OT-Sicherheitsanforderungen für Ethernet-APL-Feldgeräte : Technologischer Wandel kann zu besserem Schutz führen

Karl-Heinz Niemann, Simon Merklin

Suggested citation:

Niemann, Karl-Heinz, and Simon Merklin. 2022. "OT-Sicherheitsanforderungen für Ethernet-APL-Feldgeräte : Technologischer Wandel kann zu besserem Schutz führen." *atp Magazin* 63 (5). https://doi.org/10.25968/opus-2320.

Abstract

Die Konvergenz von Netzwerken ist ein zunehmender Trend im Bereich der Automatisierung. Immer mehr Anlagenbetreiber streben eine Vereinheitlichung der Netzwerke in ihren Anlagen an. Dies führt zu einer nahtlosen Netzwerkstruktur, einer vereinfachten Überwachung und einem geringeren Schulungsaufwand für das Personal, da nur eine einheitliche Netzwerktechnologie gehandhabt werden muss. Ethernet-APL ist ein Teil des Puzzles für ein solches konvergentes Netzwerk und unterstützt verschiedene Echtzeitprotokolle wie PROFINET, EtherNet, HART-IP sowie das Middleware-Protokoll OPC UA. Dieses Papier gibt einen Überblick über die Auswirkungen von Ethernet-APL-Feldgeräten auf die OT-Sicherheit und schlägt vor, wie die OT-Sicherheit für diese Geräte gewährleistet werden kann.

atp magazin

SONDERDRUCK
Transforming Automation
Ausgabe 05 2022

Peer-Review: 02.12.2021

OT-Sicherheitsanforderungen für Ethernet-APL-Feldgeräte

Technologischer Wandel kann zu besserem Schutz führen

Karl-Heinz Niemann, Hochschule Hannover, Simon Merklin, Endress + Hauser Digital Solutions

Zusammenfassung: Die Konvergenz von Netzwerken ist ein zunehmender Trend im Bereich der Automatisierung. Immer mehr Anlagenbetreiber streben eine Vereinheitlichung der Netzwerke in ihren Anlagen an. Dies führt zu einer nahtlosen Netzwerkstruktur, einer vereinfachten Überwachung und einem geringeren Schulungsaufwand für das Personal, da nur eine einheitliche Netzwerktechnologie gehandhabt werden muss. Ethernet-APL ist ein Teil des Puzzles für ein solches konvergentes Netzwerk und unterstützt verschiedene Echtzeitprotokolle wie PROFINET, EtherNet, HART-IP sowie das Middleware-Protokoll OPC UA. Dieses Papier gibt einen Überblick über die Auswirkungen von Ethernet-APL-Feldgeräten auf die OT-Sicherheit und schlägt vor, wie die OT-Sicherheit für diese Geräte gewährleistet werden kann.

#Ethernet-APL #IT-Security #Feldgeräte

1. Die Entwicklung der Systemstrukturen in der Prozessindustrie

Die Prozessindustrie verwendet seit vielen Jahren Systemarchitekturen mit Feldbustechnologie in Kombination mit Ethernet auf den oberen Schichten. Abbildung 1 zeigt die Systemarchitektur eines Automatisierungssystems in der Prozessindustrie.

Die Sensoren und Aktuatoren sind über eine 4 ... 20-mA-Stromschleife an ein Remote-I/O-System angeschlossen, in der Regel mit zusätzlicher HART-Funktionalität. Die Remote-I/Os und andere E/A-Geräte, wie z. B. Frequenzumrichter, sind über einen Feldbus, wie PROFIBUS DP, mit der Steuerung verbunden. In einigen Anlagen verbindet ein Gateway, z. B. ein DP/PA-Koppler, den Feldbus mit einem Sensor-/Aktuator-Bus, wie PROFIBUS PA / Foundation Fieldbus H1. Der Controller ist über Ethernet mit den Bedienkonsolen verbunden. In vielen Fällen ist der Systembus Ethernet-basiert und verwendet entweder ein standardisiertes Protokoll wie PROFINET, EtherNet/IP oder ein steuerungssystemspezifisches Protokoll. Oft sind zusätzliche Server zwischen den Steuerungen und den Bedienkonsolen platziert. Um die Beschreibung zu vereinfachen, werden diese Server nicht Abbildung 1 dargestellt.

Eine Security Appliance verbindet die Leitsystemkomponenten am Systembus mit der übergeordneten Ebene, die durch das Firmennetzwerk repräsentiert wird. In vielen Fällen wird ein zusätzlicher Server, z.B. ein OPC UA Server, zur Anbindung eingesetzt. Die Security Appliance (z.B. eine Multi-Port-Firewall) kann so eingesetzt werden, dass sich der Server in einer sogenannten demilitarisierten Zone (DMZ) befindet. Das System besteht aus vier verschiedenen Netzwerken (Firmennetzwerk, Systembus, Feldbus, Sensor/Aktuator-Bus), die hierarchisch angeordnet sind.

Die im vorigen Abschnitt beschriebenen Feldgeräte liefern den Messwert und ermöglichen darüber hinaus eine digitale Kommunikation, z. B. für Konfigurations- oder Diagnosezwecke. HART und PROFIBUS PA fehlt es an Kommunikationsgeschwindigkeit und damit an Potenzial für zukünftige Anwendungen, die höhere Bandbreiten für Asset Management, Energiemanagement, Firmware-Updates, System-Backups usw. erfordern.

Um diesen Mangel zu beheben, könnte die Verwendung von Ethernet für eine Sensor/Aktuator-Verbindung in Betracht gezogen werden. Der Standard IEEE 802.3cg [1] spezifiziert ein Zweidraht-Ethernet für den Anschluss von Sensoren und Aktuatoren, welches Energie und ausreichende Bandbreite liefert. Die Ethernet-APL-Group hat diesen Standard um eine Port-Profil-Spezifikation [2] erweitert, die es erlaubt, das Zweidraht-Ethernet auch in rauen Umgebungen und in explosionsgefährdeten Bereichen mit einer Vollduplex-Kommunikationsgeschwindigkeit von 10 Mbit/s einzusetzen. Das Ergebnis nennt sich Advanced Physical Layer for Ethernet: Ethernet-APL [3]. Detaillierte Informationen über den Einsatz von Ethernet-APL finden sich in [4]. Ethernet-APL ist ein Physical Layer für Ethernet, der es erlaubt, Sensoren und Aktuatoren

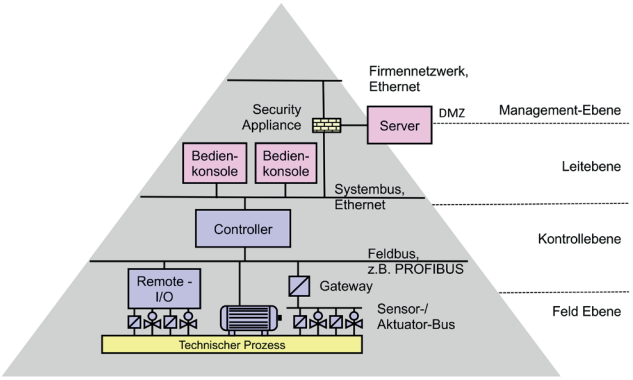

Abbildung 1: Systemarchitektur mit Feldbus, Remote I/O und Sensor- / Aktuator-Bus

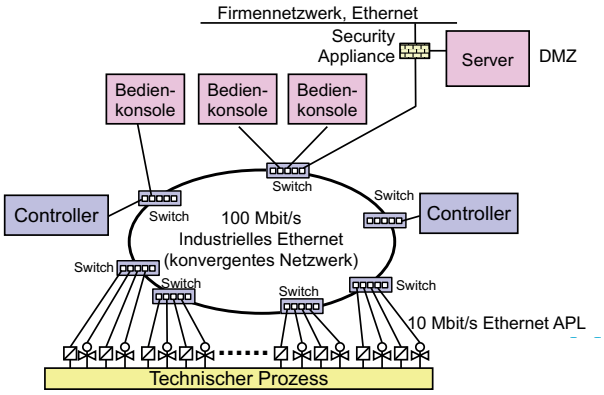

Abbildung 2: Systemstruktur mit APL-Feldgeräten

Tabelle 1: Vergleich der Systemtopologien

Merkmal	Hierarchische Topologie basierend auf verschiedenen Bussen mit Stromschleife und HART	Hierarchische Topologie auf der Grundlage verschiedener Busse	Flache Topologie mit Ethernet-APL und Industrial Ethernet Protokoll.
Verwendete Kommunikationsprotokolle	Ethernet mit Fast-Ethernet-Physical Layer, PROFIBUS DP, Stromschleife mit HART-Protokoll	Ethernet mit Fast Ethernet Physical Layer, PROFIBUS DP, PROFIBUS PA	Physical Layer: Ethernet-APL und Fast-Ethernet
Schulungsaufwand für das Personal	Kenntnisse in allen oben genannten Kommunikationstechnologien erforderlich	Kenntnisse in allen oben genannten Kommunikationstechnologien erforderlich	Nur Kenntnisse für Ethernet erforderlich
Übermittlung von Diagnosedaten vom Gerät an ein Asset-Management-System (AMS)	Muss die verschiedenen Schichten des Systems durchlaufen. Kommunikationsfunktionalitäten in Remote I/Os und Steuerungen erforderlich, die für die Weiterleitung der HART-Diagnosedaten an das AMS sorgen.	Muss die verschiedenen Schichten des Systems durchlaufen. Kommunikations-funktionalitäten in der Steuerung werden benötigt, um die PROFIBUS-PA-Diagnosedaten an das AMS weiterzuleiten.	Direkte Kommunikation zwischen Feldgerät und AMS möglich. Kommunikation über PROFINET, EtherNet/IP oder OPC UA möglich.
Kommunikation von Messwerten	Über 4 ... 20 mA Stromschleife zum Remote IO. Dann über PROFIBUS DP zum Controller	Über PROFIBUS PA zum DP/PA Gateway. Dann über PROFIBUS DP zur Steuerung	Über Ethernet und Protokoll wie PROFINET oder EtherNet/IP direkt zur Steuerung
Genauigkeit der Messwertübertragung	Analoge Übertragung über Stromschleife	Digitale Übertragung	Digitale Übertragung
Verfügbare Datenrate zum Herunterladen eines Parametersatzes auf ein Feldgerät	1,2 kbit/s	31,25 kbit/s	10 000 kbit/s = 10 Mbit/s
Kommunikationsmodus	Halbduplex	Halbduplex	Vollduplex
Komplexität, um einem Cyber-Angreifer Zugang zum Gerät zu verschaffen	Hoch	Mittel	Niedrig

direkt an ein Ethernet-basiertes Netzwerk anzuschließen. Mögliche Systemstrukturen und die Zuordnung zu Ex-Zonen sind in [4] dargestellt. Die Kombination von Ethernet-APL mit einem Sicherheitsprofil wie PROFIsafe [5] ist möglich. Eine kurze Zusammenfassung findet sich in [6].

Im Rahmen dieser Arbeit wird davon ausgegangen, dass die APL-Feldgeräte an ein konvergentes Netzwerk angeschlossen sind, das 100 Mbit/s Industrial Ethernet mit Ethernet-APL mit einer Datenrate von 10 Mbit/s kombiniert, wie in Abbildung 2 dargestellt.

Es ist zu erkennen, dass der Ansatz eines hierarchischen Netzes, wie in Abbildung 1 dargestellt, durch ein flaches, konvergentes Netz ersetzt wurde, wie in Abbildung 2 dargestellt. Das flache, einheitliche Netzwerk auf Basis von

Ethernet hat einige Vorteile, aber auch Nachteile gegenüber der hierarchischen Topologie. Tabelle 1 vergleicht die Anbindung der Feldgeräte mit Stromschleife und HART, PROFIBUS PA und Ethernet-APL.
Es zeigt sich, dass die Ethernet-APL-Topologie eine Reihe von Vorteilen mit sich bringt: Einheitliches Netzwerk, hohe Datenraten, einfache Übertragung von Diagnosedaten an ein Asset-Management-System. Im Hinblick auf die Cybersicherheit hat die flache Netzwerkarchitektur jedoch einen Nachteil: Die Ethernet-APL-Feldgeräte können leichter von einem Eindringling angegriffen werden. Das folgende Kapitel 2 wird sich mit diesem Thema im Detail befassen.

2. Die Exposition der Feldgeräte heute und morgen

Der typische Sicherheitskontext eines Feldgeräts ist wie folgt definiert: Die Anlage ist durch eine Eingrenzung, wie Zäune oder Mauern, geschützt. Der physische Zugriff auf das Gerät ist nur für das in der Anlage arbeitendes Personal und für externe Dienstleister, wie Inbetriebnahme- oder Wartungspersonal, möglich. Das Feldgerät ist entweder mit dem Remote I/O, dem Feldbus (PROFIBUS PA) oder dem Ethernet-Netzwerk verbunden. Das Ethernet-Netzwerk ist vom Büronetzwerk durch eine Security-Appliance, wie z. B. eine Firewall, getrennt. Das Feldgerät hat keine direkte Verbindung zum Internet.
Im Allgemeinen ist ein Feldgerät über verschiedene Schnittstellen für Cyberangriffe anfällig. Dies kann ein lokales Display in Kombination mit lokalen Tasten sein, Bluetooth, Wireless HART, ein Handheld mit kabelgebundenem HART-Modem, die Stromschleife, der Feldbus oder die Ethernet-APL-Verbindung sein. Eine detaillierte Risikoanalyse für ein Feldgerät, die alle beschriebenen Kanäle abdeckt, ist in [7] verfügbar. In diesem Beitrag wird nur auf die Stromschleife / HART, den Feldbus und die Ethernet-APL-Verbindung eingegangen.
Die Exposition eines Feldgeräts muss in den Kontext möglicher Angreifer, entsprechender Angriffsarten und Angriffsorte gestellt werden. In diesem Papier werden drei verschiedene Standorte von Angreifern betrachtet:

- **A1:** Angreifer, der im Büronetz operiert, die Security Appliance überwindet und über das Ethernet-Netzwerk in der OT-Domäne kommunizieren kann (Systembus bzw. konvergentes Netzwerk nach Abbildung 1 und Abbildung 2).
- **A2:** Lokaler Angreifer (Innentäter), der Zugriff auf das Ethernet-Netzwerk in der OT-Domäne hat (Systembus bzw. konvergentes Netzwerk gemäß Abbildung 1 und Abbildung 2).
- **A3:** Lokaler Angreifer (Innentäter), der Zugriff auf die Feldbusse wie PROFIBUS DP, PROFIBUS PA oder auf die Stromschleife mit HART hat und in der Lage ist, die Datenübertragung auf diesen Systemen zu manipulieren.

Abbildung 3: Mögliche Angriffswege

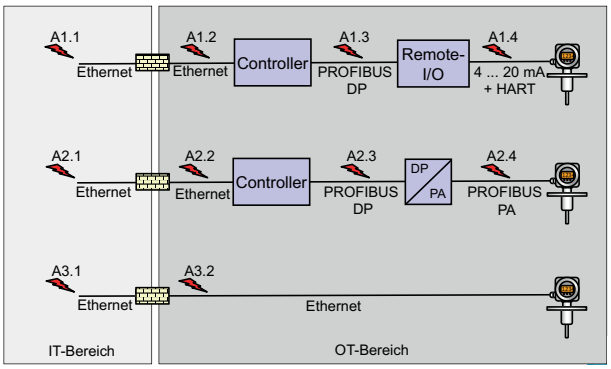

Abbildung 3: Mögliche Verbindungswege zwischen Angreifer und Sensor

Zusätzlich zum Standort des Angreifers sind zwei Arten von Angriffen zu berücksichtigen. Die eine Angriffsart ist ein Denial-of-Service-Angriff. Ein Denial-of-Service-Angriff verhindert den autorisierten Zugriff auf Ressourcen oder führt zu einer Verzögerung von zeitkritischen Operationen [8]. Diese Angriffsart macht die Anlage funktionsunfähig (Shutdown), führt aber nicht dazu, dass manipulierte IO-Werte übertragen werden können. Diese Angriffsart beeinträchtigt das Schutzziel "Verfügbarkeit". Die zweite Angriffsart betrachtet die Manipulation von IO-Werten. Dies würde dazu führen, dass die Steuerung manipulierte, verfälschte Eingangswerte erhält, aber der Angriff führt nicht zu einem sofortigen Stopp der Anlage, wie im ersten Fall. Dieser Angriff beeinträchtigt das Schutzziel "Integrität". Die folgenden Abschnitte werden sich auf diesen Aspekt konzentrieren.
Abbildung 3 zeigt drei verschiedene Systemtopologien und mögliche Angriffspunkte, an denen das Feldgerät angegriffen werden könnte.

Der Fall ❶ beschreibt ein Leitsystem mit PROFIBUS DP, einem Remote I/O und einem Feldgerät, welches über eine 4 ... 20 mA-Stromschleife mit HART-Protokoll angeschlossen ist. Die Angreifer A1.1, A2.1 und A3.1 befinden sich in der IT-Domäne. Um das Feldgerät anzugreifen, sind die folgenden Schritte notwendig: Die Angreifer A1.1, A2.1 und A3.1 müssen die Firewall überwinden oder umgehen. Dann muss die Steuerung so manipuliert werden, dass über PROFIBUS DP Kommandos an das Remote IO gegeben werden, die im Remote IO falsche HART-Kommandos erzeugen, z. B. um den Messbereich des Feldgerätes zu ändern. Die Angreifer A1.2, A2.2 und A3.2 sind Innentäter und müssen die Security Appliance nicht zu überwinden. Der Rest des Angriffs erfolgt, wie zuvor beschrieben. Es ist zu erkennen, dass der beschriebene Angriff auf den Controller abzielt, um das Feldgerät zu manipulieren, aber er ist nicht in der Lage, das Gerät selbst direkt anzugreifen, da Controller und Remote IO zwischen dem Angreifer und dem angegriffenen Gerät liegen.
Die Angreifer A1.3 und A2.3 könnten den PROFIBUS angreifen und z.B. gefälschte Befehle an die Remote IO einfügen, die falsche HART-Befehle an das Feldgerät ausgeben. In [9] beschreibt der Autor mehrere Angriffsvektoren für PROFIBUS DP, die auch für PROFIBUS PA gelten. Angreifer A1.4 könnte

sich in die Stromschleife einklinken und falsche HART-Befehle an das Gerät geben oder sogar einen Widerstand parallel zum Gerät schalten, um den Messwert zu verfälschen. Weitere Angriffsvektoren für HART sind in [10] beschrieben.
Der Fall ❷ beschreibt ein Steuerungssystem mit PROFIBUS DP und PROFIBUS PA oder Foundation Fieldbus H1. Die Angriffsvektoren für die Angreifer A2.1, A2.2 und A2.3 sind dem Fall ❶ sehr ähnlich. Anstelle von gefälschten HART-Kommandos müssen gefälschte PROFIBUS PA-Kommandos, z. B. zur Gerätekonfiguration, verwendet werden. Der Angreifer A2.4 kann sich in den PROFIBUS PA einklinken und die PROFIBUS PA Kommunikation direkt blockieren oder verfälschen.
Fall ❸ stellt ein Automatisierungssystem dar, das die Feldgeräte über Ethernet verbindet, wie es bei Ethernet-APL der Fall ist. Netzwerk-Switches wie Ethernet-APL-Power-Switches und APL-Feld-Switches sind für die Kommunikation transparent und werden daher in Abbildung 3 nicht dargestellt. Diese Topologie ist aus Sicht der Angreifer die einfachste. Nachdem man sich Zugang zum Netzwerk verschafft hat, kann das Feldgerät direkt identifiziert und angegriffen werden, da es z. B. Teil der PROFINET- oder EtherNet/IP-Kommunikation ist. Beispielhafte Angriffe auf ein PROFINET-Gerät sind z. B. in [11] und [12] beschrieben.
Auf den ersten Blick scheint Fall ❸ der problematischste zu sein, da die Angreifer A3.1 und A3.2 direkten Zugriff auf das Gerät erhalten, ohne dass irgendwelche Geräte dazwischengeschaltet sind und ohne dass sich die Übertragungsmedien oder das Übertragungsprotokoll ändern. Das ist richtig, wenn keine Schutzmaßnahmen getroffen werden. Wenn jedoch die Kommunikation zum Feldgerät durch kryptografische Mittel geschützt ist, wird die Komplexität eines Angriffs im Vergleich zu Fall ❶ und ❷ als komplexer angesehen. Die Standards Developing Organizations (SDOs) bieten heute bereits eine sichere Kommunikation für PROFINET [13, 14], EtherNet/IP [15, 16] oder OPC UA [17, 18] an oder arbeiten daran.

Die Schlussfolgerung dieses Abschnitts lässt sich wie folgt zusammenfassen:

» PROFIBUS DP, PROFIBUS PA und HART können ohne großen Aufwand angegriffen werden. Mögliche Angriffe sind bekannt und dokumentiert.

Tabelle 2: Sicherheitskonzepte und Empfehlungen sowie Verweise auf weitere Informationen

Nr.	Sicherheitskonzepte und Empfehlungen	Erläuterung
1	Managementsystem für Informationssicherheit (ISMS)	Ein ISMS ist der elementare Bestandteil einer erfolgreichen Umsetzung von Cyber-Sicherheitsmaßnahmen in einer verfahrenstechnischen Anlage und der Organisation selbst. Idealerweise sollte das ISMS nach IEC 62443-2-1 [21] implementiert werden. Alternativ kann es auch nach ISO 27001 [22] aufgebaut werden. Ein Vergleich der beiden Ansätze kann in [23] nachgelesen werden.
2	Defense-in-Depth	Grundsätzlich ist es nicht empfehlenswert, die Sicherheitsvorgaben mit nur einer Schutzmaßnahme zu erfüllen. Aus diesem Grund beschreibt der Defense -in-Depth-Ansatz die Nutzung von koordinierten Schutzmaßnahmen durch verschiedene Sicherheitsebenen in einer Anlage [24]. Für weitere Informationen wird auch auf [25] verwiesen.
3	Zoneneinteilung der Anlage	Es wird empfohlen, die verfahrenstechnische Anlage in Zonen mit unterschiedlichen Sicherheitsvorgaben zu unterteilen. Dadurch wird sichergestellt, dass jede Zone der Anlage das optimale Maß an Sicherheitsmaßnahmen erhält [21].
4	Vertikale und horizontale Segmentierung	Die Zonen sollten vertikal und horizontal segmentiert werden. So wird einerseits ein Angriff von außen erschwert (vertikale Zonierung) und gleichzeitig kann ein Angriff im Falle einer Kompromittierung auf andere Zellen verhindert werden (horizontale Zonierung) [21].
5	Schutz der Zonengrenzen	Die Zonengrenzen einer Anlage sollten durch geeignete Schutzmaßnahmen geschützt werden. Dies kann durch den Einsatz von Sicherheitseinrichtungen, wie z. B. Firewalls, geschehen. Beim Schutz der Zonengrenzen sollte auch der physische Zugangsschutz in Bezug auf Personen berücksichtigt werden [21].
6	Schutz der Kommunikation zwischen Feldgeräten und Controller	Die Kommunikation in einer Zone sollte durch kryptographische Methoden (Integrität und Authentizität) gesichert werden [26].
7	Eindeutiger Nachweis der Identität und Authentifizierung von Geräten in einer Zone	Die Geräte sollten in der Lage sein, sich mit kryptografischen Methoden in einer Zone zu identifizieren [27].
8	Einsatz von sicheren Feldgeräten	Die Komponenten sollten gemäß dem Secure Development Lifecycle nach 62443-4-1 [27] entwickelt werden und die Anforderungen von 62443-4-2 [20] erfüllen.

Tabelle 3: Beispiele für potenzielle Bedrohungen und entsprechende Schutzmaßnahmen

Nr.	Potenzielle Bedrohungen	Mögliche Schutzmaßnahmen	Bezug auf IEC 62443-4-2 [20]
1	Der Angreifer verändert die Kommunikationsdaten im Netzwerk	Integrität und Authentizität der Kommunikation - Die Integrität und Authentizität der Netzkommunikation zwischen Ethernet-APL-Feldgeräten sollte durch kryptografische Methoden gesichert werden. Dies kann durch ein sicheres Protokoll in Kombination mit einer Public Key Infrastructure (PKI), wie in Abschnitt 4 beschrieben, erreicht werden.	CR 3.1/ CR 3.1 RE (1)
2	Angreifer nimmt ohne Authentifizierung an der Netzwerkkommunikation teil	Authentifizierung der Geräte - Ethernet-APL-Feldgeräte und andere Komponenten müssen in der Lage sein, sich gegenseitig zu authentifizieren. Dies kann durch ein sicheres Protokoll in Kombination mit einer Public Key Infrastructure in der Anlage erreicht werden. (siehe Abschnitt 4)	CR 1.8
3	Angreifer gibt sich als APL Field Device aus	Das Ethernet-APL-Feldgerät muss in der Lage sein, die Echtheit von Hardware und Firmware zu beweisen. Dies kann mit Hilfe von kryptographischen Hashes [20] erfolgen.	EDR 3.12
4	Angreifer manipuliert die Firmware des Geräts	Die Integrität und Authentizität des Bootvorgangs ist ein entscheidendes Merkmal, um sicherzustellen, dass die Gerätefirmware nicht von einem Angreifer manipuliert wurde. Aus diesem Grund muss das Ethernet-APL-Feldgerät während des Bootvorgangs Authentizitätsprüfungen durchführen, um sicherzustellen, dass das Gerät nicht in einen unsicheren oder manipulierten Zustand bootet.	EDR 3.14 EDR 3.14 RE(1)
5	Angreifer manipuliert Firmware durch Update	Das Ethernet-APL-Feldgerät ist updatefähig und akzeptiert nur signierte Firmware vom Hersteller.	EDR 3.10 EDR 3.10 RE (1)
6	Angreifer verschafft sich Zugang zu sensiblen Daten (wie Anmeldeinformationen und Authentifikatoren) von Ethernet-APL-Geräten	Vertraulichkeit der kritischen Daten: Das Ethernet-APL-Feldgerät schützt Daten, die für den sicheren Betrieb der Anlage entscheidend sind.	CR 4.1
7	Der Angreifer führt einen DoS-Angriff auf das Netz durch	Das APL-Feldgerät schützt sich gegen DoS-Angriffe, um die wesentliche Funktionalität des Gerätes zu erhalten. Dies kann z.B. dadurch geschehen, dass Datenpakete, die das Gerät erreichen und für die wesentliche Funktion des Gerätes nicht relevant sind, verworfen werden.	CR 7.1
8	Besondere Anforderungen an Ethernet-APL-Feldgeräte, wie lange Produktlebensdauer und Ressourcenbeschränkungen	Beim Gerätedesign sollte berücksichtigt werden, dass Ethernet-APL-Feldgeräte mitunter eine sehr lange Produktlebensdauer haben. Ein angemessenes Schutzniveau der verwendeten kryptografischen Algorithmen sollte ebenfalls berücksichtigt werden, ebenso wie die besonderen Anforderungen für Geräte mit eingeschränkten Ressourcen [26].	---

» Es ist nicht zu erwarten, dass HART, PROFIBUS DP und PROFIBUS PA in Zukunft mit Sicherheitsfunktionen aufgerüstet werden.

» Die einzige Möglichkeit für eine sichere Kommunikation von IO-Werten vom Feld zur Steuerung ist die Verwendung eines Ethernet-basierten Protokolls in Kombination mit den Protokollen, die Sicherheitsmechanismen unterstützen.

Daraus ergibt sich, dass Ethernet-APL-Feldgeräte die Sicherheitsfunktionen des von ihnen unterstützten Kommunikationsprotokolls (z. B. PROFINET, EtherNet/IP und/oder OPC UA) unterstützen müssen. Bei der Entwicklung sind Vorkehrungen hinsichtlich der Rechenleistung, der Speichergröße und gegebenenfalls der Bereitstellung eines sicheren Elements (z. B. eines Trusted Platform Module o. ä.) zu berücksichtigen. Denial-of-Service-Angriffe müssen bis zu einem gewissen Grad berücksichtigt werden, auch wenn davon ausgegangen wird, dass die Geräte nicht direkt mit dem Internet verbunden sind und in einer geschützten Umgebung arbeiten.
Der nächste Abschnitt zeigt im Detail, welche Sicherheitsanforderungen ein Ethernet-APL-Feldgerät erfüllen muss.

3. OT-Security-Anforderungen für Ethernet-APL-Feldgeräte

Für die Definition der Sicherheitsanforderungen einer verfahrenstechnischen Anlage mit Ethernet-APL-Feldgeräten sollten die Design- und Schutzmechanismen nach den Grundkonzepten der IEC 62443-1-1 [19] berücksichtigt werden.

Dieser Schritt ist wichtig, da viele Komponentenanforderungen (CRs) und Anforderungserweiterungen (REs) der 62443-4-2 [20] zur Erfüllung der Anforderungen der IEC 62443-1-1 [19] beitragen. Ein Auszug aus den Konzepten und Empfehlungen für eine sicheres Automatisierungssystem ist aus der 62443-1-1 abgeleitet und in Tabelle 2 dargestellt.

Ein Ethernet-APL-Feldgerät sollte nach dem Secure Development Lifecycle gemäß 62443-4-1 [27] entwickelt werden. Dadurch wird sichergestellt, dass das Gerät die Sicherheitsanforderungen erfüllt, die für den beabsichtigten Einsatz des Geräts angemessen sind. Beispiele für die erfolgreiche Durchführung des Prozesses sind eine Bedrohungsanalyse und ein Anforderungsmanagement, eine Defense-in-Depth-Strategie, sichere Kodierungskonventionen sowie eine Dokumentation der Sicherheitsmerkmale

Die in Tabelle 3 aufgeführten Beispiele sind eine Auswahl potenzieller Bedrohungen und Schutzmaßnahmen, die für ein sicheres Ethernet-APL-Feldgerät erforderlich sind. Aufgrund des begrenzten Umfangs dieses Beitrages werden in Tabelle 3 nur die wichtigsten Anforderungen aufgeführt. Um weiteren Bedrohungen in einer Ethernet-APL-Prozessanlage begegnen zu können, sind weitere Schutzmaßnahmen notwendig.

4. Sichere Kommunikation in der OT-Domäne

Wie in Abschnitt 3 beschrieben, ist die sichere Kommunikation im OT-Umfeld eines der zentralen Bestandteile eines Sicherheitskonzepts für ein Ethernet-APL-System. Die Kombination aus der Verwendung von Industrial-Ethernet-Sicherheitskonzepten sowie der Implementierung einer Topologie analog zum NOA-Sicherheitskonzept (Second Channel) verspricht die Lösung vieler OT-Sicherheitsherausforderungen [28, 29].

Im folgenden Abschnitt wird näher darauf eingegangen, wie die Kommunikation einer Prozessanlage gesichert werden kann. Die Standards-entwickelnden-Organisationen wie PI, ODVA und OPC Founation verwendn ein gesichertes Kommunikationsprotokoll in Kombination mit einer Public Key Infrastructure (PKI).

Dies ermöglicht:

» Sicherstellung der Integrität und Authentizität der Kommunikations(partner): Hierdurch wird sichergestellt, dass die an einen Kommunikationspartner gesendeten Daten während der Übertragung nicht verändert wurden und auch von einem vertrauenswürdigen Kommunikationspartner stammen.

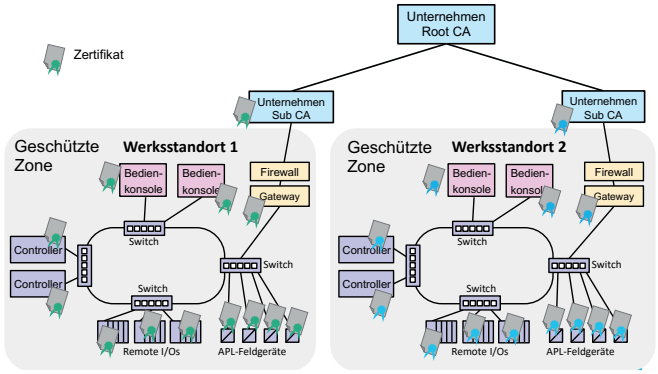

Abbildung 4: PKI-Einrichtung im verteilten Automatisierungssystem

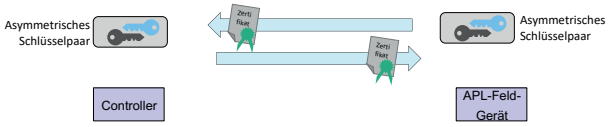

Abbildung 5: Austausch öffentlicher Schlüssel

» Authentifizierung der Geräte im Netzwerk: Die Ethernet-APL-Feldgeräte im Netzwerk kommunizieren nur mit vertrauenswürdigen Kommunikationspartnern.

» Verschlüsselung für bestimmte Anwendungsfälle, z. B. Konfigurationsdaten: Ein Teil der Kommunikation zwischen Komponenten wird verschlüsselt. Diese Funktion macht es für Angreifer unmöglich, die aufgezeichnete Kommunikation im Netz zu verstehen. Die Verschlüsselung unterstützt den Aspekt der Vertraulichkeit, z. B. bei Produktionsrezepten.

Eine Public Key Infrastructure (PKI) ist ein System, das die Kommunikation von Ethernet-APL-Feldgeräten und anderen Komponenten durch das Ausstellen, Verteilen, Validieren und ggf. Widerrufen von digitalen Zertifikaten absichert.

Ein digitales Zertifikat ist ein digitaler Datensatz, der nach Standards wie X.509 [30] aufgebaut ist. Durch die Verwendung von digitalen Zertifikaten ist es möglich, dem Ethernet-APL-Feldgerät eine kryptographische Identität zuzuordnen, die zur Identifikation eines Gerätes im PKI-System und beim Verbindungsaufbau verwendet werden kann. Ebenso kann die vom Gerät ausgehende Kommunikation durch andere PKI-Teilnehmer authentifiziert werden.

Eine Zertifizierungsstelle (CA) stellt ein Stammzertifikat zur Verfügung und signiert die Signaturanforderungen der Sub-CAs. Durch diese Methode kann ein hierarchisches Vertrauen aufgebaut werden. Die Sub-CAs übernehmen die Verwaltung der Zertifikate in den verschiedenen Anlagenteilen. Je nach Größe der Anlage kann es auch sinnvoll sein, Sub-CAs in verfahrenstechnischen Anlagen einzuführen, um die Verwaltung der privaten Schlüssel der Sub-CAs zu vereinfachen. Wird ein Zertifikat vor Ablauf seiner Lebensdauer kompromittiert, kann es mittels einer Certificate Revocation List (CRL) im PKI-System widerrufen werden [31].

Abbildung 4 zeigt einen möglichen PKI-Aufbau für ein Unternehmen mit einer verteilten Anlage. Die Root-Zertifizierungsstelle (Root-CA) stellt die Vertrauensbasis für die Zertifikate des Unternehmens dar. Verschiedene Werksstandorte können dann ihre Sub-CA einrichten, um Zertifikate für den jeweiligen Standort bereitzustellen. Alle Komponenten des Systems erhalten dann Zertifikate von dieser Sub-CA als Vertrauensbasis für den Aufbau einer sicheren Kommunikation. Ein Vorschlag und eine detaillierte Beschreibung einer PKI für den Einsatz in dezentralen Automatisierungssystemen ist in [32] zu finden.
Sobald die PKI, wie in Abbildung 4 dargestellt, eingerichtet ist und sobald die digitalen Zertifikate an die Ethernet-APL-Feldgeräte und alle anderen Komponenten verteilt wurden, können sie sich gegenseitig authentifizieren.
Der Mechanismus der gegenseitigen Authentifizierung erfolgt während des Hochlaufs der Kommunikation durch Senden des jeweiligen öffentlichen Schlüssels (Teil des Zertifikats) an den Kommunikationspartner. Siehe Abbildung 5.

Der Kommunikationspartner kann den öffentlichen Schlüssel verwenden, um die vom Kommunikationspartner gesendeten signierten oder verschlüsselten Daten zu verifizieren. Auf der Basis dieses sicheren Kommunikationsaufbaus mit den asymmetrischen Schlüsseln können die Geräte dann auf eine Kommunikation mit symmetrischen Schlüsseln umschalten, die weniger Rechenaufwand erfordern. Für PROFINET ist die sichere Kommunikation in einer Übersicht in [33] beschrieben. Die entsprechenden aktualisierten PROFINET-Spezifikationen [34, 35] sind derzeit in Arbeit. Für EtherNet/IP [36] [16] und OPC UA [17] gibt es bereits Spezifikationen zur sicheren Kommunikation.

Um Ethernet-APL-Feldgeräte auf sichere Weise in die Kommunikation einzubinden, müssen sie ein gesichertes Kommunikationsprotokoll unterstützen, wie zum Beispiel PROFINET, EtherNet/IP oder OPC UA. Alle drei Protokolle unterstützen oder werden künftig eine sichere Kommunikation unterstützen.

5. Zusammenfassung und Ausblick

Das Papier zeigte, dass Ethernet-APL Feldgeräte potenziellen Angriffen ausgesetzt sind. Die flache Netzwerkstruktur bietet Angreifern einen einfachen Zugang zu den Geräten, da sie direkt mit dem Anlagennetzwerk verbunden sind. Daraus ergibt sich die Anforderung, dass für Ethernet-APL-Geräte eine sichere Kommunikation benötigt wird. Die Sicherheitsanforderungen für Automatisierungskomponenten, wie sie in der IEC 62443-4-2 [20] beschrieben sind, gelten daher auch für APL-Geräte. Sie müssen in der gleichen Weise behandelt werden wie bei Steuerungen oder Remote I/Os. Durch die Verwendung eines sicheren Kommunikationsprotokolls, wie es in [33] beschrieben ist, ist es erstmals möglich, die Integrität und Authentizität der Sensorwerte vom Sensor zum Controller und vom Controller zum Aktuator zu schützen. Dies ist derzeit mit HART oder PROFIBUS PA nicht möglich. Neben der sicheren Kommunikation soll ein Defense-in-Depth-Konzept den Anlagenbereich gegen Angriffe von außen schützen. Hersteller von Ethernet-APL-Feldgeräten sollten die zukünftige Integration einer Sicherheitsschicht planen und ausreichend Ressourcen (Speicher, Rechenleistung, evtl. ein sicheres Element wie ein Trusted Platform Module o.ä.) in ihren Geräten vorsehen.

Referenzen

[1] IEEE Standard for Ethernet - Amendment 5: Physical Layer Specifications and Management Parameters for 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductors, IEEE 802.3cg-2019, IEEE Computer Society, Nov. 2019. URL: https://standards.ieee.org/standard/802_3cg-2019.html.

[2] APL Projekt, Ethernet APL Port Profil Spezifikation: Ethernet-APL Netzwerk- und Port-Anforderungen. URL: https://www.profibus.com/download/port-profile-specification-ethernet-apl.

[3] PROFIBUS und PROFINET Intenational, ODVA Inc., OPC-Foundation und FieldComm Group, Ethernet to the field: White Paper. [Online]. Available: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=107608&token=97abc376e3e83e010df1902d93deba94d1a30d22

[4] K.-H. Niemann, Ethernet APL Engineering Leitfaden: Planung, Installation und Inbetriebnahme von Ethernet-APL-Netzwerken. URL: https://www.profibus.com/download/engineering-guideline-ethernet-apl.

[5] Profibus Nutzerorganisation e. V., PROFIsafe - Profil für Sicherheitstechnik an PROFIBUS DP und PROFINET IO: Profilteil, bezogen auf IEC 61784-3-3. URL: https://www.profibus.com/download/profisafe.

[6] K.-H. Niemann, „Der Ethernet-APL-Engineering-Prozess: Ein kurzer Blick auf die Ethernet-APL-Engineering-Richtlinie“, atp Magazin, Nr. 9, S. 78-83, 2021, doi: 10.25968/opus-2087.

[7] K.-H. Niemann und M. Hoh, „Anforderungen an die IT-Sicherheit von Feldgeräten: Schutzlösungen für hoch vernetzte Produktionsanlagen,“ atp-edition, vol. 59, no. 12, pp. 42-53, 2017.

[8] Eine Einführung in die Informationssicherheit, NIST 800-12, NIST National Institute of Standards and Technology. URL: https://doi.org/10.6028/NIST.SP.800-12r1.

[9] V. M. Igure, Sicherheitsbewertung von SCADA-Protokollen: Eine taxonomiebasierte Methodik zur Identifizierung von Sicherheitsschwachstellen in SCADA-Protokollen. Saarbrücken: AV Akademikerverlag, 2012.

[10] A. U. Bhurke und F. Kazi, „Methods of Formal Analysis for ICS Protocols and HART - IP CPN modelling,“ in 2021 Asian Conference on Innovation in Technology (ASIANCON), PUNE, India, Aug. 2021 - Aug. 2021, pp. 1-7.

[11] M. Runde, „Echtzeitfähige Protokollerweiterung zum Schutz Ethernet-basierter Automatisierungskomponenten: Dissertation zur Erlangung des akademischen Grades Doktoringenieur (Dr.-Ing.)“, Dissertation, Otto von Guericke Universität, Magdeburg, 2014. Accessed: 17. Dezember 2014. URN: urn://nbn:de:gbv:ma9:1-5041. URL: https://d-nb.info/1057913936/34 .

[12] S. Mehner und H. König, „No Need to Marry to Change Your Name! Attacking Profinet IO Automation Networks Using DCP,“ in Lecture Notes in Computer Science, Detection of Intrusions and Malware, and Vulnerability Assessment, Perdisci, Ed., Cham: Springer International Publishing, 2019, pp. 396-414.

[13] PROFIBUS Nutzerorganisation e.V., PROFINET Sicherheitsleitfaden. URL: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=47893&token=f543743e30d8aa3b51b883d00cdc304926678fe8

[14] K.-H. Niemann, „IT security extensions for PROFINET," in 2019 IEEE 17th International Conference on Industrial Informatics (INDIN), Helsinki, Finland, Jul. 2019 - Jul. 2019, pp. 407-412.

[15] ODVA Inc, Absicherung von Ethernet/IP-Netzwerken. URL: https://www.odva.org/wp-content/uploads/2020/05/PUB00269R1.1_ODVA-Securing-EtherNetIP-Networks.pdf.

[16] J. Visoky und J. Wiberg, CIP-Sicherheit und IEC 62443-4-2. URL: https://www.odva.org/wp-content/uploads/2020/05/2020-ODVA-Conference_CIP_Security_and_IEC_62443_Visoky_Wiberg_Final.pdf.

[17] OPC Unified Architecture - Teil 2: Sicherheitsmodell, IEC TR 62541-2:2020, IEC- International Electrotechnical Commission, Nov. 2020. URL: https://webstore.iec.ch/publication/61110.

[18] Bundesamt für Sicherheit in der Informationstechnik (BSI), Sicherheitsanalyse OPC UA. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/OPCUA/OPCUA.pdf?__blob=publicationFile&v=2.

[19] IEC - Internationale Elektrotechnische Kommission: Industrielle Kommunikationsnetze - Netz- und Systemsicherheit - Teil 1-1: Terminologie, Konzepte und Modelle, IEC TS 62443-1-1:2009. URL: https://webstore.iec.ch/preview/info_iec62443-1-1%7Bed1.0%7Den.pdf

[20] [IEC- Internationale Elektrotechnische Kommission: Sicherheit für industrielle Automatisierungs- und Steuerungssysteme - Teil 4-2: Technische Sicherheitsanforderungen für IACS-Komponenten, IEC 62443-4-2, , Feb. 2019. URL: https://webstore.iec.ch/publication/34421.

[21] IEC- Internationale Elektrotechnische Kommission: Industrielle Kommunikationsnetze - Netz- und Systemsicherheit - Teil 2-1: Einrichtung eines Sicherheitsprogramms für industrielle Automatisierungs- und Steuerungssysteme, IEC 62443-2-1-2010, Nov. 2010. URL: https://webstore.iec.ch/publication/7030.

[22] CEN und CENELEC: Informationstechnik - Sicherheitstechniken - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 mit Cor 1:2014 und Cor 2:2015), EN ISO/IEC 27001, , Feb. 2017.

[23] K.-H. Niemann, Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443 : eine Sicht auf automatisierungstechnische Anlagen der Fertigungs- und Prozessindustrie. URL: https://doi.org/10.25968/opus-1973.

[24] IEC- Internationale Elektrotechnische Kommission: Sicherheit für industrielle Automatisierungs- und Steuerungssysteme - Teil 2-2: IACS-Schutzstufen, IEC 62443-2-2 TC65/717/NP, , Sep. 2018.

[25] Department of Homeland Security, Empfohlene Praxis: Verbesserung der Cybersicherheit von industriellen Steuerungssystemen mit Defense-in-Depth-Strategien. URL: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[26] K.-H. Niemann, „IT-Security-Konzepte für die Prozessindustrie: Anforderungen im Kontext von Industrie 4.0", atp-edition, Bd. 56, 7-8/2014, S. 62-69, 2014.

[27] Sicherheit für industrielle Automatisierungs- und Steuerungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus der sicheren Produktentwicklung, IEC 62443-4-1, IEC- International Electrotechnical Commission, Jan. 2018.

[28] NAMUR Open Architecture - NOA Konzept, NE 175, NAMUR - Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, Jul. 2020.

[29] T. Tauchnitz, Hrsg., NAMUR Offene Architektur (NOA): Das Konzept zur Öffnung der Prozessautomatisierung, 1st ed. Essen: Vulkan Verlag, 2021.

[30] ISO - Internationale Organisation für Normung; IEC - Internationale Elektrotechnische Kommission: Informationstechnik - Open Systems Interconnection - Das Verzeichnis - Teil 8: Rahmenwerke für Public-Key- und Attribut-Zertifikate, ISO/IEC 9594-8:2020, , Nov. 2020. URL: https://www.iso.org/standard/80325.html.

[31] Network Working Group IETF: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, , Mai. 2008. URL: https://datatracker.ietf.org/doc/html/rfc5280.

[32] S. Tebbje, G. Karthikeyan, M. Friesen, K. Steinke, S. Heiss, and K.-H. Niemann, Entwicklung einer IT-Sicherheitsinfrastruktur für verteilte Automatisierungssysteme: Schlussbericht zu IGF-Vorhaben Nr. 19117 N. URL: https://doi.org/10.25968/opus-1626.

[33] PROFIBUS Nutzerorganisation e.V., Sicherheitserweiterungen für PROFINET - PI White Paper für PROFINET. URL: https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/.

[34] PROFIBUS Nutzerorganisation e.V., Application Layer Protokoll für dezentrale Peripherie Technische Spezifikation für PROFINET IO: Version 2.4 MU3 - Juni 2022. URL: https://www.profibus.com/download/profinet-specification.

[35] PROFIBUS Nutzerorganisation e.V., Application Layer Services für die dezentrale Peripherie: Technische Spezifikation für PROFINET IO, Version 2.4 MU3 - Juni 2022. URL: https://de.profibus.com/downloads/profinet-specification/.

[36] ODVA Inc, Überblick über die CIP-Sicherheit. [Online]. Verfügbar: https://www.odva.org/wp-content/uploads/2020/05/PUB00319R1_CIP-Security-At-a-Glance.pdf.

AUTOREN

Prof. Dr.-Ing. Karl-Heinz Niemann (geb. 1959) vertritt seit 2005 die Bereiche Industrieinformatik und Automatisierungstechnik an der Hochschule Hannover. Von 2002 bis 2005 war er an der Fachhochschule Nordostniedersachsen (heute Leuphana Universität) für den Bereich Prozessdatenverarbeitung zuständig. Zuvor war er in führenden Positionen in der Entwicklung von Prozessleitsystemen bei ABB, Elsag Bailey und Hartmann & Braun tätig.

Prof. Dr.-Ing. Karl-Heinz Niemann
Hochschule Hannover
Fakultät I – Elektro- und Informationstechnik
Postfach 92 02 61
30441 Hannover
✆ +49 511 92 96 12 64
@ karl-heinz.niemann@HS-Hannover.de

M. Sc. Simon Merklin (geb. 1989) ist Cyber Security Spezialist und Leiter des Product Security Marketings bei Endress+Hauser. Er hat am Karlsruher Institut für Technologie Wirtschaftsinformatik mit Schwerpunkt Sicherheit und Kryptographie studiert und seine Masterarbeit über Distributed Ledger Technologies geschrieben. Darüber hinaus war er an der IEC 62443-4-1 Zertifizierung von Endress+Hauser beteiligt und ist Mitglied der PROFINET Security Working Group bei PROFIBUS und PROFINET International.

M. Sc. Simon Merklin
Endress+Hauser Digital Solutions
Christoph Merian-Ring 12
4153 Reinach
Switzerland
@ simon.merklin@endress.com