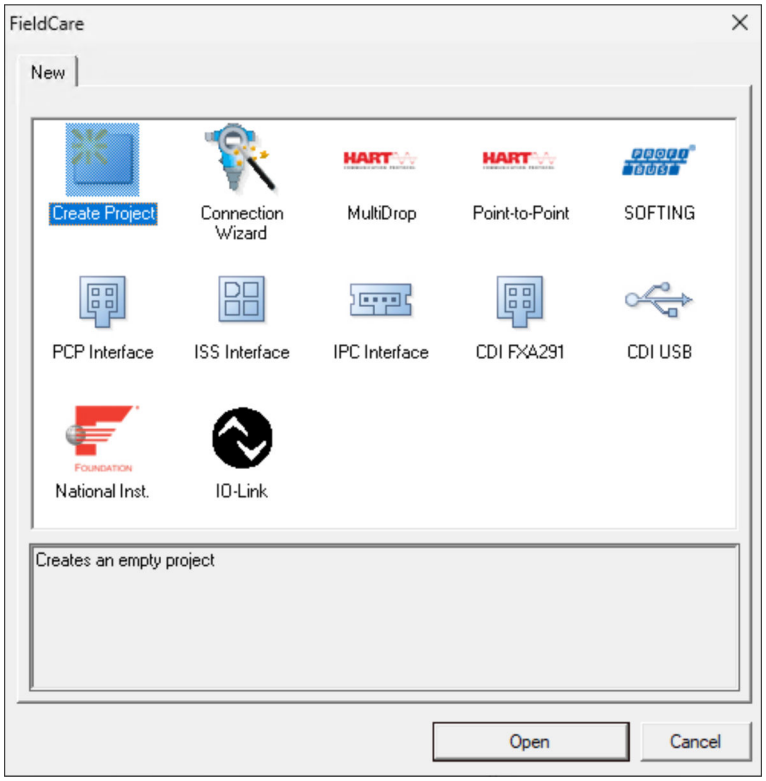
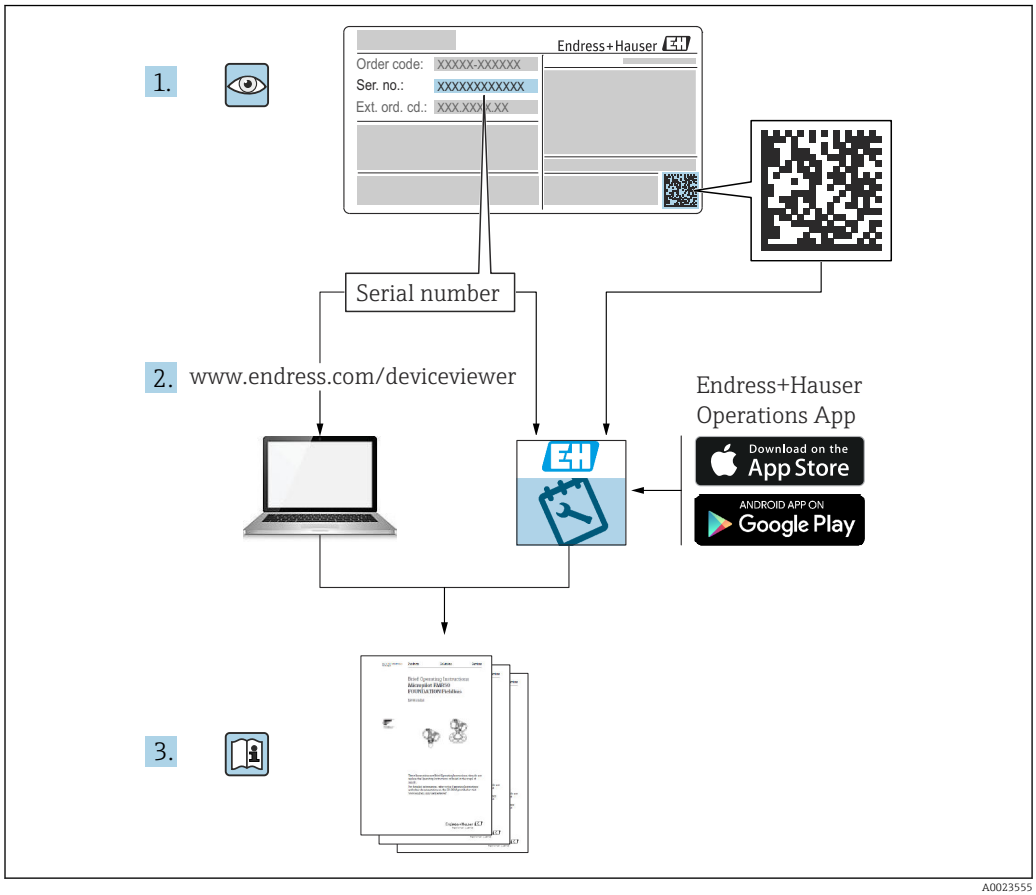
SD03193S/04/DE/01.23-00
71637580
2023-12-15

Sonderdokumentation
Security-Handbuch FieldCare SFE500

Universelles Feldgeräte-Konfigurationstool für HART, PROFIBUS, FOUNDATION Fieldbus, Modbus, IO-Link, EtherNet/IP, PROFINET und PROFINET APL



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:
- *Device Viewer*: Seriennummer vom Typenschild eingeben
  www.endress.com/deviceviewer
- Downloadbereich der Endress+Hauser Internetseite
  www.endress.com/downloads

Mitgeltende Dokumente FieldCare SFE500

- Technische Information TI00028S
- Betriebsanleitung BA00065S

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

FieldCare ist ein Tool für die universelle Gerätekonfiguration, das diverse Protokolle sowie die Endress+Hauser Serviceprotokolle unterstützt.

Die Feldgeräte können direkt über ein geeignetes Interface wie z.B. einem Modem (Punkt-zu-Punkt), über ein Bussystem (Punkt-zu-Bus) oder ein Netzwerk (LAN) verbunden werden. FieldCare zeichnet sich durch eine einfache, schnelle und intuitive Bedienung aus.

In die FieldCare Gerätebibliothek können Sie über 2700 Geräte- und Kommunikationstreiber installieren. Damit sind alle Endress+Hauser Feldgeräte und fast alle HART- und FOUNDATION Fieldbus-Geräte bedienbar (FieldComm Group-Bibliotheken).

Des Weiteren können Sie weitere Gerätetreiber (DTMs) nachinstallieren. Zusätzlich ermöglichen der Generic HART DTM und die PROFIBUS Profil DTMs die Bedienung aller wichtigen Grundfunktionen der jeweiligen Feldgeräte.

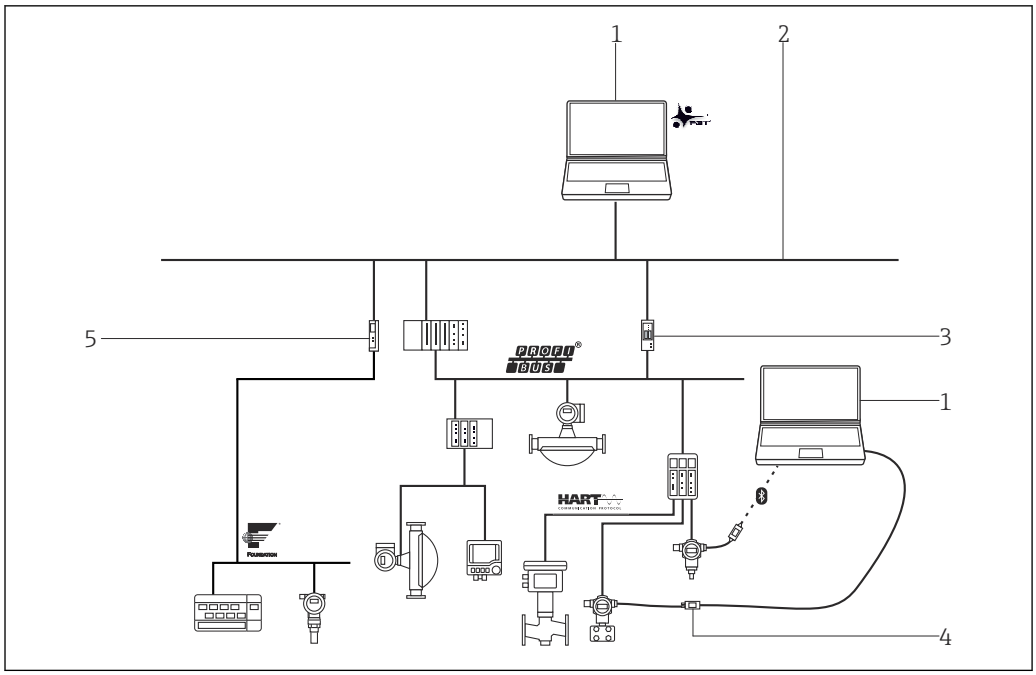
3.2.2 Systemaufbau und Systemgrenzen

Unterstützte Feldgeräte
- Alle Endress+Hauser Feldgeräte
- Fast alle Feldgeräte von Fremdherstellern

Unterstützte Protokolle
- HART
- PROFIBUS DP/PA
- FOUNDATION Fieldbus
- Modbus
- IO-Link
- PROFINET
- EtherNet/IP

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

Zusätzlich können Sie weitere FDT DTMs installieren und die Liste der unterstützten Feldgeräte und Protokolle erweitern.



1 Beispiel: Systemarchitektur mit FieldCare

1 FieldCare
2 Ethernet
3 Ethernet/PROFIBUS Gateway z.B. Fieldgate SFG500
4 Commubox FXA195
5 Ethernet/FOUNDATION Fieldbus Gateway

FieldCare SFE500 wird auf Microsoft Windows ausgeführt. Microsoft Windows wird in diesem Handbuch als Hostsystem bezeichnet und kann entweder nativ auf einem PC, Laptop oder in einer virtuellen Umgebung installiert sein.

Für die Anbindung der Feldgeräte stehen folgende Möglichkeiten zur Verfügung:
- über Modem
- über Gateway zwischen TCP/IP-Netzwerk und entsprechendem Feldbus
- über Gateway zwischen verschiedenen Feldbussen wie z.B. HART-over-PROFIBUS
- über eine drahtlose Übertragung wie z.B. WirelessHART

Neben FieldCare SFE500 läuft in der prozesstechnischen Anlage ein Leitsystem, das für die Steuerung der Anlage verantwortlich ist und zu diesem Zweck auf die Prozesswerte der Feldgeräte zugreifen muss.

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.
- Die Sicherheit der 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 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.

Um das Risiko eines nichtautorisierten Fremdzugriffs zu minimieren, sollte das Hostsystem auf dem FieldCare SFE500 installiert ist, das Werksgelände nicht verlassen.

Besteht der Verdacht eines unautorisierten Zugriffs, führen Sie folgende Punkte durch:
- Signaturen der FieldCare SFE500 Installation und die Signaturen der installierten DTMs prüfen. → 13
- Checksumme mit einer Referenzinstallation vergleichen.
- FieldCare SFE500 oder FieldCare-Projekte aus einem Backup wiederherstellen. → 19
- Die DTD-Datenbank aus einer vertrauenswürdigen Quelle neu aufsetzen.
  FieldCare SFE500 nutzt zum Ermitteln der Feldgerätestatus die DTDs (Device Type Descriptions) aus der Datenbank. Wenn ein Angreifer diese DTDs manipuliert hat, werden falsche Feldgerätestatus angezeigt. Diese Feldgerätestatus dürfen Sie nicht mehr als Entscheidungsgrundlage verwenden.

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

FieldCare SFE500 ist eine Anwendung, die in einem Produktionssystem eingesetzt wird.

Ein Produktionssystem kann schnell zu einem Stückwerk aus verschiedenen Endgeräten werden. Jedes abweichende Produkt stellt bei solchen heterogenen Gesamtlösungen eine neue Gefahrenquelle dar, das Brüche an den Schnittstellen erzeugt und zu unsicheren Übertragungswegen führen kann.

In diesem Handbuch wird FieldCare SFE500 von Endress+Hauser betrachtet. Für das Gesamtsystem sind zusätzliche Analysen erforderlich.

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.

Da in FieldCare SFE500 der Communication Server über den Communication Service unverschlüsselt kommuniziert, kann ein Angreifer einen vollständigen Zugriff auf Komponenten des Steuerungssystems wie z.B. Feldgeräte erlangen. Die Communication Server Schnittstelle (Communication Service) ist standardmäßig deaktiviert. → 17

DTMs

Für die Konfiguration von Feldgeräten über FieldCare SFE500 werden DTMs verwendet. Die DTMs dürfen nur aus vertrauenswürdigen Quellen stammen und die Herkunft muss vor der Installation über digitale Signaturen validiert werden.

Produkt härten: → 15

Update-Management: → 21

FDI Packages

Für die Konfiguration von Feldgeräten über FieldCare SFE500 werden FDI Packages verwendet. Die FDI Packages dürfen nur aus vertrauenswürdigen Quellen stammen. Die Person, die die FDI Packages installiert, muss die Herkunft vor der Installation über digitale Signaturen validieren.

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 FieldCare SFE500 ist ein Benutzermanagement implementiert. Damit ist in dem Bereich Zugriffsmanagement die Anforderung für den Security-Level SL1 erfüllt.

Dabei ist zu beachten, dass jeder Anwender, der auf das Hostsystem zugreifen kann, potenziell den vollständigen Funktionsumfang von FieldCare SFE500 verwenden kann.

Host- und Clientsystem

Wir empfehlen, für den Zugriff auf das Hostsystem 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 für das Hostsystem folgende Punkte:
- Hostsystem nur für FieldCare SFE500 verwenden
- Keine weiteren Anwendungen auf das Hostsystem installieren
- Nur autorisierte und geschulte Anwender dürfen auf dem Hostsystem arbeiten

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.

FieldCare SFE500 ist eine Software im Produktionssystem. Die Erkennung von Anomalien ist eine Aufgabe des übergeordneten Systems.

Überwachung der Feldbusse

FieldCare SFE500 ist über verschiedene Protokolle an das Steuerungssystem angebunden. Die Kommunikation mit den Feldgeräten erfolgt unverschlüsselt. Der physikalische Schutz sowie die Erkennung und Behebung von Anomalien ist Aufgabe des Betreibers des Steuerungssystems.

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 FieldCare SFE500 selbstständig auf verfügbare Updates und weist darauf hin.

Besteht keine Internetverbindung, können Sie Updates unter folgender Adresse herunterladen: https://software-products.endress.com/

Produkt härten: → 15

Update-Management: → 21

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 sollte auch der Schutz der mobilen und stationären Endgeräte gewährleistet sein, die auf FieldCare SFE500 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.

1. Festplatte verschlüsseln. → 13
2. Installationsdateien prüfen. → 13
3. Zugriff auf das Hostsystem einschränken. → 14
4. Für die Datenbank die aufgeführten Regeln befolgen. → 14

Festplatten verschlüsseln

Da FieldCare SFE500 Geräte- und Anlagedaten unverschlüsselt auf Festplatten speichert, empfehlen wir, die Festplatten des Hostsystems zu verschlüsseln.

Installationsdateien prüfen

Vor dem Ausführen des FieldCare SFE500 Setups muss der Anwender, der FieldCare installiert, eine Integritäts- und Authentizitätsprüfung der Installationsdateien durchführen. Die Installationsdateien sind dafür digital signiert.

Folgende Prüfung für jede Installationsdatei (*.exe) durchführen. Sollten Sie FieldCare SFE500 über den "Installation Manager" des FieldCare Packages installieren, vor dem Ausführen die Signatur der Datei "InstallationManager.exe" prüfen.

HINWEIS

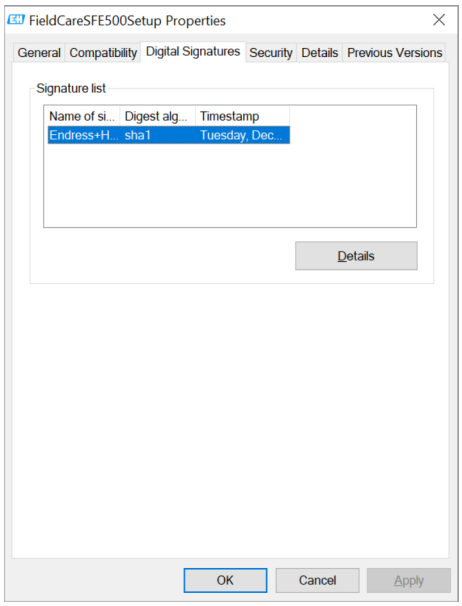
Falsche Installationsdateien

Installation von Schadsoftware

- Nur Installationsdateien ausführen, die für **Name of signer** den Eintrag **Endress+Hauser Process Solutions AG** enthalten.

Installationsdateien (*.exe) prüfen

1. Installationsdatei mit der Maus markieren.
2. Über das Kontextmenü die Eigenschaften für die Datei öffnen.



3. Reiter **Digital Signatures** wählen.
4. Prüfen, ob **Name of signer** den Eintrag **Endress+Hauser Process Solutions AG** enthält. Ist der Reiter **Digital Signatures** nicht vorhanden oder weicht der Eintrag für **Name of signer** ab, dürfen Sie die Installationsdatei **nicht** ausführen. Die Installationsdatei ist in diesem Fall nicht von Endress+Hauser und könnte Schadsoftware enthalten.

Zugriff auf Hostsystem einschränken

FieldCare SFE500 speichert die Daten standardmäßig in die lokale Microsoft SQL Server Installation. Die Daten beinhalten Projektinformation, statische und dynamische Gerätedaten wie z.B. Herstellerinformationen, Tags und Konfigurationsdaten sowie Informationen über die Anlagenstruktur, historische Gerätestatus und Benutzeranmeldeinformationen.

Diese Daten werden unverschlüsselt gespeichert. Jeder Anwender, der Zugang zu dem Hostsystem hat, kann diese Daten einsehen und modifizieren.

Regeln für die Datenbank befolgen

Da nach einer Neuinstallation von FieldCare SFE500 und Microsoft SQL Server die Datenbank nur lokal zur Verfügung steht, kann nur der lokale Anwender auf die Daten auf dem Hostsystem zugreifen.

Wir raten davon ab, die Datenbank per TCP/UDP im Netzwerk verfügbar zu machen. Steht die Datenbank per TCP/UDP im Netzwerk zur Verfügung, kann ein Angreifer auf die Daten von FieldCare SFE500 zugreifen und diese modifizieren.

4.4.2 Firewall konfigurieren

Windows verfügt über eine 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 von Windows.

Jeder infizierte PC 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

FieldCare SFE500 benötigt im normalen Betrieb keine Einträge in der Windows-Firewall.

Für den Betrieb bestimmter DTMs kann es allerdings sein, dass Sie von der FieldCare SFE500 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 freigeschaltet werden, die für den ordentlichen Betrieb des Produkts für den vorliegenden Anwendungsfall erforderlich sind.

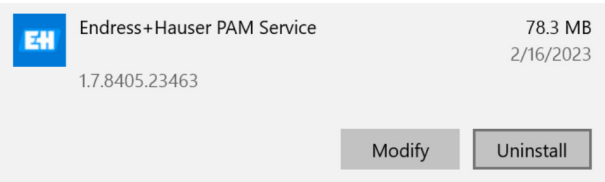
DTMs

Wir empfehlen für die DTMs folgende Maßnahmen:
- DTMs nur aus vertrauenswürdigen Quellen installieren. Vor der Installation die digitale Signatur prüfen. → 13
- Nicht genutzte DTMs deinstallieren, um die Angriffsfläche zu verringern.

Mit FieldCare SFE500 wird der PAM Service installiert, der mit Adminrechten ausgeführt wird. Unter bestimmten Umständen lädt dieser Service-DTMs und führt diese mit erhöhten Rechten aus.

Sie können den PAM Service deinstallieren, wenn folgende Punkte zutreffen:
- Sie suchen regelmäßig manuell nach Produktupdates und installieren diese Updates manuell → 21
- Der Device Agent von FieldCare SFE500 wird **nicht** als Configuration Client für die Asset Health Monitoring Solution SAH70 eingesetzt.

▶ In den Windows Einstellungen den Dienst **PAM Service** deinstallieren.

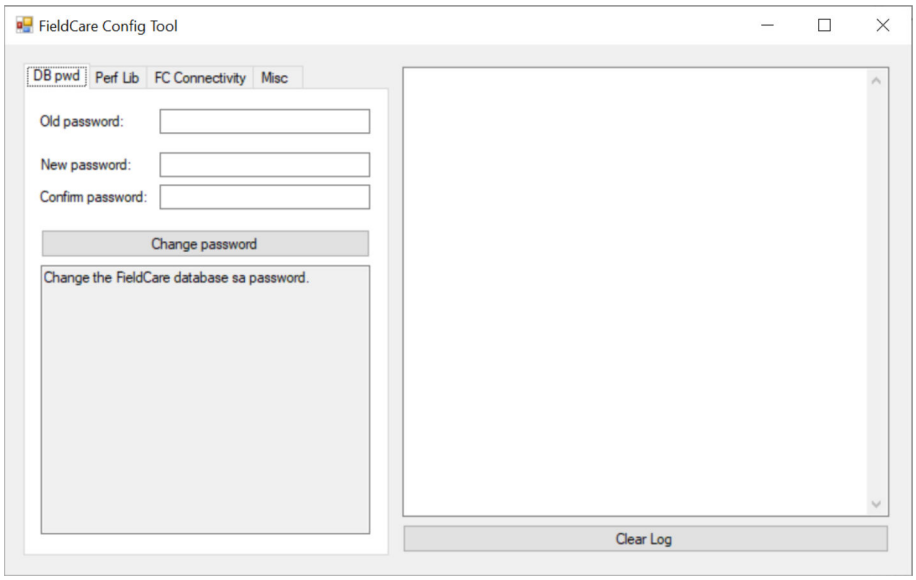


2 *PAM Service deinstallieren*

Voreingestellte Standard-Passwörter

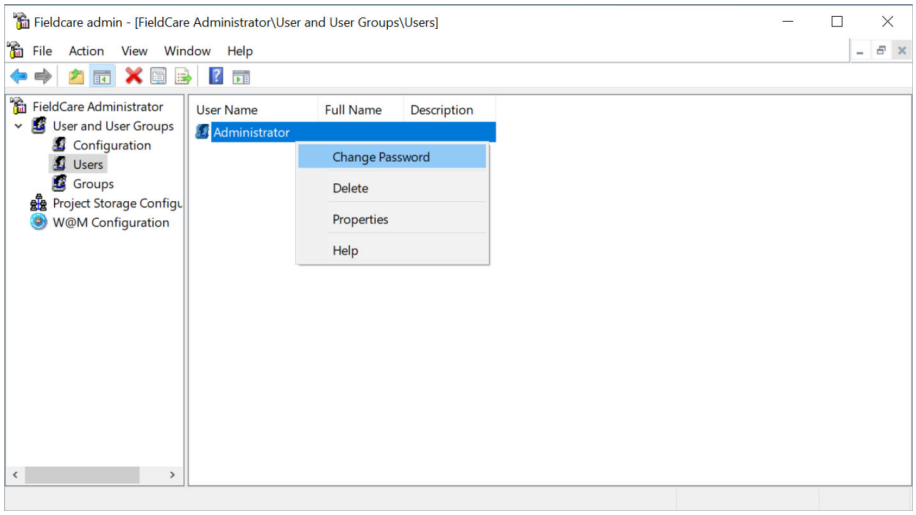
Nach einer Neuinstallation sind Standard-Passwörter für die Datenbank und "FieldCare Administration" konfiguriert.

1. Folgendes Programm öffnen:
   %ProgramData%\Endress+Hauser\FieldCare SFE500\Configuration\FC_ConfTool.exe.



3 *FieldCare Config Tool: Passwort ändern*

2. Altes und neues Passwort eingeben.
3. Auf **Change password** klicken.
4. **FieldCare Administration** öffnen.
5. Login gemäß Betriebsanleitung durchführen → 6.
   ↳ Das Fenster "FieldCare admin" wird geöffnet.
6. In der linken Spalte den Eintrag **Users** markieren.
7. **Administrator** markieren.
8. Über das Kontextmenü **Change Password** das Passwort ändern.



4 *FieldCare Administration: Passwort ändern*

Der Zugang von FieldCare auf die Microsoft SQL Datenbank funktioniert **nur** ohne Passwort.

Da der Zugang auf die Datenbank ohne Passwortschutz ist, empfehlen wir folgende Maßnahmen:
- Datenbank nicht im Netzwerk verfügbar machen.
- Hostsystem vor Zugriffen durch unautorisierte Personen schützen.

4.4.4 Anwenderdaten konfigurieren

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

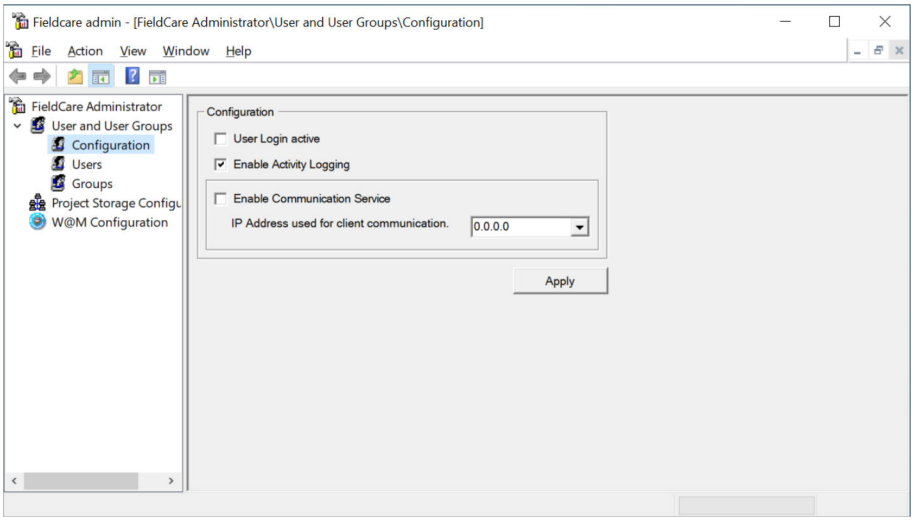
Detaillierte Informationen zur Benutzerverwaltung: Siehe Betriebsanleitung BA00065S

4.4.5 Security-relevante Einstellungen des Produkts

Communication Service

Standardmäßig ist in FieldCare Administration der Communication Service deaktiviert. Aus Sicherheitsgründen empfehlen wir, diesen Service deaktiviert zu lassen.

Der Communication Service muss nur für eine Client-Server-Kommunikation aktiviert werden (z.B. Asset Health Monitoring Solution SAH70). Der Service ermöglicht die Kommunikation mit den in FieldCare SFE500 konfigurierten Feldgeräten ohne Anwenderauthentifizierung und ohne Verschlüsselung. Somit kann jeder Anwender im selben Netzwerk wie das Hostsystem auf die Feldgeräte zugreifen.



5 *FieldCare Administration: Communication Service deaktiviert*

4.4.6 User-Management und Auswirkung auf die Security

FieldCare SFE500 verfügt über eine eigene Benutzerverwaltung, die nach der Installation von FieldCare SFE500 zunächst deaktiviert ist.

Die Aktivierung der Benutzerverwaltung in FieldCare SFE500 kann eine weitere Sicherheitsschicht im Defence-in-Depth-Konzept sein.

Detaillierte Informationen zur Benutzerverwaltung: Siehe Betriebsanleitung BA00065S

FieldCare SFE500 speichert das Benutzerpasswort obfuskiert und damit nicht vollständig sicher ab.

Wir raten davon ab, für die Benutzerverwaltung von FieldCare SFE500 und für Windows dieselben Passwörter zu verwenden.

Zusätzlich empfehlen wir, Windows automatisch bei Inaktivität zu sperren.

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.

5.3.1 Allgemeine Empfehlungen

- Passwörter nur unbeobachtet eingeben.
- Wenn ein Passwort nicht mehr vertrauenswürdig ist, zugehöriges Benutzerkonto sofort sperren und Passwort ändern.
- Beim Verlassen des Arbeitsplatzes PC sperren, um einen unbefugten Zugriff auf das Produkt auszuschließen.

5.3.2 Daten exportieren und drucken

Über FieldCare SFE500 können Sie Daten wie z.B. über das Projekt, die Anlagentopologie und Feldgeräte exportieren und drucken.

Da durch FieldCare SFE500 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 Projekte exportieren und importieren

FieldCare SFE500 stellt für den Export und Import von Dateien folgende Dateiformate zur Verfügung: *.fcproj, *.fcp, *.fcdtm, *.csv oder *.xml.

FieldCare SFE500 exportiert die Daten ungeschützt. Da die exportierten Dateien modifiziert werden können, ist es Aufgabe des Betriebspersonals die Dateien gegen Modifikationen zu schützen.

FieldCare SFE500 führt beim Import von Dateien keine Validierung durch. Es ist Aufgabe des Betriebspersonals, darauf zu achten, nur Dateien aus vertrauenswürdigen Quellen zu importieren.

5.3.4 Regelmäßige Backups durchführen

Um nach einem Ausfall oder nach einem Sicherheitsproblem FieldCare SFE500 mit den zugehörigen Projekten schnell wieder herstellen zu können, empfehlen wir regelmäßige Backups durchzuführen.

Für ein Backup gibt es folgende Möglichkeiten:
- Backup der gesamten Festplatten inklusive Windows und aller Dateien
- Backup aller FieldCare-Projekte

Beide Backup-Möglichkeiten bieten nur geringe Maßnahmen zum Schutz des Inhalts. Es liegt in der Verantwortung des Betriebspersonals, die Backup-Daten zu schützen und sicher zu behandeln.

Backup der gesamten Festplatten inklusive Windows und aller Dateien

Aufgrund der Funktionsweise von FDT, empfehlen wir, regelmäßig die komplette Festplatte inklusive Windows und aller Dateien zu sichern. Damit ist sichergestellt, dass nach dem Wiederherstellen auch alle DTMs auf dem System wieder verfügbar sind.

Beachten Sie, dass beim Wiederherstellen des Systems auf einer neuen Hardware Ihre FieldCare SFE500 Lizenz ungültig wird. Kontaktieren Sie in diesem Fall Ihren Endress+Hauser Service. Wenn möglich, sollten Sie vor einem Backup die Software-Lizenz in das Endress+Hauser Software-Portal zurückgeben (deaktivieren).

Backup aller FieldCare-Projekte

Sollte ein komplettes Backup der Festplatte nicht möglich sein, empfehlen wir die FieldCare SFE500 Projekte zu sichern. Zusammen mit den Installationsdateien für FieldCare SFE500 sowie den benötigten DTMs und FDI Packages können Sie die Funktionalität wiederherstellen.

Die Wiederherstellung kann mehrere Stunden dauern.

Bei dieser Variante der Wiederherstellung müssen Sie die FieldCare SFE500 Lizenz wiederherstellen. Kontaktieren Sie in diesem Fall Ihren Endress+Hauser Service.

FieldCare-Projekt speichern

1. In FieldCare SFE500 das Projekt wählen.
2. Auf **File** → **Import/Export** → **Export Project** klicken.
   ↳ Das Dialogfenster "Export Project" wird angezeigt.
3. Einen Speicherort wählen, einen Namen eingeben und auf **Save** klicken.
   ↳ Die Abfrage nach einem Passwort wird angezeigt.
4. **Password protected** wählen.
5. Passwort eingeben.
6. Auf **OK** klicken.

FieldCare-Projekt wieder herstellen

1. Auf **File** → **Import/Export** → **Import Project** klicken.
   ↳ Das Dialogfenster **Import Project** wird angezeigt.
2. Projekt wählen.
3. Auf **Open** klicken.
   ↳ Wenn das Projekt bei dem Export mit einem Passwort geschützt wurde, erscheint die Abfrage nach dem Passwort.
4. Passwort eingeben.
5. Auf **OK** klicken.

5.4 Security-Aspekte während des Betriebes

Folgende Aufgaben während des Betriebes regelmäßig durchführen:
- Windows-Updates
- Updates für Feldgeräte-Treiber FDT/DTM und FDI Packages
- Updates für FieldCare → 11

5.5 Update-Management

Das Update-Management für FieldCare SFE500 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 FieldCare SFE500 auf den Endress+Hauser S3 Server bereit. Danach werden die Updates automatisiert im Hintergrund auf den FieldCare SFE500 Host 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. → 11

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. → 13

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.

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.	Hostsysteme ausschalten. Wenn ein Ausschalten der Hostsysteme nicht möglich ist, alle Prozesse beenden.
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 FieldCare SFE500 sind unter Umständen Credentials in der Datenbank gespeichert. 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. → 🖹 8 Falls erforderlich, Ersatzmaßnahmen berücksichtigt.	❑
	Planungsarbeiten in der Engineering-Phase beachtet. Bedrohungsanalyse und Risikobeurteilung durchgeführt.→ 🖹 9	❑
	Sofern möglich, risikomindernde Maßnahmen berücksichtigt. → 🖹 10	❑
Wareneingang / Transport	Geprüft, dass die Signatur der gelieferten Dateien Endress+Hauser als Hersteller identifiziert. → 🖹 13	❑
Inbetriebnahme	Produkt für den Anwendungsfall gehärtet. → 🖹 15	❑
Betrieb	Vorgaben zum Betrieb beachtet. → 🖹 19	❑
	Vorgaben zum Update-Management beachtet. → 🖹 21	❑
	Planung der wiederkehrenden Bedrohungsanalyse vorgenommen. → 🖹 21	❑
Außerbetriebnahme	Produkt außer Betrieb genommen. → 🖹 22	❑

7.2 Versionshistorie

Dokumentenversion	Softwareversion	Änderungen
01.00	Ab 02.18	Erste Version

www.addresses.endress.com

Endress+Hauser

People for Process Automation