of symmetric key-based authentication	(✔)	Not applicable since the authentication protocol does not use pre-shared symmetric keys.
CR 1.14 RE (1) Hardware security for symmetric key-based authentication	(✔)	Not applicable since the authentication protocol does not use pre-shared symmetric keys.
CR 2.1 Authorization enforcement	✔	Fulfilled for SmartBlue app.
CR 2.2 Wireless use control	✔	Fulfilled for SmartBlue app.
CR 2.3 – Use control for portable and mobile devices	(✔)	No component level requirement
EDR 2.4 Mobile Code	(✔)	Not applicable as no mobile code is used

Requirement	Status	Explanation
EDR 2.4 RE (1) Mobile code authenticity check	(✔)	Not applicable as no mobile code is used
CR 2.5 Session lock	✔	Fulfilled for SmartBlue app.
CR 2.6 Remote session termination	(✔)	Not applicable as there are no remote sessions. Furthermore, only required from Security Level 2 onward
CR 2.7 – Concurrent session control	(✔)	Only required from Security Level 3 onward
CR 2.8 Auditable events	✔	Fulfilled for SmartBlue app.
CR 2.9 Audit storage capacity	✔	Fulfilled by ring buffers.
CR 2.10 Response to audit processing failures	✔	Fulfilled - no known audit processing failures.
CR 2.11 Timestamps	✔	Fulfilled
CR 2.12 Non-repudiation	✔	Fulfilled
EDR 2.13 Use of physical diagnostic and test interface	✔	Fulfilled
CR 3.1 Communication integrity	✔	Fulfilled for SmartBlue app.
CR 3.1 RE (1) Communication authentication	✔	Fulfilled for SmartBlue app.
EDR 3.2 Protection from malicious code	✔	Fulfilled for the field device and the rail-mounted device. Not fulfilled for a portable external display that can leave the Trust Zone → 3.3
CR 3.3 – Security functionality verification	✔	Follow the instructions and check regularly to ensure that the logging and authentication functions are working properly.
CR 3.4 Software and information integrity	✔	Fulfilled
CR 3.4 RE (1) Authenticity of software and information	✔	Fulfilled
CR 3.4 RE (2) Automated notification of integrity violations	✔	Fulfilled
CR 3.5 Input validation	✔	Fulfilled
CR 3.6 Deterministic output	✔	Fulfilled
CR 3.7 Error handling	✔	Fulfilled
CR 3.8 Session integrity	✔	Fulfilled
CR 3.9 Protection of audit information	✔	Fulfilled
EDR 3.10 Support for updates	✔	Fulfilled
EDR 3.10 RE (1) Update authenticity and integrity	✔	Fulfilled
EDR 3.11 – Physical tamper resistance and detection	(✔)	Required from Security Level 2 onward.
EDR 3.12 Provisioning product supplier roots of trust	✔	Fulfilled
EDR 3.13 Provisioning asset owner roots of trust	(✔)	Required from Security Level 2 onward.
EDR 3.14 Integrity of the boot process	✔	Update process guarantees integrity.
EDR 3.14 RE(1) Authenticity of the boot process	✔	Update process guarantees authenticity.
CR 4.1 Information confidentiality	✔	Fulfilled for SmartBlue app

Requirement	Status	Explanation
CR 4.2 Information persistence	(✔)	Hardware and firmware logbooks cannot be reset. Required from Security Level 2 onward.
CR 4.3 Use of cryptography	✔	Fulfilled for SmartBlue app.
CR 5.1 Network segmentation	✔	Fulfilled
CR 6.1 Audit log accessibility	✔	A security log will be implemented in Release 1.1.
CR 6.2 – Continuous monitoring	(✔)	Required from Security Level 2 onward.
CR 7.1 Denial of service protection	✔	Fulfilled for Bluetooth and fieldbus interface.
CR 7.2 Resource management	✔	Fulfilled
CR 7.3 Control system backup	✔	Upload and download of functional parameters possible
CR 7.4 Control system recovery and reconstitution	✔	Achieved by factory reset in conjunction with upload or download of functional parameters
CR 7.5 – Emergency power	(✔)	No component level requirement
CR 7.6 Network and security configuration settings	✔	Bluetooth® and HART can be switched on and off.
CR 7.7 Least functionality	✔	Fulfilled
CR 7.8 – Control system component inventory	(✔)	Required from Security Level 2 onward.

10.3 Version history

Version history

Document version	Firmware version	Hardware version	Changes
01.26	01.01.00	/	First version

www.adresses.endress.com

Endress+Hauser

People for Process Automation