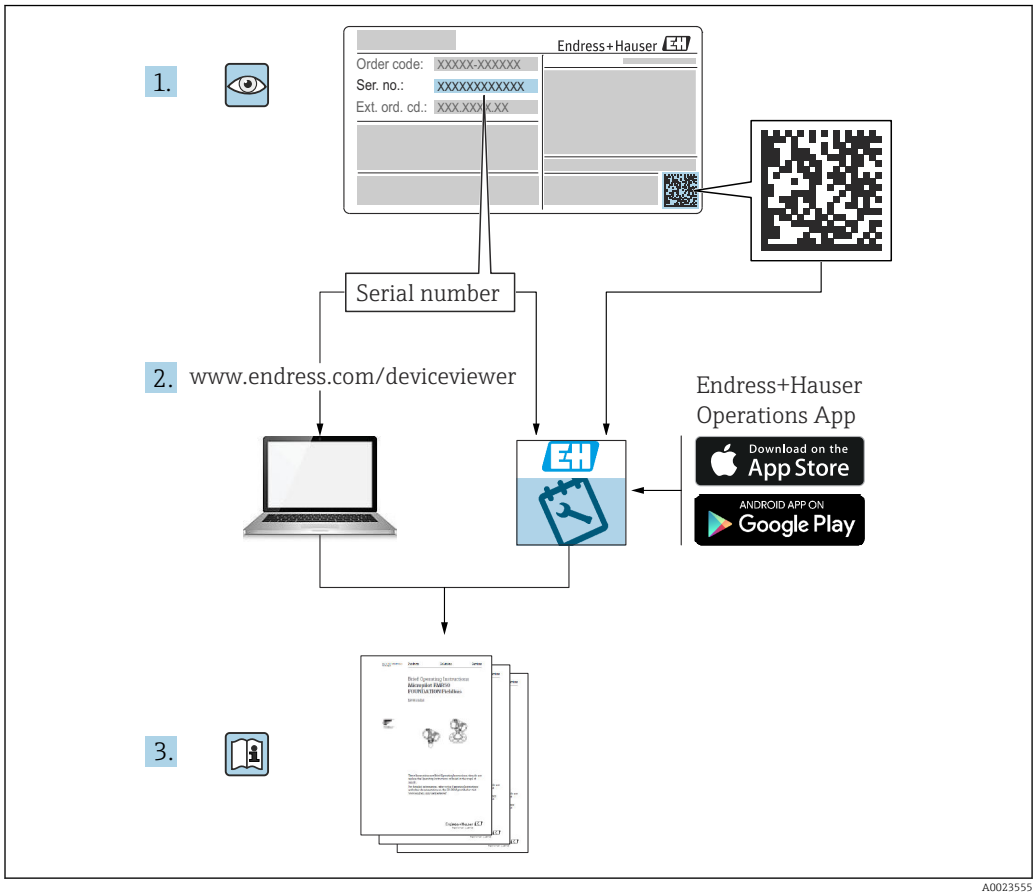
SD03405S/04/DE/01.25-00
71704721
2025-05-30

Sonderdokumentation
Security-Handbuch Field Xpert

Universeller, leistungsstarker Tablet PC zur Gerätekonfiguration

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 8
3.2.1 Allgemeine Informationen 8
3.2.2 Systemaufbau und Systemgrenzen 9
3.2.3 Kommunikation und Datenverarbeitung 9
3.2.4 Betriebssystem 10
3.3 Security-Level festlegen 10
3.4 Typische Einsatzumgebung des Produkts 10
3.5 Maßnahmen, falls erforderliche Einsatzumgebung nicht erfüllbar ist 11
3.6 Bedrohungsanalyse und Risikobeurteilung durchführen 11
3.7 Empfehlung für risikomindernde Maßnahmen 11
3.7.1 Gesamtsystem betrachten 11
3.7.2 Anwender schulen 12
3.7.3 Zugriffsmanagement optimieren 12
3.7.4 Gerätedaten und Gerätestatus überwachen 13
3.7.5 Produkt-Software updaten 13
3.7.6 Anwendungen und Apps schützen . . . 14

4 Inbetriebnahme (Installation und Konfiguration) 15
4.1 Zielgruppe 15
4.2 Anforderungen an das Personal 15
4.3 Installation 15
4.4 Konfiguration 15
4.4.1 Erforderliche Security-Schritte während der Inbetriebnahme 15
4.4.2 Firewall konfigurieren 15
4.4.3 Produkt härten 16
4.4.4 Anwenderdaten konfigurieren 16
4.4.5 Security-relevante Einstellungen des Produkts 16

5 Betrieb 18
5.1 Zielgruppe 18
5.2 Anforderungen an das Personal 18
5.3 Aufgaben während des Betriebes 18
5.3.1 Allgemeine Empfehlungen 18
5.3.2 Daten exportieren und drucken 18
5.3.3 Gerätedaten exportieren und laden . . 18
5.4 Security-Aspekte während des Betriebes 19
5.5 Update-Management 19
5.5.1 Betriebssystem 19
5.5.2 Field Xpert Software 19
5.6 Wiederholung der Bedrohungsanalyse 19
5.7 Reparatur und Entsorgung 20

6 Außerbetriebnahme 21
6.1 Zielgruppe 21
6.2 Anforderungen an das Personal 21
6.3 Produkt außer Betrieb nehmen 21

7 Anhang 22
7.1 Security-Checkliste für den Produktlebenszyklus 22
7.2 Versionshistorie 22

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 Field Xpert

Field Xpert SMT50
- Technische Information TI01555S
- Betriebsanleitung BA02053S
- Herstellerinformation MI01495S

Field Xpert SMT70
- Technische Information TI01342S
- Betriebsanleitung BA01709S
- Herstellerinformation MI01422S

Field Xpert SMT70B
- Technische Information TI01814S
- Betriebsanleitung BA02390S
- Herstellerinformation MI01514S

Field Xpert SMT77
- Technische Information TI01418S
- Betriebsanleitung BA01923S
- Herstellerinformation MI01440S

Netilion
- 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

Der Tablet PC Field Xpert für die universelle Gerätekonfiguration unterstützt diverse Protokolle, die Endress+Hauser Serviceprotokolle und die Verbindung zu Endress+Hauser Bluetooth-Feldgeräten und Endress+Hauser WLAN-Feldgeräte. Die Feldgeräte können Sie direkt über ein geeignetes Interface wie z. B. einem Modem (Punkt-zu-Punkt), über ein Bussystem (Punkt-zu-Bus) oder kabellos (WLAN / Bluetooth) verbinden.

Die Field Xpert Software zeichnet sich durch einfache, schnelle und intuitive Bedienung aus.

In der Field Xpert Gerätebibliothek sind bereits mehrere Tausend Geräte- und Kommunikationstreiber vorinstalliert. Damit sind nahezu alle HART- und FOUNDATION Fieldbus-Geräte bedienbar (Field-Comm Group-Bibliotheken). Des Weiteren sind alle Endress+Hauser Feldgerätetreiber installiert. Der Generic HART DTM und die PROFIBUS Profil DTMs erlauben zusätzlich die Bedienung aller wichtigen Grundfunktionalitäten der jeweiligen Feldgeräte.

Zusätzlich ist der Tablet PC mit dem FDI Package Manager für die Installation von FDI Packages und mit dem IODD DTM Configurator für die Installation von IODDs ausgestattet. Sie können jederzeit neue Gerätetreiber (DTMs, FDI Packages und IODDs) auf den Tablet PC installieren.

Die Verbindung von dem Tablet PC zu den Feldgeräten entfolgt entweder über eine Schnittstelle, ein Modem, ein Gateway, über WLAN oder Bluetooth.

Optional können Sie den Tablet PC direkt an die Endress+Hauser Netilion Cloud anmelden. Von dem Tablet PC können Sie Daten wie z.B. Parameterdatensätze hochladen

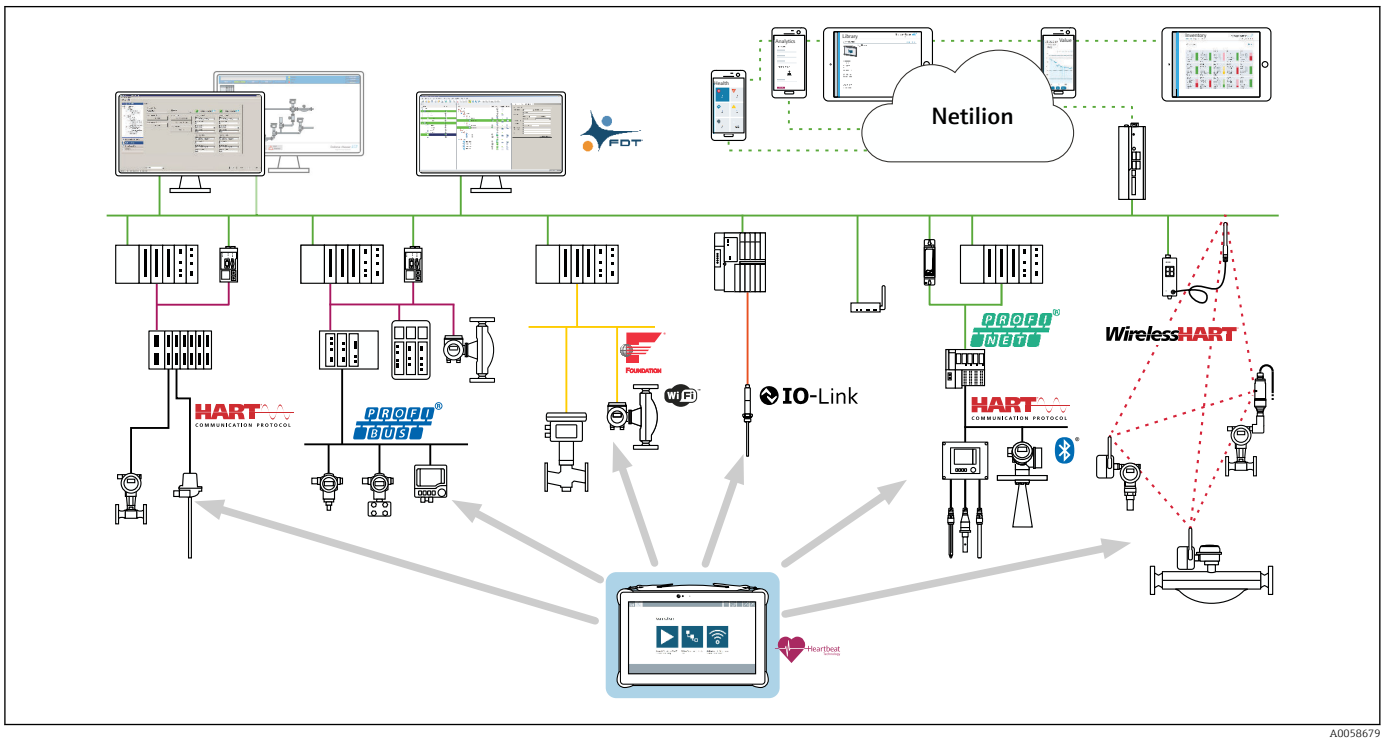
In prozesstechnischen Anlagen ist das Leitsystem für die Steuerung der Anlage und für die Prozessüberwachung verantwortlich. Der Tablet PC Field Xpert dient nur dazu – auch während des laufenden Betriebes – einzelne Feldgeräte in Betrieb zu nehmen und zu konfigurieren.

Unterstützte Feldgeräte und Protokolle
Endress+Hauser Feldgeräte und 3rd-Party-Feldgeräte
- HART
- PROFIBUS DP/PA
- PROFINET
- FOUNDATION Fieldbus
- Modbus
- IO-Link
- Bluetooth: Endress+Hauser Feldgeräte mit Bluetooth-Funktion
- WLAN: Endress+Hauser WLAN-Feldgeräte

Unterstützte Endress+Hauser Serviceprotokolle
- CDI
- IPC
- ISS
- PCP

3.2.2 Systemaufbau und Systemgrenzen

In diesem Security-Handbuch wird der Tablet PC Field Xpert, die Field Xpert Software inklusive der Field Xpert Hilfsprogramme, die vorinstallierten Treiber sowie das Betriebssystems des Tablet PC betrachtet. Die mit dem Tablet PC angeschlossenen bzw. verbundenen Geräte wie Feldgeräte, Gateways usw. werden in in diesem Security-Handbuch **nicht** betrachtet. In der folgenden Abbildung ist die Systemgrenze blau markiert.



A0058679

1 *Einsatzmöglichkeiten Field Xpert, hier SMT70 / SMT70B dargestellt (blaue Markierung zeigt die Systemgrenzen für dieses Handbuch)*

3.2.3 Kommunikation und Datenverarbeitung

Abhängig von der Variante des Tablet PCs Field Xpert ist der Tablet PC mit folgenden Anschlüssen und Funktionen für die Kommunikation und Datenverarbeitung ausgestattet.

Detaillierte Informationen: Technische Information SMTxx → 6

Field Xpert SMT50
- Anschlüsse wie Video und Serial Ports
- Erweiterungssteckplätze
- USB
- Wireless LAN
- Bluetooth
- Wireless WAN + GPS

Field Xpert SMT70
- Anschlüsse wie Kofphörerausgang und Mikrofoneingang
- Erweiterungssteckplätze
- USB
- Wireless LAN
- Bluetooth
- Wireless WAN + GPS

Field Xpert SMT70B
- I/O-Ports
- USB
- Wireless LAN
- Bluetooth
- Wireless WAN
- GPS-Sensor

Field Xpert SMT77
- Anschlüsse wie MicroSD-Kartenspeicherplatz
- Anschluss an Docking-Station
- Erweiterungssteckplatz für HART Add-On-Modul
- USB
- Wireless LAN
- Bluetooth
- Abhängig von der Variante, entweder "Wireless LAN" oder "Wireless WAN + GPS"

3.2.4 Betriebssystem

Auf dem Tablet PC Field Xpert läuft ein Betriebssystem von Microsoft Windows. Die Aktualisierung des Betriebssystem liegt in der Verantwortung des Betreibers.

Detaillierte Informationen: Technische Information SMTxx → 6

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, beispielsweise Ethernet-basierte Schnittstellen und / oder drahtlose Schnittstellen wie WLAN oder Bluetooth. Schnittstellen: Siehe Kapitel "Systemüberblick".
- Das Produkt wird in einer industriellen Umgebung betrieben.
- Der Zugang zum Produkt ist reglementiert. Nur autorisierte Personen haben Zugang zum Produkt.
- Das Personal ist in dem Gebrauch des Produkts und in die Security-Risiken unterwiesen.
- Das Produkt verfügt optional über eine durch HTTPS geschützte Datenverbindung, die den Produktionsbereich z.B. für Updates und die Netilion Cloud verlässt.
  Die Sicherheit aller verwendeten Netzwerkkomponenten wird durch den Betreiber sichergestellt.
- Das Automatisierungsnetz ist über einen Perimeterschutz gegen Angriffe von außen wie z.B. einen Denial-of-Service-Angriff geschützt.

- 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.
- 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.

3.5 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 das Risiko eines nichtautorisierten Fremdzugriffs zu minimieren, sollte der Tablet PC Field Xpert das Werksgelände nicht verlassen.

Besteht der Verdacht eines unautorisierten Zugriffs, führen Sie folgende Punkte durch:
- Checksumme mit einer Referenzinstallation vergleichen.
- Auslieferungszustand des Tablet PC Field Xpert mittels der Recovery-Partition wiederherstellen.

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 Tablet PC Field Xpert dient zum Einsatz in einem Produktionssystem zur Inbetriebnahme und Konfiguration von einzelnen Feldgeräten. Bei Bedarf kann der Tablet PC

zusätzlich an das IIoT-Ökosystem Netilion Cloud von Endress+Hauser angemeldet werden und dort Daten abspeichern.

Systeme – wie Produktionssysteme und / oder IIoT-Ökosysteme – können aufgrund ihrer dezentralen Modularität schnell zu einem Stückwerk aus verschiedenen Komponenten 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 der Tablet PC Field Xpert von Endress+Hauser betrachtet. Für das Gesamtsystem sind zusätzliche Analysen erforderlich.

- Produkt härten: → 16
- Update-Management: → 19

Netzwerk

Beachten Sie besonders die eingesetzten Netzwerkkomponenten wie z.B. Router und Switches.

Die Integrität der Komponenten sowie der Zugriff auf das Netzwerk muss vom Betreiber sichergestellt oder eingeschränkt werden.

Treiber

Für die Konfiguration von Feldgeräten mittels der Field Xpert Software werden Gerätetreiber wie z.B. DTMs verwendet. Die Gerätetreiber dürfen nur aus vertrauenswürdigen Quellen stammen, und die Herkunft muss vor der Installation über digitale Signaturen validiert werden.

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

In der Field Xpert Software ist kein explizites Benutzermanagement implimentiert. Der Zugriff auf Netilion und das Software License Management von Endress+Hauser sind passwortgeschützt.

Beachten Sie, dass jeder Anwender, der sich über das Windows Login auf dem Field Xpert anmelden kann, potenziell den vollständigen Funktionsumfang von der Field Xpert Software verwenden kann.

Wir empfehlen, für den Zugriff auf das Betriebssystem (Windows) die gleichen Regeln für das Identitäts- und Zugriffsmanagement wie für die anderen Unternehmensbereiche anzusetzen. Zum Beispiel:
- 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
- Für verschiedene Dienste verschiedene Passwörter verwenden
- Automatisches Sperren, wenn das System nicht mehr verwendet wird

Wir empfehlen, den Tablet PC nur für die Field Xpert Software und den zugehörigen Hilfsprogrammen zu verwenden.

Nur autorisierte und geschulte Anwender sollten mit dem Tablet PC arbeiten. Über den Tablet PC haben die Anwender Zugriff auf die Konfigurationen und die Daten des Tablet PCs sowie auf die Feldgeräte.

3.7.4 Gerätedaten und Gerätestatus überwachen

Viele Angriffe auf ein Produkt in einem System erzeugen Anomalien im Netzwerkverkehr. 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 und des Netzwerks überwacht und bei Abweichungen informiert.

Der Tablet PC Field Xpert ist ein Gerät mit Software in einem Produktionssystem. Die Erkennung von Anomalien ist eine Aufgabe des übergeordneten Systems.

Überwachung der Feldbusse

Der Tablet PC Field Xpert kann über verschiedene Protokolle an ein Leitsystem angebunden werden. Die Kommunikation mit den Feldgeräten erfolgt heutzutage unverschlüsselt. Der physikalische Schutz sowie die Erkennung und Behebung von Anomalien ist Aufgabe des Betreibers des Leitsystems.

3.7.5 Produkt-Software updaten

Aufgrund der Dynamik in der IT, wachsenden Anforderungen in der Vernetzung und dem Einsatz von Softwarebibliotheken sind 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.

Bei bestehender Internetverbindung prüft die Field Xpert Software selbstständig auf verfügbare Updates und weist darauf hin.

Besteht keine Internetverbindung, können Sie die Updates über das Endress+Hauser Software Portal herunterladen: https://software-products.endress.com/

Update-Management: → 19

Treiber

Wenn Sie die Field Xpert Software starten und der Tablet PC mit dem Internet verbunden ist, sucht die Software automatisch nach neuen DTMs. Neue DTMs werden auf den Tablet PC heruntergeladen und automatisch installiert.

FDI Packages müssen Sie manuell herunterladen und über den FDI Package Manager auf den Tablet PC installieren.

IODDs müssen Sie manuell herunterladen und über den IODD DTM Configurator auf den Tablet PC installieren.

Alle Gerätetreiber und Kommunikationstreiber können Sie über Endress+Hauser Software Portal herunterladen: https://software-products.endress.com/

Betriebssystem

Auf dem Tablet PC Field Xpert läuft ein Betriebssystem von Microsoft Windows. Die Aktualisierung des Betriebssystem liegt in der Verantwortung des Betreibers.

Detaillierte Informationen: Technische Information SMTxx → 6

3.7.6 Anwendungen und Apps schützen

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

Zur Sicherung der Anwendungen sollte auch der Schutz der mobilen und stationären Endgeräte gewährleistet sein, die auf den Tablet PC Field Xpert Zugriff haben. Dieses beinhaltet regelmäßiges Installieren von Betriebssystemupdates und Anwendungsupdates sowie der Einsatz eines Virenscanners.

Zum Schutz des Kundensystems und der Kundendaten sollte auch der Schutz der Zugangsdaten der Endgeräte gewährleistet sein. Zugangsdaten und Zertifikate müssen 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 installieren.

4.4 Konfiguration

4.4.1 Erforderliche Security-Schritte während der Inbetriebnahme

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

Detaillierte Informationen: Dokumentation SMTxx: → 6

Beachten Sie während der Inbetriebnahme hinsichtlich der Security folgenden Punkt:
- Produkt gemäß den definierten Anforderungen an die Einsatzumgebung integrieren → 10.
- Betriebssystem auf aktuellen Stand halten.
- Booten von einem externen physischen Medium deaktivieren.
- BIOS-Einstellungen mit einem Kennwort sichern.
- Für den Betrieb nicht erforderliche USB-Anschlüsse deaktivieren.
- Wenn für den Betrieb nicht erforderlich, Bluetooth und WLAN deaktivieren.
- Wenn für den Betrieb nicht erforderlich, optionales WWAN deaktivieren.
- Nach der Inbetriebnahme das Admin-Passwort ändern.
- Die interne Festplatte mit Bitlocker, dem Verschlüsselungsverfahren von Microsoft, verschlüsseln. Neuere Versionen der Field Xpert Software sind bereits bei Auslieferung verschlüsselt.

4.4.2 Firewall konfigurieren

Der Tablet PC Field Xpert verfügt über eine Windows-Firewall.

Die Windows-Firewall kann merklich dabei helfen, eine "First Line of Defense" (erste Verteidigungslinie) aufzubauen oder im LAN als "Defense in Depth" (Sicherheit in der Tiefe) zu funktionieren.

Das Deaktivieren der Windows-Firewall erhöht die Angriffsfläche auf die Software, die auf dem Tablet PC Field Xpert installiert ist.

Jeder infizierte PC oder mobiles Endgerät mit Zugriff auf das Unternehmens-Intranet, kann eine Verbindung zu einem ungeschützten Server herstellen und durch Nutzung einer Schwachstelle in einem Windows-Dienst oder in einer Drittanbieter-Anwendung den Server gefährden.

Zusätzlich kann die Windows-Firewall Denial-of-Service-Angriffe abwehren. Bei einem Denial-of-Service-Angriff wird ein Windows-PC mit Netzwerkverkehr bombardiert und dadurch entweder zum Absturz gebracht oder für das restliche Netzwerk unzugänglich gemacht.

Wir empfehlen die Windows-Firewall einzuschalten, indem Sie die Einstellung für private Netzwerke und öffentliche Netzwerke wie folgt festlegen:
- Status Windows-Firewall: Ein
- Eingehende Verbindungen: Blockieren
- Ausgehende Verbindungen: Zulassen

Die Field Xpert Software benötigt im normalen Betrieb keine Einträge in der Windows-Firewall.

Für den Betrieb bestimmter Grätetreiber kann es allerdings sein, dass Sie von der Field Xpert Software zum Freigeben von Ports in der Windows-Firewall aufgefordert werden.

4.4.3 Produkt härten

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

Treiber

Wir empfehlen nicht genutzte Treiber zu deinstallieren, um die Angriffsfläche zu verringern.

4.4.4 Anwenderdaten konfigurieren

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

Benutzer-Accounts gemäß Windows-Dokumentation anlegen, ändern und löschen.

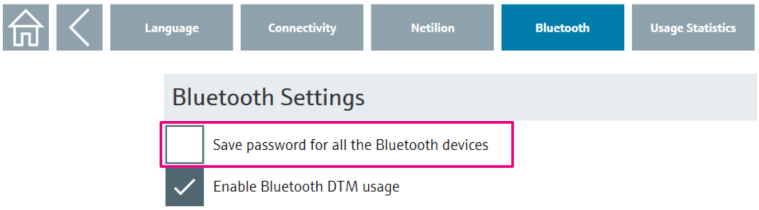
4.4.5 Security-relevante Einstellungen des Produkts

Bluetooth-Einstellungen

Sie können Passwörter für Bluetooth-Feldgeräte auf dem Tablet PC speichern, damit diese automatisch bei der nächsten Verbindung genutzt werden. Falls Sie diese Funktion **nicht** wünschen, müssen Sie die Option **Save Password for all the Bluetooth devices** deaktivieren.

1. In der Kopfzeile der Startseite auf das Symbol tippen.
   ↳ Die Seite "DTM Catalog" wird angezeigt.
2. Auf den Reiter **Settings** tippen.
   ↳ Die Seite "Language" wird angezeigt.

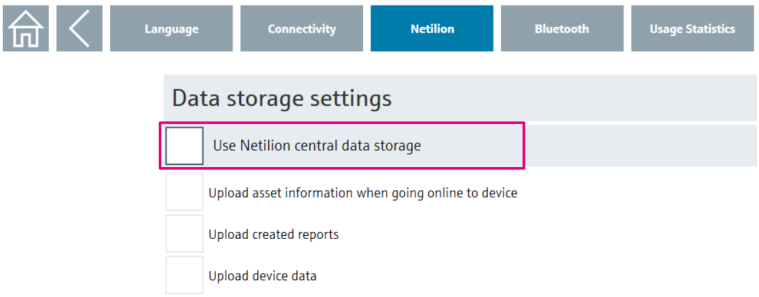
3. Auf den Reiter **Bluetooth** tippen.
   ↳ Die Einstellungen für Bluetooth werden angezeigt.



Netilion-Einstellungen

Sie können Gerätedaten und Geräteberichte auf dem Tablet PC speichern, um diese zu einem späteren Zeitpunkt in die Netilion-Cloud hochzuladen. Falls Sie diese Funktion **nicht** wünschen, müssen Sie die Option **Use Netilion central data storage** deaktivieren.

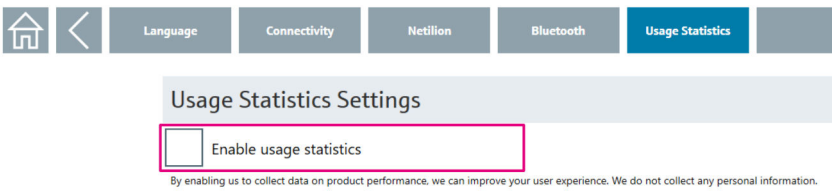
1. In der Kopfzeile der Startseite auf das Symbol tippen.
   ↳ Die Seite "DTM Catalog" wird angezeigt.
2. Auf den Reiter **Settings** tippen.
   ↳ Die Seite "Language" wird angezeigt.
3. Auf den Reiter **Netilion** tippen.
   ↳ Die Einstellungen für die Datenspeicher werden angezeigt.



Nutzungsstatistik-Einstellungen

Standardmäßig werden zur Produktverbesserung, Daten über die Nutzung gesammelt. Wenn Sie wünschen, dass keine Daten gesammelt werden, müssen Sie die Option **Enable usage statistics** deaktivieren.

1. In der Kopfzeile der Startseite auf das Symbol tippen.
   ↳ Die Seite "DTM Catalog" wird angezeigt.
2. Auf den Reiter **Settings** tippen.
   ↳ Die Seite "Language" wird angezeigt.
3. Auf den Reiter **Usage Statistics** tippen.
   ↳ Die Einstellungen für die Nutzungsstatistik werden angezeigt.



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 die folgenden Kapitel beachten.

5.3.1 Allgemeine Empfehlungen

- Passwörter nur unbeobachtet eingeben.
- Wenn ein Passwort nicht mehr vertrauenswürdig ist, zugehöriges Benutzerkonto sofort sperren und Passwort ändern.
- Wenn der Tablet PC nicht genutzt wird, den Tablet PC sperren und wegschließen oder mittels Sicherheitskabel vor Diebstahl schützen, um einen unbefugten Zugriff auf das Produkt auszuschließen.

5.3.2 Daten exportieren und drucken

Über die Field Xpert Software können Sie Konfigurationen von Feldgeräten exportieren und drucken.

Da durch die Field Xpert Software diese Daten nicht verschlüsselt und nicht geschützt sind, ist es die Aufgabe des Betriebspersonals diese Daten vertraulich zu behandeln und zu schützen.

5.3.3 Gerätedaten exportieren und laden

Die Field Xpert Software stellt für den Export und Import von Dateien folgende Dateiformate zur Verfügung: *.dcdtm, *.deh, *.curves, *.crv oder *.csv.

Die Field Xpert Software exportiert die Daten ungeschützt. Da die exportierten Dateien modifiziert werden können, ist es Aufgabe des Betriebspersonals die Dateien gegen Modifikationen zu schützen.

Die Field Xpert Software führt beim Import von Dateien keine Validierung durch. Es ist Aufgabe des Betriebspersonals, darauf zu achten, nur Dateien aus vertrauenswürdigen Quellen zu importieren.

5.4 Security-Aspekte während des Betriebes

Folgende Aufgaben während des Betriebes regelmäßig durchführen:
- Windows-Updates
- Updates der Field Xpert Software
- Updates der Gerätetreiber wie z.B. FDT/DTM und FDI Packages

5.5 Update-Management

5.5.1 Betriebssystem

Das Betriebssystem des Tablet PC Field Xpert wird automatisch durch Microsoft-Update-Routinen aktualisiert. Die Aktualisierung des Betriebssystem liegt in der Verantwortung des Betreibers, d.h. z.B. die Updates müssen zugelassen werden und der Tablet PC muss in regelmäßig mit dem Internet verbunden werden.

5.5.2 Field Xpert Software

Das Update-Management für die Field Xpert Software umfasst folgende Varianten:
- Automatisiert durch Endress+Hauser
- Manuell durch den Anwender

Die Updates werden bereitgestellt für:
- Security-Patches
- Fehlerbehebungen
- Neue Funktionen

Update-Management automatisiert durch Endress+Hauser

Endress+Hauser stellt die Updates für die Field Xpert Software auf den Endress+Hauser S3 Server bereit. Danach werden die Updates automatisiert im Hintergrund auf den Tablet PC Field Xpert geladen. Ein manueller Eingriff ist nicht erforderlich.

Der Zeitpunkt der Updates wird durch Endress+Hauser oder den Anwender festgelegt.

Endress+Hauser stellt die Integrität und Authentizität der Updates sicher. Eine Überprüfung der Integrität der Updates durch das nutzende Unternehmen ist nicht erforderlich.

Update-Management manuell durch den Anwender / Betreiber

Sollte eine Internetverbindung nicht möglich sein, können Sie Updates auch manuell beziehen und installieren → 13.

Updates werden im Endress+Hauser Software-Portal veröffentlicht:
https://software-products.endress.com/

Der Zeitpunkt der Updates wird durch den Anwender festegelegt.

Endress+Hauser stellt durch Prüfsummen und Signaturen in der Software die Integrität und Authentizität der Updates sicher. Die Person, die das Update durchführt, muss eine Integritäts- und Authentizitätsprüfung durchführen.

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.	1. Alle Programme auf dem Tablet PC schließen. 2. Windows herunterfahren.
Das Produkt hat eine Störung und Sie können die Störung nicht beheben.	Endress+Hauser Service kontaktieren.
Das Produkt soll entsorgt werden.	Wir empfehlen vor der Entsorgung oder Verschrottung der physikalischen Medien, auf denen das Produkt installiert war, gemäß folgender Richtlinie vorzugehen: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization Intelligente Geräte können Credentials enthalten, die es dem Gerät ermöglichen innerhalb der Produktionsanlage zu kommunizieren oder auf bestimmte Dienste zuzugreifen. Credentials sind Zugangsdaten (Login-Daten) wie z.B. Namen, Passwörter und digitale Zertifikate. Bei der Entsorgung darauf achten, dass der Datenträger vollständig und sicher gelöscht ist und somit eine Datenwiederherstellung ausgeschlossen ist. Alternativ Datenträger physisch zerstören.

7 Anhang

7.1 Security-Checkliste für den Produktlebenszyklus

Lebenszyklus	Tätigkeit	Geprüft
Planung	Typische Einsatzumgebung des Produkts definiert und bei der Planung berücksichtigt. → 🖹 10 Falls erforderlich, Ersatzmaßnahmen berücksichtigt. → 🖹 11	❑
	Planungsarbeiten in der Engineering-Phase beachtet. Bedrohungsanalyse und Risikobeurteilung durchgeführt.→ 🖹 11	❑
	Sofern möglich, risikiomindernde Maßnahmen berücksichtigt. → 🖹 11	❑
Wareneingang / Transport	Bei der Warenannahme geprüft, dass die Verpackung unbeschädigt ist.	❑
Inbetriebnahme	Produkt für den Anwendungsfall gehärtet. → 🖹 16	❑
Betrieb	Vorgaben zum Betrieb beachtet. → 🖹 18	❑
	Vorgaben zum Update-Management beachtet. → 🖹 19	❑
	Planung der wiederkehrenden Bedrohungsanalyse vorgenommen. → 🖹 19	❑
Außerbetriebnahme	Produkt außer Betrieb genommen. → 🖹 21	❑

7.2 Versionshistorie

Dokumentenversion	Softwareversion	Änderungen
01.25	ab 1.08.10	Erste Version

www.addresses.endress.com

Endress+Hauser

People for Process Automation