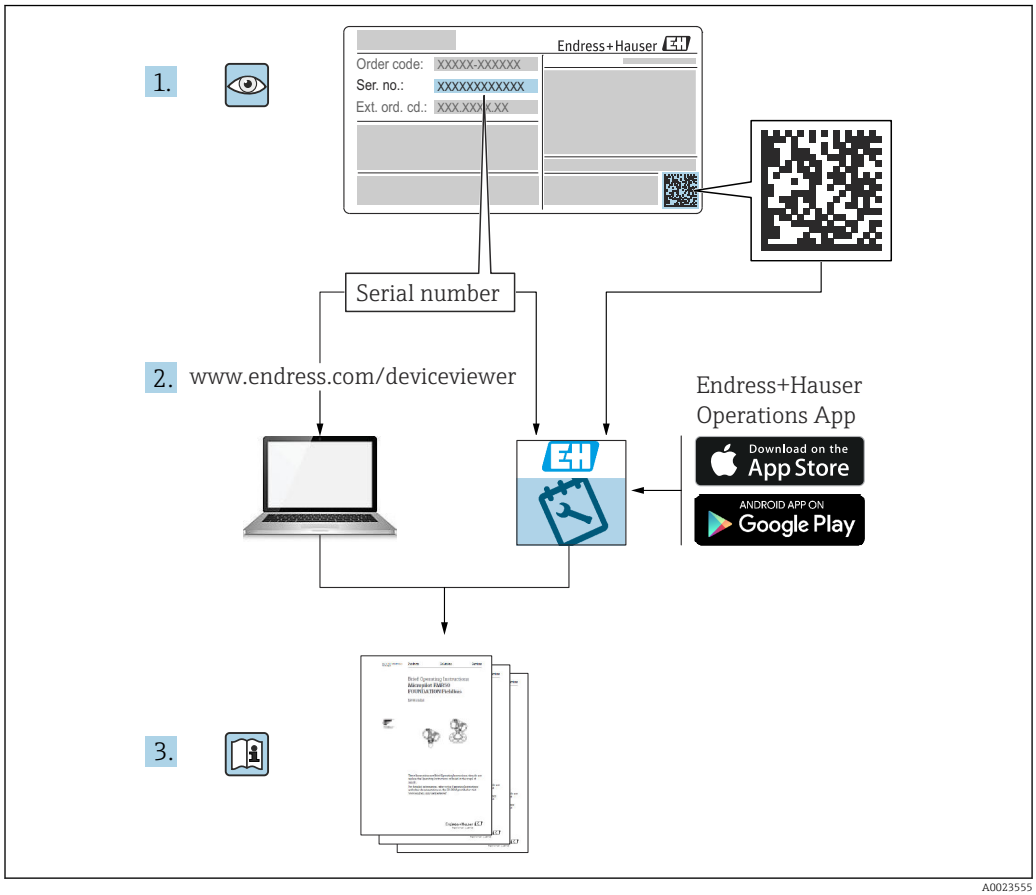
SD03430F/09/DE/01.25-00
71709122
2025-05-31



# Sonderdokumentation
# **FlexView FMA90**

Steuereinheit mit Farbanzeige und Touch-Control für bis zu 2 Ultraschall-, Radar-, Hydrostatik- oder universelle 4-20 mA/HART® Füllstandssensoren

Endress+Hauser
People for Process Automation


1.
Endress+Hauser
Order code: XXXXX-XXXXXX
Ser. no.: XXXXXXXXXXX
Ext. ord. cd.: XXX XXX 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 . . . . . 7**
3.1 Zielgruppe . . . . . 7
3.2 Systemüberblick . . . . . 7
3.2.1 Allgemeine Informationen . . . . . 7
3.2.2 Systemaufbau und Systemgrenzen . . . . 7
3.3 Security-Level festlegen . . . . . 8
3.4 Typische Einsatzumgebung des Produkts . . . . . 9
3.5 Maßnahmen, falls erforderliche Einsatzumgebung nicht erfüllbar ist . . . . . 9
3.6 Bedrohungsanalyse und Risikobeurteilung durchführen . . . . . 9
3.7 Empfehlung für risikomindernde Maßnahmen . . . . . 10
3.7.1 Gesamtsystem betrachten . . . . . 10
3.7.2 Anwender schulen . . . . . 10
3.7.3 Zugriffsmanagement optimieren . . . . 10
3.7.4 Gerätedaten und Gerätestatus überwachen . . . . . 11
3.7.5 Produkt-Software updaten . . . . . 11

**4 Inbetriebnahme (Installation und Konfiguration) . . . . . 12**
4.1 Zielgruppe . . . . . 12
4.2 Anforderungen an das Personal . . . . . 12
4.3 Installation . . . . . 12
4.4 Konfiguration . . . . . 12
4.4.1 Produkt in Betrieb nehmen und konfigurieren . . . . . 12
4.4.2 Erforderliche Security-Schritte während der Inbetriebnahme . . . . . 12
4.4.3 Produkt härten . . . . . 12
4.4.4 Anwenderdaten konfigurieren . . . . . 12
4.4.5 Security-relevante Einstellungen des Produkts . . . . . 13
4.4.6 User-Management und Auswirkung auf die Security . . . . . 13

**5 Betrieb . . . . . 14**
5.1 Zielgruppe . . . . . 14
5.2 Anforderungen an das Personal . . . . . 14
5.3 Aufgaben während des Betriebes . . . . . 14
5.4 Security-Aspekte während des Betriebes . . . . . 14
5.5 Update-Management . . . . . 14
5.6 Wiederholung der Bedrohungsanalyse . . . . . 15
5.7 Reparatur und Entsorgung . . . . . 15

**6 Außerbetriebnahme . . . . . 16**
6.1 Zielgruppe . . . . . 16
6.2 Anforderungen an das Personal . . . . . 16
6.3 Produkt außer Betrieb nehmen . . . . . 16

**7 Anhang . . . . . 17**
7.1 Security-Checkliste für den Produktlebenszyklus . . . . . 17
7.2 Versionshistorie . . . . . 17
7.3 Security-Level gemäß IEC 62443-4-2 . . . . . 17

# 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 FlexView FMA90

- Technische Information TI01689F
- Betriebsanleitung BA02254
- Kurzanleitung KA01584F
- Geräteparameter GP01189F

### 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

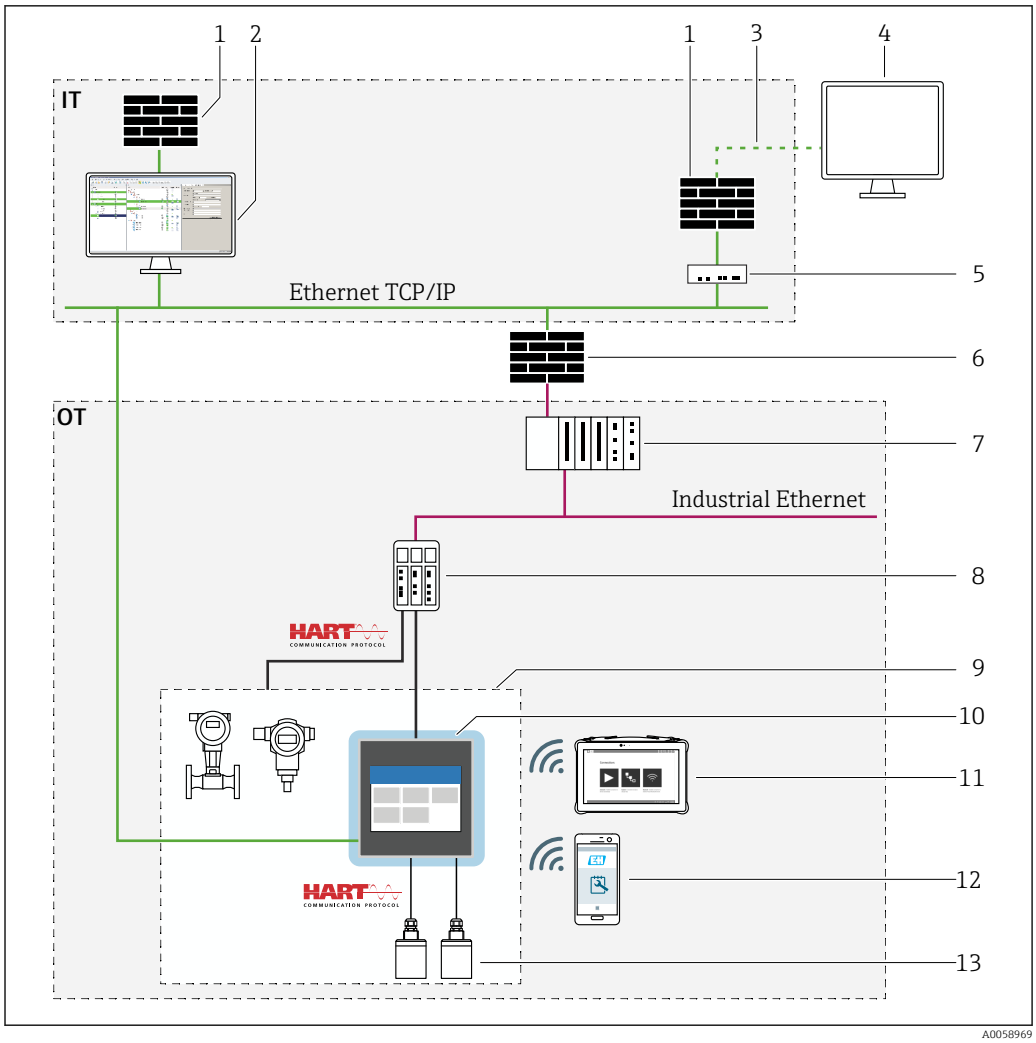
### 3.2.1 Allgemeine Informationen

Der FlexView FMA90 ist mit folgenden Schnittstellen ausgestattet:
- Standardmäßig:
  - HART Device, drahtgebunden
    Im Betrieb überträgt der FlexView die Messwerte und die berechneten Werte über 4-20 mA/HART an eine übergeordnete Steuerung (PLC / DCS).
  - HART Master
    An den FlexView können Sie 4-20 mA/HART-Feldgeräte anschließen.
  - Ethernet RJ45
- Optional:
  - WLAN
  - Vor-Ort-Display

Sie können den FlexView über folgende digitale Applikationen konfigurieren:
- Standardmäßig:
  - Ethernet/TCP und dem im FlexView integrierten Webserver
  - HART mit eingeschränkter Konfiguration
- Optional:
  - WLAN und dem im FlexView integrierten Webserver
  - Vor-Ort-Display

### 3.2.2 Systemaufbau und Systemgrenzen

In diesem Security-Handbuch wird der FlexView FMA90 und die Anbindung an eine PLC / DCS via 4-20 mA/HART betrachtet. Die weiteren Komponenten wie angeschlossene Feldgeräte und die Bedientools sind keine Bestandteile dieses Security-Handbuches. In der folgenden Abbildung ist die Systemgrenze farblich markiert.




1 *Einsatzmöglichkeiten FlexView FMA90, blaue Markierung zeigt die Systemgrenzen für dieses Handbuch*

*IT Information Technology, hier Unternehmensnetzwerk*
*OT Operational Technology, hier Netzwerk zur Prozessautomatisierung*
*1 Firewall des Unternehmensnetzwerk (IT)*
*2 Host-Anwendung wie z.B. Endress+Hauser FieldCare SFE500 oder DeviceCare oder direkt über Webserver*
*3 Ethernet TCP/IP*
*4 Fernzugriff via Webserver*
*5 Router*
*6 Anlagenfirewall*
*7 Steuerung PLC / DLC*
*8 Gateway zur Umsetzung von HART auf Industrial Ethernet*
*9 Anlagenkomponenten wie Endress+Hauser Feldgeräte und Feldgeräte anderer Hersteller*
*10 FlexView FMA90*
*11 Endress+Hauser Field Xpert SMTxx via WLAN und Webserver*
*12 Bedienung und Konfiguration via WLAN und Webserver*
*13 4-20 mA/HART-Feldgeräte, hier z.B. Endress+Hauser Füllstandssensoren*

Der FlexView FMA90 wird in diesem Dokument in den allgemeinen Texten abhängig vom Zusammenhang entweder als Produkt, Endgerät oder Steuereinheit 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

Die Betrachtung der Einsatzumgebung für das Produkt soll zu den Security-Anforderungen führen, die durch die Umgebung erbracht werden müssen.

Beispielsweise können Sie einen Denial-of-Service-Angriff betrachten.

Beispiel für eine typische Einsatzumgebung des Produkts:
- 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 FlexView im freien Feld einsetzen wie z.B. zur Pumpensteuerung für ein Hebewerk in einem Kanalsystem oder zur Durchflussmessung an offenen Gerinnen und Wehren.

Die Maßnahmen zur Verhinderung von physischen Manipulationen und Remote-Manipulationen des FlexView müssen kundenseitig vorgenommen werden.

Sie können den FlexView plombieren, wodurch ein mechanischer Zugriffsschutz gewährleistet ist.

## 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 FlexView FMA90 ist eine Steuereinheit, die entweder als Stand-Alone-Gerät oder in einem geschlossenen Automatisierungssystem eingesetzt wird. Ein geschlossenes Automatisierungssystem kann z.B. eine Kläranlage sein.

In diesem Handbuch werden der Einsatz des FlexView als Stand-Alone-Gerät oder in einem geschlossenen Automatisierungssystem betrachtet. Wird der FlexView in ein anderes System integriert, sind zusätzliche Analysen erforderlich.

Der FlexView wurde gemäß den Anforderungen der IEC 62443-4-1 entwickelt und erreicht gemäß der IEC 62433-4-2 den Security-Level 1 (SL 1).

Weitere Informationen: → 17

### 3.7.2 Anwender schulen

Je nach Anwendungsszenario können auch fachfremde Anwender mit dem FlexView in Berührung kommen. Wir empfehlen, alle Anwender und insbesondere fachfremde Anwender für den sicheren Gebrauch mit dem FlexView, mit allen genutzten Schnittstellen und allen angeschlossenen und verbunden Komponenten zu schulen und für die Security zu sensibilisieren.

### 3.7.3 Zugriffsmanagement optimieren

Um eine Manipulation des FlexView zu verhindern, muss die Benutzerrolle „Instandhalter“ mit einer PIN gesichert werden.

Detaillierte Informationen zu Benutzerrollen und Rechte: Betriebsanleitung → 6

#### Webserver via Ethernet

Damit Sie auf den FlexView über den Webserver zugreifen können, benötigen Sie entsprechende Zugangsdaten. Für die erste Anmeldung müssen Sie die Initial-PIN verwenden. Wir empfehlen, die PIN nach der ersten Anmeldung zu ändern und sicher aufzubewahren.

Detaillierte Informationen zur Initial-PIN und Anmeldung: Betriebsanleitung → 6

#### Webserver via WLAN (optional)

Damit Sie auf den FlexView über den Webserver via WLAN zugreifen können, müssen Sie zuerst eine Verbindung zum FlexView via WLAN herstellen.

Für die erste Anmeldung auf den Webserver müssen Sie die Initial-PIN verwenden. Wir empfehlen, die PIN nach der ersten Anmeldung zu ändern und sicher aufzubewahren.

Detaillierte Informationen für den Verbindungsaufbau via WLAN, zur Initial-PIN und Anmeldung: Betriebsanleitung → 6

#### HART

HART ist eine Schnittstelle ohne besondere Security-Funktionen.

Bei Nutzung der HART-Schnittstelle empfehlen wir, nach der Inbetriebnahme entweder die Hardware-Verriegelung zu aktivieren oder einen Perimeterschutz zu implementieren.

### 3.7.4 Gerätedaten und Gerätestatus überwachen

#### Überwachung über HART

Der FlexView kann über HART an ein Automatisierungssystem angebunden sein. In diesem Fall ist eine Erkennung und die Behebung von Anomalien eine Aufgabe des Betreibers des Automatisierungssystems.

#### Überwachung bei Einbindung in ein Netzwerk (LAN)

Der FlexView kann ein Endgerät in einem Area-Network sein und die Erkennung von Anomalien ist eine Aufgabe des übergeordneten Systems.

### 3.7.5 Produkt-Software updaten

Netzwerkfähige Endgeräte müssen so entwickelt werden, dass möglichst wenige Nachbesserungen per Updates erforderlich sind. Aufgrund der Dynamik in der IT/OT 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.

Update-Management: → 14

# 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 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 → 9.

### 4.4.3 Produkt härten

Eine Härtung des FlexView erfolgt durch Deaktivierung nicht benutzter Schnittstellen.

Die Schnittstellen deaktivieren Sie über das Menü „System“.

Detaillierte Informationen: Beschreibung Geräteparameter (GP) → 6

### 4.4.4 Anwenderdaten konfigurieren

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

Alle Anwenderdaten können Sie konfigurieren. Die Anwenderdaten konfigurieren Sie über das Menü „System“.

Detaillierte Informationen: Beschreibung Geräteparameter (GP) → 6

### 4.4.5 Security-relevante Einstellungen des Produkts

Alle Security-relevanten Einstellungen, die für den FlexView erforderlich sind, können Sie konfigurieren. Die Security-relevanten Einstellungen konfigurieren Sie über das Menü „System“.

Beachten Sie zusätzlich die Vorgaben der folgenden Kapitel:
- Produkt härten: → 12
- User-Management → 13

Detaillierte Informationen: Beschreibung Geräteparameter (GP) → 6

### 4.4.6 User-Management und Auswirkung auf die Security

Der FlexView bietet mehrere Benutzerrollen mit spezifischen Lese- und Schreibrechten und unterschiedlichen Login-Daten.

Einstellungen gemäß Kapitel "Zugriffsmanagement optimieren" und gemäß Betriebsanleitung durchführen.

Zugriffsmanagement optimieren: → 10

Detaillierte Informationen zu Benutzerrollen, Rechte und Einstellungen: Betriebsanleitung und Beschreibung Geräteparameter (GP) → 6

# 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

Der FlexView erfordert keine Interaktionen während des Betriebes.

## 5.4 Security-Aspekte während des Betriebes

Der FlexView besitzt ein integriertes TLS/SSL-Zertifikatsmanagement für den HTTPS-Webserver.

Zertifikate haben eine spezifische Ablaufdauer. Vor dem Ablauf werden Diagnosemeldungen generiert.

Das neue Zertifikat müssen Sie über das Bedienmenü importieren.

Detaillierte Informationen zur Zertifikatsverwaltung und Zertifikate: Beschreibung Geräteparameter (GP) → 6

## 5.5 Update-Management

Endress+Hauser stellt Updates über die Produktseite des FlexView FMA90 zur Verfügung https://www.endress.com/FMA90.

Für die Durchführung eines Updates Endress+Hauser Service kontaktieren.

Ein Update ist nur über den Webserver möglich.

Weitere Informationen zur Firmware-Updates: Betriebsanleitung → 6

Nach jedem Update ist ein Neustart für den FlexView erforderlich. Der Neustart wird automatisch durchgeführt.

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

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. | Wir empfehlen, das Produkt auf Werkseinstellung zurückzusetzen.<br>Produkt von der Versorgungsspannung trennen und bei Bedarf ausbauen und lagern. |
| Das Produkt hat eine Störung und Sie können die Störung nicht beheben. | 1. Endress+Hauser kontaktieren.<br>2. Schritte gemäß den Anweisungen von Endress+Hauser durchführen. |
| Das Produkt benötigt einen Service von Endress+Hauser. | 1. Endress+Hauser kontaktieren.<br>2. Schritte gemäß den Anweisungen von Endress+Hauser durchführen. |
| Das Produkt ist defekt und muss daher entsorgt werden. | 1. Produkt von der Versorgungsspannung trennen.<br>2. Produkt zerstören. |
| Das Produkt soll entsorgt werden. | Wir empfehlen, das Produkt auf Werkseinstellung zurückzusetzen. Produkt von der Versorgungsspannung trennen. |

# 7 Anhang

## 7.1 Security-Checkliste für den Produktlebenszyklus

| Lebenszyklus | Tätigkeit | Geprüft |
|---|---|---|
| Planung | Typische Einsatzumgebung des Produkts definiert und bei der Planung berücksichtigt. → 🖹 9<br>Falls erforderlich, Ersatzmaßnahmen berücksichtigt. → 🖹 9 | ❑ |
| | Planungsarbeiten in der Engineering-Phase beachtet. Bedrohungsanalyse und Risikobeurteilung durchgeführt. → 🖹 9 | ❑ |
| | Sofern möglich, risikomindernde Maßnahmen berücksichtigt. → 🖹 10 | ❑ |
| Wareneingang / Transport | Geprüft, dass die Verpackung ungeöffnet ist und dass das Siegel unbeschädigt ist. | ❑ |
| Inbetriebnahme | Produkt für den Anwendungsfall gehärtet. → 🖹 12 | ❑ |
| Betrieb | Vorgaben zum Update-Management beachtet. → 🖹 14 | ❑ |
| | Planung der wiederkehrenden Bedrohungsanalyse vorgenommen. → 🖹 15 | ❑ |
| 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 |
|---|---|---|---|
| 01.00 | ab 01.00.00 | Dev. Rev. 1 | Erste Version |

## 7.3 Security-Level gemäß IEC 62443-4-2

Der FlexView FMA90 erreicht gemäß IEC 62443-4-2 den Security-Level 1 (SL 1) und erfüllt das Endress+Hauser Schutzprofil ProtectBlue Essential.

*Erklärung der Symbole in der Spalte "Status"*

✔ Anforderung ist erfüllt

(✔) Anforderung ist für das Produkt nicht anwendbar

*FR 1 – Identifizierung und Authentifikation (IAC)*

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 1.1 | Identifizierung und Authentifikation von menschlichen Nutzern | ✔ | |
| CR 1.2 | Identifizierung und Authentifikation von Softwareprozessen und Geräten | (✔) | |
| CR 1.3 | Nutzerkontenverwaltung | ✔ | |
| CR 1.4 | Verwaltung der Kennungen | ✔ | Das Produkt besitzt festgelegte Kontokennungen. |
| CR 1.5 | Verwaltung der Authentifizierer | ✔ | |

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 1.7 | Stärke der Authentifikation durch Passwörter | (✔) | |
| CR 1.8 | PKI-Zertifikate | ✔ | |
| CR 1.9 | Stärke der Authentifikation durch öffentliche Schlüssel | ✔ | |
| CR 1.10 | Rückmeldung vom Authentifizierer | ✔ | |
| CR 1.11 | Erfolglose Anmeldeversuche | ✔ | |
| CR 1.12 | Nutzungshinweis des Systems | ✔ | |
| CR 1.14 | Stärke der Authentifikation durch symmetrische Schlüssel | ✔ | |

*FR 2 – Nutzungskontrolle (UC)*

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 2.1 | Durchsetzung der Autorisierung | ✔ | |
| CR 2.2 | Nutzungskontrolle von Funkverbindungen | ✔ | |
| EDR 2.4 | Mobiler Code | (✔) | |
| CR 2.5 | Sitzungssperrung | ✔ | |
| CR 2.6 | Beendigung einer Fernzugriffssitzung | ✔ | |
| CR 2.8 | Prüfbare Ereignisse | ✔ | |
| CR 2.9 | Speicherkapazität für Ereignisdatensätze | ✔ | Der Ereignisspeicher ist als Ringspeicher mit 10000 Einträgen realisiert. Ab 10001 Ereignissen wird das älteste Ereignis überschrieben. |
| CR 2.10 | Verhalten bei Verarbeitungsfehlern von Ereignisdaten | ✔ | |
| CR 2.11 | Zeitstempel | ✔ | |
| | RE (1) Zeitsynchronisierung | ✔ | Datum und Uhrzeit können per NTP synchronisiert werden. |
| CR 2.12 | Nichtabstreitbarkeit | ✔ | Das Produkt erzeugt automatisch lokale sicherheitsrelevante Ereignisdatensätze (Log-Einträge) mit Echtzeitstempel. |
| EDR 2.13 | Nutzung von physikalischen Diganose- und Prüfschnittstellen | ✔ | |

*FR 3 – Systemintegrität (SI)*

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 3.1 | Kommunikationsintegrität | ✔ | |
| EDR 3.2 | Schutz vor Schadcodes | ✔ | Secure-boot-Funktionalität implementiert. |
| CR 3.3 | Verifikation der IT-Sicherheitsfunktionalität | ✔ | Security-Funktionen können vom Anwender getestet werden. Z.B. erfolglose Login-Versuche werden im Logbuch erfasst, Timeout für erneute Eingabe wird gestartet. Der Timeout erhöht sich mit der Anzahl der erfolglosen Versuche. |
| CR 3.4 | Software- und Informationsintegrität | ✔ | |
| | RE (1) Authentizität der Software und der Informationen | ✔ | |

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 3.5 | Eingabevalidierung | ✔ | |
| CR 3.6 | Vorbestimmte Zustände der Ausgänge | ✔ | |
| CR 3.7 | Fehlerbehandlung | ✔ | |
| CR 3.8 | Sitzungsintegrität | ✔ | |
| CR 3.9 | Schutz von Prüfinformationen | ✔ | |
| EDR 3.10 | Unterstützung von Updates | ✔ | |
| | RE (1) Authentizität und Integrität von Updates | ✔ | |
| EDR 3.11 | Physikalische Manipulationssicherheit und -erkennung | ✔ | Das Produkt kann plombiert werden, wodurch ein mechanischer Zugriffsschutz gewährleistet ist. |
| EDR 3.12 | Bereitstellung von Hersteller-Vertrauensankern | ✔ | Nur von Endress+Hauser autorisierte Firmware kann in das Produkt geladen werden. |
| EDR 3.13 | Bereitstellung von Betreiber-Vertrauensankern | (✔) | |
| EDR 3.14 | Integrität von Boot-Prozessen | ✔ | |
| | RE (1) Authentizität des Boot-Prozesses | ✔ | |

*FR 4 – Vertraulichkeit der Daten (DC)*

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 4.1 | Vertraulichkeit von Informationen | (✔) | |
| CR 4.2 | Dauerhaftigkeit von Informationen | ✔ | |
| | RE (1) Löschen gemeinsam genutzter Speicherressourcen | ✔ | |
| CR 4.3 | Verwendung von Verschlüsselung | ✔ | |

*FR 5 – Eingeschränkter Datenfluss (RDF)*

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 5.1 | Netzaufteilung | ✔ | |

*FR 6 – Rechtzeitige Reaktion auf Ereignisse (TRE)*

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 6.1 | Zugriffsmöglichkeit auf Ereignisprotokolle | ✔ | |
| CR 6.2 | Kontinuierliche Überwachung | (✔) | |

*FR 7 – Verfügbarkeit der Ressourcen (RA)*

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 7.1 | Schutz vor Denial-of-Service-Ereignissen | ✔ | |
| CR 7.2 | Ressourcenmanagement | ✔ | |
| CR 7.3 | Datensicherung im Automatisierungssystem (Backup) | ✔ | Ab Firmwareversion 1.1 |
| | RE (1) Verifikation der Integrität der Datensicherung | ✔ | Ab Firmwareversion 1.1 |

| Anforderung | | Status | Bemerkung |
|---|---|---|---|
| CR 7.4 | Wiederherstellung des Automatisierungssystems | ✔ | Ab Firmwareversion 1.1 |
| CR 7.6 | Netzwerk- und IT-Sicherheitseinstellungen | ✔ | |
| CR 7.7 | Geringste Funktionalität | ✔ | |
| CR 7.8 | Verzeichnis der Komponenten eines Automatisierungssystems | (✔) | |

www.addresses.endress.com

Endress+Hauser

People for Process Automation