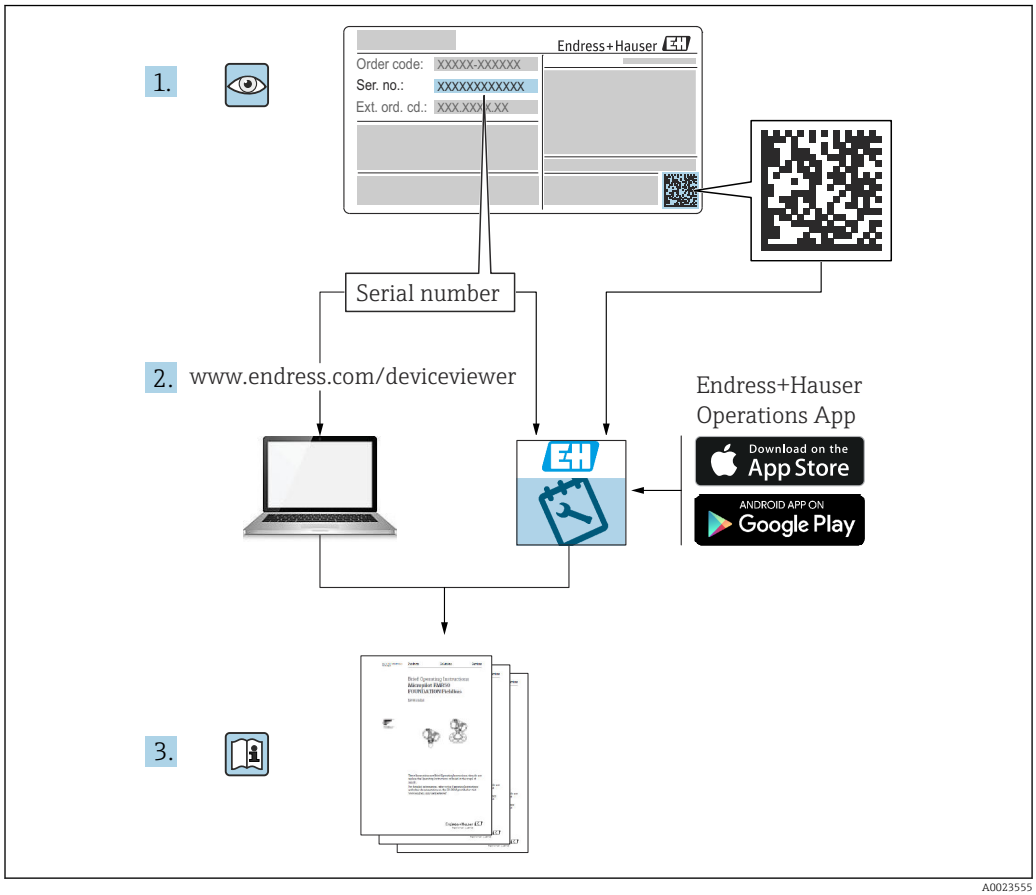
SD03377C/07/DE/01.24-00
71687877
2024-12-11



# Sonderdokumentation
# **Liquiline Edge Module CYY7**

Anbindung an Netilion über Mobilfunk oder Ethernet
Mobilfunk/Ethernet-Ausführung (EMR) und Ethernet-Ausführung (EME)
Security-Handbuch


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 Meldung von Sicherheitslücken und Sicherheitshinweisen

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 Sicherheitshinweise für Endress+Hauser Produkte
- Endress+Hauser Kontakt: PSIRT@endress.com

# 3 Hinweise zum Dokument

## 3.1 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.

## 3.2 Warnhinweise

| Struktur des Hinweises | Bedeutung |
|---|---|
| ⚠ GEFAHR<br>**Ursache (/Folgen)**<br>Ggf. Folgen der Missachtung<br>▶ Maßnahme zur Abwehr | Dieser Hinweis macht Sie auf eine gefährliche Situation aufmerksam. Wenn Sie die gefährliche Situation nicht vermeiden, **wird** dies zum Tod oder zu schweren Verletzungen führen. |
| ⚠ WARNUNG<br>**Ursache (/Folgen)**<br>Ggf. Folgen der Missachtung<br>▶ Maßnahme zur Abwehr | Dieser Hinweis macht Sie auf eine gefährliche Situation aufmerksam. Wenn Sie die gefährliche Situation nicht vermeiden, **kann** dies zum Tod oder zu schweren Verletzungen führen. |
| ⚠ VORSICHT<br>**Ursache (/Folgen)**<br>Ggf. Folgen der Missachtung<br>▶ Maßnahme zur Abwehr | Dieser Hinweis macht Sie auf eine gefährliche Situation aufmerksam. Wenn Sie die gefährliche Situation nicht vermeiden, kann dies zu mittelschweren oder leichten Verletzungen führen. |
| HINWEIS<br>**Ursache/Situation**<br>Ggf. Folgen der Missachtung<br>▶ Maßnahme/Hinweis | Dieser Hinweis macht Sie auf Situationen aufmerksam, die zu Sachschäden führen können. |

## 3.3 Symbole

- Zusatzinformationen, Tipp
- erlaubt
- empfohlen
- verboten oder nicht empfohlen
- Verweis auf Dokumentation zum Gerät
- Verweis auf Seite
- Verweis auf Abbildung
- Ergebnis eines Handlungsschritts

## 3.4 Dokumentation

Netilion Policies beachten:
- 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

# 4 System-Design

## 4.1 Zielgruppe

Dieses Kapitel richtet sich an Planer und Systemintegratoren.

## 4.2 Allgemeine Informationen

In diesem Security-Handbuch wird das Liquiline Edge Module CYY7, die Schnittstelle zum Feldgerät und die Schnittstelle zur Endress+Hauser Netilion Cloud betrachtet. Die weiteren Komponenten wie Steuerungskomponenten, die Endress+Hauser Netilion Cloud und Bedientools sind keine Bestandteile dieses SecurityHandbuches. In den folgenden Abbildungen sind die Systemgrenzen blau markiert. Ausgehende Verbindungen zur Netilion-Cloud sind Ende-zu-Ende nach TLS 1.2 verschlüsselt und verwenden gegenseitige Authentifizierung (mTLS) mittels TLS-Zertifikate.

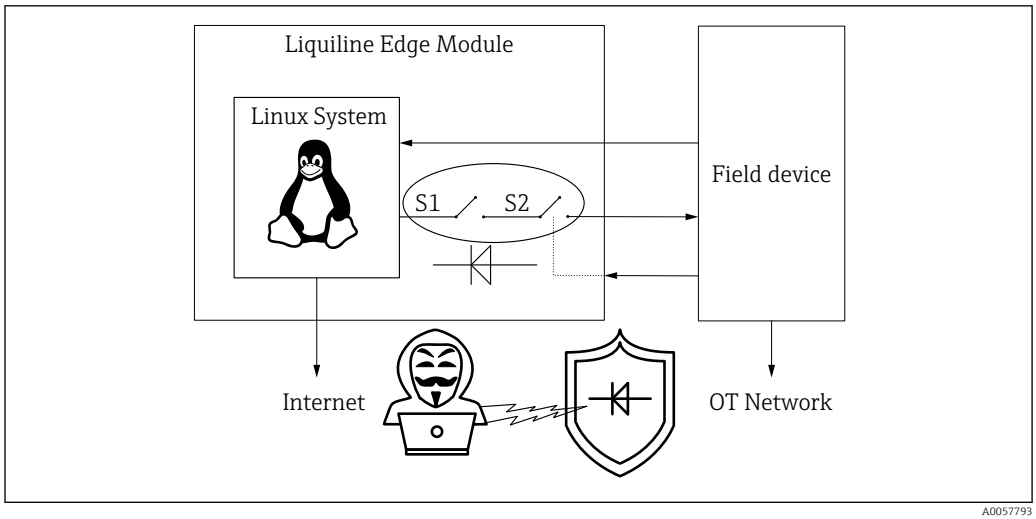
Das Liquiline Edge-Modul wird als Einsteckmodul in einem Feldgerät betrieben und verbindet dieses Feldgerät mit der Netilion Cloud von Endress+Hauser. Diese Verbindung erfordert eine Inter-netverbindung, die entweder über Ethernet oder über ein Mobilfunknetz hergestellt wird. Um das Feldgerät sicher und ohne Beeinflussung durch die Kommunikation mit dem Internet betreiben zu können, sind zusätzlich zu den durch das Liquiline Edge-Modul bereitgestellten Sicherheitsmechanismen verschiedene Maßnahmen erforderlich.

Das Liquiline Edge Modul verwendet verschiedene Mechanismen, um ein hohes Maß an Schutz zu erreichen:
- Secure Boot
- A/B Firmware Update
- Verschlüsseltes Dateisystem
- Sichere Schlüsselspeicherung
- Verschlüsselte HTTPS-Verbindung mit 2-Wege-Authentifizierung (mTLS)
- Keine Hintertüren und Servicezugänge

Eine Beeinflussung des Feldgeräts ist möglich, wenn es trotz dieser Maßnahmen einem Angreifer gelingt, das Liquiline Edge-Modul zu übernehmen. Um auch in diesem Fall das Feldgerät zu schützen, kann die Datenkommunikation vom Liquiline Edge-Modul zum Feldgerät beschränkt oder unterbunden werden.

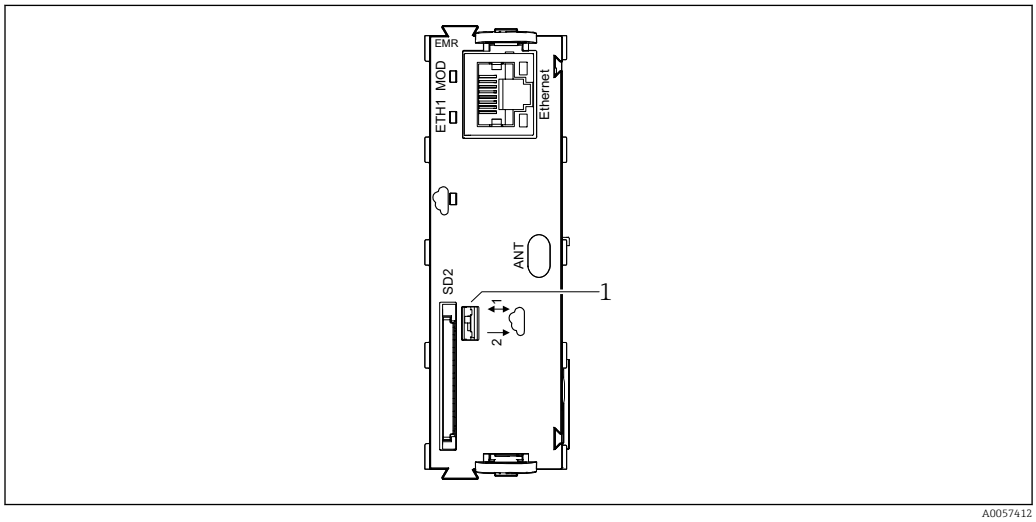
Das Feldgerät kann immer Daten an das Liquiline Edge-Modul senden.

Die Datenrichtung vom Liquiline Edge-Modul kann in mehreren Stufen eingeschränkt werden. Hierzu befindet sich eine Reihenschaltung von zwei Schaltern S1 und S2 in der Datensignalleitung vom Liquiline Edge-Modul zum Feldgerät. Der Schalter S1 ist mechanisch und ist über die Modulblende bedienbar. Der Schalter S2 ist elektronisch und wird vom Feldgerät aus angesteuert.




Im Auslieferungszustand sind die Schalter S1 und S2 geschlossen, so dass eine bidirektionale Kommunikation zwischen Feldgerät und Liquiline Edge-Modul möglich ist.

Bei geöffnetem mechanischem Schalter S1 ist keine Datenkommunikation vom Liquiline Edge-Modul zum Feldgerät möglich.




*1 Edge-Modul*

*1 Mechanischer Schalter S1: bidirektionale/unidirektionale Datenübertragung. Schalterstellung 1: geschlossen. Schalterstellung 2: geöffnet.*

Bei geschlossenem mechanischem Schalter S1 kann die Datenkommunikation vom Liquiline Edge-Modul zum Feldgerät über den elektronischen Schalter S2 eingeschränkt oder unterbunden werden. Einstellmöglichkeiten siehe Betriebsanleitung des Liquiline Edge-Moduls.

Pfad: **Menü/Allgemeine Einstellungen/Erweitertes Setup/Edge-Modul/Sicherheit/Bidir. Datenübertragung**

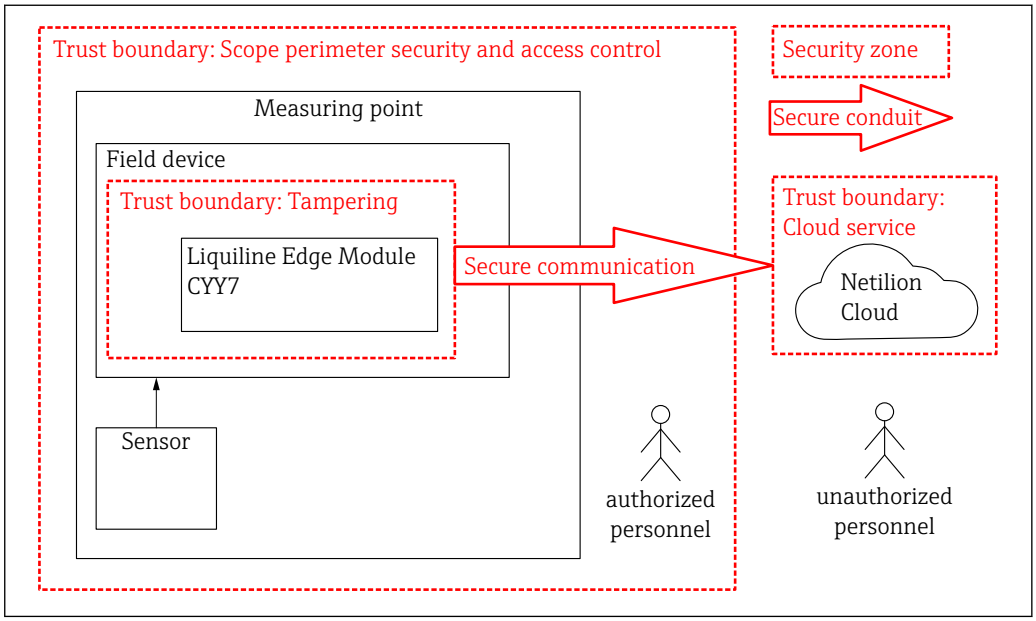
Als Anwender des Liquiline Edge Modul müssen Sie mindestens die folgenden Maßnahmen treffen: - Zugangsschutz zur Verhinderung physischer Angriffe (Tampering) - Die Anforderungen aus diesem Dokument beachten

Folgende Maßnahmen sind kundenseitig erforderlich:

1. Zugangsschutz zur Verhinderung physischer Angriffe (Tampering) sicherstellen.
2. Die Anforderungen aus diesem Dokument beachten.

## 4.3 Systemüberblick

### 4.3.1 Systemaufbau und Systemgrenzen




Die für die Sicherheitsbetrachtung notwendigen Systemstrukturen und Systemgrenzen (Trustzonen) unterscheiden sich je nachdem, ob mit der Netilion-Cloud über Ethernet oder Mobilfunk kommuniziert wird.

**Netilion-Verbindung über Ethernet**

**IPv4-Adresse des Edge-Moduls automatisch von DHCP-Server beziehen (Werkseinstellung):**

- Navigieren zu Pfad: **Menü/Allgemeine Einstellungen/Erweitertes Setup/Edge-Modul/Ethernet ETH1/IP-Einstellungen/Automatisch (DHCP)**

**IPv4-Adresse des Edge-Moduls manuell eingeben:**

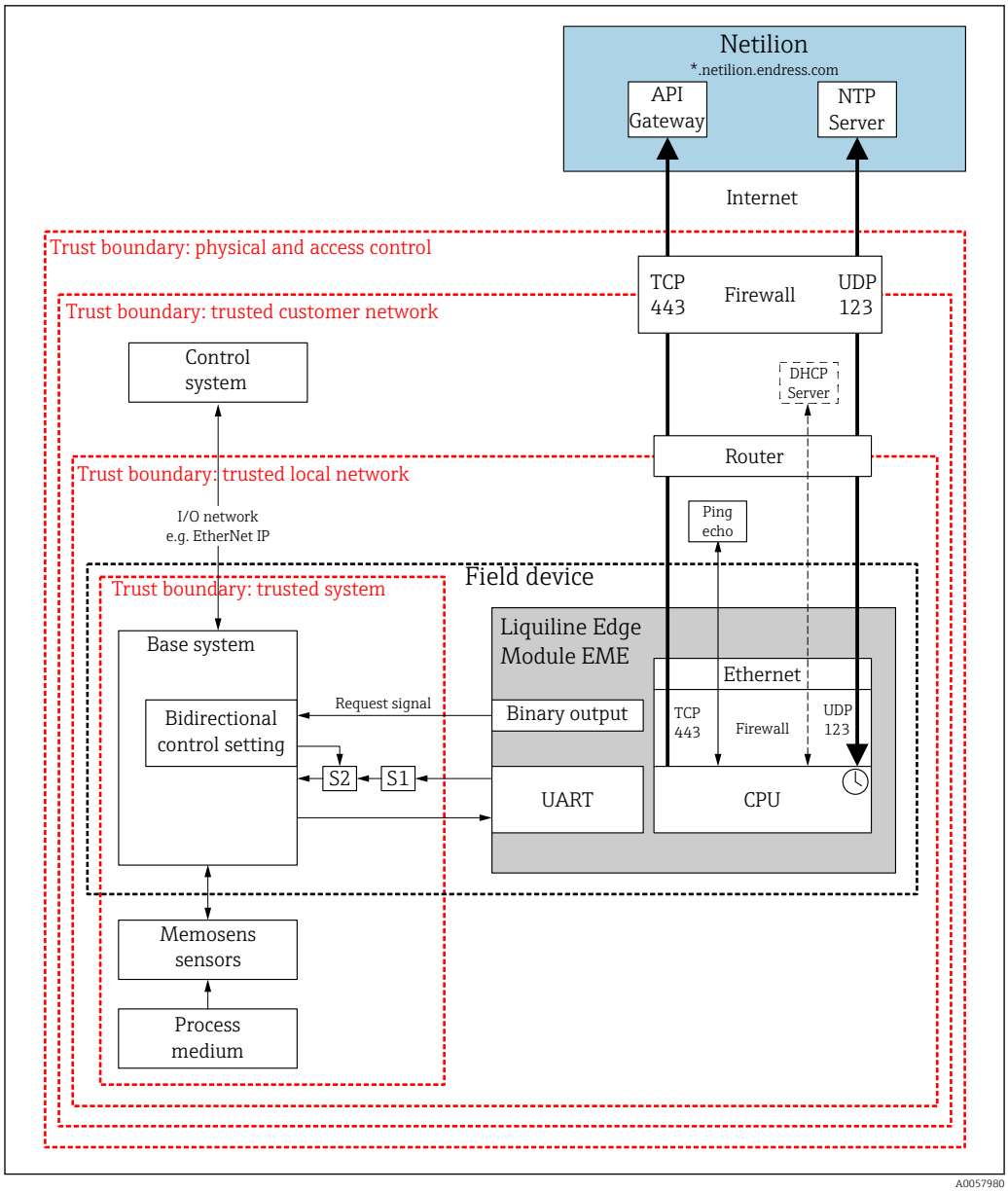
1. Navigieren zu Pfad: **Menü/Allgemeine Einstellungen/Erweitertes Setup/Edge-Modul/Ethernet ETH1/IP-Einstellungen/Manuell einstellen (statisch)**
2. **IP-Adresse**, **Netzmaske**, **Gateway** und **DNS** über das Menü eingeben.
3. Mit dem Softkey **SAVE** übernehmen.

**Firewall-Konfiguration:**

1. Über eine kundenseitige Firewall müssen alle eingehenden Verbindungen zum Edge-Modul blockiert werden.
2. TCP-Port 443 für ausgehende HTTPS-Verbindungen zu **dis.lem.netilion.endress.com** freigeben.
3. UDP-Port 123 für **time.netilion.endress.com** freigeben.

**Firewall-Konfiguration prüfen:**

- Die URL https://api.netilion.endress.com über einen Webbrowser aufrufen. Ein Aufruf dieser Seite muss bei aktivierter Firewall möglich sein.



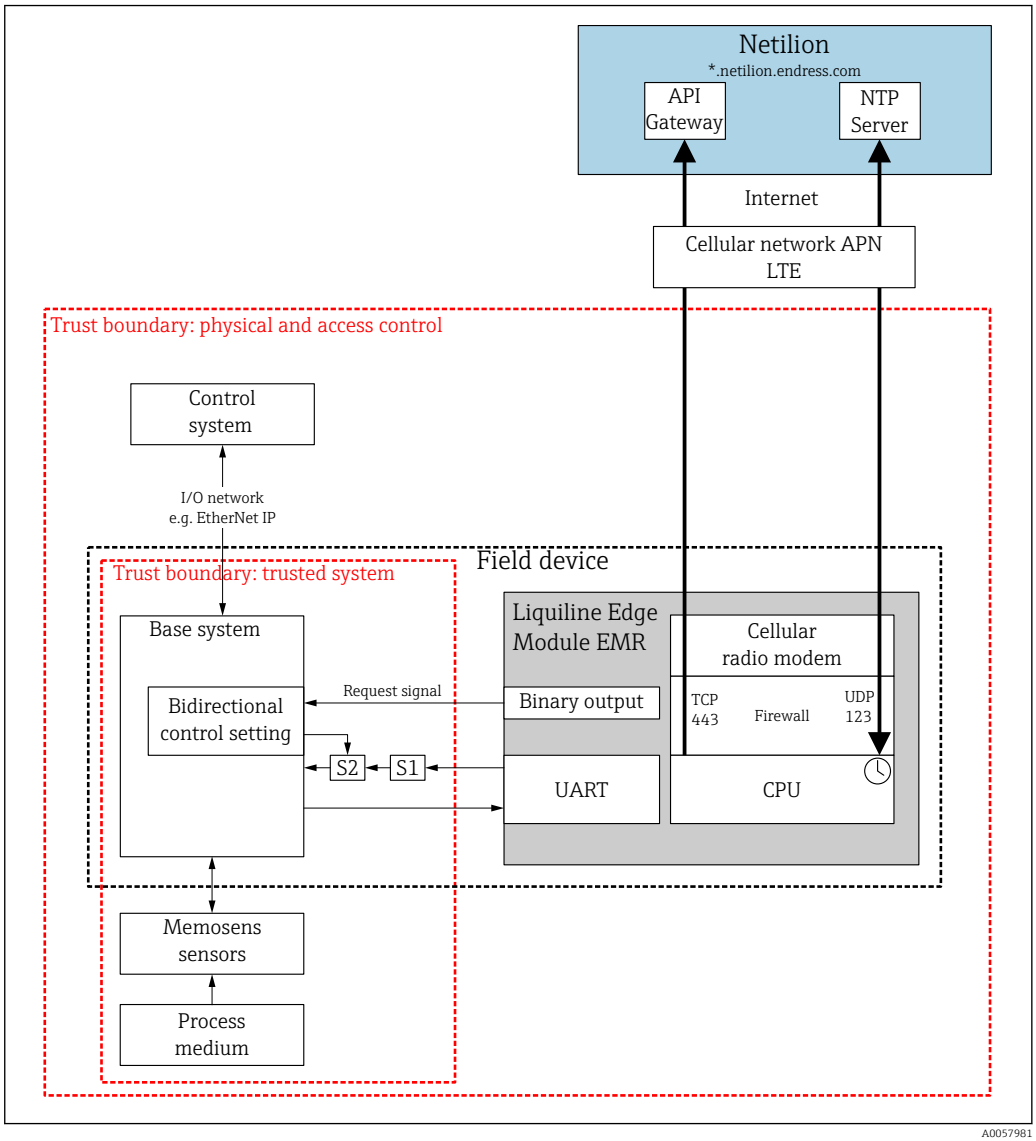

Ping-Anfragen werden vom Edge-Modul nur beantwortet, wenn eine der folgenden Bedingungen erfüllt, ist:
- Die Quell-IP des Pings befindet sich im IPv4-Subnetz der Ethernet-Schnittstelle
- Die Quell-IP des Pings stammt aus dem Adressbereich für Intranet-IPs (RFC 1918)

Das Liquiline Edge Modul akzeptiert keine eingehenden Verbindungen.

Nach dem Hochfahren synchronisiert das Liquiline Edge Modul seine Uhrzeit mit einem von Endress+Hauser bereitgestellten NTP-Server.Anschließend wird eine HTTPS mTLS 1.2 Verbindung zu Netilion aufgebaut. Die TLS-Verbindung verwendet eine Zwei-Wege-Authentifizierung. Jedes Edge-Modul verwendet dazu ein individuelles Client-Zertifikat, das vom Netilion API Gateway validiert wird. Das Edge-Modul überprüft seinerseits das Serverzertifikat der Netilion-Cloud. Die Client-Zertifikate haben eine Ablauf-Dauer von 5 Jahren und werden spätestens 90 Tage vor Ablauf automatisch erneuert.

Wenn die Feldgeräte-Diagnose einen Zertifikat-Fehler anzeigt, den Service von Endress +Hauser kontaktieren.

**Netilion-Verbindung über Mobilfunk**




Nach dem Hochfahren stellt das Edge-Modul über ein Mobilfunknetz (LTE-M oder NB-IoT) eine Internetverbindung her und synchronisiert seine Uhrzeit mit einem von Endress +Hauser bereitgestellten NTP-Server. Anschließend stellt es eine TLS 1.2 Verbindung mit der Netilion Cloud her. Die TLS-Verbindung verwendet eine Zwei-Wege-Authentifizierung. Jedes Edge-Modul verwendet zu diesem Zweck ein individuelles Client-Zertifikat. Das Liquiline Edge Modul prüft das Server-Zertifikat des API-Gateway der Netilion Cloud. Die Client-Zertifikate haben eine Ablaufdauer von 5 Jahren und werden vor Ablauf automatisch erneuert.

Wenn die Feldgeräte-Diagnose einen Zertifikat-Fehler anzeigt, den Service von Endress +Hauser kontaktieren.

## 4.4 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.

## 4.5 Typische Einsatzumgebung des Produkts

Das Edge-Modul wurde für die folgenden Einsatzbedingungen ausgerichtet und optimiert. Sollte die Einsatzumgebung davon abweichen, ggf. weitere Schutzmaßnahmen ergreifen. Das Edge-Modul wird im Rahmen des Produktsicherheitskontexts als Netzwerkgerät betrachtet, da es Daten von einer Sicherheitszone in eine andere überträgt.

Das Edge-Modul wird hauptsächlich in Wasser-/Abwasseraufbereitungsanlagen eingesetzt, in denen ein unbefugter Zugang physisch eingeschränkt ist. Innerhalb des Perimeters ist es unwahrscheinlich, dass es weitere Zugangsbeschränkungen gibt (keine Schränke oder ausgewiesenen Bereiche), sodass das Personal innerhalb der Vertrauenszone in der Regel vom Anlagenbetreiber autorisiert ist und dafür verantwortlich ist, sicherzustellen, dass das Gerät nicht manipuliert wird.

## 4.6 Maßnahmen, falls erforderliche Einsatzumgebung nicht erfüllbar ist

Sofern die spezifizierten Anforderungen an die Einsatzumgebung nicht eingehalten werden können, ggf. Ersatzmaßnahmen vorsehen. 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.

Die Maßnahmen vor physischer Manipulation müssen kundenseitig vorgenommen werden.

## 4.7 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.

## 4.8 Empfehlungen für risikomindernde Maßnahmen

### 4.8.1 Gesamtsystem betrachten

Das Edge-Modul ist ein IIoT-Gateway, das in ein sogenanntes geschlossenes IIoT-Ökosystem eingesetzt wird.

Ein IIoT-Ökosystem kann aufgrund seiner dezentralen Modularität schnell zu einem Stückwerk aus verschiedenen Komponenten werden. Jede abweichende Komponente stellt bei solchen heterogenen Gesamtlösungen eine neue potenzielle Schwachstelle dar, die möglichweise von einem Angreifer ausgenutzt werden kann.

### 4.8.2 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.

### 4.8.3 Zugriffsmanagement optimieren

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

- Mitarbeitern nur die Zugriffsrechte geben, die der Mitarbeiter zur Erfüllung seiner Aufgaben benötigt
- Benutzerkonten (Accounts) nur mit starken Passwörtern vergeben
- Passwörter über einen Passwort-Manager generieren, sichern und verwalten

### 4.8.4 Produkt-Software updaten

Endgeräte für ein IIoT-Ökosystem müssen so entwickelt werden, dass möglichst wenige Nachbesserungen per Updates erforderlich sind. Aufgrund der Dynamik in der IT und den wachsenden Anforderungen in der Vernetzung sind in der Realität Updates erforderlich. Wir empfehlen, regelmäßig zu prüfen, ob neue Updates zur Verfügung stehen und die Updates zu installieren. Versäumte Updates sind ein akutes Security-Risiko, da auch Angreifer über die zu behebenden Schwachstellen informiert sein könnten.

Firmware-Updates können über Netilion oder über SD-Karte installiert werden.

Ein Downgrade auf ältere Firmwareversionen ist nicht möglich.

In Netilion kann das Firmware-Update geplant werden. Das Remote-Firmware-Update so planen, dass das Feldgerät zum geplanten Zeitpunkt für mindestens 30 Minuten nicht vom Netz getrennt oder neu gestartet wird. Die Zeit von der Planung bis zur Update-Installation muss min. 24 h sein. In dieser Zeit wird die Firmware zum Edge-Modul übertragen. Das Firmware-Update beginnt zum geplanten Zeitpunkt.

Während des Firmware-Updates startet das Edge-Modul neu und führt Selbsttests mit der neuen Firmware durch. Im Fehlerfall wird die zuvor installierte Firmwareversion wiederhergestellt. Das Firmware-Update kann erneut versucht werden

### 4.8.5 Anwendungen und Apps schützen

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

Zur Sicherung der Anwendungen, Apps und Cloud-Server sollte auch der Schutz der mobilen und stationären Endgeräte gewährleistet sein, die auf das Steuerungssystem oder das Endgerät Zugriff haben.

Zum Schutz des Kundensystems und der Kundendaten sollte auch der Schutz der Zugangsdaten der Endgeräte gewährleistet sein. Zugangsdaten und Zertifikate sicher aufbewahren.

# 5 Inbetriebnahme

## 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 Installation

Produkt gemäß zugehöriger Kurzanleitung / Betriebsanleitung montieren und elektrisch anschließen.

Um einen physischen Zugriff auf das Gerät zu verhindern, empfehlen wir das Gerät in einem abschließbaren Schaltschrank oder zutrittsgeschützten Raum zu installieren.

Des Weiteren empfehlen wir, weitere externe Maßnahmen zu implementieren wie z.B. eine Netzwerk-Segmentierung, Firewalls, ein Intrusion Detection System und einen Perimeter-Schutz.

## 5.4 Produkt vor Zugriff durch nicht autorisierte Personen schützen

## 5.5 Konfiguration

### 5.5.1 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.

### 5.5.2 Erforderliche Schritte während der Inbetriebnahme

Abhängig von den kundeseitigen Vorgaben bei der Inbetriebnahme Sicherheitseinstellungen vornehmen:

- über den den mechanischen Schalter "bidirektionale/unidirektionale Datenübertragung"
- über die Sicherheitsparameter des Edge-Moduls

Bei Wartungsarbeiten darauf achten, dass bei einer vorübergehenden Änderung der Sicherheitseinstellungen diese wieder entsprechend den Vorgaben hergestellt werden. Weitere Informationen siehe Betriebsanleitung des Edge-Moduls.

### 5.5.3 Firewall konfigurieren

Beim Betrieb über Ethernet ist kundenseitig eine Firewall zum Internet erforderlich.

Erforderliche Firewall-Konfigurationen:
- Alle eingehenden Anrufe zum Edge-Modul müssen blockiert werden.
- TCP-Port 443 für ausgehende HTTPS-Verbindungen zu **dis.lem.netilion.endress.com** freigeben.
- UDP-Port 123 für **time.netilion.endress.com** freigeben.

Firewall-KOnfiguration prüfen:
Die URL https://api.netilion.endress.com über einen Webbrowser aufrufen. Ein Aufruf dieser Seite muss bei aktivierter Firewall möglich sein.

### 5.5.4 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 Edge-Moduls ist nicht möglich und auch nicht erforderlich. Das Edge-Modul ver-wendet nur Dienste, die für die Funktion erforderlich sind.

### 5.5.5 Anwenderdaten konfigurieren

Anwenderdaten sind z. B. Login-Daten. Im Edge-Modul sind keine Anwenderdaten abgelegt. Daten im Pufferspeicher des Edge-Moduls werden automatisch gelöscht, wenn das Edge-Modul in ein anderes Feldgerät gesteckt wird.

### 5.5.6 Security-relevante Einstellungen des Produkts

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

Die Betriebssicherheit des Feldgeräts betreffenden Einstellungen siehe → 14.

# 6 Betrieb

## 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 Aufgaben während des Betriebs

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

In regelmäßigen Abständen prüfen, ob es für das Edge-Modul Firmware-Updates gibt und diese Updates durchführen.

## 6.4 Security-Aspekte während des Betriebs

Wenn das Edge-Modul mit der Netilion-Cloud verbunden ist, wird sein TLS-Zertifikat 90 Tage vor Ablauf automatisch erneuert.

Läuft das Zertifikat ab, während das Edge-Modul offline ist, wird das abgelaufene Zertifikat für die Ausstellung eines neuen Zertifikats akzeptiert und automatisch ersetzt. Dies gilt nicht, wenn das Zertifikat zurückgezogen wurde. In diesem Fall muss der Endress+Hauser Service kontaktiert werden.

## 6.5 Update-Management

Endress+Hauser stellt Remote-Updates über die Netilion Cloud bereit. Der Anwender muss das Update über die Netilion Cloud anstoßen. Der Zeitpunkt für ein Update ist einstellbar. Während aller Updates wird ein Neustart des Edge Moduls automatisch durchgeführt. Der Betrieb des Feldgeräts wird dabei nicht beeinflusst.

Endress+Hauser stellt 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.

Zusätzlich können Updates mittels SD-Karte installiert werden.

## 6.6 Funktionale Erweiterung

Funktionale Erweiterungen werden nach Verfügbarkeit unangekündigt von Endress+Hauser in der Netilion Cloud Plattform ausgeliefert. Der Zeitpunkt der funktionalen Erweiterung wird durch En-dress+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

## 6.7 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.

## 6.8 Reparatur und Entsorgung

Produkt gemäß Betriebsanleitung reparieren oder entsorgen.

# 7 Außerbetriebnahme

## 7.1 Zielgruppe

Dieses Kapitel richtet sich an das Betriebspersonal.

## 7.2 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.

## 7.3 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. | ▶ Keine Maßnahme erforderlich. |
| Das Produkt hat eine Störung und Sie können die Störung nicht beheben. | ▶ Endress+Hauser kontaktieren. |
| Das Produkt soll entsorgt oder veräußert werden. | ▶ Vor der Entsorgung oder Veräußerung das Netilion-Asset des Edge-Moduls löschen. Hierzu werden die Zugangsdaten für den Netilion-Account benötigt. |

# 8 Anhang

## 8.1 Security-Checkliste für den Produktlebenszyklus

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

## 8.2 7.2 Anforderungen der IEC62443-4-2

In Anlehnung an die NAMUR-Empfehlung NE177 erfüllt dieses Produkt folgende Anforderungen der IEC 62443-4-2 gemäß dem Schutzprofil "NOA Security Gateway Basic".

Legende der Spalte "Status":
- ✔: erfüllt
- (✔): nicht anwendbar
- ✗: nicht erfüllt

| Anforderung | Status | Erläuterung |
|---|---|---|
| CR 1.1 Human user identification and authentication | (✔) | Keine Bedienschnittstelle für menschliche Benutzer vorhanden. |
| CR 1.1 RE (1) Unique identification and authentication | (✔) | vgl. CR1.1 |
| CR1.2 Software process and device identification and authentication | ✔ | |
| CR 1.3 Account management | (✔) | vgl. CR1.1 |
| CR 1.4 Identifier management | (✔) | Keine Identifizierer und Identifiziererverwaltung vorhanden, da es keine Schnittstelle zum Anwendernetzwerk gibt. Gegenseitige Identifikation zur Kommunikation mit Netilion erfolgt mit von Endress +Hauser erzeugten Zertifikaten. |
| CR 1.5 Authenticator management | (✔) | Geräteeigene Schlüsselpaare zur Authentifikation über asymmetrische Kryptographie sind geschützt abgelegt und nicht austauschbar. |
| CR 1.5 RE (1) Hardware security for authenticators | (✔) | vgl. CR1.5 |
| NDR 1.6 Wireless access management | (✔) | Keine drahtlose Schnittstelle zum Zugriff auf dieses Produkt vorhanden. |

| Anforderung | Status | Erläuterung |
|---|---|---|
| NDR 1.6 RE(1) Unique identification and authentication | (✔) | vgl. NDR1.6 |
| CR 1.7 Strength of password-based authentication | (✔) | vgl. CR1.1 |
| CR 1.10 Authenticator feedback | (✔) | vgl. CR1.1 |
| CR 1.11 Unsuccessful login attempts | (✔) | vgl. CR1.1 |
| CR 1.12 System use notification | (✔) | vgl. CR1.1 |
| NDR 1.13 Access via untrusted networks | ✔ | |
| CR 1.14 Strength of symmetric key-based authentication | (✔) | vgl. CR1.5 |
| CR 2.1 Authorization enforcement | (✔) | vgl. CR1.1 |
| CR 2.1 RE (1) Authorization enforcement for all users (humans, software processes and devices) | ✔ | |
| CR 2.1 RE (2) Permission mapping to roles | (✔) | vgl. CR1.1 |
| CR 2.1 RE (3) Supervisor override | (✔) | vgl. CR1.1 |
| CR 2.2 Wireless use control | (✔) | vgl. NDR1.6 |
| EDR 2.4 Mobile code | (✔) | Keine Möglichkeit zur Einspeisung oder Abarbeitung von Befehlsdateien, Skripts, Macros oder sonstigem Code vorhanden. |
| EDR 2.4 RE (1) Mobile code authenticity check | (✔) | vgl. EDR2.4 |
| CR 2.5 Session lock | (✔) | Keine Verwendung von Sessions. |
| CR 2.6 Remote session termination | (✔) | vgl. CR 2.5 |
| CR 2.8 Auditable events | ✗ | Da keine Bedienschnittstelle für menschliche Benutzer vorhanden ist, ist auch keine lokale Logbuch-Funktionalität implementiert. |
| CR 2.9 Audit storage capacity | (✔) | vgl. CR2.8 |
| CR 2.10 Response to audit processing failures | (✔) | vgl. CR2.8 |
| CR 2.11 Timestamps | ✔ | |
| CR 2.12 Non-repudiation | (✔) | vgl. CR1.1 |
| EDR 2.13 Use of physical diagnostic and test interfaces | ✔ | |
| CR 3.1 Communication integrity | ✔ | |
| CR 3.1 RE (1) Communication authentication | ✔ | |
| EDR 3.2 Protection from malicious code | (✔) | vgl. EDR 2.4 |
| CR 3.3 Security functionality verification | ✗ | Security Mechanismen sind immer aktiv und können nicht deaktiviert werden. |
| CR 3.4 Software and information integrity | ✗ | vgl. CR 3.3 |
| CR 3.4 RE (1) Authenticity of software and information | (✔) | vgl. 3.4 |
| CR 3.5 Input validation | ✔ | |
| CR 3.6 Deterministic output | ✔ | |
| CR 3.7 Error handling | ✔ | |
| CR 3.8 Session integrity | (✔) | vgl. CR 2.5 |
| CR 3.9 Protection of audit information | (✔) | vgl. CR 2.8 |
| EDR 3.10 Support for updates | ✔ | |
| EDR 3.10 RE (1) Update authenticity and integrity | ✔ | |

| Anforderung | Status | Erläuterung |
|---|---|---|
| EDR 3.12 Provisioning product supplier roots of trust | ✔ | |
| EDR 3.13 Provisioning asset owner roots of trust | (✔) | Kein Betreiberdienst verfügbar, der eine Betreiber Root of Trust erfordert. |
| EDR 3.14 Integrity of the boot process | ✔ | |
| EDR 3.14 RE(1) Authenticity of the boot process | ✔ | |
| CR 4.1 Information confidentiality | ✔ | |
| CR 4.2 Information persistence | ✔ | |
| CR 4.3 Use of cryptography | ✔ | Verwendung von TLS1.2 (u.a. RSA3072, P256, AES) für die secure Connection in die Netilion-Cloud. |
| CR 5.1 Network segmentation | ✔ | |
| NDR 5.2 Zone boundary protection | ✔ | |
| NDR 5.2 RE(1) Deny all, permit by exception | ✔ | |
| NDR 5.3 General purpose, person-to-person communication restrictions | ✔ | |
| CR 6.1 Audit log accessibility | (✔) | vgl. CR 2.8 |
| CR 6.2 Continuous monitoring | ✗ | Kein kontinuierliches Monitoring auf Geräteseite. |
| CR 7.1 Denial of service protection | ✔ | Die eintragbare Last ist limitiert. |
| CR 7.1 RE (1) Manage communication load from component | (✔) | vgl. CR 7.1 |
| CR 7.2 Resource management | ✔ | |
| CR 7.3 Control system backup | ✔ | |
| CR 7.3 RE (1) Backup integrity verification | ✔ | |
| CR 7.4 Control system recovery and reconstitution | ✔ | |
| CR 7.6 Network and security configuration settings | (✔) | Nur ein Kommunikationspfad Richtung Netilion-Cloud. Security Mechanismen fest eingestellt. vgl. CR1.4 Diese Produkt tritt im Netzwerk des Betreibers nicht eigenständig, sondern maximal als Ausstattungsmerkmal eines Messumformers in Erscheinung. |
| CR 7.7 Least functionality | ✔ | |
| CR 7.8 Control system component inventory | (✔) | vgl. CR1.4<br>Diese Produkt tritt im Netzwerk des Betreibers nicht eigenständig, sondern maximal als Ausstattungsmerkmal eines Messumformers in Erscheinung. |

## 8.3 Versionshistorie

| Datum | Firmware-Version Edge-Modul | Änderungen in der Firmware | Dokumentation |
|---|---|---|---|
| 02/2025 | 01.00.00 | Release | SD03377C/07/DE/01.24 |


www.addresses.endress.com

Endress+Hauser

People for Process Automation