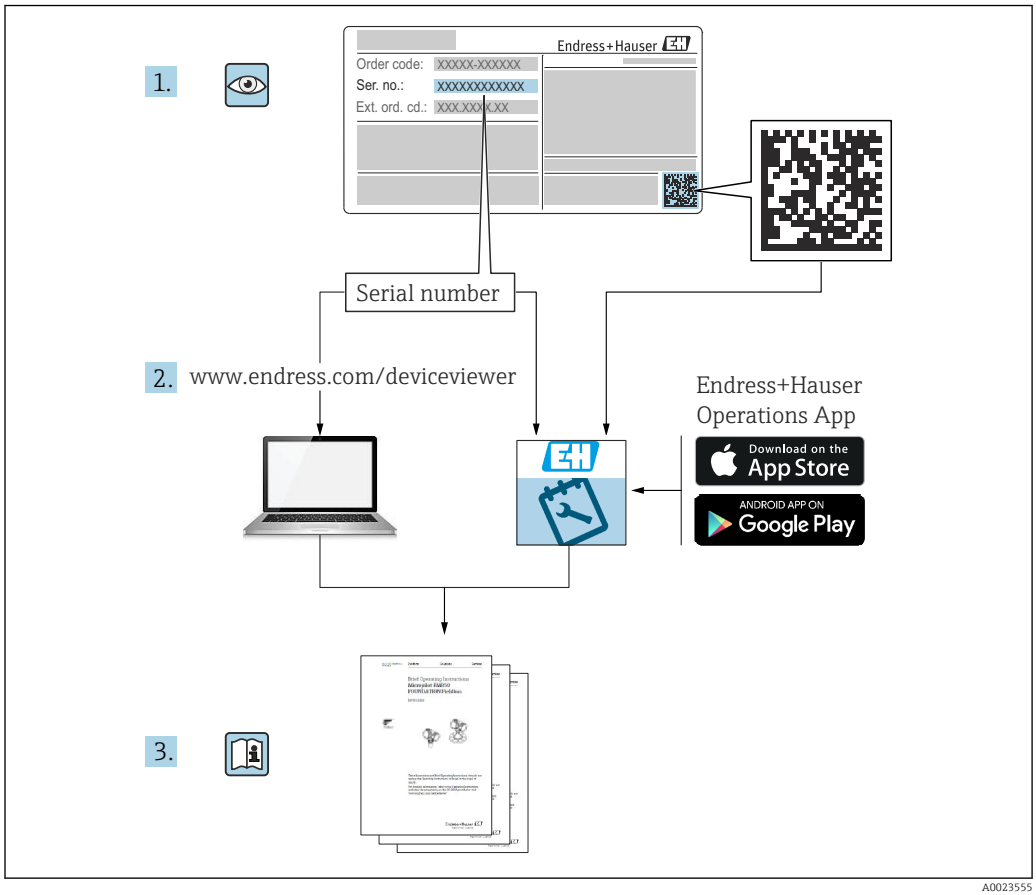
SD02984S/00/DE/01.22-00
71574837
2022-07-01

Sonderdokumentation
Security-Handbuch FieldPort SWA50

Intelligenter Bluetooth®- und/oder WirelessHART-Adapter für alle HART-Feldgeräte

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 FieldPort SWA50

- Technische Information TI01468S (Bluetooth und WirelessHART)
- Betriebsanleitung BA01987S (Bluetooth)
- Kurzanleitung KA01436S (WirelessHART)
- Betriebsanleitung BA02046S (WirelessHART)
- Zugangsdaten Bluetooth: 71499893
- 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 FieldPort SWA50 über folgende digitale Applikationen konfigurieren und betreiben:
- Endress+Hauser SmartBlue-App
- Endress+Hauser Field Xpert SMTxx (Bluetooth über MSD, HART über DTM)

Die WirlelessHART-Variante ist zusätzlich wie folgt bedienbar:
Fernkonfiguration mit FieldCare SFE500 via WirelessHART-Fieldgate SWGxx und DTMs

Der FieldPort SWA50 ist mit folgenden Schnittstellen ausgestattet:
- Bluetooth®
- HART (drahtgebunden)
- WirelessHART-Variante zusätzlich: WirelessHART

Über den FieldPort SWA50 und einem FieldEdge können HART-Feldgeräte an die Netilion Cloud angebunden werden.
- Netilion: https://netilion.endress.com
- Netilion Value: https://Netilion.endress.com/app/value

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

Die Bluetooth-Verbindung zwischen FieldPort SWA50 und mobilen Endgeräten wie Smartphones, Tablets oder EdgeDevices ist durch CPace geschützt. Weitere Informationen erhalten Sie unter folgendem Link:

https://www.endress.com/cybersecurity > Abschnitt "Sichere Bluetooth®-Verbindung von Endress+Hauser

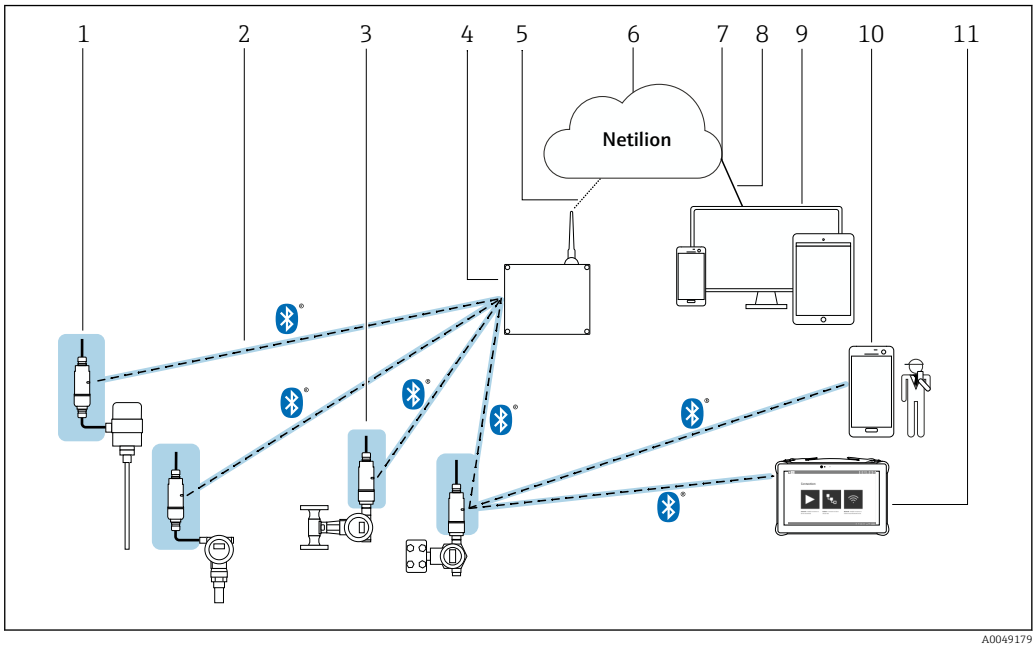
Die WirelessHART-Verbindung zwischen FieldPort SWA50 und WirlessHART-Gateway ist gemäß dem WirelessHART-Standard end-to-end mit AES-128 Bit verschlüsselt. Weitere Informationen erhalten Sie unter folgendem Link:

https://fieldcommgroup.org/wirelesshart-security

3.2.2 Systemaufbau und Systemgrenzen

In diesem Security-Handbuch wird der FieldPort SWA50, die Schnittstelle zum drahtgebundenen Feldgerät, die Bluetooth-Verbindung und die WirelessHART-Verbindung betrachtet. Die weiteren Komponenten wie angeschlossene Feldgeräte, Gateways, Edge Devices, die Endress+Hauser Netilion Cloud und Bedientools sind keine Bestandteile dieses Security-Handbuches. In den folgenden Abbildungen sind die Systemgrenzen farblich markiert.

Systemaufbau FieldPort SWA50 Bluetooth-Variante

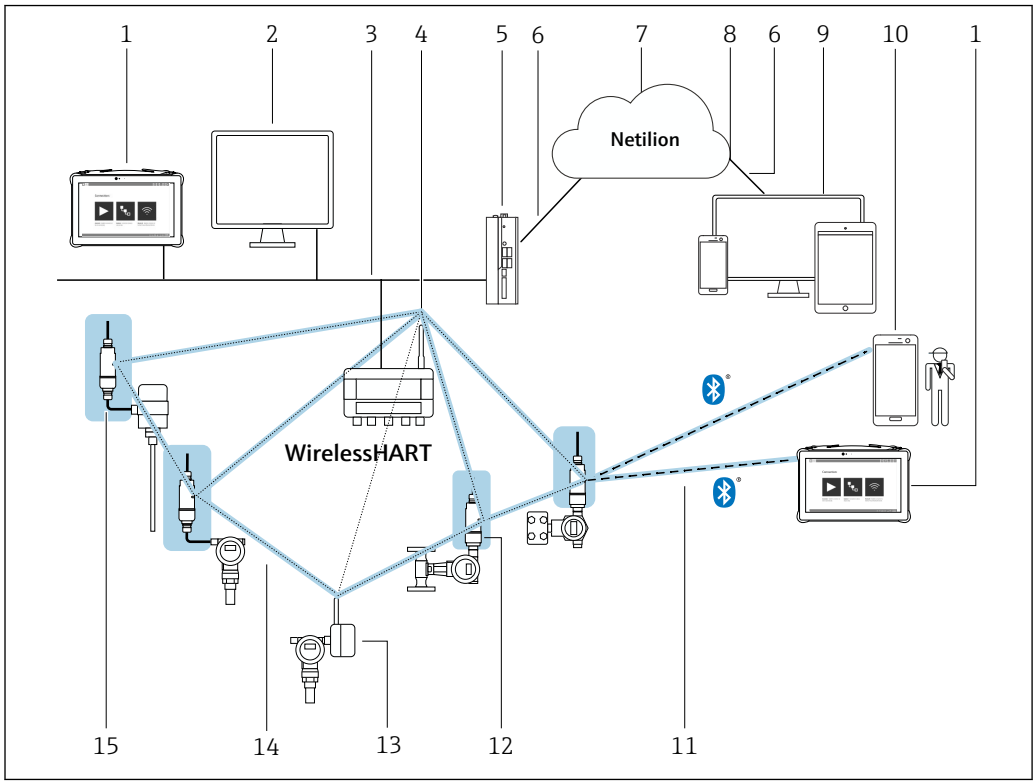


1 *Systemaufbau SWA50 Bluetooth-Variante (farbliche Markierung zeigt die Systemgrenzen für dieses Handbuch)*

1 *HART-Feldgerät mit FieldPort SWA50, abgesetzte Montage*
2 *Verschlüsselte drahtlose Verbindung über Bluetooth®*
3 *HART-Feldgerät mit FieldPort SWA50, direkte Montage*
4 *FieldEdge SGC200*
5 *LTE-Verbindung*
6 *Netilion Cloud*
7 *Application Programming Interface (API)*
8 *Internetverbindung https*
9 *Internetbrowser basierte Netilion Service App oder Nutzeranwendung*
10 *Endress+Hauser SmartBlue-App*
11 *Endress+Hauser Field Xpert wie z.B. SMTxx*

Der FieldPort SWA50 wird in diesem Dokument in den allgemeinen Texten abhängig vom Zusammenhang entweder als Produkt oder als Endgerät bezeichnet.

Systemaufbau FieldPort SWA50 WirelessHART-Variante



2 *Systemaufbau SWA50 WirelessHART-Variante (farbliche Markierung zeigt die Systemgrenzen für dieses Handbuch)*

1 *Endress+Hauser Field Xpert wie z.B. SMTxx*
2 *Host-Anwendung / FieldCare SFE500*
3 *Ethernet Kommunikation*
4 *WirelessHART-Fieldgate wie z.B. SWG70*
5 *FieldEdge SGC500*
6 *Internetverbindung https*
7 *Netilion Cloud*
8 *Application Programming Interface (API)*
9 *Internetbrowser basierte Netilion Service App oder Nutzeranwendung*
10 *Endress+Hauser SmartBlue-App*
11 *Verschlüsselte drahtlose Verbindung über Bluetooth®*
12 *HART-Feldgerät mit FieldPort SWA50, direkte Montage*
13 *HART-Feldgerät mit WirelessHART-Adapter wie z.B. SWA70*
14 *Verschlüsselte drahtlose Verbindung über WirelessHART*
15 *HART-Feldgerät mit FieldPort SWA50, abgesetzte Montage*

Der FieldPort SWA50 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 FieldPort SWA50 im freien Feld einsetzen. Die Maßnahmen vor physischer Manipulation des FieldPort SWA50 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 Standardpasswörten usw. Diese Maßnahmen werden in den folgenden Kapiteln vorgestellt.

3.7 Empfehlung für risikomindernde Maßnahmen

3.7.1 Gesamtsystem betrachten

Der FieldPort SWA50 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 FieldPort SWA50 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

Bluetooth

Damit Sie auf den FieldPort SWA50 über Bluetooth zugreifen können, benötigen Sie entsprechende Zugangsdaten wie Login und Passwort. Für die erste Anmeldung müssen Sie das werksseitig eingestellte Passwort verwenden. Wir empfehlen, das Passwort nach der ersten Anmeldung zu ändern und sicher aufzubewahren. Das Initialpasswort ist auf dem Typenschild und auf dem mitgelieferten Blatt "Zugangsdaten Bluetooth" angegeben.

Weitere Informationen: Betriebsanleitung BA01987S (Bluetooth) und Zugangsdaten Bluetooth → 6

WirelessHART

Für den Betrieb des FieldPort SWA50 in einem WirelessHART-Netzwerk, benötigen Sie die Netzwerk-ID (Network Identification) und das Netzwerkpasswort (Join Key) des entsprechenden WirelessHART-Netzwerkes. Wir empfehlen, diese Zugangsdaten vertraulich zu behandeln und sicher aufzubewahren.

Weitere Informationen: Kurzanleitung KA01436S (WirelessHART) und Betriebsanleitung BA02046S (WirelessHART) → 6

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

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.

Überwachung über HART

Der FieldPort SWA50 kann über HART an ein Steuerungssystem angebunden sein. Eine Erkennung und die Behebung von Anomalien ist dann eine Aufgabe des Betreibers des Steuerungssystems.

Überwachung über WirelessHART

Der FieldPort SWA50 kann ein Teilnehmer in einem WirelessHART-Netzwerk sein. Eine Erkennung und die Behebung von Anomalien ist dann eine Aufgabe des WirelssHART-Netzwerk Betreibers.

Überwachung über das IIoT-Ökosystem

Der FieldPort SWA50 kann ein Endgerät in einem IIoT-Ökosystem sein 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.

Systemüberblick FieldPort SWA50: → 🖹 8

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 → 🖹 11.

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 FieldPort SWA50 ist nur für die WirelessHART-Variante möglich. Wenn Sie die Bluetooth-Verbindung nach der Inbetriebnahme nicht mehr nutzen, können Sie die Funktion "Bluetooth-Kommunikation" über den DIP-Schalter 1 deaktivieren.

Weitere Informationen zu "DIP-Schalter": Kurzanleitung KA01436S (WirelessHART) → 🖹 6

4.4.4 Anwenderdaten konfigurieren

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

Die Anwenderdaten können Sie konfigurieren.

Weitere Informationen: Dokumentation FieldPort SWA50 → 6

4.4.5 Security-relevante Einstellungen des Produkts

Alle Security-relevanten Einstellungen, die für den FieldPort SWA50 erforderlich sind, wurden am FieldPort SWA50 werksseitig durchgeführt. Anpassungen sind nicht erforderlich.

4.4.6 User-Management und Auswirkung auf die Security

Der FieldPort SWA50 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 beachten.

Der FieldPort SWA50 erfordert keine Interaktionen während des Betriebes.

5.4 Update-Management

Im Bedarfsfall können Sie über die Endress+Hauser SmartBlue-App ein Firmware-Update für den FieldPort SWA50 duchführen. Der DIP-Schalter 2 mit der Funktion "Firmware-Update" muss auf ON stehen. In der Position OFF ist die Funktion deaktiviert.

Weitere Informationen zu "DIP-Schalter" und "Update": Betriebsanleitung BA01987S (Bluetooth) oder Kurzanleitung KA01436S (WirelessHART) → 🖹 6

5.5 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.

5.6 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 Passwort auf das werksseitig eingestellte Passwort zurückzusetzen. Das Initialpasswort ist auf dem Typenschild und auf dem mitgelieferten Blatt "Zugangsdaten Bluetooth" angegeben. ▪ Weitere Informationen Bluetooth: Betriebsanleitung BA01987S (Bluetooth) und Zugangsdaten Bluetooth → 🖹 6 ▪ Weitere Informationen WirelessHART: Kurzanleitung KA01436S und Betriebsanleitung BA02046S → 🖹 6
Das Produkt hat eine Störung und Sie können die Störung nicht beheben.	▶ Endress+Hauser kontaktieren. ↳ Endress+Hauser fordert Sie entweder auf, das Produkt zu Endress+Hauser zu senden oder das Produkt zu entsorgen.
Das Produkt ist defekt und muss daher entsorgt werden.	Wir empfehlen vor der Entsorgung oder Verschrottung des FieldPort SWA50 gemäß folgender Richtlinie vorzugehen: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization
Das Produkt soll entsorgt werden.	Wir empfehlen vor der Entsorgung oder Verschrottung des FieldPort SWA50 gemäß folgender Richtlinie vorzugehen: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

7 Anhang

7.1 Security-Checkliste für den Produktlebenszyklus

Lebenszyklus	Tätigkeit	Geprüft
Planung	Typische Einsatzumgebung des Produkts definiert und bei der Planung berücksichtigt. → 🖹 11 Falls erforderlich, Ersatzmaßnahmen berücksichtigt. → 🖹 11	❑
	Planungsarbeiten in der Engineering-Phase beachtet. Bedrohungsanalyse und Risikobeurteilung durchgeführt.→ 🖹 11	❑
	Sofern möglich, risikiomindernde Maßnahmen berücksichtigt. → 🖹 12	❑
Wareneingang / Transport	Geprüft, dass die Verpackung ungeöffnet ist und dass das Siegel unbeschädigt ist.	❑
Inbetriebnahme	Produkt für den Anwendungsfall gehärtet. → 🖹 14	❑
Betrieb	Vorgaben zum Update-Management beachtet. → 🖹 16	❑
	Planung der wiederkehrenden Bedrohungsanalyse vorgenommen. → 🖹 16	❑
Außerbetriebnahme	Produkt außer Betrieb genommen. → 🖹 17	❑

7.2 Versionshistorie

Dokumentenversion	Firmwareversion	Hardwareversion	Änderungen
01.21	ab 01.00.xx	Dev. Rev. 0	Erste Version

www.addresses.endress.com

Endress+Hauser

People for Process Automation