

# Special Documentation

## Security Manual

### Fermentation Monitor QWX43

Continuous monitoring of key parameters such as alcohol content, extract content and original gravity in beer





A0023555

# Table of contents

<b>1</b>	<b>Notification of security vulnerabilities and advisories .....</b>	<b>4</b>	4.3	Installation .....	18
<b>2</b>	<b>About this document .....</b>	<b>5</b>	4.4	Configuration .....	18
2.1	Document function .....	5	4.4.1	Commissioning and configuring the product .....	18
2.2	Symbols .....	5	4.4.2	Required security steps during commissioning .....	18
2.2.1	Safety symbols .....	5	4.4.3	Network configuration .....	19
2.2.2	Symbols for certain types of information and graphics .....	5	4.4.4	Configuring the firewall .....	19
2.3	Documentation .....	6	4.4.5	Configuring the wireless access point .....	19
2.3.1	Further applicable documents .....	6	4.4.6	Hardening the product .....	20
2.3.2	Purpose and content of the document types .....	6	4.4.7	Configuring user data .....	20
<b>3</b>	<b>System design .....</b>	<b>8</b>	4.4.8	Security-related product settings ....	20
3.1	Target group .....	8	4.4.9	User management and impact on security .....	20
3.2	System overview - direct integration version ...	8	<b>5</b>	<b>Operation .....</b>	<b>21</b>
3.2.1	General information .....	8	5.1	Target group .....	21
3.2.2	System configuration and system boundaries – “Direct integration” version .....	8	5.2	Requirements of the personnel .....	21
3.2.3	Example of system configuration and network configuration - "Direct integration" version .....	9	5.3	Tasks during operation .....	21
3.3	System overview - "Netilion server platform" version .....	11	5.4	Security aspects during operation .....	21
3.3.1	General information .....	11	5.5	Update management .....	22
3.3.2	System configuration and system boundaries – “Netilion server platform” version .....	11	5.6	Repeating the risk analysis .....	22
3.3.3	Example of system configuration and network configuration – “Netilion server platform” version .....	13	5.7	Repair and disposal .....	22
3.4	Defining the security level .....	13	<b>6</b>	<b>Decommissioning .....</b>	<b>23</b>
3.5	Typical operating environment of the product .....	14	6.1	Target group .....	23
3.6	Measures required if necessary operating environment cannot be provided .....	14	6.2	Requirements of the personnel .....	23
3.7	Carrying out risk analysis and risk assessment .....	14	6.3	Decommissioning the product .....	23
3.8	Recommended risk minimization measures ..	15	<b>7</b>	<b>Appendix .....</b>	<b>24</b>
3.8.1	Taking the entire system into account .....	15	7.1	Security checklist for the product life cycle ...	24
3.8.2	Training the users .....	15	7.2	Version history .....	24
3.8.3	Optimizing access management .....	16	7.3	Information for security audits .....	24
3.8.4	Monitoring device data and device status .....	16	7.3.1	Services for operation and integration into the control system ("Direct integration" version) .....	24
3.8.5	Updating product software .....	16	7.3.2	Services for operation and the Endress+Hauser Netilion server platform ("Netilion server platform" version) .....	25
<b>4</b>	<b>Commissioning (installation and configuration) .....</b>	<b>18</b>			
4.1	Target group .....	18			
4.2	Requirements of the personnel .....	18			

# 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](mailto: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](http://www.endress.com/deviceviewer)
- The download area of the Endress+Hauser website  
[www.endress.com/downloads](http://www.endress.com/downloads)

#### Further applicable documents Fermentation Monitor QWX43

- Technical Information TI01628F
- Operating Instructions BA02162F
- Special Documentation SD02875
  - Start Up Guide: commissioning, radio approvals
- Netilion – Terms of Service  
<https://netilion.endress.com/legal/terms-of-service>
- Netilion – Privacy Policy  
<https://netilion.endress.com/legal/privacy-policy>
- Netilion – Security Policy  
<https://netilion.endress.com/legal/security-policy>
- Netilion – Service Level Agreement  
<https://netilion.endress.com/legal/service-level-agreement>

### 2.3.2 Purpose and content of the document types

#### Technical Information (TI)

##### Planning aid

This document contains all the technical data on the product and provides an overview of everything that can be ordered with the product.

#### Brief Operating Instructions (KA)

##### Guide that takes you quickly to the 1st measured value

The Brief Operating Instructions contain all the essential information from incoming acceptance to initial commissioning.

#### Operating Instructions (BA)

##### Your comprehensive reference

The Operating Instructions contain all the information that is required in various phases of the life cycle of the product: from product identification, incoming acceptance and storage, to mounting, electrical connection, operation and commissioning through to troubleshooting, maintenance and disposal.

#### Safety Instructions (XA)

Safety Instructions (XA) are supplied with the product depending on the approval. They are an integral part of the Operating Instructions.



The nameplate indicates the Safety Instructions (XA) that are relevant to the product.

**Special Documentation (SD)****Additional information**

Special Documentation provides additional information on the product. Additional information can include graphical representation of commissioning, for example, or information on an app.

## 3 System design

### 3.1 Target group

This section is aimed at planners and system integrators.

### 3.2 System overview - direct integration version

#### 3.2.1 General information

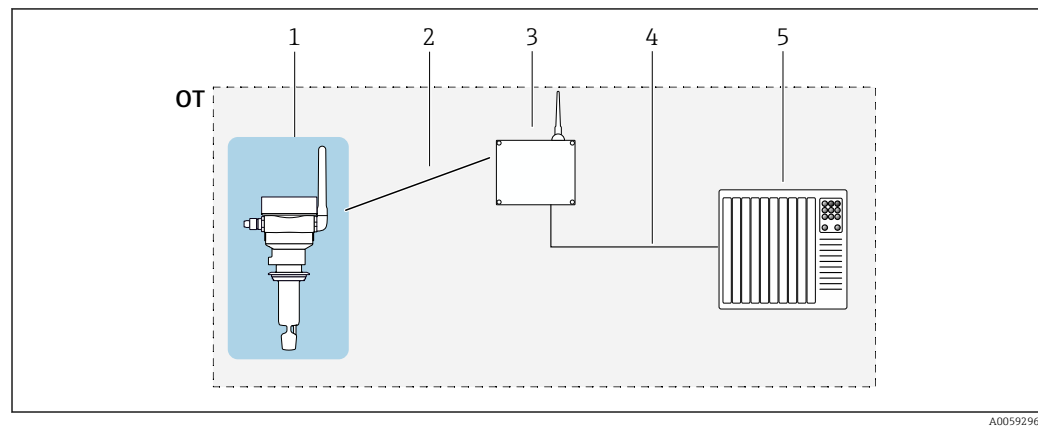
The Fermentation Monitor QWX43 is equipped with the following interfaces:

- WLAN connection TCP port 50000 / SNTP 123
- WPA2-PSK WLAN connection http (RSA) – Port 80

#### 3.2.2 System configuration and system boundaries – “Direct integration” version

**i** This Security Manual covers the "Direct integration" version of the Fermentation Monitor QWX43, as well as the local device interfaces WLAN hot spot and TCP port 50000. Other components such as customer-provided wireless access points, automation systems (e.g. PLC/SCADA), and operating tools are not part of this manual. In the following diagram, the system boundaries are marked in blue.

Firmware updates can be carried out either online via the Endress+Hauser Netilion server platform or offline. To log into the Netilion server platform, you must change the operating mode of the Fermentation Monitor → [16](#). For detailed information on the Netilion server platform, see: → [11](#)



**i** 1 System configuration Fermentation Monitor QWX43 - Direct integration; blue markings indicate the system boundaries for this manual.

OT Operational Technology, in this context, fieldbus network outside the Internet

1 Fermentation Monitor QWX43

2 WLAN connection (wireless connection)

3 Wireless access point

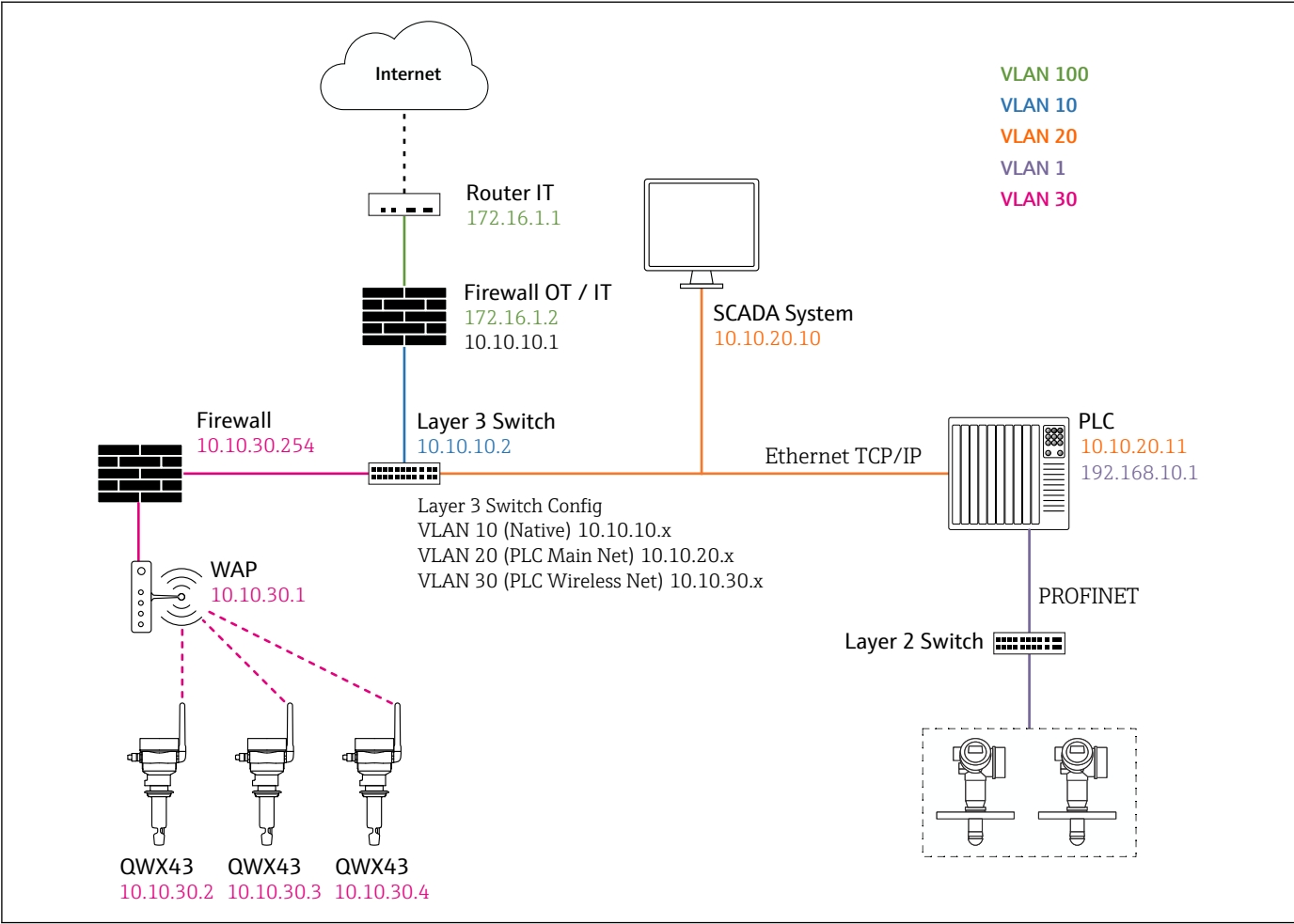
4 Wired connection: control system (TCP/IP)

5 Automation system

**i** The Fermentation Monitor is generally referred to in this document as a product or terminal, depending on the context.



3.2.3 Example of system configuration and network configuration - "Direct integration" version



A0059416

2 Example of system configuration and network configuration Fermentation Monitor QWX43 – Direct integration

VLAN configuration

The diagram shows the following VLANs used for logical separation and protection of SCADA, PLC, Fermentation Monitor devices, and IT network components.

VLAN-ID	Name/Zone	Typical components	Address range	Description/function
VLAN 100	Corporate IT VLAN	IT router, IT firewall	172.16.1.x	Standard network for office IT, Internet access and optionally for secure remote access on SCADA/ IIoT
VLAN 10	OT network management VLAN	OT firewall, Layer 3 switch	10.10.10.x	Routing between OT network (address range 10.10.x.x) and IT network (address range 172.16.1.x)
VLAN 20	SCADA/Control VLAN	SCADA system, PLC (SCADA interface)	10.10.20.x	Monitoring and operation of industrial processes with the SCADA system, such as WinCC

VLAN-ID	Name/Zone	Typical components	Address range	Description/function
VLAN 1	PROFINET VLAN	PROFINET device 1, PROFINET device 2, PLC (PROFINET port)	192.168.10.x	Real-time communication between the PLC and field devices via the PROFINET protocol
VLAN 30	QWX43 VLAN	Wireless access point, firewall wireless access point, Fermentation Monitor devices 1 to 3	10.10.30.x	Secured WLAN access for all Fermentation Monitor devices

#### *Firewall configuration of the QWX43 VLAN*

To secure the wireless access points (WAP) and isolate the QWX43 VLANs, a dedicated firewall is configured to ensure controlled and secure access.

The QWX43 VLAN firewall is configured as follows:

- Data traffic from the Fermentation Monitor devices in the 10.10.30.x IP range to the SCADA system and to the PLC in the 10.10.20.x IP range is permitted.
- For data transmission between the control system and Fermentation Monitor, only connections on port 50000 are permitted.
- All other data traffic between the QWX43 VLAN and the other networks VLAN 1 and VLAN 10 is blocked. This prevents unauthorized connections or potential attack vectors from the QWX43 VLAN.

This firewall configuration protects the QWX43 VLAN and the other segments of the OT network, while still allowing the necessary data exchange with the control system.

#### **Components**

The diagram shows the following components with associated VLANs, IP addresses, and functions.

Component	VLAN	IP address	Function
Internet/Netilion server platform	–	Public IP (dynamic IP)	Remote monitoring, device management, updates via Netilion server platform
IT router	VLAN 100	172.16.1.1	Internet gateway for secure access to the Internet
IT firewall	VLAN 100	172.16.1.2	Separation between OT and IT networks, Deep Packet Inspection enabled
OT firewall	VLAN 10	10.10.10.1	Segments OT network and IT networks, implements access controls (Zone Border)
Layer 3 switch	VLAN 10	10.10.10.2	Routing within the OT network between VLAN 30, VLAN 20 and VLAN 1
SCADA system	VLAN 20	10.10.20.10	Monitoring and control of processes in the OT network via HMI
PLC (SCADA-side)	VLAN 20	10.10.20.11	Communication interface between SCADA and PLC
PLC (PROFINET-side)	VLAN 1	192.168.10.1	Primary control for PROFINET components in VLAN 1
PROFINET device 1	VLAN 1	192.168.10.2	PROFINET device for process data acquisition
PROFINET device 2	VLAN 1	192.168.10.3	PROFINET device for process data acquisition
Fermentation Monitor Device 1	VLAN 30	10.10.30.2	Fermentation Monitor for process data acquisition
Fermentation Monitor Device 2	VLAN 30	10.10.30.3	Fermentation Monitor for process data acquisition
Fermentation Monitor Device 3	VLAN 30	10.10.30.4	Fermentation Monitor for process data acquisition

Component	VLAN	IP address	Function
Wireless access point	VLAN 30	10.10.30.1	Access point for wireless communication to the Fermentation Monitor devices
Firewall for wireless access point	VLAN 30	10.10.30.254	<ul style="list-style-type: none"> <li>Protects the QWX43 VLAN and other segments of the OT network</li> <li>Allows necessary data exchange with the control system</li> <li>Allows only outgoing HTTPS connections</li> </ul>

### 3.3 System overview - "Netilion server platform" version

#### 3.3.1 General information

The Fermentation Monitor QWX43 is equipped with the following interfaces:

- WLAN connection https (mTLS) – Port 443/SNTP 123
- WPA2-PSK WLAN connection http (RSA) – Port 80

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

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

If the Fermentation Monitor is operated in **Netilion Cloud** mode, all outgoing connections to the Netilion server platform are encrypted via HTTPS using mutual authentication (mTLS). The data is end-to-end encrypted using **TLS 1.2**. The Fermentation Monitor authenticates itself using device certificates on both the client and server sides.

User-related access to Netilion services is authorized via **OAuth 2.0**.

You can operate the Fermentation Monitor with the following digital application:

Netilion Fermentation <https://netilion.endress.com/app/fermentation>

The Netilion Fermentation is commissioned via WLAN through the integrated web server or the setup wizard of the Fermentation Monitor.

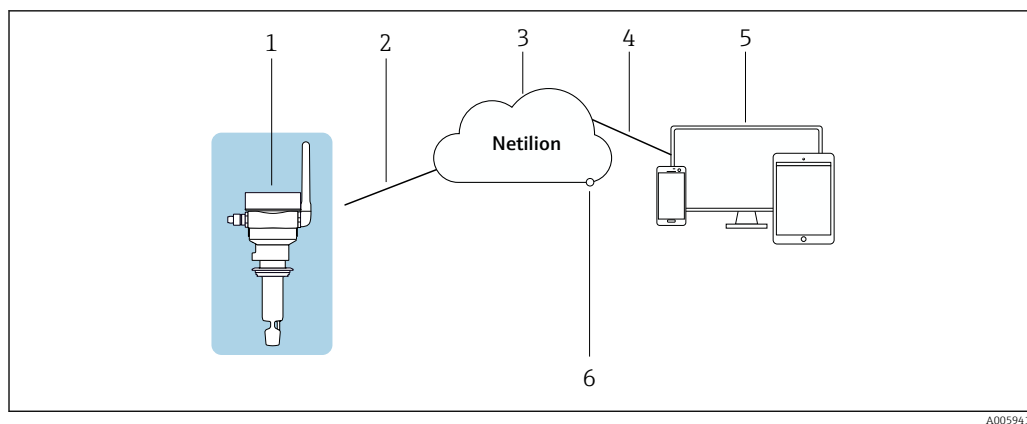



For detailed information, see the Operating Instructions. → 6

#### 3.3.2 System configuration and system boundaries – “Netilion server platform” version




This Security Manual covers the "Netilion server platform" version of the Fermentation Monitor QWX43, as well as the local device interface WLAN hot spot and the interface to the Endress+Hauser Netilion server platform. Other components, such as customer-provided automation systems like PLC/SCADA, the Netilion server platform, and operating tools, are not part of this manual. In the following diagram, the system boundaries are marked in blue.

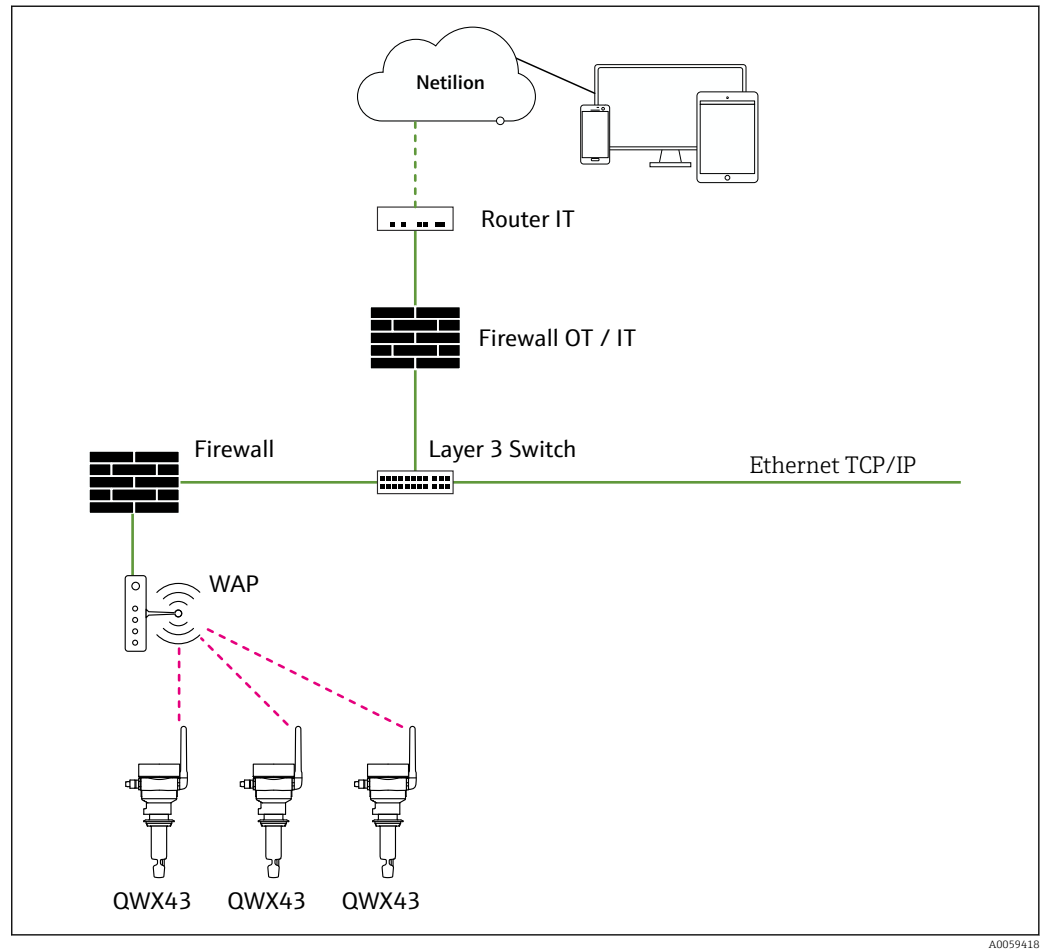


 3 System configuration Fermentation Monitor QWX43, blue markings indicate the system boundaries for this manual.

- 1 Fermentation Monitor QWX43
- 2 WLAN HTTPS Internet connection (mTLS 1.2)
- 3 Netilion server platform
- 4 https Internet connection
- 5 Netilion Services: browser-based Netilion service app
- 6 Netilion Connect: Application Programming Interface (API)

 The Fermentation Monitor is generally referred to in this document as a product or terminal, depending on the context.

### 3.3.3 Example of system configuration and network configuration – “Netilion server platform” version



4 Example of system configuration and network configuration Fermentation Monitor QWX43 – Netilion server platform

## 3.4 Defining the security level

Depending on the required security level, the system and the products installed on it must meet various requirements. Initially, you must specify the required **security level** SL1 to SL4 for the system. Depending on the security level, you define the requirements for the system in accordance with IEC 62443-3-3 and the requirements for the product in accordance with EN 62443-4-2.

The Fermentation Monitor as a field device alone cannot meet any security level in accordance with IEC 62443-3-3.

The Fermentation Monitor was developed in accordance with IEC 62443-4-1, taking into account a secure development cycle (SDL). In addition, the Fermentation Monitor meets the requirements of the EN 18031 (cybersecurity for radio equipment).

The system in which the Fermentation Monitor is integrated must meet the targeted security level.

The actually achievable security level results only from the combination of:

- Secure device configuration
- Integration into a segmented and hardened network environment
- Integration into an overall system architecture based on the zone/conduit model in accordance with IEC 62443-3-2 and IEC 62443-3-3.

### 3.5 Typical operating environment of the product

We recommend that you define the typical operating environment of the product in order to draw up the security-related properties.

The requirements of the environment should be determined by assessing the operating environment. For example, you may observe a denial-of-service attack.

The following considerations may apply for a typical operating environment for example:

- The product is a system component.
- The product is equipped with at least one Ethernet-based interface (WLAN). 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 by authorized personnel.
- Only authorized personnel can access the product via the associated Human Machine Interface (HMI).

Since the computing power of the product under consideration is limited, it can only withstand attacks to a limited extent.

### 3.6 Measures required if necessary operating environment cannot be provided

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

To prevent physical access to the Fermentation Monitor, we recommend mounting the Fermentation Monitor at a process connection point that is accessible only to authorized personnel. This mounting location could, for example, be within a sealed tank dome or in a secured operational fermentation/storage tank area.

Additionally, we recommend mounting the access point within a secured area and away from publicly accessible zones.

### 3.7 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.

## 3.8 Recommended risk minimization measures

### 3.8.1 Taking the entire system into account

The Fermentation Monitor is a terminal that can be used either in a conventional production system or in a closed IIoT ecosystem. The modular architectures of such systems promote the use of various components. This can result in interface mismatches between products, increasing the attack surface.

For the "Direct integration" version, observe the following:

- The fieldbus network (OT-WLAN, 2.4 GHz, WPA2-PSK) and company network (IT) must be strictly separated. Filters or VLAN rules must not allow local PLC data traffic on TCP port 50000 to leave the fieldbus network segment.
- To ensure consistent implementation of defense-in-depth, Endress+Hauser recommends segmenting fieldbus networks in accordance IEC 62443-3-3 (zone/conduit model).
- The wireless access point for the Fermentation Monitor must be treated as a separate security zone. SSID, password, and transmission power must be configured according to the least privilege principle.
- The default password must be changed during commissioning and centrally managed.


Observe the following for the "Netilion server platform" version:

- Connection of the Fermentation Monitor to the Internet in "Netilion Cloud" operating mode must occur at a minimum via a firewall that explicitly allows mTLS traffic on TCP port 443 and SNTP port 123.
- To ensure consistent implementation of defense-in-depth, Endress+Hauser recommends segmenting fieldbus networks in accordance IEC 62443-3-3 (zone/conduit model).
- The wireless access point for the Fermentation Monitor must be treated as a separate security zone. SSID, password, and transmission power must be configured according to the least privilege principle.
- The default password must be changed during commissioning and centrally managed.
- Use IDS/IPS monitoring at the transition points between OT fieldbus zones and the Netilion server platform to detect anomalies or DoS attempts at an early stage. The Fermentation Monitor can only defend itself from such attacks to a limited extent due to its limited resources.

### 3.8.2 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.

### 3.8.3 Optimizing access management

You will require appropriate access credentials such as user name and password to access the Fermentation Monitor via the integrated web server. You must use the default initial password when logging in for the first time. The password must be changed, stored securely, and treated confidentially after you have logged in for the first time →  20.



For detailed information about the password, see the Operating Instructions →  6

#### **Additional for version "Direct integration"**

You will also need the following for operating the Fermentation Monitor in a WLAN-based OT network (control):

- SSID and WPA2-PSK of the configured wireless access point
- Static IP address or DHCP assignment within the OT network
- Enabling TCP port 50000 in firewall/VLAN rules

#### **Additional version "Netilion server platform"**

You will also need the following for operating the Fermentation Monitor in a WLAN-based OT network (control):

SSID and WPA2-PSK of the configured wireless access point

### **IIoT ecosystem**

We recommend that the same rules be applied for identity and access management for access to the IIoT ecosystem as for other company areas.

- Grant employees only the access rights they need to perform their tasks.
- Only allocate user accounts with strong passwords.
- Use a password manager to generate, store, and manage passwords.

### 3.8.4 Monitoring device data and device status

As real-time monitoring is not a realistic possibility for most users, this process has to be automated. We recommend using monitoring software that monitors specific parameters and the status of the product and of the network and reports any deviations.

#### **Monitoring via WLAN**

The Fermentation Monitor is a participant in a WLAN network. Detecting and correcting anomalies is the responsibility of the network operator.

#### **"Direct integration" version: monitoring communication via a control system**

The Fermentation Monitor is part of a network in a process automation system and can communicate with the PLC via TCP port 50000 using proprietary OUC telegram structures. Communication with the PLC is not encrypted. If the Fermentation Monitor suddenly reports unrealistic values, this may be an indication of an attack. Physical protection, as well as the detection and resolution of anomalies, is the responsibility of the control system operator.

#### **"Netilion server platform" version: monitoring via the IIoT ecosystem**

The Fermentation Monitor can act as a terminal in an IIoT ecosystem, and the detection of anomalies is the responsibility of the higher-level system.

### 3.8.5 Updating product software

The requirements for connectivity, IT security, and the libraries used are constantly changing. Regular firmware updates are therefore necessary.

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.



You have the following options for performing a firmware update:

- Online via the Netilion server platform
- Offline via the web server of the Fermentation Monitor

To perform an update via the Netilion server platform, you must log in to Netilion.

Before you can perform a firmware update via Netilion with the direct integration variant, you must set the Fermentation Monitor to hotspot mode and switch the **Operation Mode**.



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

For a firmware update via the web server, contact Endress+Hauser Service.

Firmware updates can be downloaded from the following address: <https://www.endress.com/downloads>

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

To prevent physical access to the Fermentation Monitor, we recommend mounting the Fermentation Monitor at a process connection point that is accessible only to authorized personnel. This mounting location could, for example, be within a sealed tank dome or in a secured operational fermentation/storage tank area.

Additionally, we recommend mounting the access point within a secured area and away from publicly accessible zones.

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



- For detailed information on network management, see: → 13
- For detailed information on the firewall configuration, see: → 19

### 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 → 14.

### 4.4.3 Network configuration

A secure network configuration forms the basis for protected operation of the Fermentation Monitor. The following recommendations can help minimize attack surfaces, depending on the network context, and enable reliable, tamper-proof data exchange.

- Assign a static IP address to each Fermentation Monitor to each associated access point.
- Disable DHCP to avoid unauthorized IP assignments.
- Use a dedicated separate network segment for the Fermentation Monitor devices. This network segment must be clearly separated from other operational and administrative networks.
- The use of a VLAN is suitable for virtual separation. A VLAN enables granular control of access and data flows.
- Use a firewall between the network segment with the Fermentation Monitor devices and the other network segments.
- Block all other communication connections from the network segment with the Fermentation Monitor devices.
- Use IP whitelisting to ensure that only authorized devices access the network.



For detailed information on the firewall configuration, see: → 19

#### Example of VLAN-based network segmentation

The Fermentation Monitor does not support IEEE 802.1Q and is therefore not VLAN-aware. For secure operation in segmented networks, however, we recommend assigning the WLAN in which the Fermentation Monitor is incorporated to a dedicated VLAN via access points. This enables logical separation from the remaining OT/IT network and reduces potential attack surfaces. Network segmentation should be implemented using VLAN-compatible access points, routers or firewalls.



For detailed information on network management, see: → 13

### 4.4.4 Configuring the firewall

The Fermentation Monitor does not have an integrated firewall. Additional firewalls or networking devices with firewall functionality must be provided by the customer.

We recommend installing a firewall between the network segment containing the Fermentation Monitor devices and other network segments.



For detailed information on the firewall configuration, see Operating Instructions: → 6

In addition, follow the instructions below:

- Only allow the TCP/IP ports that are required for operation of the Fermentation Monitor → 24.
- Block all ports that are not required for operation.
- "Direct integration" version: Limit outgoing data traffic to the target device (e.g. PLC) and to port 50000.

### 4.4.5 Configuring the wireless access point

We recommend applying the following settings after activating the hotspot:

- Set up WPA2-PSK as the authentication method and configure the wireless access point accordingly.
- Use a strong, randomly generated password with at least 16 characters and change it regularly.
- Enable MAC filtering. Allow only the MAC addresses of authorized Fermentation Monitor devices.
- Install the access point within a secured area and away from publicly accessible areas.

The wireless access point is not part of this manual. The actual security level achieved by the wireless access point is the responsibility of the plant operator.

#### 4.4.6 Hardening the product

In the field of security, "hardening" means enabling only those services that are required for the proper operation of the product in the intended application.



The Fermentation Monitor uses a hardened operating system. The operating system is configured according to the "minimum principle". Only the necessary services/ports are installed and active.

Endress+Hauser has taken the following measures for the operating system:

- **Secure Services**  
Security-relevant functions run in mutually isolated processes to prevent cross-interference.
- **Secure Boot**  
A signed boot loader checks the integrity of the firmware during startup and prevents execution of unauthorized software.
- **Secure Storage**  
Keys, certificates, and passwords are stored in encrypted memory areas. Direct external access is blocked.
- **Password Policy**  
For integrating the Fermentation Monitor with the wireless access point (direct integration) or into the plant's local WLAN (Netilion server platform), the Fermentation Monitor provides a WLAN (hotspot). Commissioning the Fermentation Monitor is carried out in hotspot mode using a factory-set initial password. The password must be changed during initial commissioning.

Password - requirement and recommendation



- At least 16 characters Shorter passwords are rejected.
- Use a strong, randomly generated password with numbers, upper- and lowercase letters, and special characters.
- Keep passwords confidential.
- Only enter passwords when unobserved.



 For detailed information on commissioning and the initial password, see the Operating Instructions. →  6

#### 4.4.7 Configuring user data

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

In addition, for the "Netilion server platform" version, a Netilion account is required if a firmware update is to be performed online. The user sets the access credentials and can change them later.

 For detailed information on passwords, see: →  20

 For detailed information on creating a Netilion Account, see the Operating Instructions →  6

#### 4.4.8 Security-related product settings

For the Fermentation Monitor, no security-relevant settings need to be configured.

#### 4.4.9 User management and impact on security

The Fermentation Monitor has only one user level (admin).

## 5 Operation

### 5.1 Target group

This section is aimed at operating personnel.

### 5.2 Requirements of the personnel

Personnel must fulfill the following requirements:

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

### 5.3 Tasks during operation

Operate the product in accordance with the associated Operating Instructions. With regard to security, please also refer to this section and the following sections.

The Fermentation Monitor does not require any intervention during operation.

### 5.4 Security aspects during operation


The certificates saved in the Fermentation Monitor have a limited validity period of 5 years.

Approximately 1 year before the certificates expire, Endress+Hauser renews the certificates for the Fermentation Monitor via the Netilion server platform. Log the Fermentation Monitor into the Netilion server platform at least once a year.

To ensure continuous data collection and secure transmission of measurement data, technical and organizational measures must be implemented throughout the entire operating period. These measures are based on the intended security level for the system in accordance with IEC 62443-3-3.


#### Security measures depending on the required security level

The following measures are required for security levels SL 1 to SL 4:

- Perform firmware updates regularly →  16.
- Update the access point firmware regularly.
- Ensure the integrity of network connections.
- Check firewall and port configurations.

For a security level SL 3, the following measures are necessary. For a security level SL 2, these measures are recommended.

- Carry out periodic security audits, e.g. in accordance with VDI/VDE 2182 or NIST SP 800-82.
- Log access and operating data.
- Replace or rotate access credentials at regular intervals.
- Monitor network infrastructure, including anomaly detection.

 The Fermentation Monitor as a field device alone cannot meet any security level in accordance with IEC 62443-3-3. The system in which the Fermentation Monitor is integrated must meet the targeted security level. Implementing the required security measures is the responsibility of the plant operator.

## 5.5 Update management

Endress+Hauser provides firmware updates via the Netilion server platform and the Downloads area of Endress+Hauser.

To perform a firmware update via the Netilion server platform, the user must initiate the update through the Netilion server platform. The timing of the update can be adjusted. It is necessary to restart the Fermentation Monitor following some of the updates. The restart is performed automatically.

Contact Endress+Hauser Service if you want to perform the firmware update offline.



For detailed information on firmware updates: → 16

Endress+Hauser provides updates for the following purposes:

- 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.

## 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.	No action required.
The product has a fault that you are unable to rectify.	<ol style="list-style-type: none"> <li>1. Contact Endress+Hauser.</li> <li>2. Follow instructions from Endress+Hauser.</li> </ol>
The product is defective and must therefore be disposed of.	<ul style="list-style-type: none"> <li>▶ Physically destroy the product and dispose of it according to the operating instructions.</li> </ul>
The product is to be disposed of.	<ul style="list-style-type: none"> <li>▶ Physically destroy the product and dispose of it according to the operating instructions.</li> </ul>
The Netilion Service Subscription has terminated.	<p>No action required.</p> <p> Once a new Netilion service subscription has been activated, the Fermentation Monitor can be used again.</p>

## 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. → 14 If required, alternative measures taken into account. → 14	<input type="checkbox"/>
	Engineering-phase planning work considered Threat analysis and risk assessment carried out. → 8	<input type="checkbox"/>
	Where possible, risk minimization measures have been taken into account. → 15	<input type="checkbox"/>
Goods receipt/transport	Verified that the packaging is unopened. → 18	<input type="checkbox"/>
Commissioning	Product hardened for specific application → 20	<input type="checkbox"/>
Operation	Update management requirements observed → 22	<input type="checkbox"/>
	Planning for renewed threat analysis performed → 22	<input type="checkbox"/>
Decommissioning	Product taken out of service → 23 Depending on reason for decommissioning, disable or destroy the product.	<input type="checkbox"/>

### 7.2 Version history

Document version	Firmware version	Hardware version	Changes
01.25	From 04.03.zz	Dev. Rev. 1	First version

### 7.3 Information for security audits

#### 7.3.1 Services for operation and integration into the control system ("Direct integration" version)

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

Service/function	Port	Protocol	Comment
OUC data communication (PLC)	50000	TCP (Open User Communication)	Proprietary port for connection to a Siemens controller and Rockwell controller
DHCP (client IP assignment)	67 (Server) 68 (Client)	UDP	DHCP is enabled by default. It is recommended to disable DHCP and configure a static IP address for the Fermentation Monitor.
Web server	80	HTTP (local only)	<ul style="list-style-type: none"> <li>For setup (hotspot): access via <a href="http://10.10.0.1">http://10.10.0.1</a> for WLAN configuration and to select the "PLC" or "Netilion Cloud" operating mode.</li> <li>Local access via IP of the Fermentation Monitor</li> </ul>



### 7.3.2 Services for operation and the Endress+Hauser Netilion server platform ("Netilion server platform" version)

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

Service/ function	Port	Protocol	Comment
HTTPS to Netilion API	443	TCP/HTTPS (mTLS)	Main connection to Netilion server platform: TLS 1.2/1.3 and client certificate (Amazon CA)
SNTP (time server)	123	UDP/SNTP	Time synchronization with Internet time server
DNS (name resolution)	53	UDP/TCP	Required for *.netilion.endress.com, e.g. API resolution
DHCP (client IP assignment)	67 (Server) 68 (Client)	UDP	DHCP is enabled by default. It is recommended to disable DHCP and configure a static IP address for the Fermentation Monitor.
Web server	80	HTTP (local only)	<ul style="list-style-type: none"> <li>For setup (hotspot): access via <a href="http://10.10.0.1">http://10.10.0.1</a> for WLAN configuration and to select the "PLC" or "Netilion Cloud" operating mode.</li> <li>Local access via IP of the Fermentation Monitor</li> </ul>







[www.addresses.endress.com](http://www.addresses.endress.com)

---