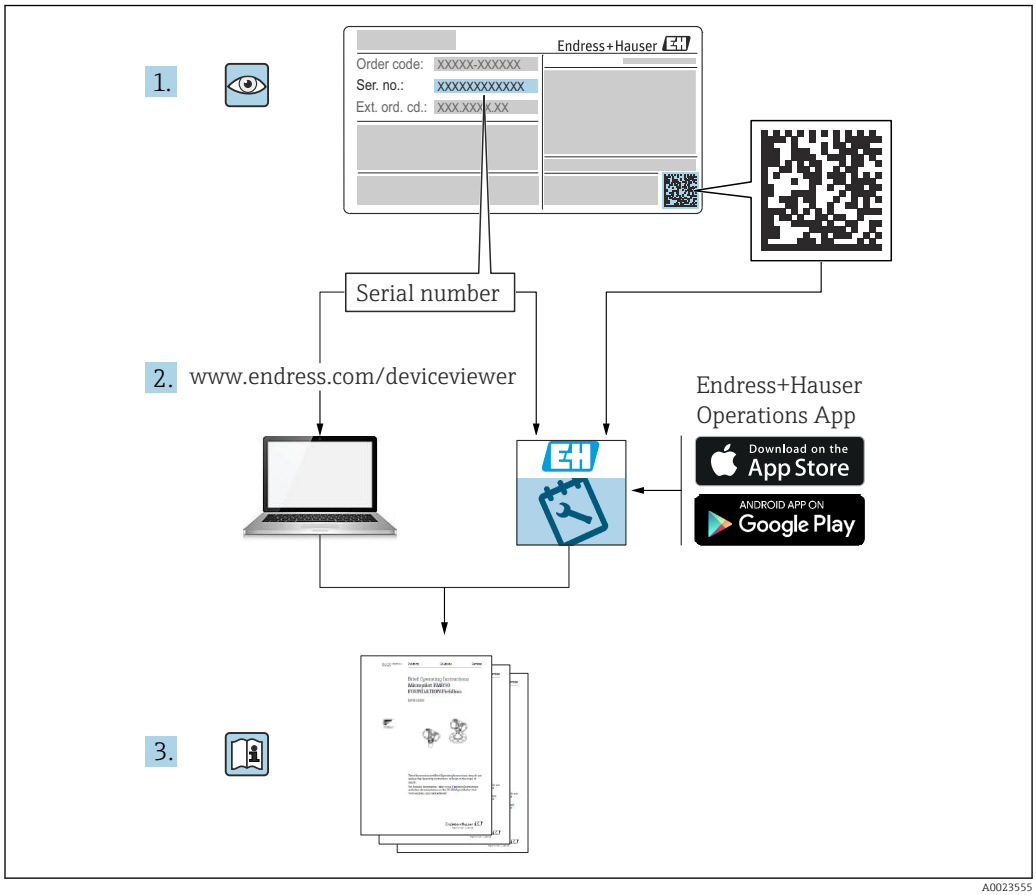
SD02985F/00/DE/01.22-00
71574838
2022-07-01



# Sonderdokumentation
# **Security-Handbuch Micropilot FWR30**

Freistrahlendes Radar

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

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:
- *W@M Device Viewer* (www.endress.com/deviceviewer): Seriennummer vom Typenschild eingeben
- Downloadbereich der Endress+Hauser Internetseite (www.endress.com/download)

**Mitgeltende Dokumente Micropilot FWR30**

- Technische Information TI01499F
- Betriebsanleitung BA01991F
- Sonderdokumentation SD02474F (Free space radar)
- Sonderdokumentation SD02672S (Netilion Value)
- 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

### 3.2.1 Allgemeine Informationen

Sie können den Micropilot FWR30 mit folgenden digitalen Applikationen betreiben:
- Netilion Value: https://Netilion.endress.com/app/value
- Netilion Inventory: https://Netilion.endress.com/app/inventory
- SupplyCare Hosting: https://portal.endress.com
  Die Inbetriebnahme von SupplyCare Hosting erfolgt durch den Service von Endress+Hauser.

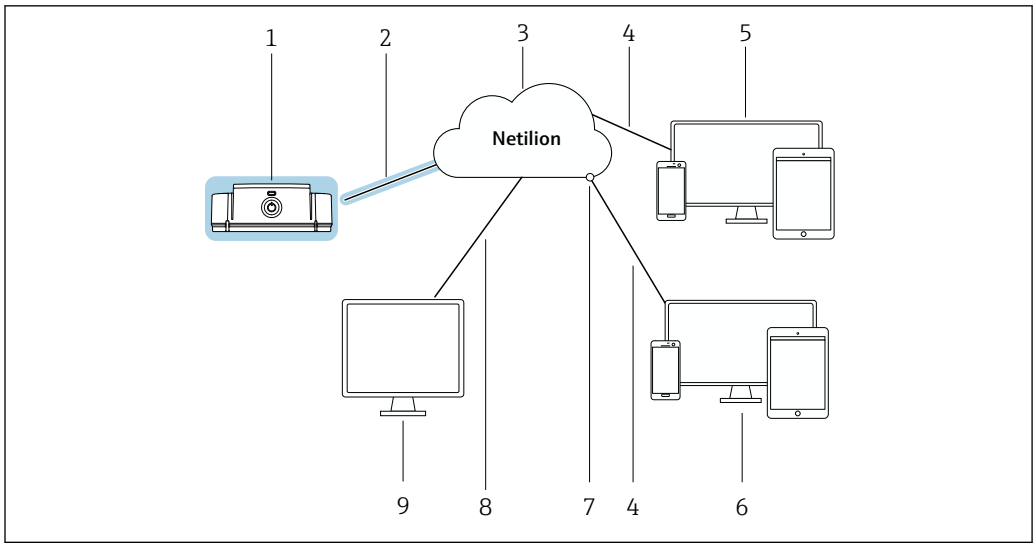
Der Micropilot FWR30 ist mit folgenden Schnittstellen ausgestattet:
Mobilfunkverbindung https

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

Die Verbindungen zwischen dem Micropilot FWR30 und Netilion Cloud sind end-to-end nach TLS 1.2 mit 2048-bit-RSA verschlüsselt. Die Authentifizierung der Verbindung wird durch ein Client-Zertifikat und ein Server-Zertifikat realisiert.

### 3.2.2 Systemaufbau und Systemgrenzen

In diesem Security-Handbuch wird der Micropilot FWR30 und die Mobilfunkverbindung zur Netilion Cloud betrachtet. Die weiteren Komponenten wie die Endress+Hauser Netilion Cloud und Bedientools sind keine Bestandteile dieses Security-Handbuches. In der folgenden Abbildung ist die Systemgrenzen farblich markiert.




1 *Systemüberblick Micropilot FWR30 (farbliche Markierung zeigt die Systemgrenzen für dieses Handbuch)*

1 *Micropilot FWR30*
2 *Mobilfunkverbindung https*
3 *Netilion Cloud*
4 *Internetverbindung https*
5 *Netilion Services: Internetbrowser basierte Netilion Service App*
6 *Nutzeranwendung*
7 *Netilion Connect: Application Programming Interface (API)*
8 *Internetverbindung https*
9 *SupplyCare Hosting*

Der Micropilot FWR30 wird in diesem Dokument in den allgemeinen Texten abhängig vom Zusammenhang entweder als Produkt oder als Endgerät bezeichnet.

## 3.3 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 DIN IEC 62443-3-3 die Anforderungen an das System und gemäß DIN EN 62443-4-2 die Anforderungen an die Produkte ab.

## 3.4 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 Schnittstelle 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.
- Passworte für das Produkt sind nur autorisierten Personen bekannt.
- Nur autorisierten Personen können über das zugehörige Human Machine Interface (HMI) auf das Produkt zugreifen.

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

## 3.5 Maßnahmen, falls erforderliche Einsatzumgebung nicht erfüllbar ist

Sofern die spezifizierten Anforderungen an die Einsatzumgebung nicht eingehalten werden können, sind ggf. Ersatzmaßnahme 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.

Beispielsweise können Sie den Micropilot FWR30 im freien Feld wie z.B. auf einen Tank eines LKWs einsetzen. Die Maßnahmen Die Maßnahmen vor physischer Manipulation müssen kundenseitig vorgenommen werden.

## 3.6 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 Standardpassworten usw. Diese Maßnahmen werden in den folgenden Kapiteln vorgestellt.

## 3.7 Empfehlung für risikomindernde Maßnahmen

### 3.7.1 Gesamtsystem betrachten

Der Micropilot FWR30 ist ein Endgerät, das in ein sogenanntes geschlossenes IIoT-Ökosystem eingesetzt wird.

Ein IIoT-Ökosystem kann aufgrund seiner dezentralen Modularität schnell zu einem Stückwerk aus verschiedenen Endgeräten werden. Jedes abweichende Produkt stellt bei solchen heterogenen Gesamtlösungen eine neue Gefahrenquelle dar, die Brüche an den Schnittstellen erzeugt und zu unsicheren Übertragungswegen führen kann.

In diesem Handbuch wird die Integration in das IIoT-Ökosystem Netilion von Endress+Hauser betrachtet. Wird der Micropilot FWR30 in ein anderes System integriert, sind zusätzliche Analysen erforderlich.

### 3.7.2 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.

### 3.7.3 Zugriffsmanagement optimieren

**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

### 3.7.4 Gerätedaten und Gerätestatus überwachen

Viele Angriffe auf ein Produkt in einem IIoT-Ökosystem erzeugen Anomalien in den Daten. Wenn ein Produkt plötzlich unrealistische Werte liefert, kann das ein Indiz für einen Angriff sein.

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 überwacht und bei Abweichungen informiert.

Der Micropilot FWR30 ist ein Endgerät im IIoT-Ökosystem und die Erkennung von Anomalien ist eine Aufgabe des übergeordneten Systems.

### 3.7.5 Produkt-Software updaten

Endgeräte für ein IIoT-Ökosystem müssen so entwickelt werden, dass möglichst wenige Nachbesserungen per Updates erforderlich sind. Aufgrund der Dynamik in der IT und den wachsenden Anforderungen in der Vernetzung sind in der Realität 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.

### 3.7.6 Anwendungen und Apps schützen

Software und insbesondere eine heterogene Software-Landschaft stellen ein weiteres Security-Risiko dar, wie z.B. Einsatz von Android-Apps auf einem Tablet und Windows-Lösungen auf einem PC.

Zur Sicherung der Anwendungen, Apps und Cloud-Server sollte auch der Schutz der mobilen und stationären Endgeräte gewährleistet sein, die auf das IIoT-Ökosystem Zugriff haben.

Zum Schutz des Kundensystems und der Kundendaten sollte auch der Schutz der Zugangsdaten der Endgeräte gewährleistet sein. Zugangsdaten und Zertifikate sollten sicher aufbewahrt werden.

# 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.

## 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 dieses Kapitel und die weiteren Kapitel beachten.

Die Inbetriebnahme von SupplyCare Hosting für den Micropilot FWR30 erfolgt durch den Service von Endress+Hauser.

Systemüberblick Micropilot FWR30: → 🖹 7

### 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 → 🖹 8.

### 4.4.3 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.

Eine Härtung des Micropilot FWR30 ist nicht möglich und auch nicht erforderlich. Der Micropilot FWR30 verwendet nur Dienste, die für die Funktion erforderlich sind.

### 4.4.4 Anwenderdaten konfigurieren

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

Im Micropilot FWR30 sind keine Anwenderdaten abgelegt.

### 4.4.5 Security-relevante Einstellungen des Produkts

Alle Security-relevanten Einstellungen, die für den Micropilot FWR30 erforderlich sind, wurden am Micropilot FWR30 werksseitig durchgeführt. Anpassungen sind nicht erforderlich.

# 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 Micropilot FWR30 erfordert keine Interaktionen während des Betriebes.

## 5.4 Security-Aspekte während des Betriebes

Die im Micropilot FWR30 hinterlegten Zertifikate haben eine begrenzte Laufzeit von 5 Jahren.

Ca. 1 Jahr bevor die Zertifikate ablaufen, erneuert Endress+Hauser über die Netilion Cloud die Zertifikate für den Micropilot FWR30. Melden Sie den Micropilot FWR30 mindestens einmal pro Jahr an die Netilion Cloud an.

## 5.5 Update-Management

Endress+Hauser stellt Remote-Updates über die Netilion Cloud bereit. Der Anwender muss das Update über die Netilion Cloud anstoßen. Der Zeitpunkt für ein Update ist einstellbar. Nach manchen Updates ist ein Neustart für den Micropilot FWR30 erforderlich. Der Neustart wird automatisch durchgeführt.

Endress+Hauser stellt Remote-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. | ▸ Produkt über einen langen Tastendruck deaktivieren. |
| Das Produkt hat eine Störung und Sie können die Störung nicht beheben. | ▸ Endress+Hauser kontaktieren.<br>↳ Endress+Hauser fordert Sie entweder auf, das Produkt zu Endress+Hauser zu senden oder das Produkt zu zerstören. |
| Das Produkt benötigt einen Service von Endress+Hauser wie z.B. eine Kalibration. | 1. Produkt über einen langen Tastendruck deaktivieren.<br>2. Produkt zu Endress+Hauser senden. |
| Das Produkt ist defekt und muss daher entsorgt werden. | ▸ Produkt über einen langen Tastendruck deaktivieren. |
| Das Produkt soll entsorgt werden. | ▸ Produkt über einen langen Tastendruck deaktivieren. |

# 7 Anhang

## 7.1 Security-Checkliste für den Produktlebenszyklus

| Lebenszyklus | Tätigkeit | Geprüft |
|---|---|---|
| Planung | Typische Einsatzumgebung des Produkts definiert und bei der Planung berücksichtigt. → 🖹 8<br>Falls erforderlich, Ersatzmaßnahmen berücksichtigt. → 🖹 9 | ❑ |
| | Planungsarbeiten in der Engineering-Phase beachtet. Bedrohungsanalyse und Risikobeurteilung durchgeführt.→ 🖹 9 | ❑ |
| | Sofern möglich, risikiomindernde Maßnahmen berücksichtigt. → 🖹 9 | ❑ |
| Wareneingang / Transport | Geprüft, dass die Verpackung ungeöffnet ist und dass das Siegel unbeschädigt ist. | ❑ |
| Inbetriebnahme | Produkt für den Anwendungsfall gehärtet. → 🖹 12 | Nicht anwendbar |
| Betrieb | Vorgaben zum Update-Management beachtet. → 🖹 14 | ❑ |
| | Planung der wiederkehrenden Bedrohungsanalyse vorgenommen. → 🖹 14 | ❑ |
| Außerbetriebnahme | Produkt außer Betrieb genommen. → 🖹 16<br>Je nach Grund für die Außerbetriebnahme Produkt deaktivieren oder das Produkt zerstören. | ❑ |

## 7.2 Versionshistorie

| Dokumentenversion | Firmwareversion | Hardwareversion | Änderungen |
|---|---|---|---|
| 01.21 | ab 01.00.01 | Dev. Rev. 1<br>Dev. Rev. 2 | Erste Version |


www.addresses.endress.com

Endress+Hauser

People for Process Automation