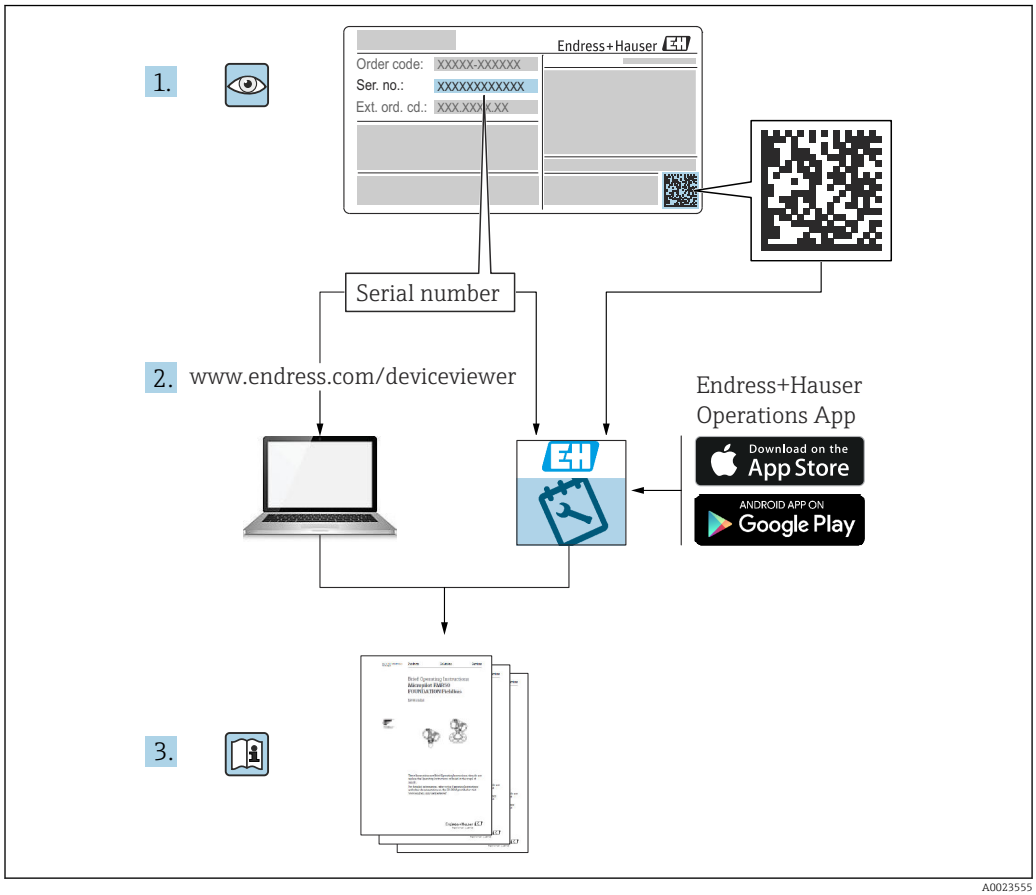
SD03430F/09/EN/01.25-00
71710108
2025-05-31



# Special Documentation
# **Security Manual FlexView FMA90**

Control unit with color display and touch control for up to two ultrasonic, radar, hydrostatic or universal 4-20 mA/ HART® level sensors


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 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

### 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:
- *Device Viewer*: Enter serial number from nameplate
  www.endress.com/deviceviewer
- The download area of the Endress+Hauser website
  www.endress.com/downloads

**Further applicable documents FlexView FMA90**

- Technical Information TI01689F
- Operating Instructions BA02254
- Brief Operating Instructions KA01584F
- Device Parameters GP01189F

### 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

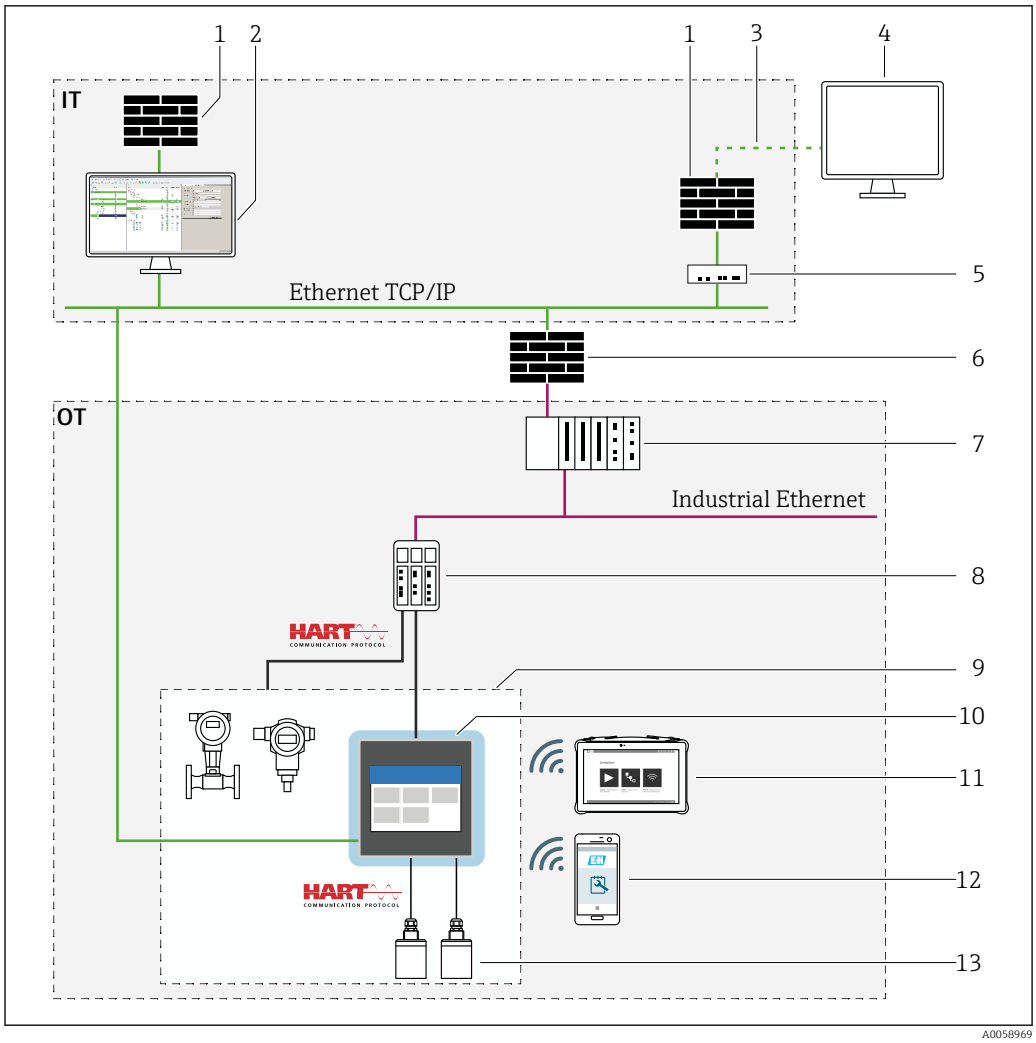
### 3.2.1 General information

The FlexView FMA90 is equipped with the following interfaces:
- Standard:
  - HART device, wired
    During operation, the FlexView transfers the measured values and calculated values via 4-20 mA/HART to a higher-level controller (PLC/DCS).
  - HART master
    4-20 mA/HART field devices can be connected to the FlexView.
  - Ethernet RJ45
- Optional:
  - WLAN
  - Local display

You can configure the FlexView via the following in digital applications:
- Standard:
  - Ethernet/TCP and the web server integrated in the FlexView
  - HART with limited configuration options
- Optional:
  - WLAN and the web server integrated in the FlexView
  - Local display

### 3.2.2 System design and system boundaries

This security manual covers the FlexView FMA90 and the connection to a PLC/DCS via 4-20 mA/HART. Other components such as connected field devices and operating tools are not part of this security manual. The system boundary is color-coded in the diagram below.




1 *Possible applications for FlexView FMA90; blue marking indicates the system boundaries for this manual*

*IT Information Technology, here: company network*
*OT Operational Technology, here: network for process automation*
*1 Firewall of the company network (IT)*
*2 Host application such as Endress+Hauser FieldCare SFE500 or DeviceCare, or directly via web server*
*3 Ethernet TCP/IP*
*4 Remote access via web server*
*5 Router*
*6 System firewall*
*7 Control system PLC/DLC*
*8 Gateway for translating HART to Industrial Ethernet*
*9 System components such as Endress+Hauser field devices and field devices from other manufacturers*
*10 FlexView FMA90*
*11 Endress+Hauser Field Xpert SMTxx via WLAN and web server*
*12 Operation and configuration via WLAN and web server*
*13 4-20 mA/HART field devices, here e.g. Endress+Hauser level sensors*

The FlexView FMA90 is referred to in the general text of this document, depending on the context, as a product, terminal, or control unit.

## 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).

Since the computing performance of the product under consideration is limited, the product can only be attacked 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 must be considered. This may involve, for example, mechanical protection of the product against tampering, mechanical protection of the cabling, or organizational measures.

For example, you might use the FlexView in free field conditions, such as for pump control in a lifting station in a sewer system or for flow measurement in open channels and weirs.

Measures to prevent physical tampering and remote manipulation of the FlexView must be implemented by the customer.

You can seal the FlexView to provide mechanical access protection.

## 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 Analyzing the whole system

The FlexView FMA90 is a control unit that can be used either as a stand-alone device or within a closed automation system. A closed automation system might be, for example, a wastewater treatment plant.

This manual considers the use of the FlexView as a stand-alone device or within a closed automation system. If the FlexView is integrated in another system, additional analyses are required.

The FlexView was developed in accordance with the requirements of IEC 62443-4-1 and, in accordance with IEC 62433-4-2, achieves Security Level 1 (SL 1).

Further information: → 17

### 3.7.2 Training users

Depending on the application scenario, users who are not specialized in this area may come in contact with the FlexView. We recommend training all users - and especially non-technical users - on the safe use of the FlexView, including all used interfaces and all connected and related components, and raising their awareness of security issues.

### 3.7.3 Optimizing access management

To prevent tampering with the FlexView, the "Maintenance“ user role should be protected with a PIN.

For detailed information on user roles and rights, see Operating Instructions → 6

#### Web server via Ethernet

To access the FlexView via the web server, you need the appropriate access credentials. For the first login, you must use the initial PIN. We recommend changing the PIN after the first login and storing it securely.

For detailed information on initial PIN and login, see Operating Instructions → 6

#### Web server via WLAN (optional)

To access the FlexView via the web server over WLAN, you must first establish a connection to FlexView via WLAN.

For the first login to the web server, you must use the initial PIN. We recommend changing the PIN after the first login and storing it securely.

For detailed information on establishing a connection via WLAN, initial PIN, and login, see Operating Instructions → 6

#### HART

HART is an interface without special security functions.

When using the HART interface, we recommend that you either activate the hardware lock or implement perimeter protection after commissioning.

### 3.7.4 Monitoring device data and device status

**Monitoring via HART**

The FlexView can be connected to an automation system via HART. In this case, detecting and addressing anomalies is the responsibility of the operator of the automation system.

**Monitoring in the context of network integration (LAN)**

The FlexView can be a terminal in an area network, and the detection of anomalies is the responsibility of the higher-level system.

### 3.7.5 Updating product software

Network-capable terminals must be designed so that as few fixes via updates as possible are required. Given the dynamic nature of IT/OT 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 pose a serious security risk, as attackers could have information on the vulnerabilities they are meant to rectify.

Update management: → 14

# 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 the additional sections.

### 4.4.2 Required 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 check the hardware for tampering.

With regard to security, pay attention to the following during commissioning:
Integrate the product in the operating environment in accordance with the specified requirements → 9.

### 4.4.3 Hardening the product

Hardening of the FlexView is performed by deactivating unused interfaces.

Interfaces are deactivated via the "System" menu.

For detailed information, see Description of device parameters (GP) → 6

### 4.4.4 Configuring user data

User data includes, for example login details, users, tag name, passwords, IDs, etc.

You can configure all user data. Application data are configured via the "System" menu.

For detailed information, see Description of device parameters (GP) → 6

### 4.4.5 Security-related product settings

You can configure all security-relevant settings required for the FlexView. Security-related settings are configured via the "System" menu.

Also observe the specifications in the following sections:
- Hardening the product: → 12
- User management → 13

For detailed information, see Description of device parameters (GP) → 6

### 4.4.6 User management and impact on security

The FlexView provides multiple user roles with specific read and write permissions and different login credentials.

Apply settings according to the "Optimizing access management" section and the operating instructions.

Optimizing access management: → 10

For detailed information on user roles, rights and settings, see the Operating Instructions and Description of device parameters (GP) → 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

The FlexView does not require any interactions during operation.

## 5.4 Security aspects during operation

The FlexView includes an integrated TLS/SSL certificate management system for the HTTPS web server.

Certificates have a specific expiration date. Diagnostic messages are generated before expiry.

You must import new certificates via the user interface.

For detailed information on certificate management and certificates, see Description of device parameters (GP) → 6

## 5.5 Update management

Endress+Hauser provides updates via the FlexView FMA90 product page https://www.endress.com/FMA90.

To carry out an update, contact Endress+Hauser Service.

Updates can only be performed via the web server.

For further information on firmware updates, see the Operating Instructions. → 6

A restart of the FlexView is required after every update. The restart is performed automatically.

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

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

## 5.6 Repeating the risk analysis

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

## 5.7 Repair and disposal

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

# 6 Decommissioning

## 6.1 Target group

This section is aimed at operating personnel.

## 6.2 Requirements of the personnel

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

## 6.3 Decommissioning the product

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

| Reason for decommissioning | Actions required |
|---|---|
| The product is not being used for a prolonged period of time. | We recommend resetting the product to factory settings.<br>Disconnect from the supply voltage and, if necessary, uninstall and store. |
| The product has a fault that you are unable to rectify. | 1. Contact Endress+Hauser.<br>2. Carry out steps according to Endress+Hauser instructions. |
| The product requires servicing from Endress+Hauser. | 1. Contact Endress+Hauser.<br>2. Carry out steps according to Endress+Hauser instructions. |
| The product is defective and must therefore be disposed of. | 1. Disconnect the product from the supply voltage.<br>2. Destroy the product. |
| The product is to be disposed of. | We recommend resetting the product to factory settings. Disconnect the product from the supply voltage. |

# 7 Appendix

## 7.1 Security checklist for the product life cycle

| Life cycle | Task | Checked |
|---|---|---|
| Planning | Typical operating environment of the product defined and taken into account for planning. → 🖹 9<br>If required, alternative measures taken into account. → 🖹 9 | ❑ |
| | Engineering-phase planning work considered Threat analysis and risk assessment carried out. → 🖹 9 | ❑ |
| | Where possible, measures to reduce risks considered. → 🖹 10 | ❑ |
| Goods receipt/transport | Packaging checked to ensure it is unopened and seal is intact | ❑ |
| Commissioning | Product hardened for specific application → 🖹 12 | ❑ |
| Operation | Update management requirements observed → 🖹 14 | ❑ |
| | Planning for renewed threat analysis performed → 🖹 15 | ❑ |
| Decommissioning | Product taken out of service. → 🖹 16<br>Depending on reason for decommissioning, disable or destroy the product. | ❑ |

## 7.2 Version history

| Document version | Firmware version | Hardware version | Changes |
|---|---|---|---|
| 01.00 | as of 01.00.00 | Dev. Rev. 1 | First version |

## 7.3 Security level in accordance with IEC 62443-4-2

The FlexView FMA90 achieves Security Level 1(SL 1)in accordance with IEC 62443-4-2 and complies with the Endress+Hauser ProtectBlue Essential protection profile.

*Explanation of symbols in the "Status" column*

✔ Requirement is fulfilled

(✔) The requirement is not applicable for the product.

*FR 1 - Identification and authentication control*

| Requirement | | Status | Note |
|---|---|---|---|
| CR 1.1 | Human user identification and authentication | ✔ | |
| CR 1.2 | Software process and device identification and authentication | (✔) | |
| CR 1.3 | Account management | ✔ | |
| CR 1.4 | Identifier management | ✔ | The product has predefined account identifiers. |
| CR 1.5 | Authenticator management | ✔ | |
| CR 1.7 | Strength of password-based authentication | (✔) | |
| CR 1.8 | Public key infrastructure certificates | ✔ | |

| Requirement | | Status | Note |
|---|---|---|---|
| CR 1.9 | Strength of public key-based authentication | ✔ | |
| CR 1.10 | Authenticator feedback | ✔ | |
| CR 1.11 | Unsuccessful login attempts | ✔ | |
| CR 1.12 | System use notification | ✔ | |
| CR 1.14 | Strength of symmetric key-based authentication | ✔ | |

*FR 2 – Use control*

| Requirement | | Status | Note |
|---|---|---|---|
| CR 2.1 | Authorization enforcement | ✔ | |
| CR 2.2 | Wireless use control | ✔ | |
| EDR 2.4 | Mobile code | (✔) | |
| CR 2.5 | Session lock | ✔ | |
| CR 2.6 | Remote session termination | ✔ | |
| CR 2.8 | Auditable events | ✔ | |
| CR 2.9 | Audit storage capacity | ✔ | The event log is implemented as a ring buffer with 10,000 entries. Once 10,001 events are reached, the oldest event is overwritten. |
| CR 2.10 | Response to audit processing failures | ✔ | |
| CR 2.11 | Timestamps | ✔ | |
| | RE (1) Time synchronization | ✔ | Date and time can be synchronized via NTP. |
| CR 2.12 | Non-repudiation | ✔ | The product automatically generates local security-relevant event records (log entries) with real-time timestamps. |
| EDR 2.13 | Use of physical diagnostic and test interfaces | ✔ | |

*FR 3 – System integrity*

| Requirement | | Status | Note |
|---|---|---|---|
| CR 3.1 | Communication integrity | ✔ | |
| EDR 3.2 | Protection from malicious code | ✔ | Secure boot functionality implemented. |
| CR 3.3 | Security functionality verification | ✔ | Security functions can be tested by the user. For example: failed login attempts are logged; a timeout is triggered for a new login attempt. The timeout duration increases with the number of failed attempts. |
| CR 3.4 | Software and information integrity | ✔ | |
| | RE (1) Authenticity of software and information | ✔ | |
| CR 3.5 | Input validation | ✔ | |
| CR 3.6 | Deterministic output | ✔ | |
| CR 3.7 | Error handling | ✔ | |
| CR 3.8 | Session integrity | ✔ | |
| CR 3.9 | Protection of audit information | ✔ | |

| Requirement | | Status | Note |
|---|---|---|---|
| EDR 3.10 | Support for updates | ✔ | |
| | RE (1) Update authenticity and integrity | ✔ | |
| EDR 3.11 | Physical tamper resistance and detection | ✔ | The product can be sealed, providing mechanical access protection. |
| EDR 3.12 | Provisioning product supplier roots of trust | ✔ | Only firmware authorized by Endress+Hauser can be loaded onto the product. |
| EDR 3.13 | Provisioning asset owner roots of trust | (✔) | |
| EDR 3.14 | Integrity of the boot process | ✔ | |
| | RE (1) Authenticity of the boot process | ✔ | |

*FR 4 – Data confidentiality*

| Requirement | | Status | Note |
|---|---|---|---|
| CR 4.1 | Information confidentiality | (✔) | |
| CR 4.2 | Information persistence | ✔ | |
| | RE (1) Erase of shared memory resources | ✔ | |
| CR 4.3 | Use of cryptography | ✔ | |

*FR 5 - Restricted data flow*

| Requirement | | Status | Note |
|---|---|---|---|
| CR 5.1 | Network segmentation | ✔ | |

*FR 6 – Timely response to events*

| Requirement | | Status | Note |
|---|---|---|---|
| CR 6.1 | Audit log accessibility | ✔ | |
| CR 6.2 | Continuous monitoring | (✔) | |

*FR 7 - Resource availability*

| Requirement | | Status | Note |
|---|---|---|---|
| CR 7.1 | Denial of service protection | ✔ | |
| CR 7.2 | Resource management | ✔ | |
| CR 7.3 | Control system backup | ✔ | As of firmware version 1.1 |
| | RE (1) Backup integrity verification | ✔ | As of firmware version 1.1 |
| CR 7.4 | Control system recovery and reconstitution | ✔ | As of firmware version 1.1 |
| CR 7.6 | Network and security configuration settings | ✔ | |
| CR 7.7 | Least functionality | ✔ | |
| CR 7.8 | Control system component inventory | (✔) | |


www.addresses.endress.com

Endress+Hauser

People for Process Automation