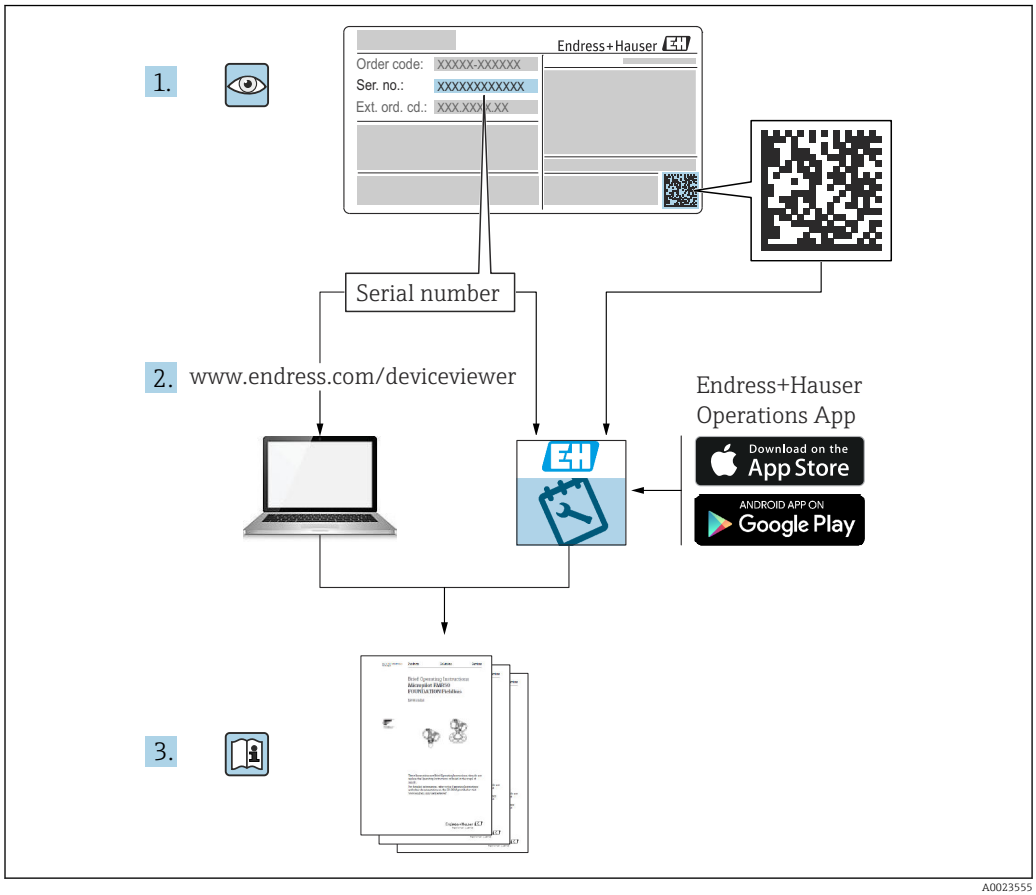
SD03029S/04/DE/03.25-00
71692077
2025-01-13

Sonderdokumentation
Security-Handbuch FieldEdge SGC500

Industrielles Edge Device zur Anbindung von Feldgeräten an die Netilion Cloud

Endress+Hauser
People for Process Automation


1.
Endress+Hauser
Order code: XXXXX-XXXXXX
Ser. no.: XXXXXXXXXXX
Ext. ord. cd.: XXX XXX XXX
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 FieldEdge SGC500

- Technische Information TI01525S
- Betriebsanleitung BA02035S
- 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

In diesem Security-Handbuch wird das FieldEdge SGC500, die Schnittstelle zum Feldgerät und die Schnittstelle zur Endress+Hauser Netilion Cloud betrachtet. Die weiteren Komponenten wie angeschlossene Feldgeräte, Feldbus-Gateways, die Endress+Hauser Netilion Cloud und Bedientools sind keine Bestandteile dieses Security-Handbuches. In den folgenden Abbildungen sind die Systemgrenzen blau markiert.

Die ausgehenden Aufrufe zur Netilion Cloud sind end-to-end nach TLS 1.2 verschlüsselt. Netilion Cloud Aufrufe werden authentifiziert – (OAuth 2.0).

Anwendungsgebiet

Das FieldEdge SGC500 umfasst ein Edge Device und die darauf implementierte Endress+Hauser Software.

Das FieldEdge liest die Informationen der Feldgeräte, interpretiert diese und überträgt diese über die Internetverbindung in die Netillion Cloud. Das FieldEdge ist für den Einsatz in einem Schaltschrank in einem zutrittsgeschützten Kontrollraum vorgesehen. Idealerweise wird das FieldEdge über zwei getrennte Ethernetleitungen mit dem Feldbusnetzwerk (OT) und mit dem Unternehmensnetzwerk (IT) verbunden.

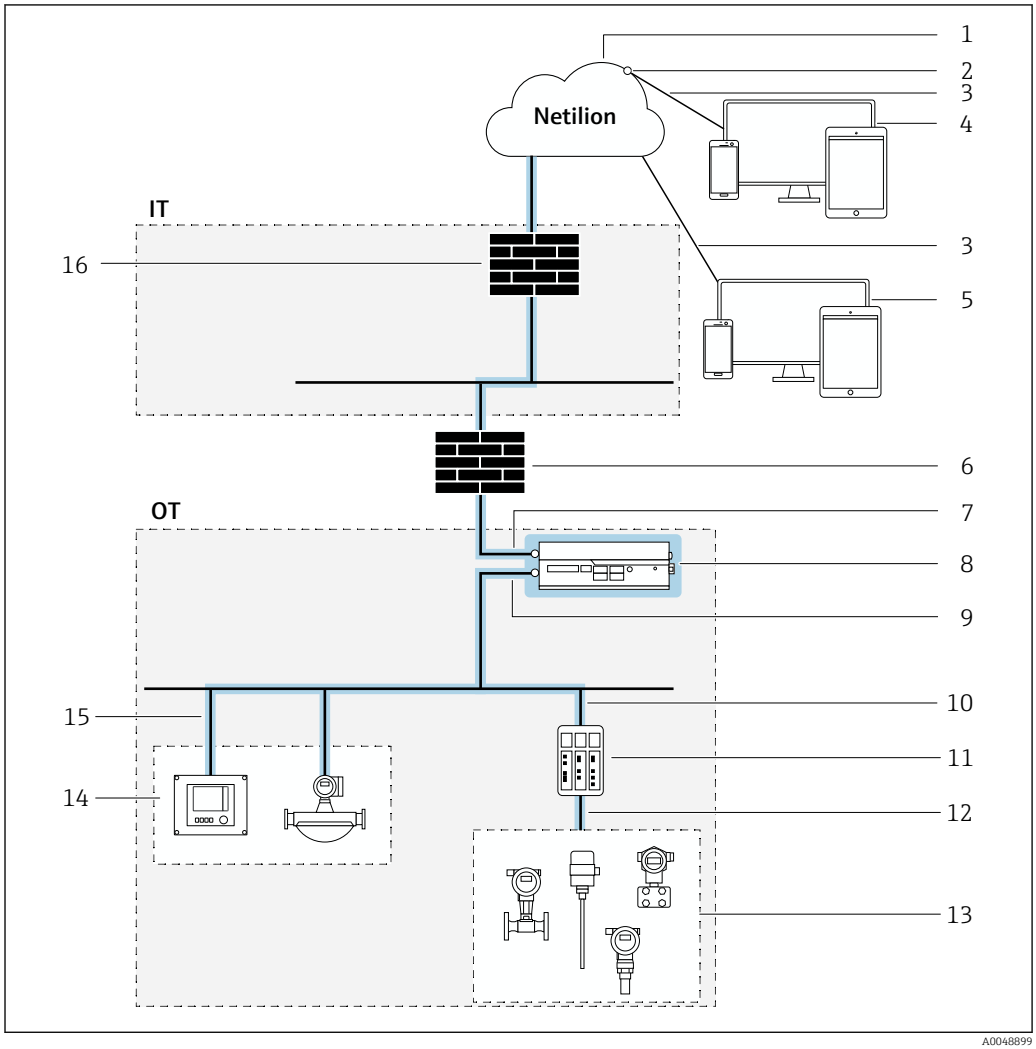
Die Endress+Hauser Software bietet folgendes:
- Read Only Verbindung zu Feldgeräten über verschiedene Feldbus-Protokolle und Feldbus-Gateways.
  Optionale Feldgeräteschreibzugriffe sind bei den Netilion Services dokumentiert und erfordern eine Nutzerbestätigung.
- Datenaufbereitung und verschlüsselte Übermittlung der Daten ausschließlich in die Netilion Cloud.
- Spezifische Datenerfassung für die abonnierten digitalen Dienste in Netilion.
- Automatische Aktualisierungen im Hintergrund: Sicherheitsaktualisierungen, Softwareanpassungen und funktionale Erweiterungen.

Eingehende Kommunikation aus dem Internet ist nicht vorgesehen und muss in der Firewall geblockt werden. Ein Durchrouten zum Feldbusnetzwerk ist nicht möglich.

Informationen zu Einstellungen für die Firewall: → 20

3.2.2 Anbindung des SGC500 über getrennte Schnittstellen für Internet und Feldbusnetzwerk

Anbindung eines Feldbusnetzwerkes



1 *Anbindung des FieldEdge SGC500 über getrennte Schnittstellen für Internet und Feldbusnetzwerk (blaue Markierung zeigt die Systemgrenzen für dieses Handbuch)*

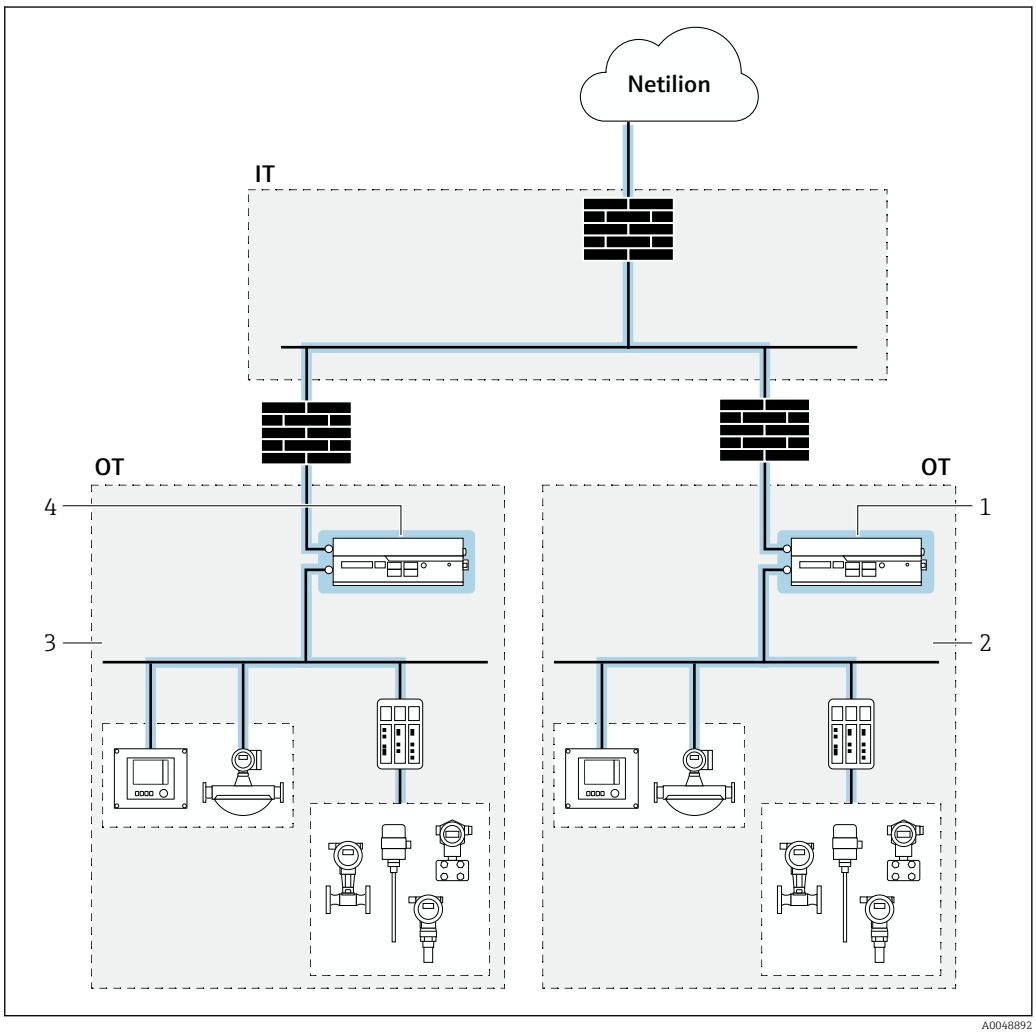
IT Information Technology, hier: Unternehmensnetzwerk zur Informationsverarbeitung und mit Internetanbindung
OT Operational Technology, hier: Netzwerk zur Prozessautomatisierung
1 Netilion Cloud
2 Netilion Connect: Application Programming Interface (API)
3 Internetverbindung https
4 Nutzersystem mit Nutzeranwendung
5 Netilion Services: Internetbrowser basierte Netilion Service App
6 Anlagenfirewall
7 Internetverbindung WAN – https, anlagenseitige Anbindung
8 FieldEdge SGC500 liest Feldgerätedaten und überträgt diese sicher in die Netilion Cloud
9 Feldbusnetzwerk
10 Ethernet-Kommunikation
11 Unterstützte Feldbus-Gateways zur Umsetzung von einem Feldbus-Protokoll auf ein IP-Protokoll
12 Feldbus-Kommunikation
13 Anlagenkomponenten wie Endress+Hauser Feldgeräte und Feldgeräte anderer Hersteller
14 Ethernet-Protokoll-basierte Feldgeräte
15 Industrial Ethernet
16 Firewall des Unternehmensnetzwerkes

Die Abbildung zeigt das FieldEdge SGC500 und alle am Informationsfluss beteiligten Komponenten, die zur Erfassung von Gerätestatusinformationen und deren Weiterleitung in die Endress+Hauser Netilion Cloud erforderlich sind.

Das FieldEdge SGC500 ist ein Edge Device. Die Kommunikation zwischen dem FieldEdge SGC500 und den Anlagenkomponenten basiert auf Industrial Ethernet Protokollen wie z.B. HART/IP oder auch proprietären Protokollen. Das FieldEdge SGC500 leitet nur vom FieldEdge angefragte, dedizierte Informationen der unterlagerten Anlagenkomponenten über die Webadresse netilion.endress.com in die Netilion Cloud.

Eine generelle Weiterleitung von Daten aus dem Feldbusnetzwerk (OT) in das Unternehmensnetzwerk (IT) erfolgt nicht. Der Betreiber muss eine Firewall bereitstellen.

Anbindung mehrere Feldbusnetzwerksegmente



2 *Empfohlene Segmentierung bei mehreren Feldbusnetzwerken mit mehreren FieldEdge SGC500 (blaue Markierung zeigt die Systemgrenzen für dieses Handbuch)*

1 *FieldEdge SGC500 für das Feldbusnetzwerk 1*
2 *Feldbusnetzwerk 1*
3 *Feldbusnetzwerk 2*
4 *FieldEdge SGC500 für das Feldbusnetzwerk 2*

Die Abbildung zeigt die empfohlene Segmentierung eines Feldbusnetzwerkes bei Einsatz von zwei FieldEdge SGC500. Bei dieser Variante werden zwei unterlagerte Feldbusnetzwerke an die Netilion Cloud angebunden. Jedes Feldbusnetzwerk (OT) wird über ein eigenes FieldEdge SGC500 an das übergeordnete Unternehmensnetzwerk (IT) angebunden. Mit dieser Verdrahtung ist sichergestellt, dass beide Feldbusnetzwerksegmente getrennt sind.

3.2.3 Segmentierte Feldbusnetzwerke

Eine feldseitige Netzwerksegmentierung z.B. mittels VLANs wird nicht unterstützt.

3.3 Security-Level festlegen

Abhängig vom angestrebten Security-Level müssen das System und die darin installierten Produkte unterschiedlich hohe Anforderungen erfüllen. Als erstes müssen Sie den erforderlichen **Security-Level** SL1 bis SL4 für das System festlegen. Abhängig von dem Security-Level leiten Sie gemäß DIN IEC 62443-3-3 die Anforderungen an das System und gemäß DIN EN 62443-4-2 die Anforderungen an die Produkte ab.

3.4 Typische Einsatzumgebung des Produkts

Die Betrachtung der Einsatzumgebung für das Produkt soll zu den Security-Anforderungen führen, die durch die Umgebung erbracht werden müssen. Beispielsweise können Sie einen Denial-of-Service-Angriff betrachten.

Beispiel für eine typische Einsatzumgebung des Produkts:
- Das Produkt ist eine Systemkomponente.
- Das Produkt ist mit mindestens einer Schnittstelle ausgestattet. Schnittstellen: Siehe Kapitel "Systemüberblick".
- Das Produkt wird in einer industriellen Umgebung betrieben.
- Der Zugang zum System ist reglementiert. Nur autorisierte Personen haben Zugang zum System.
- Das Personal ist in dem Gebrauch des Produkts und in die Security-Risiken unterwiesen.
- Das Produkt wird in einem Ethernet-Netzwerk, das nur für industrielle Zwecke vorgesehen ist, betrieben. Das Netzwerk ist entweder vollständig vom restlichen Unternehmensnetzwerk getrennt oder durch Firewalls geschützt.
- Das Produkt verfügt über mindestens eine Datenverbindung, die den Produktionsbereich verlässt.
- Das Automatisierungsnetz ist über einen Perimeterschutz gegen Angriffe von außen wie z.B. einen Denial-of-Service-Angriff geschützt.
- Das Produkt ist in einer Umgebung installiert, die nach dem Defense-in-Depth-Konzept abgesichert ist.
- Passworte für das Produkt sind nur autorisierten Personen bekannt.
- Nur autorisierten Personen können über das zugehörige Human Machine Interface (HMI) auf das Produkt zugreifen.

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

3.5 Maßnahmen, falls erforderliche Einsatzumgebung nicht erfüllbar ist

Sofern die spezifizierten Anforderungen an die Einsatzumgebung nicht eingehalten werden können, sind ggf. Ersatzmaßnahme vorzusehen. Dabei kann es sich z.B. um einen mechanischen Schutz des Produkts gegen Manipulation, einen mechanischen Schutz der Verkabelung oder auch um organisatorische Maßnahmen handeln.

Das FieldEdge ist für den Einsatz in einem zutrittsgeschützten Kontrollraum in einem Gebäude vorgesehen.

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

Das FieldEdge ist ein Edge Device, 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.

Folgendes beachten:
- Die Anbindung des FieldEdge an das Internet muss mindestens über eine Firewall erfolgen.
- Feldbusnetzwerk (OT) und Unternehmensnetzwerk (IT) müssen strikt getrennt sein.
- Endress+Hauser empfiehlt eine Segmentierung der Feldbusnetzwerke gemäß DIN IEC 62443-3-3. Dieses kann durch den Einsatz mehrerer FieldEdge erreicht werden → 9.

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

Wir empfehlen, für den Zugriff auf das IIoT-Ökosystem die gleichen Regeln für das Identitäts- und Zugriffsmanagement wie für die anderen Unternehmensbereiche anzusetzen.

Folgendes beachten:
- FieldEdge nur in einem zutrittsgeschützten Kontrollraum in einem Gebäude montieren
- Mitarbeitern nur die Zugriffsrechte geben, die der Mitarbeiter zur Erfüllung seiner Aufgaben benötigt
- Falls während der Inbetriebnahme eine lokale Konfiguration erforderlich ist, Login gemäß Betriebsanleitung durchführen → 🖹 6

3.7.4 Gerätedaten und Gerätestatus überwachen

Das FieldEdge ist Teil eines Netzwerkes in einer Prozessautomatisierungsanlage. Das feldseitige Netzwerkmonitoring ist Aufgabe des Anlagenbetreibers.

Der Online-Status des FieldEdge wird in Netilion angezeigt. Die Verfügbarkeit der Netilion Services können Sie über https://status.netilion.endress.com/ abrufen.

3.7.5 Produkt-Software updaten

Durch Endress+Hauser erfolgt eine automatische Aktualisierung der Software für das FieldEdge.

Update-Management: → 🖹 16

3.7.6 Anwendungen und Apps schützen

Zur Sicherung des Kundensystems, der Kundendaten, der Apps und des Webportals muss auch der Schutz der Zugangsdaten des FieldEdge gewährleistet werden, die auf das IIoT-Ökosystem Zugriff haben. Dies kann dadurch gewährleistet werden, dass die Zugangsdaten und Zertifikate sicher aufbewahrt werden.

Während der Inbetriebnahme kann es erforderlich sein, dass das FieldEdge lokal konfiguriert werden muss. Das FieldEdge ist über ein Login geschützt. Die lokale Konfiguration muss temporär über ein direkt verbundenes Ethernetkabel innerhalb des zutrittsgeschützten Kontrollraums vorgenommen werden.

Weitere Informationen zum "Login (manuelle Verbindung)": Betriebsanleitung → 🖹 6

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 FieldEdge SGC500: → 7

4.4.2 Erforderliche Security-Schritte während der Inbetriebnahme

Produkte von Endress+Hauser werden in Paketen geliefert, die mit einem Endress+Hauser Klebeband versiegelt sind. Ein Lieferschein und ein Beleg mit dem Endress+Hauser Logo sind beigelegt. Ein Siegel versiegelt das Gehäuse und dient als Sicherheit, falls das Gehäuse geöffnet wurde.

Beachten Sie während der Inbetriebnahme hinsichtlich der Security folgenden Punkt: Produkt gemäß den definierten Anforderungen an die Einsatzumgebung integrieren → 10.

4.4.3 Firewall konfigurieren

In dem FieldEdge ist keine Firewall integriert. Eine Firewall zum Internet muss kundenseitig vorgesehen werden → 7.

Wir empfehlen für das FieldEdge die Anbindung an das Internet und das Feldbusnetzwerk über getrennte Schnittstellen → 8.

Firewall wie folgt konfigurieren:
- Port 443 für den https-Dienst für ausgehende Aufrufe vom FieldEdge zur Netilion Cloud freischalten https://*.netilion.endress.com. Alternativ für eine detaillierte Firewall-Regel folgende URLs freischalten: https://api.netilion.endress.com und https://downloads.netilion.endress.com
- Die Netilion Services sind bei AWS Heroku gehostet. Hinweis: Aufrufe vom FieldEdge an andere URLs können Sie in der Firewall blocken.
- Die Firewall-Konfiguration können Sie über die URL https://api.netilion.endress.com in einem Webbrowser prüfen. Der Aufruf dieser Webseite muss bei aktiver Firewall möglich sein.
- Alle eingehenden Aufrufe zum FieldEdge müssen geblockt werden.

4.4.4 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 FieldEdge ist nicht möglich und auch nicht erforderlich. Das FieldEdge nutzt nur Dienste, die für die Funktion erforderlich sind.

4.4.5 Anwenderdaten konfigurieren

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

Account für die Netilion Cloud

Für die Anbindung des FieldEdge an die Netilion Cloud wird während der werksseitigen Konfiguration ein Account im FieldEdge verschlüsselt gespeichert.

Mit diesem Account wird das FieldEdge in der Netilion Cloud authentifiziert. Somit sind die in der Netilion Cloud gespeicherten Informationen der Feldgeräte nur für den authentifizierten Netilion Account des FieldEdge Bestellers oder einem von ihm autorisierten Account verfügbar.

Hinweise zu Accounts / Zugangsdaten

Für den Betrieb des FieldEdge sind folgende Accounts erforderlich:
- Account für die Anbindung des FieldEdge an die Netilion Cloud. Dieser Account wird von Endress+Hauser während der werksseitigen Konfiguration verschlüsselt im FieldEdge gespeichert.
  Dieser Account kann nicht geändert werden.
- Account für die lokale Konfiguration des FieldEdge. Für den Zugang über diesen Account sind ein Benutzername und ein Passwort erforderlich. (Zugangsdaten: Benutzername "admin" und Passwort "Seriennummer des FieldEdge".)
  Die Zugangsdaten können Sie nicht ändern.
- Account für Netilion
  Der Anwender legt die Zugangsdaten selbst fest und kann diese auch ändern.

Weitere Informationen zum "Login (manuelle Verbindung)": Betriebsanleitung → 6

4.4.6 Security-relevante Einstellungen des Produkts

Alle Security-relevanten Einstellungen, die für das FieldEdge erforderlich sind, wurden am FieldEdge werksseitig durchgeführt. Anpassungen sind nicht erforderlich.

4.4.7 User-Management und Auswirkung auf die Security

Das FieldEdge realisiert zur Anbindung an die Netilion Cloud folgendes User-Management:

- Das User-Management für das FieldEdge sieht einen fest ab Werk eingestellten User vor → 14
- Der Zugang zur lokalen Konfiguration erfolgt über ein gerätespezifisches und vordefiniertes Passwort → 14
- Ein weitergehendes User-Management wird im FieldEdge nicht bereitgestellt

Weitere Informationen zum User-Management der Netilion Cloud: Dokument "Netilion – Terms of Service" → 6

5 Betrieb

5.1 Zielgruppe

Dieses Kapitel richtet sich an das Betriebspersonal.

5.2 Anforderungen an das Personal

Das Personal muss folgende Bedingungen erfüllen:
- Über eine fachliche Qualifikation verfügen, die dieser Funktion und Tätigkeit entspricht.
- Vom Anlagenbetreiber autorisiert.
- Mit den nationalen Vorschriften vertraut.
- Vor Arbeitsbeginn: Anweisungen in Anleitung und Zusatzdokumentation sowie Zertifikate (je nach Anwendung) lesen und verstehen.
- Anweisungen und Rahmenbedingungen befolgen.

5.3 Aufgaben während des Betriebes

Produkt gemäß zugehöriger Betriebsanleitung betreiben. Für den Bereich "Security" zusätzlich dieses Kapitel beachten.

Das FieldEdge erfordert keine Interaktionen während des Betriebes.

Damit die Firmware des FieldEdge aktualisiert werden kann, muss eine permanente Spannungsversorgung des FieldEdge und eine permanente Internetverbindung zur Netilion Cloud gewährleistet sein.

Update-Management: → 16

5.4 Security-Aspekte während des Betriebes

Folgende Punkte müssen während des laufenden Betriebes beachtet werden:
- Die im FieldEdge hinterlegten Zertifikate haben eine begrenzte Laufzeit.
- Vor dem Ablauf werden die Zertifikate automatisch und im Hintergrund von Remote über Betriebssystemupdates durch Endress+Hauser erneuert → 16.
  Ein manueller Eingriff ist nicht erforderlich.

5.5 Update-Management

Endress+Hauser stellt Remote-Updates über die Netilion Cloud bereit. Der Zeitpunkt des Updates wird durch Endress+Hauser festgelegt und kann durch den Anwender nicht beeinflusst werden. Nach manchen Updates ist ein Neustart für das FieldEdge erforderlich. Der Neustart wird automatisch durchgeführt.

Da das FieldEdge nicht direkt in die Automatisierung der Anlage eingreift, werden von Endress+Hauser für die neuen Softwareversionen keine spezifischen Testroutinen für die Anwendung empfohlen.

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

Endress+Hauser stellt durch Prüfsummen und Signaturen in der Firmware die Integrität und Authentizität der Updates sicher. Eine Integritäts- und Authentizitätsprüfung der Updates durch den Anwender ist nicht erforderlich.

Sie können die Software-Version des FieldEdge wie folgt ermitteln: Die aktuell im FieldEdge geladene Software-Version wird im Netilion Account bei den SGC500 Details des jeweiligen SGC500 angezeigt.

5.6 Funktionale Erweiterung

Funktionale Erweiterungen werden nach Verfügbarkeit unangekündigt von Endress+Hauser in das FieldEdge ausgeliefert. Der Zeitpunkt der funktionalen Erweiterung wird durch Endress+Hauser festgelegt und kann durch den Anwender nicht beeinflusst und nicht blockiert werden.

Funktionale Erweiterungen können folgendes beinhalten:
- Verbesserung existierender Services
- Unterstützung neuer, buchbarer Services

5.7 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.

5.8 Reparatur und Entsorgung

5.8.1 Störungsbehebung und Reparatur

Störungsbehebung

Gehen Sie wie folgt vor, falls für das FieldEdge eine Störung vorliegt:

1. In Netilion anmelden.
2. Über Netilion Supportticket erstellen. Netilion > Auswahl eines Service > Netilion > Main Menu > Support Create a ticket
   ↳ Das Supportticket wird an Endress+Hauser Service gesendet.
   Endress+Hauser Service analysiert den Fehler und ermittelt die erforderlichen Maßnahmen.
   Falls Endress+Hauser Service feststellt, dass das FieldEdge defekt ist, folgende Handlungsanweisung befolgen → 17.

FieldEdge ist defekt

Endress+Hauser Service hat festgestellt, dass das FieldEdge defekt ist und ein Auswechseln des FieldEdge erforderlich ist. Endress+Hauser Service versendet ein vorkonfiguriertes Ersatzgerät.

Des Weiteren werden Sie aufgefordert das defekte FieldEdge an Endress+Hauser zurückzusenden oder das defekte FieldEdge zu zerstören und zu entsorgen.

Gehen Sie wie folgt vor, falls das FieldEdge defekt ist:

1. Nach Anweisung von Endress+Hauser Service die Zugangsdaten vom FieldEdge zur Netilion Cloud von dem defekten FieldEdge löschen.

2. In Netilion die Daten auf den folgenden Seiten löschen bzw. zurücksetzen: "Network Interface Details", "Field Gateways" und / oder "EtherNet/IP Activation Status"
3. Abhängig von der Anweisung von Endress+Hauser Service: Defektes FieldEdge umgehend an Endress+Hauser zurücksenden oder defektes FieldEdge zerstören und entsorgen.
4. Neues FieldEdge gemäß Betriebsanleitung anschließen, konfigurieren und in Betrieb nehmen.

Wir empfehlen Ihre Zugangsdaten / Nutzerdaten vom FieldEdge zu löschen, wenn Sie das FieldEdge aufgrund eines Defekts außer Betrieb nehmen müssen. Mit dem Löschen verhindern Sie einen Missbrauch Ihrer Daten.

5.8.2 Entsorgung

Gehen Sie wie folgt vor, wenn Sie das FieldEdge entsorgen müssen:

1. Nach Anweisung von Endress+Hauser Service die Zugangsdaten vom FieldEdge zur Netilion Cloud von dem defekten FieldEdge löschen.
2. In Netilion die Daten auf den folgenden Seiten löschen bzw. zurücksetzen: "Network Interface Details", "Field Gateways" und / oder "EtherNet/IP Activation Status"
3. Defektes FieldEdge zerstören und entsorgen. Folgende Hinweise beachten.

- Wir empfehlen Ihre Zugangsdaten / Nutzerdaten vom FieldEdge zu löschen, wenn Sie das FieldEdge entsorgen müssen. Mit dem Löschen verhindern Sie einen Missbrauch Ihrer Daten.
- Wir empfehlen vor der Entsorgung oder Verschrottung des FieldEdge gemäß folgender Richtlinie vorzugehen: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

Gemäß der Richtlinie 2012/19/EU über Elektro- und Elektronik-Altgeräte (WEEE) sind Produkte von Endress+Hauser mit dem abgebildeten Symbol gekennzeichnet, um die Entsorgung von WEEE als unsortierten Hausmüll zu minimieren. Diese Produkte dürfen nicht als unsortierter Hausmüll entsorgt werden und können an Endress+Hauser zur Entsorgung zurückgegeben werden. Die Rückgabe erfolgt gemäß den Allgemeinen Geschäftsbedingungen oder individuell vereinbarten Bedingungen von Endress+Hauser.

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 soll aus der Subscription entfernt werden.	1. In Netilion auf der Seite "Network Interface Details" die kundenspezifischen Netzwerkdaten für das FieldEdge löschen. 2. In Netilion auf der Seite "Field Gateways / Devices" das FieldEdge wählen. 3. Auf der Seite "Edge Device Details" auf "Delete" tippen. ↳ Ein Dialogfenster wird geöffnet. 4. Das Löschen des Field Edge bestätigen.
Das Produkt wird für längere Zeit nicht genutzt.	Keine Maßnahmen erforderlich.
Das Produkt hat eine Störung und Sie können die Störung nicht beheben.	Endress+Hauser Service kontaktieren und den Anweisungen von Endress+Hauser Service folgen → 17.
Das Produkt ist defekt und muss daher entsorgt werden. Der Defekt wurde von Endress+Hauser Service festgestellt → 17.	Informationen zur Entsorgung: → 18
Das Produkt soll entsorgt werden. Sie möchten das Produkt entsorgen.	Informationen zur Entsorgung: → 18
Die Netilion Service Subscription wurde beendet.	Um Ihre Daten und / oder Ihr System sicher vor einem Zugriff zu schützen, empfehlen wir das FieldEdge zu verschrotten. Hierzu empfehlen wir gemäß folgender Richtlinie vorzugehen: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization Wenn Sie das FieldEdge nicht verschrotten möchten, empfehlen wir Ihnen zwingend die Software von dem FieldEdge zu löschen. Für weitere Informationen Endress+Hauser Service kontaktieren. Nach Rücksprache mit Endress+Hauser Service können Sie das FieldEdge auch zurücksenden.

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. → 🖹 10	❑
	Planungsarbeiten in der Engineering-Phase beachtet. Bedrohungsanalyse und Risikobeurteilung durchgeführt.→ 🖹 11	❑
	Sofern möglich, risikiomindernde Maßnahmen berücksichtigt. → 🖹 11	❑
Wareneingang / Transport	Geprüft, dass die Verpackung ungeöffnet ist und dass das Siegel unbeschädigt ist. → 🖹 13	❑
Inbetriebnahme	Produkt für den Anwendungsfall gehärtet. → 🖹 14	Nicht anwendbar
Betrieb	Vorgaben zum Update-Management beachtet. → 🖹 16	❑
	Planung der wiederkehrenden Bedrohungsanalyse vorgenommen. → 🖹 17	❑
Außerbetriebnahme	Produkt außer Betrieb genommen. → 🖹 19 Je nach Grund für die Außerbetriebnahme Produkt deaktivieren oder das Produkt zerstören.	❑

7.2 Versionshistorie

Dokumentenversion	Firmwareversion	Hardwareversion	Änderungen
SD03029S/04/DE/01.22-00	Ab 3.00.02	Dev. Rev. 1	Erste Version
SD03029S/04/DE/02.23-00	Ab 3.00.02	Dev. Rev. 1	Modbus TCP ergänzt. Kapitel "Anhang" ergänzt.
SD03029S/04/DE/03.25-00	Ab 3.04.01	Dev. Rev. 1	PROFINET ergänzt. Tankvision Tank Scanner NXA820 ergänzt.

7.3 Informationen für Security-Audits

7.3.1 Für den Betrieb erforderliche Dienste

Für den Betrieb des FieldEdge sind die in diesem Kapitel aufgeführten Dienste erforderlich.

Dienste für die Anbindung an die Endress+Hauser Netilion Cloud

Die in der folgenden Tabelle aufgeführten Dienste müssen je nach Netzwerkstruktur verfügbar sein, bzw. in der Firewall freigeschaltet werden.

Dienst	Port	Bemerkung
https	443	Übertragung der Feldinformationen an die Netilion Cloud
DNS	53/853	Ein TCP-DNS-Server mit aktueller Adressauflösung muss erreichbar sein.

Dienst	Port	Bemerkung
UDP DHCP (IPv4)	67	Bootstrap Protocol (BOOTP) Server, auch genutzt von DHCP
TCP/UDP (IPv6)	547	DHCPv6-Server

Dienste für die Anbindung an das Feldbusnetzwerk

Zur Unterstützung von künftigen Feldbus-Gateways oder Industrial Ethernet Netzwerken müssen Sie gegebenenfalls weitere Dienste auf der Feldgeräteseite freischalten.

Dienst	Port	Bemerkung
TCP/IP http	80	Temporäre Nutzung während der Erstinbetriebnahme
SSH	22 SSH	Dieser Dienst wird nur bei einem fehlerhaften FieldEdge zur forensischen Analyse genutzt. SSH ist über einen Private key abgesichert. Der Private key ist nur auf Endress+Hauser Entwicklungs-PCs verfügbar. Im laufenden Betrieb ist ein Zugriff über SSH von Endress+Hauser nicht vorgesehen. Wir empfehlen, diesen Dienst in der Firmenfirewall zu blocken.
TCP/UDP	–	Spezifische Kommunikation über Feldbus-Gateway ▪ Dienst für die Kommunikation via PROFIBUS Fieldgate SFG500: → 🖹 22 ▪ Dienst für die Kommunikation via HART Fieldgate SFG250: → 🖹 22 ▪ Dienst für die Kommunikation mit dem WirelessHART-Fieldgate SWG70: → 🖹 22 ▪ Spezifische Kommunikation für Ethernet-basierte Protokolle: → 🖹 21
UDP DHCP	67	Bootstrap Protocol (BOOTP) Server, auch genutzt von DHCP
TCP/UDP (IPv6)	547	DHCPv6-Server

Dienst für Remote-Updates über das Netzwerk LAN1

Bei Remote-Updates stellt Endress+Hauser sicher, dass nur die für den Service benötigten Dienste ausgeführt werden.

Dienst	Port	Bemerkung
https	443	Die Aktualisierungen des FieldEdge SGC500 werden in einer Antwort auf eine Anfrage über https (Port 443) in das FieldEdge übertragen.

7.3.2 Von der Anwendung abhängige Dienste

Dienst für die Kommunikation via EtherNet/IP-Netzwerk

Die Verbindung wird immer vom FieldEdge SGC500 zu den EtherNet/IP-Feldgeräten aufgebaut.

Dienst	Port	Bemerkung
TCP/UDP	44818	Empfohlene Hersteller-Default-Einstellungen: Siehe ODVA Spezifikation 5-4.3.2.13.1 CIP Security Considerations Die erforderlichen Hersteller-Default-Einstellungen für Produkte, die EtherNet/IP over (D)TLS unterstützen.
TCP/UDP	2221	

Dienst für die Kommunikation via HART-Fieldgate SFG250

Die Verbindung wird immer vom FieldEdge SGC500 zum Fieldgate SFG250 aufgebaut.

Dienst	Port	Bemerkung
TCP/UDP	5094	Default HART/IP Port

Dienst für die Kommunikation via Modbus TCP

Die Verbindung wird immer vom FieldEdge SGC500 zum Modbus TCP Feldgerät aufgebaut.

Dienst	Port	Bemerkung
TCP	512	Default Modbus TCP Port

Dienst für die Kommunikation via PROFIBUS Fieldgate SFG500

Die Verbindung wird immer vom FieldEdge SGC500 zum Fieldgate SFG500 aufgebaut.

Dienst	Port	Bemerkung
TCP	80	Nutzung für Anfragen vom Fieldgate
TCP/IP	60010	Nutzung für Anfragen vom Fieldgate

Dienst für die Kommunikation via PROFINET

Die Verbindung wird immer vom FieldEdge SGC500 zu den PROFINET-Feldgeräten aufgebaut.

Dienst	Port	Bemerkung
UDP	34964	PROFINET RPC Context Manager
UDP	53247	PROFINET RPC client/server

Dienst für die Kommunikation via Tankvision Tank Scanner NXA820

Die Verbindung wird immer vom FieldEdge SGC500 zum Tankvision Tank Scanner NXA820 aufgebaut.

Dienst	Port	Bemerkung
TCP	80	Identifikation und Identifizierung der verwendeten Tanknamen
TCP/IP	3000	Default-HART-Tunnel für den Zugriff auf angeschlossene HART-Feldgeräte

Dienst für die Kommunikation via WirelessHART-Fieldgate SWG50 und SWG70

Die Verbindung wird immer vom FieldEdge SGC500 zum Fieldgate SWGxx aufgebaut.

Dienst	Port	Bemerkung
TCP/UDP	5094	Default HART/IP Port

www.addresses.endress.com

Endress+Hauser

People for Process Automation