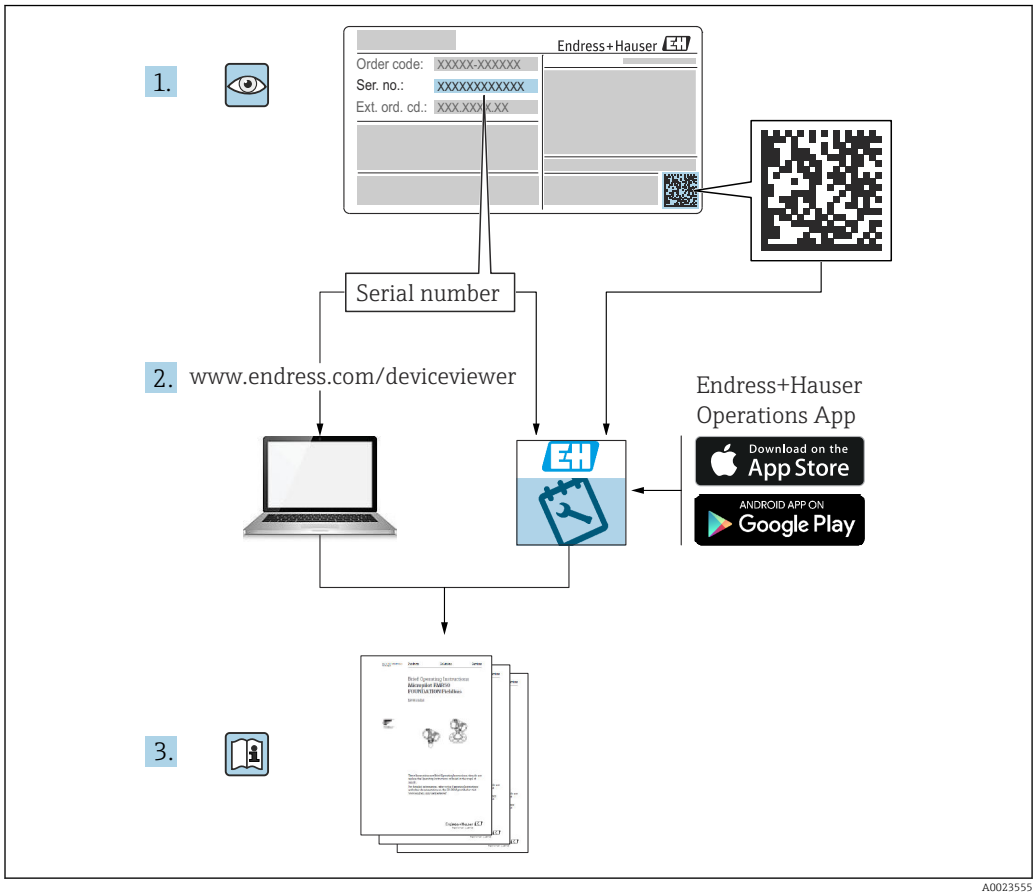
SD03441F/00/DE/01.25-00
71713214
2025-07-14

Sonderdokumentation
Security-Handbuch Fermentation Monitor QWX43

Kontinuierliche Überwachung von Schlüsselparametern wie Alkoholgehalt, Extraktgehalt und Stammwürze in Bier

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

Inhaltsverzeichnis

1 Meldung von Sicherheitslücken und Advisories 4

2 Hinweise zum Dokument 5
2.1 Dokumentfunktion 5
2.2 Verwendete Symbole 5
2.2.1 Warnhinweissymbole 5
2.2.2 Symbole für Informationstypen und Grafiken 5
2.3 Dokumentation 6
2.3.1 Mitgeltende Dokumente 6
2.3.2 Zweck und Inhalte der Dokumentationstypen 6

3 System-Design 8
3.1 Zielgruppe 8
3.2 Systemüberblick – Variante "Direktintegration" 8
3.2.1 Allgemeine Informationen 8
3.2.2 Systemaufbau und Systemgrenzen – Variante "Direktintegration" 8
3.2.3 Beispiel Systemaufbau und Netzwerkkonfiguration – Variante "Direktintegration" 9
3.3 Systemüberblick – Variante "Netilion Serverplattform" 11
3.3.1 Allgemeine Informationen 11
3.3.2 Systemaufbau und Systemgrenzen – Variante "Netilion Serverplattform" . . . 11
3.3.3 Beispiel Systemaufbau und Netzwerkkonfiguration – Variante "Netilion Serverplattform" 13
3.4 Security-Level festlegen 13
3.5 Typische Einsatzumgebung des Produkts 14
3.6 Maßnahmen, falls erforderliche Einsatzumgebung nicht erfüllbar ist 14
3.7 Bedrohungsanalyse und Risikobeurteilung durchführen 14
3.8 Empfehlung für risikomindernde Maßnahmen 15
3.8.1 Gesamtsystem betrachten 15
3.8.2 Anwender schulen 15
3.8.3 Zugriffsmanagement optimieren 16
3.8.4 Gerätedaten und Gerätestatus überwachen 16
3.8.5 Produkt-Software updaten 17

4 Inbetriebnahme (Installation und Konfiguration) 18
4.1 Zielgruppe 18
4.2 Anforderungen an das Personal 18
4.3 Installation 18
4.4 Konfiguration 18
4.4.1 Produkt in Betrieb nehmen und konfigurieren 18
4.4.2 Erforderliche Security-Schritte während der Inbetriebnahme 18
4.4.3 Netzwerk konfigurieren 19
4.4.4 Firewall konfigurieren 19
4.4.5 Wireless Access Point konfigurieren . 20
4.4.6 Produkt härten 20
4.4.7 Anwenderdaten konfigurieren 20
4.4.8 Security-relevante Einstellungen des Produkts 21
4.4.9 User-Management und Auswirkung auf die Security 21

5 Betrieb 22
5.1 Zielgruppe 22
5.2 Anforderungen an das Personal 22
5.3 Aufgaben während des Betriebes 22
5.4 Security-Aspekte während des Betriebes 22
5.5 Update-Management 23
5.6 Wiederholung der Bedrohungsanalyse 23
5.7 Reparatur und Entsorgung 23

6 Außerbetriebnahme 24
6.1 Zielgruppe 24
6.2 Anforderungen an das Personal 24
6.3 Produkt außer Betrieb nehmen 24

7 Anhang 25
7.1 Security-Checkliste für den Produktlebenszyklus 25
7.2 Versionshistorie 25
7.3 Informationen für Security-Audits 25
7.3.1 Dienste für den Betrieb und die Anbindung an das Leitsystem (Variante "Direktintegration") 25
7.3.2 Dienste für den Betrieb und die Endress+Hauser Netilion Serverplattform (Variante "Netilion Serverplattform") 26

1 Meldung von Sicherheitslücken und Advisories

Auf der folgenden Internetseite stellt Endress+Hauser Informationen zur Cybersicherheit sowie zur Security bereit: https://www.endress.com/cybersecurity

Diese Internetseite enthält beispielsweise folgende Informationen:
- Aktuelle Sicherheitswarnungen (Security Alerts), die Endress+Hauser Produkte betreffen
- Kontakt-Mailadresse, um Sicherheitslücken von Endress+Hauser Produkten zu melden. Über PGP besteht die Möglichkeit zur vertraulichen Kommunikation. Sie können den öffentlichen Schlüssel von der Internetseite herunterladen.
- Abonnement des E-Maildienstes für neue Advisories für Endress+Hauser Produkte
- Endress+Hauser Kontakt: PSIRT@endress.com

2 Hinweise zum Dokument

2.1 Dokumentfunktion

Dieses Security-Handbuch gilt ergänzend zu der mitgeltenden Produktdokumentation wie z.B. Betriebsanleitung, Technischen Information und ATEX-Sicherheitshinweisen. Die mitgeltende Produktdokumentation ist während des gesamten Lebenszyklus des Produkts zu beachten. Die für den Bereich Security zusätzlichen Anforderungen sind in diesem Security-Handbuch beschrieben.

2.2 Verwendete Symbole

2.2.1 Warnhinweissymbole

⚠ GEFAHR
Dieser Hinweis macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, zu Tod oder schwerer Körperverletzung führen wird.

⚠ WARNUNG
Dieser Hinweis macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, zu Tod oder schwerer Körperverletzung führen kann.

⚠ VORSICHT
Dieser Hinweis macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, zu leichter oder mittelschwerer Körperverletzung führen kann.

HINWEIS
Dieser Hinweis enthält Informationen zu Vorgehensweisen und weiterführenden Sachverhalten, die keine Körperverletzung nach sich ziehen.

2.2.2 Symbole für Informationstypen und Grafiken

Tipp
Kennzeichnet zusätzliche Informationen

Verweis auf Dokumentation

Verweis auf Abbildung

▶
Zu beachtender Hinweis oder einzelner Handlungsschritt

1., 2., 3.
Handlungsschritte

Ergebnis eines Handlungsschritts

1, 2, 3, ...
Positionsnummern

A, B, C, ...
Ansichten

2.3 Dokumentation

2.3.1 Mitgeltende Dokumente

Eine Übersicht über die zugehörige Dokumentation erhalten Sie wie folgt:
- *Device Viewer*: Seriennummer vom Typenschild eingeben
  www.endress.com/deviceviewer
- Downloadbereich der Endress+Hauser Internetseite
  www.endress.com/downloads

Mitgeltende Dokumente Fermentation Monitor QWX43

- Technische Information TI01628F
- Betriebsanleitung BA02162F
- Sonderdokumentation SD02875
  Start Up Guide: Inbetriebnahme, Funkzulassungen
- 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 Zweck und Inhalte der Dokumentationstypen

Technische Information (TI)

Planungshilfe
Das Dokument liefert alle technischen Daten zum Produkt und gibt einen Überblick, was rund um das Produkt bestellt werden kann.

Kurzanleitung (KA)

Schnell zum 1. Messwert
Die Anleitung liefert alle wesentlichen von der Warenannahme bis zur Erstinbetriebnahme.

Betriebsanleitung (BA)

Ihr Nachschlagewerk
Die Anleitung liefert alle Informationen, die in den verschiedenen Phasen des Lebenszyklus für das Produkt benötigt werden: Von der Produktidentifizierung, Warenannahme und Lagerung über Montage, Elektrischen Anschluss, Bedienungsgrundlagen und Inbetriebnahme bis hin zur Störungsbeseitigung, Wartung und Entsorgung.

Sicherheitshinweise (XA)

Abhängig von der Zulassung liegen dem Produkt bei Auslieferung Sicherheitshinweise (XA) bei. Diese Sicherheitshinweise sind integraler Bestandteil der Betriebsanleitung.

Auf dem Typenschild ist angegeben, welche Sicherheitshinweise (XA) für das jeweilige Produkt relevant sind.

Sonderdokumentation (SD)

Weitere Informationen
Eine Sonderdokumentation liefert weitere Informationen zu dem Produkt. Weitere Informationen können z.B. die Inbetriebnahme grafisch dargestellt oder Informationen zu einer App sein.

3 System-Design

3.1 Zielgruppe

Dieses Kapitel richtet sich an Planer und Systemintegratoren.

3.2 Systemüberblick – Variante "Direktintegration"

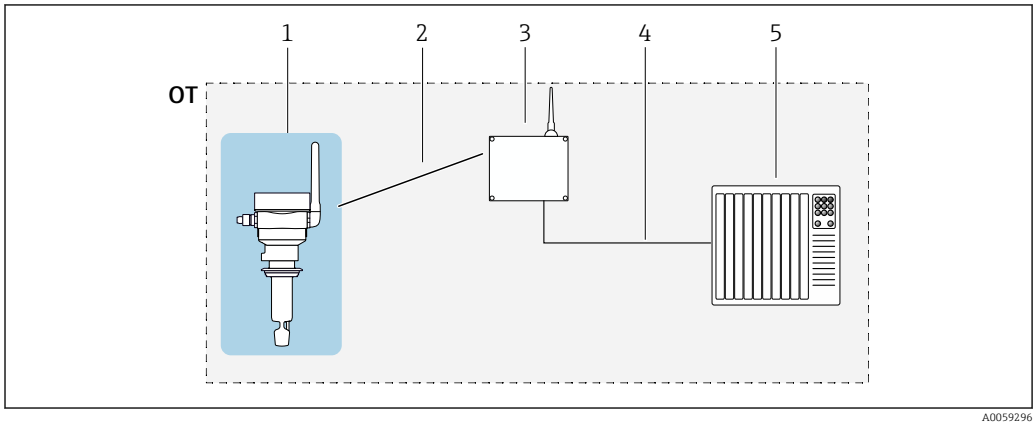
3.2.1 Allgemeine Informationen

Der Fermentation Monitor QWX43 ist mit folgenden Schnittstellen ausgestattet:
- WLAN-Verbindung TCP-Port 50000 / SNTP 123
- WPA2-PSK WLAN-Verbindung http (RSA) – Port 80

3.2.2 Systemaufbau und Systemgrenzen – Variante "Direktintegration"

In diesem Security-Handbuch werden für die Variante "Direktintegration" der Fermentation Monitor QWX43 sowie die lokalen Geräteschnittstellen WLAN-Hotspot und TCP-Port 50000 betrachtet. Weitere Komponenten wie kundenseitige Wireless Access Points, Automatisierungssysteme wie z.B. PLC / SCADA und Bedientools sind nicht Bestandteil dieses Handbuches. In der folgenden Abbildung sind die Systemgrenzen blau markiert.

Firmware-Updates können entweder online über die Endress+Hauser Netilion Serverplattform oder offline durchgeführt werden. Für die Anmeldung an die Netilion Serverplattform muss der Betriebsmodus des Fermentation Monitor geändert werden → 17. Detaillierte Informationen zur Netilion Serverplattform: → 11

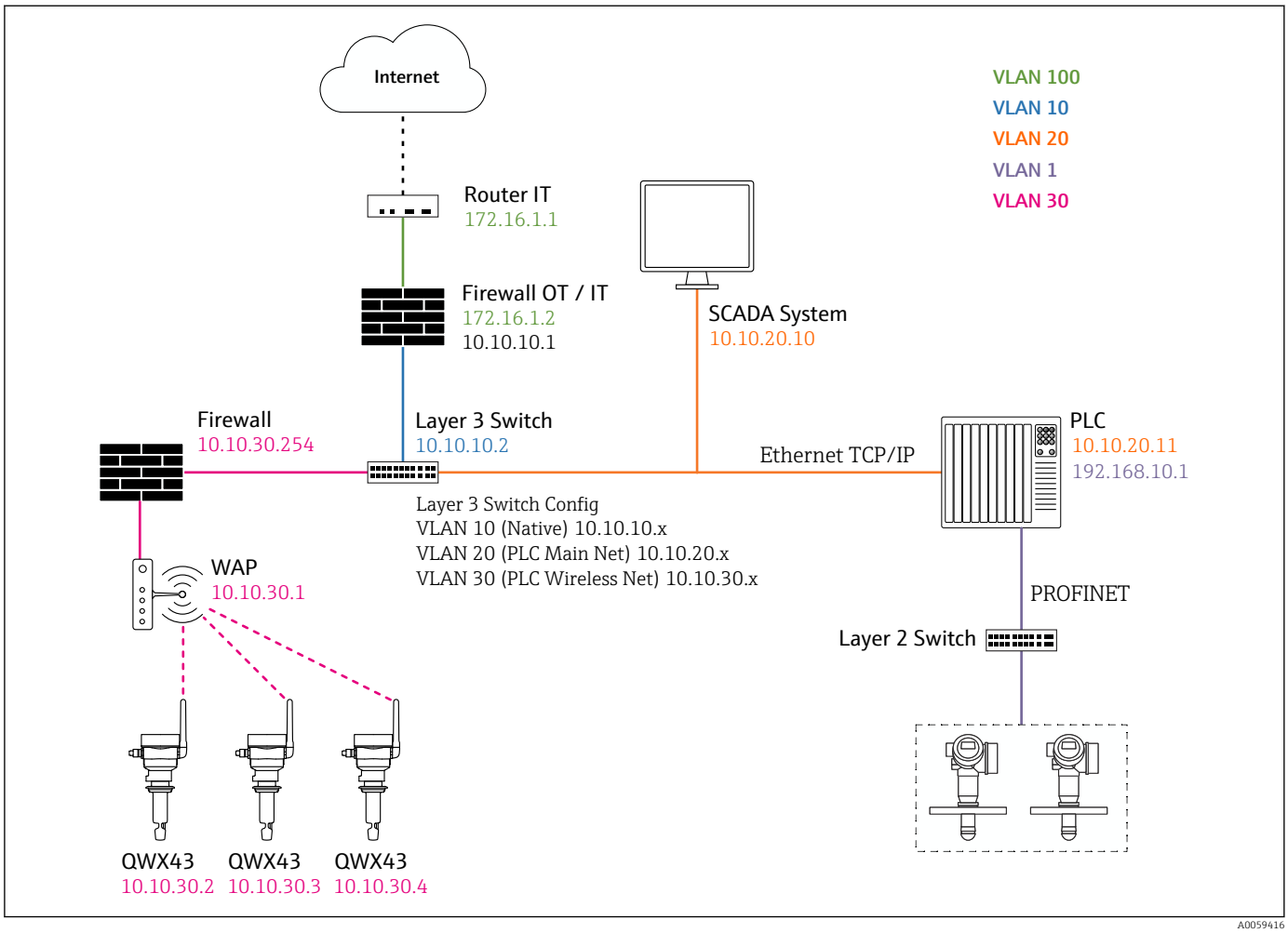


1 *Systemaufbau Fermentation Monitor QWX43 – Direktintegration, blaue Markierung zeigt die Systemgrenzen für dieses Handbuch*

OT Operational Technology, hier Feldbusnetzwerk außerhalb des Internets
1 Fermentation Monitor QWX43
2 WLAN-Verbindung (drahtlose Verbindung)
3 Wireless Access Point (drahtloser Zugangspunkt)
4 Drahtgebundene Verbindung: Leitsystem (TCP/IP)
5 Automatisierungssystem

Der Fermentation Monitor wird in diesem Dokument in den allgemeinen Texten abhängig vom Zusammenhang entweder als Produkt oder als Endgerät bezeichnet.

3.2.3 Beispiel Systemaufbau und Netzwerkkonfiguration – Variante "Direktintegration"



2 *Beispiel Systemaufbau und Netzwerkkonfiguration Fermentation Monitor QWX43 – Direktintegration*

VLAN-Konfiguration

In der Abbildung sind folgende VLANs zur logischen Trennung und Absicherung von SCADA, PLC, Fermentation Monitor Geräten sowie IT-Netzwerkkomponenten dargestellt.

VLAN-ID	Name / Zone	Typische Komponenten	Adressbereich	Beschreibung / Funktion
VLAN 100	Corporate IT VLAN	Router IT, Firewall IT	172.16.1.x	Standardnetz für Büro-IT, Internetzugang und optional für sichere Fernzugriffe auf SCADA / IIoT
VLAN 10	OT-Netzwerk-Management VLAN	Firewall OT, Layer 3 Switch	10.10.10.x	Routing zwischen OT-Netzwerk (Adressbereich 10.10.x.x) und IT-Netzwerk (Adressbereich 172.16.1.x)
VLAN 20	SCADA / Control VLAN	SCADA-System, PLC (SCADA-Schnittstelle)	10.10.20.x	Überwachung und Bedienung industrieller Prozesse durch das SCADA-System wie z.B. WinCC

VLAN-ID	Name / Zone	Typische Komponenten	Adressbereich	Beschreibung / Funktion
VLAN 1	PROFINET VLAN	PROFINET-Gerät 1, PROFINET-Gerät 2, PLC (PROFINET-Port)	192.168.10.x	Echtzeitfähige Kommunikation zwischen PLC und Feldgeräten über das PROFINET-Protokoll
VLAN 30	QWX43 VLAN	Wireless Access Point, Firewall Wireless Access Point, Fermentation Monitor Geräte 1 bis 3	10.10.30.x	Abgesicherter WLAN-Zugang für alle Fermentation Monitor Geräte

Firewall-Konfiguration des QWX43 VLANs

Zur Absicherung des Wireless Access Points (WAP) und zur Isolierung des QWX43 VLANs sorgt eine dediziert konfigurierte Firewall für einen kontrollierten und sicheren Zugriff.

Die Firewall des QWX43 VLANs ist wie folgt konfiguriert:
- Der Datenverkehr von den Fermentation Monitor Geräten im IP-Bereich 10.10.30.x zum SCADA-System und zur PLC im IP-Bereich 10.10.20.x ist zugelassen.
- Für die Übertragung von Daten zwischen Leitsystem und Fermentation Monitor ist nur eine Verbindung auf Port 50000 zugelassen.
- Jeder andere Datenverkehr zwischen dem QWX43 VLAN und den anderen Netzwerken VLAN 1 und VLAN 10 ist blockiert. Dieses verhindert unzulässige Verbindungen oder potenzielle Angriffsvektoren aus dem QWX43 VLAN heraus.

Durch diese Firewall-Konfiguration werden das QWX43 VLAN und die anderen Segmente des OT-Netzwerkes geschützt. Gleichzeitig ermöglicht diese Konfiguration den notwendigen Datenaustausch mit dem Leitsystem.

Komponenten

In der Abbildung sind folgende Komponenten mit folgenden VLANs, IP-Adressen und Funktion dargestellt.

Komponente	VLAN	IP-Adresse	Funktion
Internet / Netilion Serverplattform	–	Öffentliche IP (dynamische IP)	Fernüberwachung, Gerätemanagement, Updates über Netilion Serverplattform
Router IT	VLAN 100	172.16.1.1	Internet-Gateway für den sicheren Zugriff auf das Internet
Firewall IT	VLAN 100	172.16.1.2	Trennung zwischen OT- und IT-Netzwerk, Deep Packet Inspection aktiviert
Firewall OT	VLAN 10	10.10.10.1	Segmentiert OT-Netzwerk und IT-Netzwerk, implementiert Zugriffskontrollen (Zone Border)
Layer 3 Switch	VLAN 10	10.10.10.2	Routing innerhalb des OT-Netzwerkes zwischen VLAN 30, VLAN 20 und VLAN 1
SCADA-System	VLAN 20	10.10.20.10	Überwachung und Steuerung von Prozessen im OT-Netzwerk über HMI
PLC (SCADA-seitig)	VLAN 20	10.10.20.11	Kommunikationsschnittstelle zwischen SCADA und PLC
PLC (PROFINET-seitig)	VLAN 1	192.168.10.1	Primäre Steuerung für PROFINET-Komponenten im VLAN 1
PROFINET Gerät 1	VLAN 1	192.168.10.2	PROFINET-Gerät zur Prozessdatenerfassung
PROFINET Gerät 2	VLAN 1	192.168.10.3	PROFINET-Gerät zur Prozessdatenerfassung
Fermentation Monitor Gerät 1	VLAN 30	10.10.30.2	Fermentation Monitor zur Prozessdatenerfassung
Fermentation Monitor Gerät 2	VLAN 30	10.10.30.3	Fermentation Monitor zur Prozessdatenerfassung

Komponente	VLAN	IP-Adresse	Funktion
Fermentation Monitor Gerät 3	VLAN 30	10.10.30.4	Fermentation Monitor zur Prozessdatenerfassung
Wireless Access Point	VLAN 30	10.10.30.1	Zugangspunkt für die drahtlose Kommunikation mit den Fermentation Monitor Geräten
Firewall für Wireless Access Point	VLAN 30	10.10.30.254	▪ Schützt das QWX43 VLAN und die anderen Segmente des OT-Netzwerkes ▪ Erlaubt den notwendigen Datenaustausch mit dem Leitsystem ▪ Erlaubt nur ausgehende HTTPS-Verbindungen

3.3 Systemüberblick – Variante "Netilion Serverplattform"

3.3.1 Allgemeine Informationen

Der Fermentation Monitor QWX43 ist mit folgenden Schnittstellen ausgestattet:
- WLAN-Verbindung https (mTLS) – Port 443 / SNTP 123
- WPA2-PSK WLAN-Verbindung http (RSA) – Port 80

Die Endress+Hauser Netilion Serverplattform ist mit folgenden Schnittstellen ausgestattet:
- Internetverbindung https
- Netilion Connect: Application Programming Interface (API)

Wird der Fermentation Monitor im Betriebsmodus **Netilion Cloud** betrieben, erfolgen alle ausgehenden Verbindungen zur Netilion Serverplattform verschlüsselt über HTTPS mit gegenseitiger Authentifizierung (mTLS). Die Daten sind end-to-end mittels **TLS 1.2** verschlüsselt. Der Fermentation Monitor authentifiziert sich dabei über Geräte-Zertifikate sowohl auf der Client- als auch auf der Serverseite.

Nutzerbezogene Zugriffe auf Netilion-Services werden per **OAuth 2.0** autorisiert.

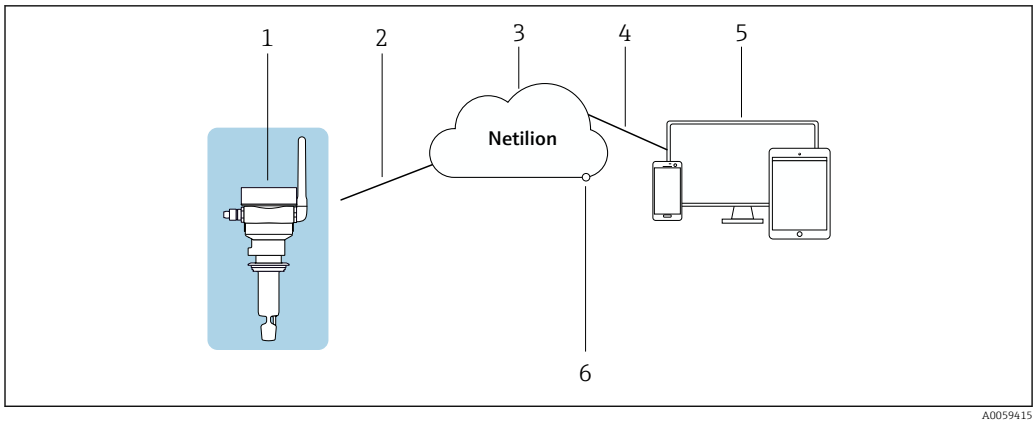
Sie können den Fermentation Monitor mit folgender digitalen Applikation betreiben:
Netilion Fermentation https://netilion.endress.com/app/fermentation

Die Inbetriebnahme von Netilion Fermentation erfolgt mittels WLAN über den integrierten Webserver bzw. Setup-Wizard des Fermentation Monitor.

Detaillierte Informationen: Betriebsanleitung → 6

3.3.2 Systemaufbau und Systemgrenzen – Variante "Netilion Serverplattform"

In diesem Security-Handbuch werden für die Variante "Netilion Serverplattform" der Fermentation Monitor QWX43 sowie die lokale Geräteschnittstelle WLAN-Hotspot und die Schnittstelle zur Endress+Hauser Netilion Serverplattform betrachtet. Weitere Komponenten wie kundenseitige Automatisierungssysteme wie z.B. PLC / SCADA, die Netilion Serverplattform und Bedientools sind nicht Bestandteil dieses Handbuches. In der folgenden Abbildung sind die Systemgrenzen blau markiert.

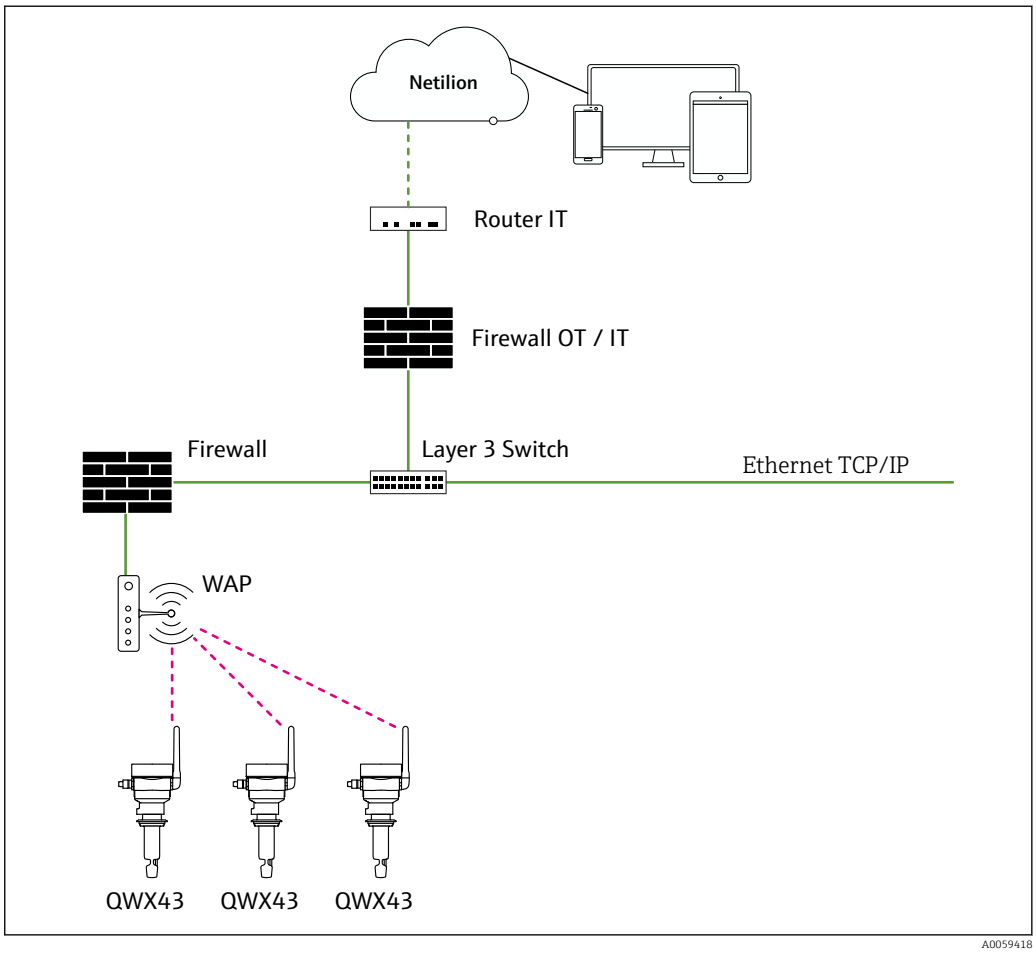


3 *Systemaufbau Fermentation Monitor QWX43, blaue Markierung zeigt die Systemgrenzen für dieses Handbuch*

1 *Fermentation Monitor QWX43*
2 *WLAN-Internetverbindung HTTPS (mTLS 1.2)*
3 *Netilion Serverplattform*
4 *Internetverbindung https*
5 *Netilion Services: Internetbrowser basierte Netilion Service App*
6 *Netilion Connect: Application Programming Interface (API)*

Der Fermentation Monitor wird in diesem Dokument in den allgemeinen Texten abhängig vom Zusammenhang entweder als Produkt oder als Endgerät bezeichnet.

3.3.3 Beispiel Systemaufbau und Netzwerkkonfiguration – Variante "Netilion Serverplattform"



4 *Beispiel Systemaufbau und Netzwerkkonfiguration Fermentation Monitor QWX43 – Netilion Serverplattform*

3.4 Security-Level festlegen

Abhängig vom angestrebten Security-Level müssen das System und die darin installierten Produkte unterschiedlich hohe Anforderungen erfüllen. Als erstes müssen Sie den erforderlichen **Security-Level** SL1 bis SL4 für das System festlegen. Abhängig von dem Security-Level leiten Sie gemäß IEC 62443-3-3 die Anforderungen an das System und gemäß IEC 62443-4-2 die Anforderungen an die Produkte ab.

Der Fermentation Monitor als Feldgerät kann allein gemäß IEC 62443-3-3 keinen Security-Level erfüllen.

Der Fermentation Monitor wurde gemäß IEC 62443-4-1 unter Berücksichtigung eines sicheren Entwicklungslebenszyklus (Secure Development Lifecycle, SDL) entwickelt. Zusätzlich erfüllt der Fermentation Monitor die Anforderungen der EN 18031 (Cybersicherheit für Funkanlagen).

Das System, indem der Fermentation Monitor integriert ist, muss den angestrebten Security-Level erfüllen.

Der tatsächlich erreichbare Security-Level ergibt sich erst durch die Kombination aus:
- Sicherer Gerätekonfiguration
- Einbindung in eine segmentierte und härtbare Netzwerkumgebung
- Einbindung in eine übergeordnete Systemarchitektur nach dem Zonen-/Kanalmodell gemäß IEC 62443-3-2 und IEC 62443-3-3.

3.5 Typische Einsatzumgebung des Produkts

Wir empfehlen für die Festlegung der Security-relevanten Eigenschaften des Produkts die typische Einsatzumgebung zu definieren.

Die Betrachtung der Einsatzumgebung soll zu den Anforderungen durch die Umgebung führen. Beispielsweise können Sie einen Denial-of-Service-Angriff betrachten.

Für eine typische Einsatzumgebung könnten z.B. folgende Punkte zutreffen:
- Das Produkt ist eine Systemkomponente.
- Das Produkt ist mit mindestens einer Ethernet-basierten Schnittstelle (WLAN) ausgestattet. Schnittstellen: Siehe Kapitel "Systemüberblick".
- Das Produkt wird in einer industriellen Umgebung betrieben.
- Der Zugang zum System ist reglementiert. Nur autorisierte Personen haben Zugang zum System.
- Das Personal ist in dem Gebrauch des Produkts und in die Security-Risiken unterwiesen.
- Das Produkt wird in einem Ethernet-Netzwerk, das nur für industrielle Zwecke vorgesehen ist, betrieben. Das Netzwerk ist entweder vollständig vom restlichen Unternehmensnetzwerk getrennt oder durch Firewalls geschützt.
- Das Produkt verfügt über mindestens eine Datenverbindung, die den Produktionsbereich verlässt.
- Das Automatisierungsnetz ist über einen Perimeterschutz gegen Angriffe von außen wie z.B. einen Denial-of-Service-Angriff geschützt.
- Das Produkt ist in einer Umgebung installiert, die nach dem Defense-in-Depth-Konzept abgesichert ist.
- Passwörter für das Produkt sind nur autorisierten Personen bekannt.
- Nur autorisierte Personen können über das zugehörige Human Machine Interface (HMI) auf das Produkt zugreifen.

Da die Rechenleistung des betrachteten Produkts begrenzt ist, kann das Produkt Angriffe nur in begrenztem Umfang abwehren.

3.6 Maßnahmen, falls erforderliche Einsatzumgebung nicht erfüllbar ist

Sofern die spezifizierten Anforderungen an die Einsatzumgebung nicht eingehalten werden können, sind ggf. Ersatzmaßnahmen vorzusehen. Dabei kann es sich z.B. um einen mechanischen Schutz des Produkts gegen Manipulation, einen mechanischen Schutz der Verkabelung oder auch um organisatorische Maßnahmen handeln.

Um einen physischen Zugriff auf den Fermentation Monitor zu verhindern, empfehlen wir den Fermentation Monitor an einem Prozessanschluss zu montieren, der nur für autorisierte Personen zugänglich ist. Dieser Montageort könnte beispielsweise innerhalb eines abgeschlossenen Tankdoms oder in einem betrieblich gesicherten Gär-/Lagertankbereich sein.

Zusätzlich empfehlen wir, den Access Point innerhalb eines gesicherten Bereiches und fern von öffentlich zugänglichen Bereichen zu montieren.

3.7 Bedrohungsanalyse und Risikobeurteilung durchführen

Bei der Planung einer Anlage müssen Sie für die gesamte Anlage eine Risikobeurteilung in einem gesamtheitlichen Ansatz durchführen. Für die Risikobeurteilung von Anlagen können Sie sich an der VDI 2182 orientieren.

Im Zuge der Risikobeurteilung führen Sie eine Risikoanalyse / Bedrohungsanalyse durch.

Beachten Sie für die Risikoanalyse folgende Aspekte:
- Schnittstellen des Produkts, über die eine Kommunikation mit dem Produkt möglich ist oder über die auf das Produkt zugegriffen werden kann.
- Datenflüsse des Produkts innerhalb der Anlage
  - Zum Produkt eingehende Daten
  - Vom Produkt ausgehende Daten
- Datenflüsse des Produkts, die den Bereich der Anlage verlassen und ggf. Firewalls überwinden

Aus der Risikoanalyse können Sie risikomindernde Maßnahmen ableiten.

Neben der Risikobeurteilung sollten im Planungsprozess auch Festlegungen getroffen werden, wie das Produkt während der Inbetriebnahme zu konfigurieren ist. Hierzu gehören z.B. das Abschalten nicht benötigter Schnittstellen und/oder Dienste. Das Abändern von Standardpasswörten usw. Diese Maßnahmen werden in den folgenden Kapiteln vorgestellt.

3.8 Empfehlung für risikomindernde Maßnahmen

3.8.1 Gesamtsystem betrachten

Der Fermentation Monitor ist ein Endgerät, das entweder in einem klassischen Produktionssystem oder in einem geschlossenen IIoT-Ökosystem eingesetzt werden kann. Die modularen Architekturen solcher Systeme begünstigen die Verwendung unterschiedlicher Komponenten. Hierbei kann es beim Einsatz unterschiedlicher Produkte zu Schnittstellenbrüchen kommen, wodurch die Angriffsfläche vergrößert wird.

Folgendes für die Variante "Direktintegration" beachten:
- Feldbusnetzwerk (OT-WLAN, 2.4 GHZ, WPA2-PSK) und Unternehmensnetzwerk (IT) müssen strikt getrennt werden. Filter oder VLAN-Regeln dürfen den lokalen PLC-Datenstrom auf dem TCP-Port 50000 nicht aus dem Feldbusnetzwerk-Segment herausleiten.
- Für die konsequente Umsetzung von Defense-in-Depth, empfiehlt Endress+Hauser eine Segmentierung der Feldbusnetzwerke gemäß IEC 62443-3-3 (Zonen-/Kanalmodell).
- Der Wireless Access Point zum Fermentation Monitor muss als eigene Sicherheitszone behandelt werden. SSID, Kennwort und Sendeleistung müssen nach dem Least-Privilege-Prinzip konfiguriert werden.
- Das werksseitig eingestellte Passwort muss während der Inbetriebnahme geändert und zentral verwaltet werden.

Folgendes für die Variante "Netilion Serverplattform" beachten:
- Die Anbindung des Fermentation Monitor an das Internet im Betriebsmodus „Netilion Cloud“ muss mindestens über eine Firewall, die den mTLS-Verkehr auf TCP-Port 443 und SNTP-Port 123 explizit zulässt, erfolgen.
- Für die konsequente Umsetzung von Defense-in-Depth, empfiehlt Endress+Hauser eine Segmentierung der Feldbusnetzwerke gemäß IEC 62443-3-3 (Zonen-/Kanalmodell).
- Der Wireless Access Point zum Fermentation Monitor muss als eigene Sicherheitszone behandelt werden. SSID, Kennwort und Sendeleistung müssen nach dem Least-Privilege-Prinzip konfiguriert werden.
- Das werksseitig eingestellte Passwort muss während der Inbetriebnahme geändert und zentral verwaltet werden.
- Setzen Sie IDS/IPS-Überwachung an den Übergängen zwischen OT-Feldbuszonen und Netilion Serverplattform ein, um Anomalien oder DoS-Versuche frühzeitig zu erkennen. Der Fermentation Monitor kann solche Angriffe aufgrund seiner begrenzten Ressourcen nur eingeschränkt selbst abwehren.

3.8.2 Anwender schulen

Je nach Anwendungsszenario können auch fachfremde Anwender mit dem IIoT-Ökosystem in Berührung kommen. Wir empfehlen, diese Anwender für den sicheren Gebrauch

mit den entsprechenden Endgeräten und / oder Schnittstellen zu schulen und für die Security zu sensibilisieren.

3.8.3 Zugriffsmanagement optimieren

Damit Sie auf den Fermentation Monitor über den integrierten Webserver zugreifen können, benötigen Sie entsprechende Zugangsdaten wie Login und Passwort. Für die erste Anmeldung müssen Sie das werksseitig eingestellte Initialpasswort verwenden. Das Passwort muss nach der ersten Anmeldung geändert, sicher aufbewahrt und vertraulich behandelt werden → 🖹 20.

Detaillierte Informationen zum Passwort: Betriebsanleitung → 🖹 6

Zusätzlich Variante "Direktintegration"
Zusätzlich benötigen Sie folgendes für den Betrieb des Fermentation Monitor in einem WLAN-basierten OT-Netzwerk (Steuerung):
- SSID und WPA2-PSK des konfigurierten Wireless Access Points
- Feste IP-Adresse oder DHCP-Zuweisung innerhalb des OT-Netzwerkes
- Freigabe des TCP-Ports 50000 in Firewall / VLAN-Regeln

Zusätzlich Variante "Netilion Serverplattform"
Zusätzlich benötigen Sie folgendes für den Betrieb des Fermentation Monitor in einem WLAN-basierten OT-Netzwerk (Steuerung):
SSID und WPA2-PSK des konfigurierten Wireless Access Points

IIoT-Ökosystem

Wir empfehlen, für den Zugriff auf das IIoT-Ökosystem die gleichen Regeln für das Identitäts- und Zugriffsmanagement wie für die anderen Unternehmensbereiche anzusetzen.

- Mitarbeitern nur die Zugriffsrechte geben, die der Mitarbeiter zur Erfüllung seiner Aufgaben benötigt
- Benutzerkonten (Accounts) nur mit starken Passwörtern vergeben
- Passwörter über einen Passwort-Manager generieren, sichern und verwalten

3.8.4 Gerätedaten und Gerätestatus überwachen

Da ein Echtzeit-Monitoring für die meisten Anwender nicht in Frage kommt, muss dieser Vorgang automatisiert werden. Wir empfehlen eine Monitoring-Software einzusetzen, die bestimmte Parameter und den Zustand des Produkts und des Netzwerks überwacht und bei Abweichungen informiert.

Überwachung über WLAN

Der Fermentation Monitor ist ein Teilnehmer in einem WLAN-Netzwerk. Eine Erkennung und die Behebung von Anomalien ist eine Aufgabe des Netzwerk-Betreibers.

Variante "Direktintegration": Überwachung der Kommunikation über ein Leitsystem

Der Fermentation Monitor ist Teil eines Netzwerkes in einer Prozessautomatisierungsanlage und kann per TCP-Port 50000 mit der PLC über proprietäre OUC-Telegrammrahmen kommunizieren. Die Kommunikation mit der PLC erfolgt unverschlüsselt. Wenn der Fermentation Monitor plötzlich unrealistische Werte liefert, kann das ein Indiz für einen Angriff sein. Der physikalische Schutz sowie die Erkennung und Behebung von Anomalien ist Aufgabe des Betreibers des Leitsystems.

Variante "Netilion Serverplattform": Überwachung über das IIoT-Ökosystem

Der Fermentation Monitor kann ein Endgerät in einem IIoT-Ökosystem sein und die Erkennung von Anomalien ist eine Aufgabe des übergeordneten Systems.

3.8.5 Produkt-Software updaten

Die Anforderungen an Vernetzung, IT-Security und eingesetzte Bibliotheken ändern sich stetig, daher sind regelmäßige Firmware-Updates erforderlich.

Wir empfehlen, regelmäßig zu prüfen, ob neue Updates zur Verfügung stehen und die Updates zu installieren. Versäumte Updates sind ein akutes Security-Risiko, da auch Angreifer über die zu behebenden Schwachstellen informiert sein könnten.

Sie haben folgende Möglichkeiten ein Firmware-Update durchzuführen:
- Online über die Netilion Serverplattform
- Offline über den Webserver des Fermentation Monitor

Für ein Update über die Netilion Serverplattform müssen Sie sich in Netilion einloggen.

Damit Sie bei der Variante Direktintegration ein Firmware-Update über Netilion durchführen können, müssen Sie den Fermentation Monitor in den Hotspot-Modus setzen und den **Operation Mode** wechseln.

Detaillierte Informationen zu Firmware-Updates: Betriebsanleitung → 6

Für ein Firmware-Update über den Webserver kontaktieren Sie den Endress+Hauser Service.

Firmware-Updates können Sie unter folgender Adresse herunterladen:
https://www.endress.com/downloads

4 Inbetriebnahme (Installation und Konfiguration)

4.1 Zielgruppe

Dieses Kapitel richtet sich an das Betriebspersonal.

4.2 Anforderungen an das Personal

Das Personal muss folgende Bedingungen erfüllen:
- Über eine fachliche Qualifikation verfügen, die dieser Funktion und Tätigkeit entspricht.
- Vom Anlagenbetreiber autorisiert.
- Mit den nationalen Vorschriften vertraut.
- Vor Arbeitsbeginn: Anweisungen in Anleitung und Zusatzdokumentation sowie Zertifikate (je nach Anwendung) lesen und verstehen.
- Anweisungen und Rahmenbedingungen befolgen.

4.3 Installation

Produkt gemäß zugehöriger Kurzanleitung / Betriebsanleitung montieren und elektrisch anschließen.

Um einen physischen Zugriff auf den Fermentation Monitor zu verhindern, empfehlen wir den Fermentation Monitor an einem Prozessanschluss zu montieren, der nur für autorisierte Personen zugänglich ist. Dieser Montageort könnte beispielsweise innerhalb eines abgeschlossenen Tankdoms oder in einem betrieblich gesicherten Gär-/Lagertankbereich sein.

Zusätzlich empfehlen wir, den Access Point innerhalb eines gesicherten Bereiches und fern von öffentlich zugänglichen Bereichen zu montieren.

Des Weiteren empfehlen wir, weitere externe Maßnahmen zu implementieren wie z.B. eine Netzwerksegmentierung, Firewalls, ein Intrusion Detection System und / oder einen Perimeterschutz.

- Detaillierte Informationen zur Netzwerksegementierung: → 13
- Detaillierte Informationen zur Firewallkonfiguration: → 19

4.4 Konfiguration

4.4.1 Produkt in Betrieb nehmen und konfigurieren

Produkt gemäß zugehöriger Kurzanleitung / Betriebsanleitung in Betrieb nehmen und konfigurieren. Für den Bereich "Security" zusätzlich die weiteren Kapitel beachten.

4.4.2 Erforderliche Security-Schritte während der Inbetriebnahme

Endress+Hauser nutzt für den Versand das Prinzip des "bekannten Versenders". Als Empfänger können Sie davon ausgehen, dass das Produkt Sie in einem definierten Zustand erreicht. Eine Prüfung der Hardware auf Manipulation ist nicht erforderlich.

Beachten Sie während der Inbetriebnahme hinsichtlich der Security folgenden Punkt: Produkt gemäß den definierten Anforderungen an die Einsatzumgebung integrieren → 14.

4.4.3 Netzwerk konfigurieren

Eine sichere Netzwerkkonfiguration bildet die Grundlage für den geschützten Betrieb des Fermentation Monitor. Die folgenden Empfehlungen können je nach Netwerkkontext, Angriffsflächen minimieren und einen zuverlässigen, manipulationssicheren Datenfluss ermöglichen.

- Jedem Fermentation Monitor und jedem zugehörigen Access Point eine statische IP-Adresse zuweisen.
- DHCP deaktivieren, um unautorisierte IP-Zuweisungen zu vermeiden.
- Für die Fermentation Monitor Geräte ein eigenes separates Netzwerksegment verwenden. Dieses Netzwerksegment muss eindeutig von anderen operativen und administrativen Netzwerken getrennt sein.
- Zur virtuellen Trennung eignet sich der Einsatz eines VLANs. Das VLAN ermöglicht eine granulare Kontrolle über Zugriffe und Datenflüsse.
- Eine Firewall zwischen dem Netzwerksegment mit den Fermentation Monitor Geräten und den anderen Netzsegmenten einsetzen.
- Alle anderen Kommunikationsverbindungen aus dem Netzwerksegment mit den Fermentation Monitor Geräten blockieren.
- Um sicherzustellen, dass nur autorisierte Geräte auf das Netzwerk zugreifen, IP-Whitelisting nutzen.

Detaillierte Informationen zur Firewallkonfiguration: → 19

Beispiel für eine VLAN-basierte Netzwerksegmentierung

Der Fermentation Monitor unterstützt kein IEEE 802.1Q und ist somit nicht VLAN-aware. Für den sicheren Einsatz in segmentierten Netzwerken empfehlen wir jedoch, das WLAN, in die der Fermentation Monitor eingebunden wird, über Access Points einem dedizierten VLAN zuzuweisen. Dies ermöglicht eine logische Trennung vom restlichen OT-/IT-Netzwerk und reduziert potenzielle Angriffsflächen. Die Netzsegmentierung sollte über VLAN-fähige Access Points, Router oder Firewalls umgesetzt werden.

Detaillierte Informationen zur Netzwerksegementierung: → 13

4.4.4 Firewall konfigurieren

In dem Fermentation Monitor ist keine Firewall integriert. Zusätzliche Firewalls oder Netzwerkgeräte mit Firewall-Funktionalitäten müssen kundenseitig bereitgestellt werden.

Wir empfehlen zwischen dem Netzwerksegment mit den Fermentation Monitor Geräten und den anderen Netzsegmenten eine Firewall einzusetzen.

Detaillierte Informationen zur Firewallkonfiguration: Betriebsanleitung → 6

Zusätzlich folgende Hinweise befolgen:

- Nur die TCP/IP-Ports, die für den Betrieb des Fermentation Monitor erforderlich sind, erlauben → 25.
- Alle Ports, die nicht für den Betrieb erforderlich sind, blockieren.
- Variante "Direktintegration: Ausgehenden Datenverkehr auf das Zielgerät wie z.B. PLC und auf den Port 50000 beschränken.

4.4.5 Wireless Access Point konfigurieren

Wir empfehlen, nach dem Aktivieren des Hotspots folgende Einstellungen vorzunehmen:
- WPA2-PSK als Authentifizierungsverfahren einrichten und Wireless Access Point entsprechend anpassen.
- Starkes Zufallspasswort mit mindestens 16 Zeichen verwenden und regelmäßig ändern.
- MAC-Filtering aktivieren. Nur die MAC-Adressen der autorisierten Fermentation Monitor Geräte zulassen.
- Access Point innerhalb eines gesicherten Bereiches und fern von öffentlich zugänglichen Bereichen montieren.

Beachten Sie, dass der Wireless Access Point kein Bestandteil des Handbuches ist. Die tatsächlich erreichte Sicherheitsstufe des Wireless Access Point liegt in der Verantwortung des Anlagenbetreibers.

4.4.6 Produkt härten

Im Bereich Security bedeutet "Härten", dass nur die Dienste freigeschaltet werden, die für den ordentlichen Betrieb des Produkts für den vorliegenden Anwendungsfall erforderlich sind.

Der Fermentation Monitor verwendet ein gehärtetes Betriebssystem. Das Betriebssystem ist nach dem "Minimalstprinzip" konfiguriert. Nur die erforderlichen Dienste/Ports sind installiert und aktiv.

Endress+Hauser hat für das Betriebssystem folgende Maßnahmen getroffen:
- Secure Services
  Sicherheitsrelevante Funktionen laufen in voneinander isolierten Prozessen, um gegenseitige Beeinflussung zu verhindern.
- Secure Boot
  Ein signierter Boot-Loader prüft beim Starten die Integrität der Firmware und verhindert das Ausführen nicht-autorisierter Software.
- Secure Storage
  Schlüssel, Zertifikate und Passwörter werden in geschützten Speicherbereichen verschlüsselt abgelegt. Ein direkter Zugriff von außen ist ausgeschlossen.
- Passwort-Policy
  Für die Einbindung des Fermentation Monitor zum Wireless Access Point (Direktintegration) bzw. in das WLAN der Anlage vor Ort (Netilion Serverplattform) stellt der Fermentation Monitor ein WLAN (Hotspot) zur Verfügung. Die Inbetriebnahme des Fermentation Monitor erfolgt im Hotspot-Modus über ein werksseitig vorgegebenes Initialpasswort. Das Passwort muss während der Inbetriebnahme geändert werden.

Passwort – Anforderung und Empfehlung
- Mindestens 16 Zeichen. Kürzere Passwörter werden abgelehnt.
- Starkes Zufallspasswort mit Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen vergeben.
- Passwörter vertraulich aufbewahren.
- Passwörter nur unbeobachtet eingeben.

Detaillierte Informationen zur Inbetriebnahme und zum Initialpasswort: Betriebsanleitung → 6

4.4.7 Anwenderdaten konfigurieren

Anwenderdaten sind z.B. Login-Daten, Benutzer, Messstellenbezeichnung (TAG), Passwörter, IDs usw.

Zusätzlich ist für die Variante "Netilion Serverplattform" und wenn eine Firmware-Update online durchgeführt werden soll, ein Netilion Account erforderlich. Der Anwender legt die Zugangsdaten fest und kann diese nachträglich ändern.

Detaillierte Informationen zu Passwörtern: → 20

Detaillierte Informationen zum Anlegen eines Netilion Accounts: Betriebsanleitung → 6

4.4.8 Security-relevante Einstellungen des Produkts

Für den Fermentation Monitor müssen Sie keine Security-relevanten Einstellungen vornehmen.

4.4.9 User-Management und Auswirkung auf die Security

Der Fermentation Monitor hat nur einen Benutzerlevel (admin).

5 Betrieb

5.1 Zielgruppe

Dieses Kapitel richtet sich an das Betriebspersonal.

5.2 Anforderungen an das Personal

Das Personal muss folgende Bedingungen erfüllen:
- Über eine fachliche Qualifikation verfügen, die dieser Funktion und Tätigkeit entspricht.
- Vom Anlagenbetreiber autorisiert.
- Mit den nationalen Vorschriften vertraut.
- Vor Arbeitsbeginn: Anweisungen in Anleitung und Zusatzdokumentation sowie Zertifikate (je nach Anwendung) lesen und verstehen.
- Anweisungen und Rahmenbedingungen befolgen.

5.3 Aufgaben während des Betriebes

Produkt gemäß zugehöriger Betriebsanleitung betreiben. Für den Bereich "Security" zusätzlich dieses Kapitel und die folgenden Kapitel beachten.

Der Fermentation Monitor erfordert keine Interaktionen während des Betriebes.

5.4 Security-Aspekte während des Betriebes

Die im Fermentation Monitor hinterlegten Zertifikate haben eine begrenzte Laufzeit von 5 Jahren.

Ca. 1 Jahr bevor die Zertifikate ablaufen, erneuert Endress+Hauser über die Netilion Serverplattform die Zertifikate für den Fermentation Monitor. Melden Sie den Fermentation Monitor mindestens einmal pro Jahr an die Netilion Serverplattform an.

Damit die kontinuierliche Erfassung und sichere Übertragung der Messdaten gewährleistet bleibt, sind über den gesamten Betriebszeitraum hinweg technische und organisatorische Maßnahmen umzusetzen. Diese Maßnahmen orientieren sich am angestrebten Security-Level für das System gemäß IEC 62443-3-3.

Security-Maßnahmen abhängig vom angestrebten Security-Level

Für die Security-Level SL 1 bis SL 4 sind folgende Maßnahmen erforderlich:
- Firmware-Updates regelmäßig durchführen → 🖹 17.
- Firmware des Access Points regelmäßig aktualisieren.
- Integrität von Netzwerkverbindungen sicherstellen.
- Firewall- und Port-Konfigurationen prüfen.

Für einen Security-Level SL 3 sind die folgenden Maßnahmen erforderlich. Für einen Security-Level SL 2 werden diese Maßnahmen empfohlen.
- Periodische Security-Audits wie z.B. gemäß VDI/VDE 2182 oder NIST SP 800-82 durchführen.
- Zugriffe und Betriebsdaten protokollieren.
- Zugangsdaten in regelmäßigen Abständen erneuern oder rotieren.
- Netzinfrastruktur inklusive Anomalieerkennung überwachen.

Der Fermentation Monitor als Feldgerät kann allein gemäß IEC 62443-3-3 keinen Security-Level erfüllen. Das System, indem der Fermentation Monitor integriert ist, muss den angestrebten Security-Level erfüllen. Die Umsetzung der dafür erforderlichen Sicherheitsanforderung liegen in der Verantwortung des Anlagenbetreibers.

5.5 Update-Management

Endress+Hauser stellt Firmware-Updates über die Netilion Serverplattform und über den Downloadbereich von Endress+Hauser bereit.

Für ein Firmware-Update über die Netilion Serverplattform muss der Anwender das Update über die Netilion Serverplattform anstoßen. Der Zeitpunkt für ein Update ist einstellbar. Nach manchen Updates ist ein Neustart für den Fermentation Monitor erforderlich. Der Neustart wird automatisch durchgeführt.

Kontaktieren Sie Endress+Hauser Service, wenn Sie das Firmware-Update offline durchführen möchten.

Detaillierte Informationen zu Firmware-Updates: → 17

Endress+Hauser stellt Updates für folgende Fälle bereit:
- Security-Updates
- Bugfixes: Fehlerbehebungen bestehender Funktionen
- Funktionale Erweiterungen des Produkts
- Erneuerung der Zertifikate

Endress+Hauser stellt durch Prüfsummen und Signaturen in der Firmware die Integrität und Authentizität der Updates sicher. Eine Integritäts- und Authentizitätsprüfung der Updates durch den Anwender ist nicht erforderlich.

5.6 Wiederholung der Bedrohungsanalyse

Die Bedrohungssituation von Anlagen kann sich durch externe Ereignisse wie z.B. durch Auftreten bisher unbekannter Angriffsmuster, ändern. Gemäß der VDI/VDE 2182-1-2011, Kapitel 4.4 muss die Bedrohungsanalyse in regelmäßigen Abständen oder bei Änderungen der Anlage, die Einfluss auf die Bedrohungsanalyse haben können, wiederholt und aktualisiert werden.

5.7 Reparatur und Entsorgung

Produkt gemäß Betriebsanleitung reparieren oder entsorgen.

6 Außerbetriebnahme

6.1 Zielgruppe

Dieses Kapitel richtet sich an das Betriebspersonal.

6.2 Anforderungen an das Personal

Das Personal muss folgende Bedingungen erfüllen:
- Über eine fachliche Qualifikation verfügen, die dieser Funktion und Tätigkeit entspricht.
- Vom Anlagenbetreiber autorisiert.
- Mit den nationalen Vorschriften vertraut.
- Vor Arbeitsbeginn: Anweisungen in Anleitung und Zusatzdokumentation sowie Zertifikate (je nach Anwendung) lesen und verstehen.
- Anweisungen und Rahmenbedingungen befolgen.

6.3 Produkt außer Betrieb nehmen

Für eine Außerbetriebnahme des Produkts gibt es verschiedene Gründe. Abhängig von dem Grund der Außerbetriebnahme sind entsprechende Handlungen erforderlich.

Grund der Außerbetriebnahme	Erforderliche Handlungen
Das Produkt wird für längere Zeit nicht genutzt.	Keine Maßnahme erforderlich.
Das Produkt hat eine Störung und Sie können die Störung nicht beheben.	1. Endress+Hauser kontaktieren. 2. Anweisung von Endress+Hauser folgen.
Das Produkt ist defekt und muss daher entsorgt werden.	▶ Produkt physisch zerstören und gemäß Betriebsanleitung entsorgen.
Das Produkt soll entsorgt werden.	▶ Produkt physisch zerstören und gemäß Betriebsanleitung entsorgen.
Die Netilion Service Subscription wurde beendet.	Keine Maßnahme erforderlich. Sobald eine neue Netilion Service Subscription abgeschlossen wird, kann der Fermentation Monitor wieder genutzt werden.

7 Anhang

7.1 Security-Checkliste für den Produktlebenszyklus

Lebenszyklus	Tätigkeit	Geprüft
Planung	Typische Einsatzumgebung des Produkts definiert und bei der Planung berücksichtigt. → 🖹 14 Falls erforderlich, Ersatzmaßnahmen berücksichtigt. → 🖹 14	❑
	Planungsarbeiten in der Engineering-Phase beachtet. Bedrohungsanalyse und Risikobeurteilung durchgeführt. → 🖹 8	❑
	Sofern möglich, risikiomindernde Maßnahmen berücksichtigt. → 🖹 15	❑
Wareneingang / Transport	Geprüft, dass die Verpackung ungeöffnet ist. → 🖹 18	❑
Inbetriebnahme	Produkt für den Anwendungsfall gehärtet. → 🖹 20	❑
Betrieb	Vorgaben zum Update-Management beachtet. → 🖹 23	❑
	Planung der wiederkehrenden Bedrohungsanalyse vorgenommen. → 🖹 23	❑
Außerbetriebnahme	Produkt außer Betrieb genommen. → 🖹 24 Je nach Grund für die Außerbetriebnahme Produkt deaktivieren oder das Produkt zerstören.	❑

7.2 Versionshistorie

Dokumentenversion	Firmwareversion	Hardwareversion	Änderungen
01.25	ab 04.03.zz	Dev. Rev. 1	Erste Version

7.3 Informationen für Security-Audits

7.3.1 Dienste für den Betrieb und die Anbindung an das Leitsystem (Variante "Direktintegration")

Die in der folgenden Tabelle aufgeführten Dienste müssen je nach Netzwerkstruktur verfügbar sein und / oder in der Firewall freigeschaltet werden.

Dienst / Funktion	Port	Protokoll	Bemerkung
OUC Datenkommunikation (PLC)	50000	TCP (Open User Communication)	Proprietärer Port für Verbindung zu einer Siemens-Steuerung und Rockwell-Steuerung
DHCP (Client-IP-Vergabe)	67 (Server) 68 (Client)	UDP	Werksseitig ist DHCP aktiviert. Wir empfehlen, DHCP zu deaktivieren und eine statische IP für den Fermentation Monitor zu verwenden.
Webserver	80	HTTP (nur lokal)	▪ Für Setup (Hotspot): Zugang über http://10.10.0.1 zur WLAN-Konfiguration und die Auswahl des Betriebsmodus "PLC" oder "Netilion Cloud". ▪ Lokaler Zugriff über IP des Fermentation Monitor

7.3.2 Dienste für den Betrieb und die Endress+Hauser Netilion Serverplattform (Variante "Netilion Serverplattform")

Die in der folgenden Tabelle aufgeführten Dienste müssen je nach Netzwerkstruktur verfügbar sein und / oder in der Firewall freigeschaltet werden.

Dienst / Funktion	Port	Protokoll	Bemerkung
HTTPS zu Netilion API	443	TCP / HTTPS (mTLS)	Hauptverbindung zur Netilion Serverplattform: TLS 1.2/1.3 und Client-Zertifikat (Amazon CA)
SNTP (Zeitserver)	123	UDP / SNTP	Zeitabgleich mit Internet-Zeitserver
DNS (Namensauflösung)	53	UDP / TCP	Erforderlich für *.netilion.endress.com, z.B. API-Auflösung
DHCP (Client-IP-Vergabe)	67 (Server) 68 (Client)	UDP	Werksseitig ist DHCP aktiviert. Wir empfehlen, DHCP zu deaktivieren und eine statische IP für den Fermentation Monitor zu verwenden.
Webserver	80	HTTP (nur lokal)	▪ Für Setup (Hotspot): Zugang über http://10.10.0.1 zur WLAN-Konfiguration und die Auswahl des Betriebsmodus "PLC" oder "Netilion Cloud". ▪ Lokaler Zugriff über IP des Fermentation Monitor

www.addresses.endress.com

Endress+Hauser

People for Process Automation