Hochschule Karlsruhe – Technik und Wirtschaft
Fakultät für Elektro- und Informationstechnik

Sicherer Verbindungsaufbau für nicht netzwerkfähige Feldgeräte auf Basis von Zertifikaten

Masterthesis (M. Sc.)

von
Kilian Nikolaus Rupp

Hochschule Karlsruhe – Technik und Wirtschaft
Fakultät für Elektro- und Informationstechnik

Sicherer Verbindungsaufbau für nicht netzwerkfähige Feldgeräte auf Basis von Zertifikaten

Masterthesis (M. Sc.)

von
Kilian Nikolaus Rupp
geb. am 06.01.1998
in Saarlouis
Matr.-Nr.: 67723

Betreuer der Firma Hager Group
M. Sc. Nils Schlegelmilch

Betreuer der Hochschule Karlsruhe
Prof. Dr.-Ing. Philipp Nenninger
Prof. Dr.-Ing. Reiner Kriesten

Karlsruhe, 01.10.2025 bis 31.03.2026

Inhaltsverzeichnis

1 Einleitung

2 Security und konzeptionelle Grundlagen von Feldgeräten

2.1 Einordnung von Feldgeräten in industrielle Systeme und Anlagen

Einleitung Kapitel schreiben

2.1.1 Funktion und Aufgaben von Feldgeräten

Feldgeräte nehmen eine zentrale Rolle in industriellen Automatisierungs- und Steuerungssystemen ein. Sie bilden die Schnittstelle zwischen der physischen Welt und übergeordneten Steuerungssystemen, indem sie Daten erfassen, verarbeiten und weiterleiten oder direkt in Prozesse eingreifen. Zu den typischen Feldgeräten gehören Sensoren, die physikalische Größen wie Temperatur, Druck, Messwerte, Füllstand oder Durchfluss messen, sowie Aktoren, die mechanische Bewegungen oder andere Aktionen ausführen. Im Fokus dieser Thesis stehen Sensoren, während Aktoren nicht Gegenstand der Untersuchung sind.

Die Einsatzgebiete von Feldgeräten sind äußerst vielfältig und erstrecken sich über nahezu alle Industriezweige. In der Prozessindustrie, beispielsweise in der Chemie- oder Öl- und Gasindustrie, überwachen sie kritische Parameter, um die Sicherheit und Effizienz von Anlagen sicherzustellen. In der Fertigungsindustrie ermöglichen Feldgeräte eine präzise Erfassung von Zuständen und Prozessgrößen und bilden die Grundlage für automatisierte Produktionsabläufe. Auch in der Energieversorgung, etwa in Kraftwerken, Stromnetzen oder der Wasserwirtschaft, sind Feldgeräte unverzichtbar für die Überwachung und Steuerung technischer Anlagen. Die hier beschriebenen Einsatzmöglichkeiten beziehen sich sowohl auf Sensoren als auch auf Aktoren, die jeweils spezifische Aufgaben in den Prozessen übernehmen.

Feldgeräte unterscheiden sich zudem hinsichtlich ihrer Interaktion mit Menschen und Maschinen. Während einige Geräte über lokale Anzeige- und Bedienelemente verfügen und eine direkte Bedienung vor Ort erlauben, werden andere Feldgeräte ausschließlich maschinell über Steuerungen, Asset-Management-Systeme oder mobile Servicegeräte angesprochen.

Eine Statistik wie viele Feldgeräte es weltweit gibt -> VEGA?

Da Feldgeräte den realen physikalischen Zustand eines Prozesses erfassen und Prozessentscheidungen auf diesen Messwerten basieren, ist ihre zuverlässige und korrekte Funktion von entscheidender Bedeutung. Fehlerhafte oder manipulierte Messwerte können unmittelbare Auswirkungen auf die Verfügbarkeit, Produktqualität und Sicherheit industrieller Systeme haben.

2.1.2 Systemarchitekturen und Einbindung von Feldgeräten

Zur Einordnung von Funktionen, Systemen und Kommunikationsbeziehungen in industriellen Umgebungen wird häufig das Purdue-Modell (auch als Purdue Enterprise Reference Architecture, PERA, referenziert) verwendet. Es beschreibt ein hierarchisches Ebenenkonzept für

industrielle Produktions- bzw. Prozesssysteme und strukturiert die Aufgabenverteilung von der operativen Prozessausführung bis zur unternehmensweiten Planung. Dabei wird zwischen horizontaler Kommunikation (innerhalb einer Ebene) und vertikaler Kommunikation (zwischen unterschiedlichen Ebenen) unterschieden. Für die Ebenen 0 bis 4 ist das Modell weitgehend kompatibel mit dem in der Praxis verbreiteten fünfstufigen Ebenenkonzept der Automatisierungspyramide. Im Purdue-Ansatz werden jedoch zusätzlich Zonen zur Abgrenzung und Kopplung unterschiedlicher Domänen berücksichtigt, insbesondere eine Übergangszone (Level 3.5, OT-DMZ) sowie eine externe bzw. Internet-nahe Zone [2]. Damit rückt weniger die reine funktionale Hierarchie als vielmehr die Netzsegmentierung und die kontrollierte Gestaltung von Übergängen in den Vordergrund, um Kommunikationsflüsse zwischen Office-IT, OT/ICS und externen Netzen gezielt zu steuern und abzusichern [4].

In ►Bild **??** ist das Purdue-Modell als hierarchische Referenzarchitektur für industrielle OT/ICS-Umgebungen dargestellt. Die Abbildung verdeutlicht die Anordnung der Ebenen sowie deren typische Kopplungspunkte und Schnittstellen. Darüber hinaus sind beispielhafte Kommunikationspfade zwischen den Ebenen eingezeichnet, wodurch sowohl horizontale Informationsflüsse innerhalb einer Ebene als auch vertikale Informationsflüsse zwischen den Ebenen nachvollziehbar werden. Ergänzend zeigt die Darstellung den Einsatz von Sicherheitskomponenten wie Firewalls und unidirektionalen Übertragungseinrichtungen (Datendioden), mit denen Kommunikationsbeziehungen segmentiert und Datenflüsse gezielt auf eine Richtung beschränkt werden können.

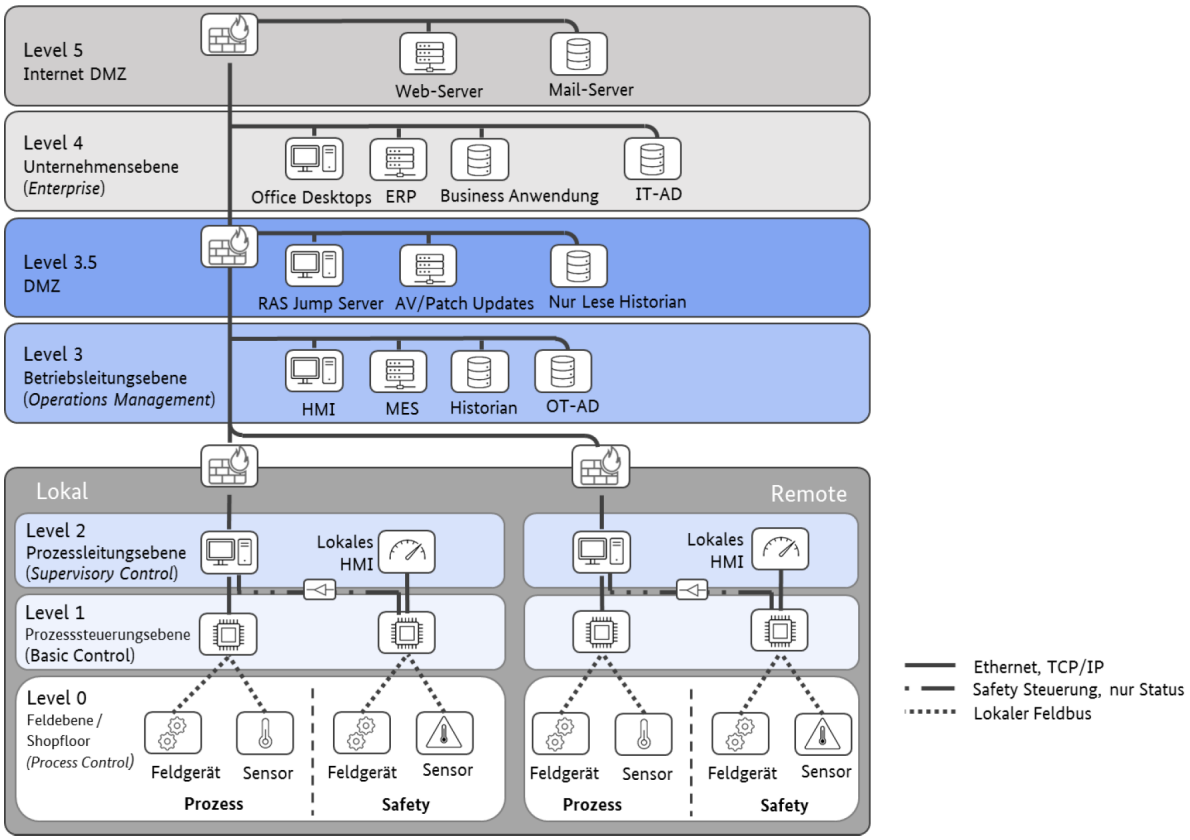

Bild 2.1. Beispiel Netzwerk nach Purdue/IEC 62443 Bildquelle: [5]

2.1.2.1 Einordnung in Ebenen des Purdue-Modells

Das Purdue-Modell ergänzt oberhalb der Produktionsführungs- und Unternehmensebene noch eine Internet Ebene, Ebene 5, welche die typische Kommunikation mit dem Internet (Web, Mail) repräsentiert.

Auf Ebene 4 (Unternehmensebene) findet typischerweise unter Nutzung eines ERP-Systems die übergeordnete Planung und Koordination betriebswirtschaftlicher Abläufe statt. Dazu zählen insbesondere die Grobplanung der Produktion sowie unterstützende Funktionen für Organisationsbereiche wie Vertrieb (z. B. Erfassung von Kundenaufträgen) und Einkauf (z. B. Beschaffung von Materialien), welche in einem ERP-System abgebildet werden können [2].

Eine weitere, wichtige Erweiterung ist die Übergangszone Ebene 3.5 (OT-DMZ) zwischen der Office-IT und der Produktion. Als Demilitarized Zone verhindert diese Zone eine direkte Kommunikation zwischen den beiden Segmenten. Informationen werden ausschließlich über in der DMZ bereitgestellte Schnittstellen ausgetauscht. Idealerweise wird die Verbindung hierbei von der Zone mit dem höheren Schutzbedarf aus aufgebaut. Da das ICS (Industrial Control System) in der Regel einen höheren Schutzbedarf als die Office-IT aufweist, wird die Verbindung von dieser Seite initiiert. So dürfen zum Beispiel ICS-Systeme Daten auf eine Datenbank in der DMZ schreiben, die Office Systeme hier aber nur lesend zugreifen.

Auf Ebene 3 (Betriebsleitungsebene) erfolgt eine detailliertere Planung und Steuerung der Produktion. Hier kommen häufig Manufacturing Execution Systems (MES) an den jeweiligen Produktionsstandorten zum Einsatz. Ein MES-System überwacht, steuert und optimiert in Echtzeit alle produktionsnahen Prozesse, einschließlich Betriebs-, Maschinen- und Personaldatenerfassung, sowie Material-, Qualitäts- und Energiemanagement, um eine effiziente Fertigung sicherzustellen [2]. Diese Ebene bildet die Schnittstelle zwischen der betriebswirtschaftlich orientierten Organisationsebene und den operativen Produktions- und Automatisierungssystemen.

Die Überwachung und operative Prozessführung erfolgt auf Ebene 2 (Prozessleitungsebene). Auf dieser Ebene werden typischerweise Supervisory Control and Data Acquisition (SCADA)-Systeme sowie Prozessleitsysteme (PLS) zur Produktionsdatenerfassung, -visualisierung und -kontrolle eingesetzt. Sie unterstützen unter anderem die Anzeige und Auswertung von Betriebsdaten sowie die Überwachung von Anlagenzuständen und Prozessparametern.[2].

Auf Ebene 1 (Prozesssteuerungsebene) übernehmen speicherprogrammierbare Steuerungen (SPS; engl. PLC) und zugehörige Ein-/Ausgabekomponenten (I/O) die lokale Steuerung und Regelung. Über diese Komponenten werden Signale aus der Feldebene verarbeitet und Stellgrößen an den Prozess ausgegeben. Die Steuerungsebene wirkt damit unmittelbar auf den Prozess ein.

In der Feldebene (Ebene 0) befinden sich die Komponenten, die Informationen aus dem materiellen Produktions- bzw. Prozessgeschehen erfassen oder als Aktoren direkt darauf einwirken. Dazu zählen beispielsweise Endschalter und Sensoren, die im Folgenden als Feldgeräte zusammengefasst werden. Diese Komponenten interagieren einerseits direkt mit dem physikalischen Prozess und andererseits, über eine zugehörige Infrastruktur (z. B. Anschluss- und Kopplungskomponenten), mit den informationsverarbeitenden Einheiten der darüberliegenden Ebenen. Für die Kommunikation auf Ebene 0 besteht grundsätzlich die Notwendigkeit, Sensordaten und Aktorbefehle unter deterministischen bzw. echtzeitnahen Bedingungen zu übertragen.

Zusätzlich müssen bei Bedarf Diagnose- und Konfigurationsdaten übermittelt werden, etwa für Inbetriebnahme, Wartung oder Parametrierung [4].

2.1.2.2 Kommunikation der Schichten

Die horizontale und vertikale Kommunikation wird in der Praxis häufig über Feldbus- und Automatisierungsnetzwerke realisiert, die je nach Systemarchitektur und Generation sowohl ethernetbasiert als auch nicht ethernetbasiert ausgeprägt sein können.

Die Kommunikation in ICS ist nicht auf die jeweilige Ebene beschränkt. So kann der Wert eines Füllstandsensor eines Ventils auf Ebene 0 über eine SPS auf Ebene 1 an eine Software auf Ebene 2 übertragen werden. Für die ebenenübergreifende Kommunikation kommen häufig Gateways zum Einsatz. Das Gateway (Ebene 1) wandelt Daten des I/O-Subsystems auf dem Feldbus (Ebene 0) in ein anderes Protokoll um und leitet diese an ein System auf Ebene 2 weiter. Von dort wird die Kommunikation zu Ebene 3 und 4 jeweils durch eine Firewall gefiltert und über die DMZ, die als Sicherheitszone eine direkte Kommunikation zwischen Netzwerken verhindert, geleitet. So können Daten zwischen verschiedenen Systemen ausgetauscht werden, aber nicht jedes System muss mit jedem direkt kommunizieren. Das ERP-System benötigt zum Beispiel keine Sensordaten von I/O Systemen auf dem Feldbus [4].

Absatz unterschied ethernet basiert und nicht

In bestimmten Industriebereichen, insbesondere in der Prozessindustrie, sind zudem weiterhin zahlreiche Feldgeräte im Einsatz, die Messwerte über eine 4–20 mA Stromschleife analog liefern. Häufig wird dies durch eine zusätzliche digitale Kommunikation ergänzt die wenig Energie benötigt und über die Konfigurations- oder Diagnosedaten übertragen werden können (z. B. über HART) [14].

Drahtlose Kommunikation kann ebenfalls Bestandteil horizontaler und vertikaler Kommunikationsstrukturen sein. Da der Fokus dieser Arbeit jedoch auf kabelgebundenen Kommunikationspfaden liegt, wird drahtlose Kommunikation im weiteren Verlauf nicht vertieft.

2.1.2.3 Abgrenzung OT/IT

Die in der Vergangenheit übliche physische Trennung der OT von anderen IT-Systemen und Datennetzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Mehrstufige Produktionsschritte und deren übergreifende Steuerung sowie regulatorische Anforderungen machen es zunehmend notwendig, die OT auch über Organisationsgrenzen hinweg zu öffnen. Dieser Prozess wird häufig als IT/OT-Konvergenz bezeichnet, ein Begriff, der die zunehmende Verschmelzung von Informationstechnologie (IT) und Betriebstechnologie (OT) beschreibt. Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen noch beschleunigt, vor allem im Rahmen der Industrie 4.0.[4].

2.1.3 Security-Relevante Bedeutung von Feldgeräten

2.1.3.1 Feldgeräte als Einfallspunkt für Angriffe

Jedes Feldgerät, das in ein OT-Netzwerk bzw. ICS integriert wird, erweitert die Funktionalität des Gesamtsystems und zugleich auch dessen Angriffsfläche. Abhängig von Fähigkeiten und Kommunikationsschnittstellen, sowie der Einbindung in die Systemarchitektur, können von einzelnen Feldgeräten verschiedene Risiken ausgehen.

Betrachtet man die grundlegende Funktionalität von Feldgeräten, insbesondere von Sensoren, so lassen sich in den meisten Fällen, ausgenommen rein analoge Geräte ohne Kommunikationsschnittstellen, zwei wesentliche Kommunikationspfade unterscheiden. Der Sensor-Channel zur Übertragung von Messwerten an übergeordnete Steuerungen sowie der Control-Channel, über den Parametrierung, Konfiguration oder Diagnose erfolgt.

Ein Angriff über den Control-Channel zielt darauf ab, eine Systemkomponente aus einer höheren Kommunikationsschicht, zu kompromittieren, um anschließend manipulierte Befehle in das System einzuschleusen[13].

In der Praxis kann dies beispielsweise über ausgenutzte Schwachstellen in Feldbus- oder Serviceprotokollen erfolgen. Wie in [1] gezeigt wurde, können manipulierte HART-Kommandos nicht nur Feldgeräte beeinflussen, sondern unter bestimmten Bedingungen auch weiterführende IT-Systeme bis hin zur Unternehmensebene kompromittieren. Der Control-Channel eines Feldgeräts kann somit als Einstiegspunkt dienen, um über legitime Kommunikationsbeziehungen weiter in den OT- oder sogar IT-Bereich vorzudringen.

Im Gegensatz dazu zielen Sensor-Channel-Angriffe auf die Manipulation der vom physikalischen Prozess gelieferten Messwerte. Hierbei werden Sensordaten verfälscht, sodass Steuerungen oder Leitsysteme auf Grundlage falscher Informationen Entscheidungen treffen. Ziel ist es, das Verhalten des Reglers gezielt zu beeinflussen oder einen realen Prozesszustand zu verschleiern. Diese als False-Data-Injection (FDI) bezeichneten Angriffe wurden ursprünglich im Kontext von Energieversorgungssystemen und Smart Grids beschrieben, gelten jedoch aufgrund der zunehmenden Vernetzung industrieller Anlagen als generisches Risiko für ICS-Umgebungen. Da industrielle Prozesse häufig sicherheitskritisch sind und erhebliche ökologische, wirtschaftliche oder gesellschaftliche Auswirkungen haben können, werden Manipulationen von Sensordaten als besonders schwerwiegender Angriffsvektor betrachtet. So kann beispielsweise eine künstlich abgesenkte Temperaturmessung dazu führen, dass die Heizleistung erhöht wird, obwohl keine tatsächliche Abweichung vorliegt, was im Extremfall zu einer unentdeckten Überhitzung führen kann. [7, 13].

2.1.3.2 Abgrenzung Safety - Security

Cybersicherheit (Security) dient dem Schutz von OT-Systemen vor mutwilligen Manipulationen, die deren bestimmungsgemäßen Betrieb beeinträchtigen oder verhindern können. Ziel ist es, die Integrität, Verfügbarkeit und Vertraulichkeit der Systeme sowie deren sichere Funktionsfähigkeit aufrechtzuerhalten. Hierzu zählt insbesondere auch der Schutz sicherheitskritischer Funktionen, die im Rahmen der Funktionalen Sicherheit implementiert sind.

Die Funktionale Sicherheit (Safety) verfolgt das Ziel, Menschen, Umwelt und Anlagen vor Gefährdungen zu schützen, die aus Fehlfunktionen technischer Systeme resultieren können [4]. Sie adressiert somit unbeabsichtigte Fehlerzustände, während Security vorsätzliche Angriffe berücksichtigt.

Cyberangriffe können jedoch unmittelbar Einfluss auf die Funktionale Sicherheit nehmen, indem sie sicherheitsgerichtete Systeme manipulieren oder außer Kraft setzen. Ein prägnantes Beispiel hierfür ist die im Jahr 2017 entdeckte TRITON-Malware. Diese zielte auf das Safety Instrumented System (SIS) einer petrochemischen Anlage in Saudi-Arabien ab und versuchte, dessen Schutzfunktionen gezielt zu manipulieren. Dadurch wurde die Fähigkeit des Systems, gefährliche Prozesszustände zu erkennen und abzusichern, beeinträchtigt, was potenziell zu schweren Personen- und Umweltschäden hätte führen können [6]. Der Vorfall verdeutlicht, dass Security-Schwachstellen direkte Auswirkungen auf die Safety eines Systems haben können.

Obwohl Safety und Security unterschiedliche Zielrichtungen verfolgen und jeweils eigene normative Rahmenwerke besitzen, sind sie in OT-Umgebungen eng miteinander verknüpft. Während Safety den Schutz von Menschen, Umwelt und Anlagen durch das System adressiert, zielt Security auf den Schutz des Systems vor externer Manipulation ab [4]. Im deutschen Sprachgebrauch wird der Begriff „Sicherheit“ häufig für beide Aspekte verwendet. Sofern in dieser Arbeit nicht ausdrücklich anders gekennzeichnet, bezieht sich der Begriff auf Security im Sinne der Informations- und Cybersicherheit.

2.2 Regulatorische Anforderungen an Feldgeräte

Mit der zunehmenden Vernetzung industrieller Systeme gewinnen regulatorische Anforderungen an die Cybersicherheit von Feldgeräten zunehmend an Bedeutung. Neben technischen Schutzmaßnahmen auf Systemebene werden auch konkrete Vorgaben an die sichere Entwicklung, Integration und den Betrieb einzelner Komponenten gestellt. Insbesondere Hersteller von Feldgeräten sind verpflichtet, Security-Aspekte bereits im Entwicklungsprozess zu berücksichtigen und geeignete Schutzmechanismen umzusetzen.

Im Folgenden werden die für Feldgeräte besonders relevanten Anforderungen der IEC 62443-4-2 sowie die regulatorischen Vorgaben des Cyber Resilience Act näher betrachtet.

2.2.1 IEC 62443-4-2

Die Normenreihe IEC 62443 stellt Anforderungen zur Gewährleistung von IT-Sicherheit für industrielle Automatisierungs- und Kontrollsysteme (IACS[1]). Sie umfasst funktionale Anforderungen an Automatisierungslösungen, -systeme und -komponenten sowie prozessorientierte Vorgehensmodelle für den Betrieb, die Systemintegration und die Produktentwicklung. Die Norm richtet sich an Hersteller, Integratoren, Betreiber und besteht aus mehreren Teilnormen [4].

[1] Der in der Normenreihe IEC 62443 verwendete Begriff Industrial Automation and Control Systems (IACS) ist Synonym mit dem in der Thesis verwendeten Begriff Industrial Control Systems (ICS).

Für die Entwicklung von Feldgeräten ist insbesondere die Teilnorm IEC 62443-4-2 von Bedeutung. Sie definiert technische Sicherheitsanforderungen auf Komponentenebene und legt fest, welche Security-Funktionen industrielle Geräte erfüllen müssen, um einem bestimmten Security-Level zu entsprechen. Dieses Security-Level spiegelt das angestrebte Schutzniveau gegenüber unterschiedlich leistungsfähigen Angreifern wider.

Die IEC 62443-4-2 legt technische Sicherheitsanforderungen für Komponenten industrieller Automatisierungs- und Kontrollsysteme fest. Grundlage bilden sieben sogenannte grundlegende Anforderungen (Foundational Requirements, FR). Diese adressieren die Bereiche:

1. Identifizierung und Authentifikation,
2. Nutzungskontrolle,
3. Systemintegrität,
4. Vertraulichkeit der Daten,
5. eingeschränkter Datenfluss,
6. rechtzeitige Reaktion auf sicherheitsrelevante Ereignisse und
7. Verfügbarkeit der Ressourcen.

Für jede FR werden Security Levels (SL) definiert, die das angestrebte Schutzniveau gegenüber Angreifern mit zunehmenden Fähigkeiten, Ressourcen und Motivation beschreiben (SL 1 bis SL 4). Für Komponenten wird der erreichbare Schutzgrad pro FR, von 0 bis 4 angegeben. Wobei SL 0 bedeutet, dass für die jeweilige FR keine spezifischen Anforderungen gelten, und SL 1 bis SL 4 steigende technische Schutzmaßnahmen voraussetzen.

Die einzelnen Security-Levels haben folgende Bedeutung:

Stufe	Definition
SL 0	Kein Security-Schutz
SL 1	Schutz vor zufälligem Abhören oder unbeabsichtigtem Aufdecken.
SL 2	Schutz vor gezieltem Abhören mit einfachen Mitteln, geringer Motivation und grundlegenden Fähigkeiten.
SL 3	Schutz vor gezieltem Abhören mit fortgeschrittenen Mitteln, mittlerer Motivation und spezialisierten Fähigkeiten.
SL 4	Schutz vor gezieltem Abhören mit hochentwickelten Mitteln, hoher Motivation und umfassenden spezialisierten Fähigkeiten.

Kann eine Anforderung nicht allein durch die Komponente erfüllt werden, sind ergänzende Maßnahmen auf Systemebene erforderlich; entsprechende Kompensationsmaßnahmen sind vom Hersteller zu dokumentieren [11].

Ist ein Produkt nach dieser Norm zertifiziert, so wird ein Zertifikat von einer unabhängigen Prüfstelle ausgestellt, die das entsprechende Security-Level angibt. In [21] ist ein solches Zertifikat dargestellt.

2.2.2 Cyber Resilience Act

Der Cyber Resilience Act (CRA) verfolgt das Ziel, die Cybersicherheit von „Produkten mit digitalen Elementen“ in der Europäischen Union zu erhöhen und hierfür einheitliche Mindestanforderungen festzulegen. Produkte mit digitalen Elementen sind im CRA solche Produkte, die direkt oder indirekt mit einem Gerät oder einem Netzwerk verbunden werden können. Damit soll Cybersicherheit nicht nur als freiwillige Qualitätsmaßnahme verstanden werden, sondern als verbindlicher Bestandteil der Produktkonformität. Hersteller sollen bereits bei der Entwicklung sicherstellen, dass ihre Produkte gegenüber typischen Bedrohungen angemessen geschützt sind, und sie müssen die Sicherheit zudem über den gesamten Produktlebenszyklus hinweg aufrechterhalten [15].

Für die Entwicklung von Feldgeräten bedeutet dies vor allem eine Verschiebung von Best Practice hin zu nachweisbaren, konformitätsrelevanten Anforderungen. Hersteller müssen Bedrohungen und Risiken systematisch bewerten und daraus technische und organisatorische Maßnahmen ableiten, beispielsweise zum Schutz vor unbefugtem Zugriff, zur Sicherstellung der Integrität von Firmware und Konfiguration, zur Geheimhaltung der gespeicherten Daten, sowie zur Etablierung eines strukturierten Schwachstellenmanagement [10].

In der Praxis kann dies über bereits etablierte Normen und Sicherheitsstandards realisiert werden. Mappings, welche CRA-Anforderungen mit bestehenden Normen und Sicherheitspraktiken in Beziehung setzen, unterstützen eine pragmatische Umsetzung und erleichtern die Ableitung konkreter Entwicklungs- und Nachweispflichten. Da viele CRA-Zielrichtungen (z. B. systematische Risikoanalyse, sichere Produktentwicklung, Schutz zentraler Sicherheitsziele) inhaltlich mit Anforderungen der IEC 62443-Familie kompatibel sind, können Hersteller, die ihre Produktentwicklung bereits an dieser Normenreihe ausrichten, wesentliche CRA-Anforderungen konsistent abdecken [9].

Eine besondere Herausforderung stellen Feldgeräte dar, die nicht ethernetbasiert sind, wie sie z. B. häufig in der Prozessindustrie vorkommen. Solche Geräte verfügen häufig nur über eingeschränkte oder gar keine kryptographischen Schutzmechanismen, da ihre Rechenleistung, Energieversorgung oder Protokolleigenschaften dies nicht vorsehen. Ihre Messwerte werden entweder analog oder über ältere Feldbus-Mechanismen übertragen, und es nicht zu erwarten, dass diese Feldbusse in Zukunft mit Sicherheitsfunktionen ausgestattet werden [14]. Da diese Geräte jedoch digitale Elemente wie Firmware, digitale Parametrierung, Diagnosedaten oder Konfigurationsschnittstellen besitzen, fallen auch diese Geräte unter die Anforderungen des CRA. Für Hersteller ergibt sich daraus die zentrale Frage, wie CRA-relevante Vorgaben bei begrenzten Kommunikations- und Sicherheitsressourcen technisch sinnvoll umgesetzt und nachvollziehbar begründet werden können.

Da die Anforderungen aus dem CRA für neue Produkte erst ab Dezember 2027 greift, liegen derzeit nur begrenzte praktische Erfahrungen zur konkreten Ausgestaltung der Konformitätsprozesse bei Feldgeräten vor [15]. Vor diesem Hintergrund ist die in dieser Arbeit vorgenommene Untersuchung besonders relevant. Sie adressiert die Frage, wie auch nicht ethernetbasierte Feldgeräte kryptographisch gestützte Sicherheitsmaßnahmen und belastbare Schutzkonzepte umsetzen können, um zukünftige regulatorische Anforderungen und Nachweiserwartungen zu erfüllen.

2.3 Zentrale Schutzziele für Feldgeräte

Die Sicherheit moderner IT- und OT-Systeme stützt sich unter anderem auf das Konzept der Informationssicherheit. Dieses umfasst Maßnahmen und Strategien, die darauf abzielen, Systeme, Daten und Kommunikation vor unbefugtem Zugriff, Manipulation und Ausfällen zu schützen Informationssicherheit bildet eine wesentliche Grundlage für die Entwicklung sicherer Feldgeräte und damit auch für den Aufbau zuverlässiger und sicherer Anlagen.

Ein zentrales Element der Informationssicherheit sind sogenannte Schutzziele. Diese beschreiben, welche sicherheitsrelevanten Eigenschaften eines Systems oder einer Komponente erhalten bleiben müssen, um einen sicheren Betrieb zu gewährleisten. Für Feldgeräte, die in sicherheitskritischen Umgebungen eingesetzt werden, sind Schutzziele von besonderer Bedeutung, da sie die Grundlage für den Schutz vor Angriffen und die Gewährleistung eines zuverlässigen Betriebs bilden.

Die CIA-Triade und deren Anwendung in OT-Systemen Die CIA-Triade ist ein zentrales Konzept der Informationssicherheit und definiert drei grundlegende Schutzziele:

- Geheimhaltung (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

Sie dient als Grundlage für die Bewertung und den Schutz von IT- und OT-Systemen.

Während in IT-Systemen die Geheimhaltung oft oberste Priorität hat, stehen in OT-Systemen die Integrität und Verfügbarkeit im Vordergrund. Dies liegt daran, dass ein Systemausfall oder die Manipulation von Daten direkte Auswirkungen auf physische Prozesse haben kann. Die Vertraulichkeit von Daten spielt hier im Vergleich eine geringere Rolle [19].

Die Normenreihe IEC 62443-4-2 konkretisiert diese Schutzziele auf Komponentenebene und definiert sieben Foundational Requirements (FR), die als normative Schutzziele interpretiert werden können. Diese Anforderungen adressieren zentrale Sicherheitsaspekte wie Authentifikation, Zugriffskontrolle und Integrität und bieten einen klaren Rahmen für die Entwicklung sicherer Feldgeräte. Es wurde auch noch das Schutzziel *Organisation* hinzugefügt, das verdeutlicht, das diese Anforderungen mittels organisatorischer Maßnahmen umgesetzt werden müssen.

Die Zuordnung in Schutzziel macht keinen Sinn

Da sich diese Thesis mit dem sicheren Verbindungsaufbau bei Feldgeräten ohne Netzwerkschnittstelle befasst, werden Anforderungen, die ausschließlich durch organisatorische oder bauliche Maßnahmen in der Umgebung umgesetzt werden können, im weiteren Verlauf nicht vertieft. Für die Eingrenzung des Untersuchungsumfangs werden die aus IEC 62443-4-2 abgeleiteten Anforderungen danach unterschieden, ob sie durch den Kommunikationsmechanismus adressierbar sind oder außerhalb des Einflussbereichs eines Protokolls liegen. Daraus ergibt sich eine Einteilung in drei Klassen, nach [15]:

Tabelle sauber beschrieben in Latex einfügen.

1. Anforderungen, die für das betrachtete Feldgerätprofil nicht relevant sind (z. B. Notstromversorgung, Schutz der Zonengrenze).

IEC	Schutzziel	Erklärung	Beispiel
1. Identifizierung und Authenfikation	Integrität	Alle Nutzer müssen sich identifizieren und authentifizieren, bevor Zugriff auf das System gewährt wird	Zertifkate
2. Nutzungskontrolle	Integrität	Rollenbasierter Zugriff Jedem Nutzer werden entsprechende Berechtigungen zugewiesen	Benutzerkonten
3. Systemintegrität	Integrität	Die Integrität der Komponente muss sichergestellt werden	Physischer Zugriffsschutz Individuelle Sitzungskennungen
4. Vertraulichkeit der Daten	Geheimhaltung	Schutz von Informationen bei Speicherung und Übertragung	Zugriffsschutz Verschlüsselung
5. eingeschränkter Datenfluss,	Organisation	Einteilung einer Anlage in verschiedene Zonen	Zugriff auf IT-Netz unterbinden
6. rechtzeitige Reaktion auf sicherheitsrelevante Ereignisse und	Organisation	Sicherheitsverletzungen werden dokumentiert	Ereignisprotokoll
7. Verfügbarkeit der Ressourcen	Verfügbarkeit	Verfügbarkeit der Komponente wird sichergestellt	Physischer Zugrifssschutz Untebinden mehrer Sessions

Bild 2.2. Mapping der Anforderungen -> DELETE

2. Anforderungen, die unmittelbar durch kryptografische Mechanismen auf der Kommunikationsstrecke umgesetzt werden können (z. B. Integritätsschutz und Vertraulichkeit der übertragenen Daten).

3. Anforderungen, die sicherheitsrelevant sind, deren Umsetzung jedoch primär von der Geräteplattform abhängt (z. B. Integrität beim Software-Update, Integrität des Boot-Prozesses).

Die vorliegende Arbeit fokussiert daher auf Klasse 2, da nur diese Anforderungen direkt durch den Verbindungsaufbau, die Authentisierung und die Aushandlung von Sitzungsschlüsseln auf Protokollebene beeinflussbar sind. Angriffe auf die Verfügbarkeit, die durch physischen Zugriff oder Zerstörung des Geräts entstehen, können durch ein Kommunikationsprotokoll hingegen nicht verhindert werden.

2.4 Stand der Technik

2.4.1 Stand der Technik bei nicht netzwerkfähigen Feldgeräten

Wie in Abschnitt **??** abgegrenzt, fokussiert diese Arbeit auf Anforderungen der Kommunikationssicherheit (Klasse 2 der Anforderungen), also auf kryptografische Mechanismen zur Authentisierung sowie zum Integritäts- und optional Vertraulichkeitsschutz der übertragenen Daten. Für nicht netzwerkfähige Feldgeräte sehen die zugehörigen Feldbusstandards solche Mechanismen typischerweise nicht vor. Keiner der gängigen Feldbusse, weder HART, PROFIBUS PA, OPC noch MODBUS unterstützt Sicherheitsfunktionen in Bezug auf Integrität, Verschlüsselung oder Authentifizierung auf Protokollebene. Auch ist nicht davon auszugehen, dass sich dies in absehbarer Zeit ändern wird [3][14]. In der Praxis werden die fehlenden Protokollmechanismen daher überwiegend durch Maßnahmen der Umgebung (Klasse 1) sowie durch gerätespezifische Härtungsmaßnahmen (Klasse 3) kompensiert.

Die Ursachen für das Fehlen protokollseitiger Sicherheitsmechanismen sind vielfältig und historisch gewachsen.

Physischer Schutz und Air-Gaps Die folgenden Maßnahmen adressieren primär Anforderungen der Klasse 1, da sie außerhalb des Einflussbereichs eines Feldbusprotokolls liegen und durch Anlagenbetrieb und Umgebung umgesetzt werden. ICS-Anlagen befinden sich in der Regel in physisch abgesicherten Bereichen, die durch Zäune, Mauern oder vergleichbare Barrieren geschützt sind. Der Zugang zu den Feldgeräten ist dabei auf das vor Ort tätige Betriebspersonal sowie auf externe Dienstleister, etwa für Inbetriebnahme oder Wartung, beschränkt [14]. Zusätzlich wurden insbesondere ältere Anlagen häufig physisch von anderen Netzwerken isoliert, um sie vor Cyberangriffen zu schützen. Da sich die Geräte in einem abgeschotteten Bereich befanden und nicht von außen erreichbar waren, wurde lange Zeit argumentiert, dass dieser Schutz ausreichend sei [4].

Diese sogenannten *Air-Gaps*, also die vollständige Trennung von IT und OT, erreichen in der Praxis jedoch selten das angestrebte Schutzniveau. Häufig ist trotz der physischen Trennung ein Datenaustausch zwischen den Netzen notwendig oder gewünscht, und genau diese Schnittstellen können von Angreifern ausgenutzt werden, um die Isolation zu überwinden [4]. Darüber hinaus ist eine vollständige Trennung der OT von der IT heute nur noch in Ausnahmefällen und bei besonders hohem Schutzbedarf umsetzbar. Mehrstufige Produktionsprozesse, deren systemübergreifende Steuerung sowie regulatorische Vorgaben erfordern zunehmend eine Vernetzung der OT, auch über Organisationsgrenzen hinweg. Verstärkt wird diese Entwicklung durch den Trend zur Optimierung von Fertigungsprozessen im Kontext von Industrie 4.0 [5].

Selbst bei ausreichender Absicherung der OT und einem physischen Zugangsschutz bestehen weiterhin Risiken, da Angreifer mit internem Zugriff auf das Automatisierungsnetzwerk oder mit direktem Zugang zum Feldgerät gezielt Schwachstellen ausnutzen könnten. Eine Studie von Bitkom zeigt, dass interne Bedrohungen eine erhebliche Gefahr darstellen: 62 % der Angriffe auf deutsche Unternehmen gehen von aktuellen oder ehemaligen Mitarbeitern aus [20]. Mit entsprechendem Zugang wäre es beispielsweise möglich, ein Feldgerät unbemerkt durch ein manipuliertes Gerät auszutauschen.

Darüber hinaus gibt es Einsatzszenarien, in denen ein flächendeckender physischer Schutz nicht realisierbar ist. Auch wenn das Feldgerät selbst und zugehörige Komponenten wie Gateways vor unbefugtem Zugriff geschützt sind, können Verbindungsleitungen, insbesondere bei größeren Distanzen, ungeschützt verlaufen. Ein charakteristisches Beispiel ist die Füllstandsmessung an einem Stausee oder Überlaufbecken, wo die Messleitungen über längere Strecken außerhalb kontrollierten Bereichs verlaufen können.

Technische Einschränkungen Neben den physischen Schutzmaßnahmen spielen auch technische Limitierungen eine wesentliche Rolle für das Fehlen protokollseitiger Sicherheitsmechanismen der Klasse 2.

Viele der heute eingesetzten Feldgeräte stammen aus einer Zeit, in der Cybersicherheitsbedrohungen noch nicht in dem heutigen Ausmaß existierten. Diese Legacy-Systeme verfügen weder über die erforderliche Hardware noch über die Softwareunterstützung, um moderne Sicherheitsverfahren umzusetzen. Da Anlagen im OT-Umfeld häufig über mehrere Jahrzehnte

betrieben werden, ist eine große installierte Basis solcher Geräte nach wie vor im Einsatz [19].

Kryptografische Verfahren, insbesondere asymmetrische Algorithmen, sind ohne dedizierte Krypto-Peripherie vergleichsweise rechenintensiv. Zusätzlicher Rechenaufwand aufgrund Berechnung kryptographischer Operationen würde die verfügbare Verarbeitungszeit zusätzlich beanspruchen und steht damit in direktem Konflikt mit den begrenzten Ressourcen der Feldgeräte [13].

Kryptographische Operationen, stehen zudem auch im Konflikt mit dem Energieverbrauch der Fedlgeräte. Nicht netzwerkfähige Feldgeräte sind häufig für besonders robuste und energieeffiziente Betriebsbedingungen ausgelegt. Bei 2-Draht-Geräten muss die gesamte Elektronik aus dem begrenzten Energiehaushalt der 4 mA–20 mA-Stromschleife versorgt werden. Abzüglich Toleranzen und Reserven stehen dabei lediglich ca. 3,5 mA für die interne Elektronik zur Verfügung [12]. Mikrocontroller werden daher häufig mit niedrigen Taktraten betrieben und die verfügbaren Ressourcen auf das für Messwerterfassung, Signalverarbeitung, Diagnose und Kommunikation notwendige Minimum optimiert. Zwischen Verarbeitungsdauer, Energieverbrauch und Sicherheitsniveau muss somit stets ein Kompromiss gefunden werden. In der Konsequenz wurden Sicherheitsmechanismen in vielen Feldgeräten entweder gar nicht vorgesehen oder auf einfache Schutzfunktionen wie Schreibschutz, PIN-basierte Sperren oder rein organisatorische Maßnahmen beschränkt [4].

Einordnung nach IEC 62443 und kompensierende Maßnahmen In der IEC-62443-Familie werden Sicherheitsanforderungen für Komponenten im Kontext eines übergreifenden Zonen- und Leitungsmodells betrachtet, das dem Prinzip einer Defense in Depth Strategie folgt, indem mehrere Schutzschichten kombiniert werden (z. B. organisatorische Maßnahmen, physischer Schutz, Netzwerksegmentierung und Komponentenhärtung). Für nicht netzwerkfähige Feldgeräte zeigt sich dabei ein typisches Bild: Anforderungen der Klasse 1 dominieren den Betriebsschutz, plattformspezifische Maßnahmen der Klasse 3 sind je nach Gerätegeneration teilweise vorhanden, während die protokollseitige Absicherung der Kommunikation (Klasse 2) auf dem Feldbus in der Regel fehlt. Insbesondere Security Level 2 wird in vielen Industriepublikationen als das niedrigste Niveau eingeordnet, ab dem Schutz gegen vorsätzlichen Missbrauch adressiert wird [15]. Dies verdeutlicht die Lücke zwischen klassischen Feldgeräteprotokollen ohne integrierte Security-Funktionen und den Anforderungen, die bei gezielten Angriffen typischerweise relevant werden.

Praxisbeispiel: Security-Umsetzung bei einem nicht netzwerkfähigen Feldgerät Am Beispiel eines 2-Draht-Feldgeräts (VEGAPULS 6X mit 4 … 20 mA/HART) zeigt sich, dass Sicherheitsfunktionen in der Praxis stark auf lokale Schutzmechanismen und organisatorische Maßnahmen verteilt werden. Die zugehörige Security Guideline [22] weist explizit darauf hin, dass das standardisierte HART-Protokoll keinen ausreichenden Schutz gegen Datenmanipulation und Spionage bietet und deshalb nur in einer Umgebung mit Schutzniveau entsprechend SL1 bzw. bei sichergestelltem physischem Zugriffsschutz auf die Signalleitungen betrieben werden soll. Damit werden zentrale Risiken durch Maßnahmen der Klasse 1 (physischer Zugriffsschutz, Betriebsvorgaben) adressiert und um ausgewählte geräteinterne Funktionen der Klasse 3 ergänzt. Für Schnittstellen und den Gerätezugang werden daher Maßnahmen wie

Zugriffsschutz per Passwort, Deaktivierung ungenutzter Kommunikationskanäle sowie physische Sicherungen (z. B. Verplombung) gefordert. Geräteseitig werden zudem Funktionen wie Firmware-Integritätsprüfungen, Ereignisspeicher und Ressourcenmanagement als Sicherheitsfunktionen genannt. Diese Maßnahmen erhöhen die Härtung des Geräts, ersetzen jedoch keinen kryptografisch geschützten Kommunikationskanal auf dem Feldbus.

Verbleibende Lücken auf Protokollebene Aus Sicht der Schutzziele Vertraulichkeit und Integrität verbleibt bei nicht netzwerkfähigen Feldgeräten insbesondere eine Lücke in den Anforderungen der Klasse 2, also in der Ende-zu-Ende-Absicherung der Kommunikation.

Während Integrität im Feldbuskontext häufig nur über einfache Prüfsummen oder CRC-Mechanismen adressiert wird, existieren typischerweise keine Verfahren zur kryptografischen Authentifizierung von Geräten, keine aushandelbaren Sitzungsschlüssel und keine Verschlüsselung der Nutzdaten auf der Leitung. Damit kann ein Angreifer mit physischem Zugriff auf die Signalleitung Daten mitlesen oder manipulieren, ohne durch das Protokoll selbst zuverlässig detektiert oder ausgeschlossen zu werden. Genau an dieser Stelle setzt die vorliegende Arbeit an, indem eine gerätebasierte Identität über Zertifikate und ein sicherer Verbindungsaufbau auch für nicht IP-basierte Kommunikationskanäle konzipiert und umgesetzt wird.

Kryptografie als Option auf modernen Feldgeräten Obwohl die Feldbusprotokolle nicht IP-basierter Geräte die Anforderungen der Klasse 2 weiterhin kaum adressieren, haben sich die technischen Rahmenbedingungen für Feldgeräte in den letzten Jahren deutlich verschoben. Moderne Mikrocontroller integrieren dedizierte Krypto-Peripherie bzw. Hardwarebeschleuniger, sodass kryptografische Verfahren nicht mehr zwangsläufig im Widerspruch zu den typischen Restriktionen (begrenzte Rechenleistung, enger Energiehaushalt, zeitliche Anforderungen) stehen. Hierbei werden kryptographische Primitive, in speziell dafür entwickelten Hardwareblöcken berechnet, wodurch einerseits der Przoessor entlastet wird und die kryptographischen Berechnungen deutlich schneller und effizienter berechnet werden [18].

Definition Kryptografische Primitive raussuchen

Beispielhafte Messungen auf einem STM32U3 verdeutlichen die Größenordnung: Für AES-128-GCM erreicht die Hardware[2] etwa 9,17 $\mathrm{MB\,s^{-1}}$, während eine Software-Implementierung auf demselben Controller bei etwa 0,76 $\mathrm{MB\,s^{-1}}$ liegt. Für SHA-256 wurden 45,87 $\mathrm{MB\,s^{-1}}$ (Hardware) gegenüber 1,355 $\mathrm{MB\,s^{-1}}$ (Software) gemessen [16]. Das entspricht einer Beschleunigung um etwa den Faktor 12 bzw. 34, während der Energieverbrauch nur leicht steigt .

Messungen hinzufügen, oder darauf verweisen

Parallel zu dieser Entwicklung im Bereich Hardware, stehen aber auch für Berechnung in Software optimierte Verfahren zur Verfügung, etwa *Curve25519* für Schlüsselaustausch und Signaturen, sowie *ChaCha* als schnelle Alternative für symmetrische Verschlüsselung [17].

Ergänzend dazu werden Secure Elements oder vergleichbare geschützte Ausführungsumgebungen eingesetzt, wenn langfristige Schlüssel und Identitäten auch gegen Softwarefehler und physische Angriffe abgesichert werden müssen. Sie trennen Schlüsselmaterial und sicherheitskritische Operationen (z. B. Signaturen oder Schlüsselaustausch) vom Mikrocontroller, sodass private Schlüssel idealerweise weder im Klartext im Hauptspeicher erscheinen noch durch die Applikation direkt verarbeitet werden. Je nach Plattform ist dies als separater Baustein oder als integrierte Sicherheitsfunktion des Mikrocontrollers realisiert. Diese Baugruppen bringen

[2]Hardware bezieht sich auf den HW-Beschleuniger und Software auf die Berechnung mittels CyclonePRO-Softwarebibliothek auf dem Mikrocontroller

noch weitere Funktionen wie sichere Schlüsselerzeugung, zertifizierte Entropiequellen, Anti-Tampering- und sichere Bootmechanismen mit sich [18].

Damit wird es möglich, die Anforderungen der Klasse 2 auch für nicht netzwerkfähige Feldgeräte auf Applikations- und Protokollebene nachzurüsten, ohne die Randbedingungen energieoptimierter Hardware grundsätzlich zu verletzen. Diese Entwicklung bildet die Grundlage für die nachfolgenden Kapitel, in denen ein entsprechender Ansatz konzipiert und auf die Randbedingungen nicht netzwerkfähiger Feldgeräte angepasst wird.

2.4.2 Stand der Technik bei netzwerkfähigen Feldgeräten

Wie in Abschnitt **??** abgegrenzt, fokussiert diese Arbeit auf Anforderungen der Kommunikationssicherheit (Klasse 2), also auf kryptografische Mechanismen für Authentisierung sowie Integritäts- und optional Vertraulichkeitsschutz. Bei ethernetbasierten Feldgeräten sind diese Mechanismen grundsätzlich verfügbar, da sich die Kommunikation entweder direkt durch Security-Erweiterungen der Feldbusprotokolle absichern lässt oder über etablierte Sicherheitsprotokolle wie TLS abgebildet werden kann. Der Stand der Technik ist damit nicht durch das Fehlen geeigneter Konzepte geprägt, sondern durch deren praktische Anwendung im Feld.

Die zunehmende Vernetzung der OT führt dazu, dass Ethernet-Technologien immer weiter in Richtung Feldgeräte verschoben werden. Single Pair Ethernet (SPE) bildet hierfür die physikalische Grundlage auf nur einem Adernpaar. Ethernet-APL ist darauf aufbauend eine prozessindustrielle Ausprägung, die zusätzliche Randbedingungen adressiert, insbesondere die Zweidrahtanbindung mit Energieversorgung, lange Leitungslängen und Konzepte für den Einsatz in explosionsgefährdeten Bereichen. Damit entsteht technisch die Möglichkeit, ethernetbasierte Kommunikationsprotokolle inklusive ihrer Security-Mechanismen bis zum Messumformer zu führen [8].

Unabhängig von der konkreten Protokollfamilie folgt Kommunikationssicherheit im Ethernet-Umfeld typischerweise einem wiederkehrenden Muster. Zunächst werden die Kommunikationspartner beim Verbindungsaufbau authentisiert, häufig auf Basis von X.509-Zertifikaten und einer Vertrauenskette. Anschließend werden symmetrische Sitzungsschlüssel abgeleitet, da diese für die laufende Datenübertragung deutlich effizienter sind als asymmetrische Verfahren. Auf dieser Grundlage werden Nachrichten gegen Manipulation geschützt (Integrität und Authentizität) und optional verschlüsselt (Vertraulichkeit). Die Schlüssellebensdauer wird durch Rekeying oder erneuten Verbindungsaufbau begrenzt [15]. Genau dieses Muster ist für die spätere Übertragung auf nicht IP-basierte Kanäle relevant.

PROFINET ist ein geeignetes Beispiel, um die Umsetzung von Klasse 2 in einem etablierten Feldbuskontext zu zeigen. Im Rahmen von PROFINET Security werden Security Classes definiert, die schrittweise Fähigkeiten von Robustheit bis zu kryptografisch geschützter Kommunikation abdecken. Security Class 1 adressiert vor allem Härtung und Robustness-Aspekte, etwa durch verbesserte Management- und Discovery-Mechanismen sowie die Möglichkeit, Gerätebeschreibungsdateien kryptografisch abzusichern, um Manipulationen in Engineering-Prozessen zu erschweren. Security Class 2 zielt auf Integrität und Authentizität der Kommunikation, sodass unbemerkte Manipulationen der PROFINET-IO-Daten verhindert werden sollen. Security Class 3 ergänzt zusätzlich den Vertraulichkeitsschutz, um ein Mitlesen und Interpretieren der Daten zu erschweren, sofern dies im jeweiligen Anwendungsfall erforderlich ist. Beim Verbindungsaufbau authentisieren sich beide Endpunkte gegenseitig über X.509-Zertifikate,

und es werden symmetrische Schlüssel für die nachfolgende Kommunikation abgeleitet. Diese Schlüssel werden im Betrieb regelmäßig erneuert, um die Auswirkungen einer möglichen Schlüsselkompromittierung zeitlich zu begrenzen. Damit zeigt PROFINET Security exemplarisch, wie Klasse 2 Anforderungen direkt auf Protokollebene adressiert werden können, ohne dass die Wirksamkeit allein auf Segmentierung oder physische Maßnahmen ausgelagert wird [23].

Ethernetbasierte Feldgeräte zeigen, dass kryptografisch abgesicherte Verbindungen auf Kommunikationsschnittstellen heute grundsätzlich realisierbar sind und in Spezifikationen bereits vorgesehen werden. Die wesentlichen Bausteine sind dabei Authentisierung über Geräteidentitäten, Ableitung symmetrischer Sitzungsschlüssel und deren Nutzung für Integritäts- und optional Vertraulichkeitsschutz. Nicht netzwerkfähige Feldgeräte besitzen diese Bausteine auf ihrer Kommunikationsschnittstelle typischerweise nicht. Die nachfolgenden Kapitel greifen daher das etablierte Muster aus dem Ethernet-Umfeld auf und übertragen es auf nicht IP-basierte Kanäle, angepasst an deren Ressourcen- und Betriebsrandbedingungen.

2.5 Public-Key-Infrastrukturen und Zertifikate

2.5.1 Geräteidentitäten und PKI als Grundlage für sichere Verbindungsaufbauten

Für kryptografisch abgesicherte Kommunikationsbeziehungen (Klasse 2) ist eine belastbare Geräteidentität eine zentrale Voraussetzung. In modernen Sicherheitsarchitekturen wird diese Identität typischerweise über X.509-Zertifikate abgebildet, die einen öffentlichen Schlüssel kryptografisch an ein Subjekt binden und von einer vertrauenswürdigen Zertifizierungsstelle signiert werden. Auf dieser Basis kann ein Kommunikationspartner die Echtheit des Gegenübers prüfen und anschließend Sitzungsschlüssel für einen effizienten Integritäts- und optional Vertraulichkeitsschutz ableiten.

Root of Trust und Validierung von Zertifikatsketten Die Vertrauensentscheidung in einer PKI basiert auf einem Root of Trust, der typischerweise als Trust Anchor im Truststore der prüfenden Instanz hinterlegt ist. Die Validierung eines End-Entity-Zertifikats erfolgt dann entlang der Zertifikatskette, indem jede Signatur mit dem öffentlichen Schlüssel des jeweils ausstellenden Zertifikats geprüft wird. Vereinfacht ergibt sich dabei folgende Prüfreihenfolge:

1. Die Signatur des Geräte- (End-Entity-) Zertifikats wird mit dem öffentlichen Schlüssel der ausstellenden Issuing-CA geprüft.

2. Die Signatur der Issuing-CA wird mit dem öffentlichen Schlüssel der übergeordneten CA (Intermediate oder Root) geprüft.

3. Für ein selbstsigniertes Root-Zertifikat kann die Signatur formal mit dem eigenen öffentlichen Schlüssel geprüft werden.

4. Entscheidend ist anschließend die Vertrauensentscheidung: Die Kette gilt nur dann als vertrauenswürdig, wenn das Root-Zertifikat als Trust Anchor im Truststore des prüfenden Kommunikationspartners hinterlegt ist.

Damit wird klar, dass nicht die Selbstsignatur der Root-CA Vertrauen erzeugt, sondern die sichere Verteilung und Hinterlegung des Trust Anchors.

Secure Device Identity nach IEEE 802.1AR (DevID) Der IEEE-Standard zu Secure Device Identifiers beschreibt DevIDs als eindeutige, kryptografisch gebundene Geräteidentitäten und unterscheidet dabei Initial Device Identifiers (IDevID) und Local Device Identifiers (LDevID). Ein DevID besteht aus einem RFC-5280-konformen X.509-Zertifikat, einem zugehörigen privaten Schlüssel (DevID secret) sowie der Zertifikatskette bis zu einem Vertrauensanker. Damit ist eine DevID nicht nur ein Identifier, sondern ein vollständiges Credential, mit dem ein Gerät seine Identität in Authentisierungsprotokollen nachweisen kann.

Die sichere Bindung an das Gerät erfolgt dadurch, dass der private Schlüssel in einem DevID-Modul geschützt gespeichert wird und ausschließlich für kryptografische Operationen genutzt werden kann. Unter einem DevID-Modul wird dabei die Kombination aus geschützter Schlüsselablage und einer Schnittstelle verstanden, die Signieroperationen ausführt, ohne den privaten Schlüssel preiszugeben. Das Gerät weist seine Identität nach, indem es Signaturoperationen mit dem DevID secret ausführt und damit den Besitz des privaten Schlüssels beweist. Dieses Prinzip der Besitzprüfung ist entscheidend, da nur so eine Nachahmung des Geräts durch Dritte verhindert wird.

Die IDevID wird vom Hersteller vor Auslieferung bereitgestellt, ist global eindeutig und gegen Modifikation geschützt. Zusätzlich kann das Gerät eine oder mehrere LDevIDs unterstützen, die durch den Betreiber erzeugt und verwaltet werden. LDevIDs erleichtern die Einbindung in eine lokale Sicherheitsinfrastruktur, da sie eine betriebsspezifische Identität bereitstellen können, ohne die herstellerseitige Grundidentität zu ersetzen. Je nach Betriebsmodell kann eine LDevID mit einem neu erzeugten Schlüssel arbeiten oder auf einem bestehenden Schlüssel aufsetzen, sofern dies durch die Sicherheitsrichtlinie zugelassen ist.

X.509-PKI nach RFC 5280 RFC 5280 beschreibt das Profil der X.509-Zertifikate und den grundlegenden PKI-Mechanismus im Internet. Zertifikate binden öffentliche Schlüssel an Subjekte und werden von einer Zertifizierungsstelle signiert, wodurch sich ein prüfbarer Vertrauensnachweis ergibt. Da ein Kommunikationspartner nur eine begrenzte Menge an vertrauenswürdigen CA-Schlüsseln im Voraus besitzt, wird die Vertrauensprüfung typischerweise über Zertifikatsketten realisiert. Dabei wird ein End-Entity-Zertifikat über eine oder mehrere Zwischenzertifizierungsstellen bis zu einem Trust Anchor validiert. Zertifikate können zudem vor Ablauf ihrer Gültigkeit ungültig werden, etwa durch Schlüsselkompromittierung oder organisatorische Änderungen. RFC 5280 beschreibt hierfür Widerrufsmechanismen wie Certificate Revocation Lists (CRLs), die es erlauben, kompromittierte oder nicht mehr gültige Zertifikate vorzeitig aus dem Vertrauensmodell zu entfernen.

Im DevID-Kontext ist relevant, dass IDevIDs typischerweise sehr lange Gültigkeitszeiten besitzen, um Gerätelebensdauern nicht künstlich zu begrenzen. Gleichzeitig bleibt die Vertrauensprüfung von der Qualität der PKI und der Integrität der Trust-Anchor-Verteilung abhängig. Der IEEE-Standard benennt hierzu Risiken wie kompromittierte Signierschlüssel in der Hersteller-PKI, fehlerhafte Trust-Anchor-Listen oder die Offenlegung des DevID secret als kritische Angriffspunkte.

CSR als Schnittstelle zwischen Gerät und PKI (PKCS#10, RFC 2986) Für die Ausstellung eines Gerätezertifikats wird in der Praxis häufig ein Certificate Signing Request verwendet. RFC 2986 (PKCS#10) definiert den CSR als signierte Datenstruktur, die den Subject Name, den öffentlichen Schlüssel und optionale Attribute enthält. Die Signatur über die Request-Information dient als Nachweis, dass der Antragsteller den zugehörigen privaten Schlüssel besitzt.

Der Ablauf ist in Abbildung **??** dargestellt. Zunächst erzeugt das Gerät ein Schlüsselpaar und erstellt daraus einen CSR, der neben dem öffentlichen Schlüssel auch Metadaten enthalten kann (z. B. Seriennummer oder Geräteattribute). Anschließend wird der CSR vom Gerät mit dem privaten Schlüssel signiert und an eine RA übermittelt. Die RA prüft den Antrag gemäß den lokalen Richtlinien und leitet ihn im Erfolgsfall an die CA weiter. Die CA stellt daraufhin ein X.509-Zertifikat aus, signiert dieses und liefert es über die RA an das Gerät zurück. Das Gerät speichert das Zertifikat zusammen mit der notwendigen Zertifikatskette und kann es anschließend verwenden, um seine Identität in Authentisierungsprotokollen nachzuweisen.

Ablauf CSR

Bezug zur Arbeit Die beschriebenen Konzepte bilden ein etabliertes Fundament für sichere Verbindungsaufbauten: Ein Gerät besitzt eine kryptografische Identität (DevID), weist diese durch Besitz des privaten Schlüssels nach und nutzt darauf aufbauend eine PKI-gestützte Vertrauenskette zur Authentisierung. Darauf aufbauend können Sitzungsschlüssel abgeleitet werden, um Kommunikationsdaten effizient gegen Manipulation zu schützen und optional zu verschlüsseln. Im weiteren Verlauf der Arbeit werden diese Bausteine aufgegriffen und auf nicht IP-basierte Kommunikationskanäle übertragen, wobei insbesondere die Bereitstellung einer herstellerseitigen IDevID als zentraler Baustein dient.

3 Security und konzeptionelle Grundlagen von Feldgeräten

3.1 Einordnung von Feldgeräten in industrielle Systeme und Anlagen

Einleitung Kapitel schreiben

3.1.1 Funktion und Aufgaben von Feldgeräten

Feldgeräte nehmen eine zentrale Rolle in industriellen Automatisierungs- und Steuerungssystemen ein. Sie bilden die Schnittstelle zwischen der physischen Welt und übergeordneten Steuerungssystemen, indem sie Daten erfassen, verarbeiten und weiterleiten oder direkt in Prozesse eingreifen. Zu den typischen Feldgeräten gehören Sensoren, die physikalische Größen wie Temperatur, Druck, Messwerte, Füllstand oder Durchfluss messen, sowie Aktoren, die mechanische Bewegungen oder andere Aktionen ausführen. Im Fokus dieser Thesis stehen Sensoren, während Aktoren nicht Gegenstand der Untersuchung sind.

Die Einsatzgebiete von Feldgeräten sind äußerst vielfältig und erstrecken sich über nahezu alle Industriezweige. In der Prozessindustrie, beispielsweise in der Chemie- oder Öl- und Gasindustrie, überwachen sie kritische Parameter, um die Sicherheit und Effizienz von Anlagen sicherzustellen. In der Fertigungsindustrie ermöglichen Feldgeräte eine präzise Erfassung von Zuständen und Prozessgrößen und bilden die Grundlage für automatisierte Produktionsabläufe. Auch in der Energieversorgung, etwa in Kraftwerken, Stromnetzen oder der Wasserwirtschaft, sind Feldgeräte unverzichtbar für die Überwachung und Steuerung technischer Anlagen. Die hier beschriebenen Einsatzmöglichkeiten beziehen sich sowohl auf Sensoren als auch auf Aktoren, die jeweils spezifische Aufgaben in den Prozessen übernehmen.

Feldgeräte unterscheiden sich zudem hinsichtlich ihrer Interaktion mit Menschen und Maschinen. Während einige Geräte über lokale Anzeige- und Bedienelemente verfügen und eine direkte Bedienung vor Ort erlauben, werden andere Feldgeräte ausschließlich maschinell über Steuerungen, Asset-Management-Systeme oder mobile Servicegeräte angesprochen.

Eine Statistik wie viele Feldgeräte es weltweit gibt -> VEGA?

Da Feldgeräte den realen physikalischen Zustand eines Prozesses erfassen und Prozessentscheidungen auf diesen Messwerten basieren, ist ihre zuverlässige und korrekte Funktion von entscheidender Bedeutung. Fehlerhafte oder manipulierte Messwerte können unmittelbare Auswirkungen auf die Verfügbarkeit, Produktqualität und Sicherheit industrieller Systeme haben.

3.1.2 Systemarchitekturen und Einbindung von Feldgeräten

Zur Einordnung von Funktionen, Systemen und Kommunikationsbeziehungen in industriellen Umgebungen wird häufig das Purdue-Modell (auch als Purdue Enterprise Reference Architecture, PERA, referenziert) verwendet. Es beschreibt ein hierarchisches Ebenenkonzept für

industrielle Produktions- bzw. Prozesssysteme und strukturiert die Aufgabenverteilung von der operativen Prozessausführung bis zur unternehmensweiten Planung. Dabei wird zwischen horizontaler Kommunikation (innerhalb einer Ebene) und vertikaler Kommunikation (zwischen unterschiedlichen Ebenen) unterschieden. Für die Ebenen 0 bis 4 ist das Modell weitgehend kompatibel mit dem in der Praxis verbreiteten fünfstufigen Ebenenkonzept der Automatisierungspyramide. Im Purdue-Ansatz werden jedoch zusätzlich Zonen zur Abgrenzung und Kopplung unterschiedlicher Domänen berücksichtigt, insbesondere eine Übergangszone (Level 3.5, OT-DMZ) sowie eine externe bzw. Internet-nahe Zone [2]. Damit rückt weniger die reine funktionale Hierarchie als vielmehr die Netzsegmentierung und die kontrollierte Gestaltung von Übergängen in den Vordergrund, um Kommunikationsflüsse zwischen Office-IT, OT/ICS und externen Netzen gezielt zu steuern und abzusichern [4].

In ►Bild **??** ist das Purdue-Modell als hierarchische Referenzarchitektur für industrielle OT/ICS-Umgebungen dargestellt. Die Abbildung verdeutlicht die Anordnung der Ebenen sowie deren typische Kopplungspunkte und Schnittstellen. Darüber hinaus sind beispielhafte Kommunikationspfade zwischen den Ebenen eingezeichnet, wodurch sowohl horizontale Informationsflüsse innerhalb einer Ebene als auch vertikale Informationsflüsse zwischen den Ebenen nachvollziehbar werden. Ergänzend zeigt die Darstellung den Einsatz von Sicherheitskomponenten wie Firewalls und unidirektionalen Übertragungseinrichtungen (Datendioden), mit denen Kommunikationsbeziehungen segmentiert und Datenflüsse gezielt auf eine Richtung beschränkt werden können.

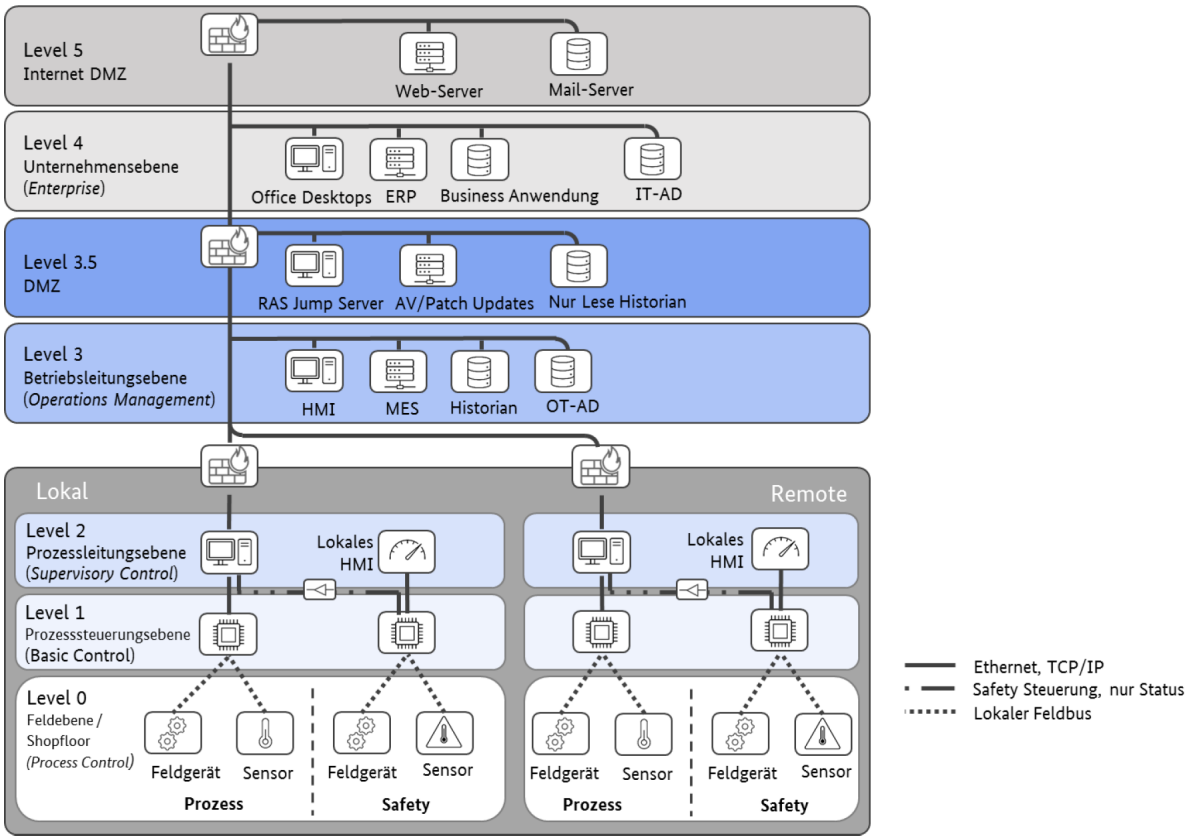

Bild 3.1. Beispiel Netzwerk nach Purdue/IEC 62443 Bildquelle: [5]

3.1.2.1 Einordnung in Ebenen des Purdue-Modells

Das Purdue-Modell ergänzt oberhalb der Produktionsführungs- und Unternehmensebene noch eine Internet Ebene, Ebene 5, welche die typische Kommunikation mit dem Internet (Web, Mail) repräsentiert.

Auf Ebene 4 (Unternehmensebene) findet typischerweise unter Nutzung eines ERP-Systems die übergeordnete Planung und Koordination betriebswirtschaftlicher Abläufe statt. Dazu zählen insbesondere die Grobplanung der Produktion sowie unterstützende Funktionen für Organisationsbereiche wie Vertrieb (z. B. Erfassung von Kundenaufträgen) und Einkauf (z. B. Beschaffung von Materialien), welche in einem ERP-System abgebildet werden können [2].

Eine weitere, wichtige Erweiterung ist die Übergangszone Ebene 3.5 (OT-DMZ) zwischen der Office-IT und der Produktion. Als Demilitarized Zone verhindert diese Zone eine direkte Kommunikation zwischen den beiden Segmenten. Informationen werden ausschließlich über in der DMZ bereitgestellte Schnittstellen ausgetauscht. Idealerweise wird die Verbindung hierbei von der Zone mit dem höheren Schutzbedarf aus aufgebaut. Da das ICS (Industrial Control System) in der Regel einen höheren Schutzbedarf als die Office-IT aufweist, wird die Verbindung von dieser Seite initiiert. So dürfen zum Beispiel ICS-Systeme Daten auf eine Datenbank in der DMZ schreiben, die Office Systeme hier aber nur lesend zugreifen.

Auf Ebene 3 (Betriebsleitungsebene) erfolgt eine detailliertere Planung und Steuerung der Produktion. Hier kommen häufig Manufacturing Execution Systems (MES) an den jeweiligen Produktionsstandorten zum Einsatz. Ein MES-System überwacht, steuert und optimiert in Echtzeit alle produktionsnahen Prozesse, einschließlich Betriebs-, Maschinen- und Personaldatenerfassung, sowie Material-, Qualitäts- und Energiemanagement, um eine effiziente Fertigung sicherzustellen [2]. Diese Ebene bildet die Schnittstelle zwischen der betriebswirtschaftlich orientierten Organisationsebene und den operativen Produktions- und Automatisierungssystemen.

Die Überwachung und operative Prozessführung erfolgt auf Ebene 2 (Prozessleitungsebene). Auf dieser Ebene werden typischerweise Supervisory Control and Data Acquisition (SCADA)-Systeme sowie Prozessleitsysteme (PLS) zur Produktionsdatenerfassung, -visualisierung und -kontrolle eingesetzt. Sie unterstützen unter anderem die Anzeige und Auswertung von Betriebsdaten sowie die Überwachung von Anlagenzuständen und Prozessparametern.[2].

Auf Ebene 1 (Prozesssteuerungsebene) übernehmen speicherprogrammierbare Steuerungen (SPS; engl. PLC) und zugehörige Ein-/Ausgabekomponenten (I/O) die lokale Steuerung und Regelung. Über diese Komponenten werden Signale aus der Feldebene verarbeitet und Stellgrößen an den Prozess ausgegeben. Die Steuerungsebene wirkt damit unmittelbar auf den Prozess ein.

In der Feldebene (Ebene 0) befinden sich die Komponenten, die Informationen aus dem materiellen Produktions- bzw. Prozessgeschehen erfassen oder als Aktoren direkt darauf einwirken. Dazu zählen beispielsweise Endschalter und Sensoren, die im Folgenden als Feldgeräte zusammengefasst werden. Diese Komponenten interagieren einerseits direkt mit dem physikalischen Prozess und andererseits, über eine zugehörige Infrastruktur (z. B. Anschluss- und Kopplungskomponenten), mit den informationsverarbeitenden Einheiten der darüberliegenden Ebenen. Für die Kommunikation auf Ebene 0 besteht grundsätzlich die Notwendigkeit, Sensordaten und Aktorbefehle unter deterministischen bzw. echtzeitnahen Bedingungen zu übertragen.

Zusätzlich müssen bei Bedarf Diagnose- und Konfigurationsdaten übermittelt werden, etwa für Inbetriebnahme, Wartung oder Parametrierung [4].

3.1.2.2 Kommunikation der Schichten

Die horizontale und vertikale Kommunikation wird in der Praxis häufig über Feldbus- und Automatisierungsnetzwerke realisiert, die je nach Systemarchitektur und Generation sowohl ethernetbasiert als auch nicht ethernetbasiert ausgeprägt sein können.

Die Kommunikation in ICS ist nicht auf die jeweilige Ebene beschränkt. So kann der Wert eines Füllstandsensor eines Ventils auf Ebene 0 über eine SPS auf Ebene 1 an eine Software auf Ebene 2 übertragen werden. Für die ebenenübergreifende Kommunikation kommen häufig Gateways zum Einsatz. Das Gateway (Ebene 1) wandelt Daten des I/O-Subsystems auf dem Feldbus (Ebene 0) in ein anderes Protokoll um und leitet diese an ein System auf Ebene 2 weiter. Von dort wird die Kommunikation zu Ebene 3 und 4 jeweils durch eine Firewall gefiltert und über die DMZ, die als Sicherheitszone eine direkte Kommunikation zwischen Netzwerken verhindert, geleitet. So können Daten zwischen verschiedenen Systemen ausgetauscht werden, aber nicht jedes System muss mit jedem direkt kommunizieren. Das ERP-System benötigt zum Beispiel keine Sensordaten von I/O Systemen auf dem Feldbus [4].

Absatz unterschied ethernet basiert und nicht

In bestimmten Industriebereichen, insbesondere in der Prozessindustrie, sind zudem weiterhin zahlreiche Feldgeräte im Einsatz, die Messwerte über eine 4–20 mA Stromschleife analog liefern. Häufig wird dies durch eine zusätzliche digitale Kommunikation ergänzt die wenig Energie benötigt und über die Konfigurations- oder Diagnosedaten übertragen werden können (z. B. über HART) [14].

Drahtlose Kommunikation kann ebenfalls Bestandteil horizontaler und vertikaler Kommunikationsstrukturen sein. Da der Fokus dieser Arbeit jedoch auf kabelgebundenen Kommunikationspfaden liegt, wird drahtlose Kommunikation im weiteren Verlauf nicht vertieft.

3.1.2.3 Abgrenzung OT/IT

Die in der Vergangenheit übliche physische Trennung der OT von anderen IT-Systemen und Datennetzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Mehrstufige Produktionsschritte und deren übergreifende Steuerung sowie regulatorische Anforderungen machen es zunehmend notwendig, die OT auch über Organisationsgrenzen hinweg zu öffnen. Dieser Prozess wird häufig als IT/OT-Konvergenz bezeichnet, ein Begriff, der die zunehmende Verschmelzung von Informationstechnologie (IT) und Betriebstechnologie (OT) beschreibt. Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen noch beschleunigt, vor allem im Rahmen der Industrie 4.0.[4].

3.1.3 Security-Relevante Bedeutung von Feldgeräten

3.1.3.1 Feldgeräte als Einfallspunkt für Angriffe

Jedes Feldgerät, das in ein OT-Netzwerk bzw. ICS integriert wird, erweitert die Funktionalität des Gesamtsystems und zugleich auch dessen Angriffsfläche. Abhängig von Fähigkeiten und Kommunikationsschnittstellen, sowie der Einbindung in die Systemarchitektur, können von einzelnen Feldgeräten verschiedene Risiken ausgehen.

Betrachtet man die grundlegende Funktionalität von Feldgeräten, insbesondere von Sensoren, so lassen sich in den meisten Fällen, ausgenommen rein analoge Geräte ohne Kommunikationsschnittstellen, zwei wesentliche Kommunikationspfade unterscheiden. Der Sensor-Channel zur Übertragung von Messwerten an übergeordnete Steuerungen sowie der Control-Channel, über den Parametrierung, Konfiguration oder Diagnose erfolgt.

Ein Angriff über den Control-Channel zielt darauf ab, eine Systemkomponente aus einer höheren Kommunikationsschicht, zu kompromittieren, um anschließend manipulierte Befehle in das System einzuschleusen[13].

In der Praxis kann dies beispielsweise über ausgenutzte Schwachstellen in Feldbus- oder Serviceprotokollen erfolgen. Wie in [1] gezeigt wurde, können manipulierte HART-Kommandos nicht nur Feldgeräte beeinflussen, sondern unter bestimmten Bedingungen auch weiterführende IT-Systeme bis hin zur Unternehmensebene kompromittieren. Der Control-Channel eines Feldgeräts kann somit als Einstiegspunkt dienen, um über legitime Kommunikationsbeziehungen weiter in den OT- oder sogar IT-Bereich vorzudringen.

Im Gegensatz dazu zielen Sensor-Channel-Angriffe auf die Manipulation der vom physikalischen Prozess gelieferten Messwerte. Hierbei werden Sensordaten verfälscht, sodass Steuerungen oder Leitsysteme auf Grundlage falscher Informationen Entscheidungen treffen. Ziel ist es, das Verhalten des Reglers gezielt zu beeinflussen oder einen realen Prozesszustand zu verschleiern. Diese als False-Data-Injection (FDI) bezeichneten Angriffe wurden ursprünglich im Kontext von Energieversorgungssystemen und Smart Grids beschrieben, gelten jedoch aufgrund der zunehmenden Vernetzung industrieller Anlagen als generisches Risiko für ICS-Umgebungen. Da industrielle Prozesse häufig sicherheitskritisch sind und erhebliche ökologische, wirtschaftliche oder gesellschaftliche Auswirkungen haben können, werden Manipulationen von Sensordaten als besonders schwerwiegender Angriffsvektor betrachtet. So kann beispielsweise eine künstlich abgesenkte Temperaturmessung dazu führen, dass die Heizleistung erhöht wird, obwohl keine tatsächliche Abweichung vorliegt, was im Extremfall zu einer unentdeckten Überhitzung führen kann. [7, 13].

3.1.3.2 Abgrenzung Safety - Security

Cybersicherheit (Security) dient dem Schutz von OT-Systemen vor mutwilligen Manipulationen, die deren bestimmungsgemäßen Betrieb beeinträchtigen oder verhindern können. Ziel ist es, die Integrität, Verfügbarkeit und Vertraulichkeit der Systeme sowie deren sichere Funktionsfähigkeit aufrechtzuerhalten. Hierzu zählt insbesondere auch der Schutz sicherheitskritischer Funktionen, die im Rahmen der Funktionalen Sicherheit implementiert sind.

Die Funktionale Sicherheit (Safety) verfolgt das Ziel, Menschen, Umwelt und Anlagen vor Gefährdungen zu schützen, die aus Fehlfunktionen technischer Systeme resultieren können [4]. Sie adressiert somit unbeabsichtigte Fehlerzustände, während Security vorsätzliche Angriffe berücksichtigt.

Cyberangriffe können jedoch unmittelbar Einfluss auf die Funktionale Sicherheit nehmen, indem sie sicherheitsgerichtete Systeme manipulieren oder außer Kraft setzen. Ein prägnantes Beispiel hierfür ist die im Jahr 2017 entdeckte TRITON-Malware. Diese zielte auf das Safety Instrumented System (SIS) einer petrochemischen Anlage in Saudi-Arabien ab und versuchte, dessen Schutzfunktionen gezielt zu manipulieren. Dadurch wurde die Fähigkeit des Systems, gefährliche Prozesszustände zu erkennen und abzusichern, beeinträchtigt, was potenziell zu schweren Personen- und Umweltschäden hätte führen können [6]. Der Vorfall verdeutlicht, dass Security-Schwachstellen direkte Auswirkungen auf die Safety eines Systems haben können.

Obwohl Safety und Security unterschiedliche Zielrichtungen verfolgen und jeweils eigene normative Rahmenwerke besitzen, sind sie in OT-Umgebungen eng miteinander verknüpft. Während Safety den Schutz von Menschen, Umwelt und Anlagen durch das System adressiert, zielt Security auf den Schutz des Systems vor externer Manipulation ab [4]. Im deutschen Sprachgebrauch wird der Begriff „Sicherheit“ häufig für beide Aspekte verwendet. Sofern in dieser Arbeit nicht ausdrücklich anders gekennzeichnet, bezieht sich der Begriff auf Security im Sinne der Informations- und Cybersicherheit.

3.2 Regulatorische Anforderungen an Feldgeräte

Mit der zunehmenden Vernetzung industrieller Systeme gewinnen regulatorische Anforderungen an die Cybersicherheit von Feldgeräten zunehmend an Bedeutung. Neben technischen Schutzmaßnahmen auf Systemebene werden auch konkrete Vorgaben an die sichere Entwicklung, Integration und den Betrieb einzelner Komponenten gestellt. Insbesondere Hersteller von Feldgeräten sind verpflichtet, Security-Aspekte bereits im Entwicklungsprozess zu berücksichtigen und geeignete Schutzmechanismen umzusetzen.

Im Folgenden werden die für Feldgeräte besonders relevanten Anforderungen der IEC 62443-4-2 sowie die regulatorischen Vorgaben des Cyber Resilience Act näher betrachtet.

3.2.1 IEC 62443-4-2

Die Normenreihe IEC 62443 stellt Anforderungen zur Gewährleistung von IT-Sicherheit für industrielle Automatisierungs- und Kontrollsysteme (IACS[1]). Sie umfasst funktionale Anforderungen an Automatisierungslösungen, -systeme und -komponenten sowie prozessorientierte Vorgehensmodelle für den Betrieb, die Systemintegration und die Produktentwicklung. Die Norm richtet sich an Hersteller, Integratoren, Betreiber und besteht aus mehreren Teilnormen [4].

[1] Der in der Normenreihe IEC 62443 verwendete Begriff Industrial Automation and Control Systems (IACS) ist Synonym mit dem in der Thesis verwendeten Begriff Industrial Control Systems (ICS).

Für die Entwicklung von Feldgeräten ist insbesondere die Teilnorm IEC 62443-4-2 von Bedeutung. Sie definiert technische Sicherheitsanforderungen auf Komponentenebene und legt fest, welche Security-Funktionen industrielle Geräte erfüllen müssen, um einem bestimmten Security-Level zu entsprechen. Dieses Security-Level spiegelt das angestrebte Schutzniveau gegenüber unterschiedlich leistungsfähigen Angreifern wider.

Die IEC 62443-4-2 legt technische Sicherheitsanforderungen für Komponenten industrieller Automatisierungs- und Kontrollsysteme fest. Grundlage bilden sieben sogenannte grundlegende Anforderungen (Foundational Requirements, FR). Diese adressieren die Bereiche:

1. Identifizierung und Authentifikation,
2. Nutzungskontrolle,
3. Systemintegrität,
4. Vertraulichkeit der Daten,
5. eingeschränkter Datenfluss,
6. rechtzeitige Reaktion auf sicherheitsrelevante Ereignisse und
7. Verfügbarkeit der Ressourcen.

Für jede FR werden Security Levels (SL) definiert, die das angestrebte Schutzniveau gegenüber Angreifern mit zunehmenden Fähigkeiten, Ressourcen und Motivation beschreiben (SL 1 bis SL 4). Für Komponenten wird der erreichbare Schutzgrad pro FR, von 0 bis 4 angegeben. Wobei SL 0 bedeutet, dass für die jeweilige FR keine spezifischen Anforderungen gelten, und SL 1 bis SL 4 steigende technische Schutzmaßnahmen voraussetzen.

Die einzelnen Security-Levels haben folgende Bedeutung:

Stufe	Definition
SL 0	Kein Security-Schutz
SL 1	Schutz vor zufälligem Abhören oder unbeabsichtigtem Aufdecken.
SL 2	Schutz vor gezieltem Abhören mit einfachen Mitteln, geringer Motivation und grundlegenden Fähigkeiten.
SL 3	Schutz vor gezieltem Abhören mit fortgeschrittenen Mitteln, mittlerer Motivation und spezialisierten Fähigkeiten.
SL 4	Schutz vor gezieltem Abhören mit hochentwickelten Mitteln, hoher Motivation und umfassenden spezialisierten Fähigkeiten.

Kann eine Anforderung nicht allein durch die Komponente erfüllt werden, sind ergänzende Maßnahmen auf Systemebene erforderlich; entsprechende Kompensationsmaßnahmen sind vom Hersteller zu dokumentieren [11].

Ist ein Produkt nach dieser Norm zertifiziert, so wird ein Zertifikat von einer unabhängigen Prüfstelle ausgestellt, die das entsprechende Security-Level angibt. In [21] ist ein solches Zertifikat dargestellt.

3.2.2 Cyber Resilience Act

Der Cyber Resilience Act (CRA) verfolgt das Ziel, die Cybersicherheit von „Produkten mit digitalen Elementen“ in der Europäischen Union zu erhöhen und hierfür einheitliche Mindestanforderungen festzulegen. Produkte mit digitalen Elementen sind im CRA solche Produkte, die direkt oder indirekt mit einem Gerät oder einem Netzwerk verbunden werden können. Damit soll Cybersicherheit nicht nur als freiwillige Qualitätsmaßnahme verstanden werden, sondern als verbindlicher Bestandteil der Produktkonformität. Hersteller sollen bereits bei der Entwicklung sicherstellen, dass ihre Produkte gegenüber typischen Bedrohungen angemessen geschützt sind, und sie müssen die Sicherheit zudem über den gesamten Produktlebenszyklus hinweg aufrechterhalten [15].

Für die Entwicklung von Feldgeräten bedeutet dies vor allem eine Verschiebung von Best Practice hin zu nachweisbaren, konformitätsrelevanten Anforderungen. Hersteller müssen Bedrohungen und Risiken systematisch bewerten und daraus technische und organisatorische Maßnahmen ableiten, beispielsweise zum Schutz vor unbefugtem Zugriff, zur Sicherstellung der Integrität von Firmware und Konfiguration, zur Geheimhaltung der gespeicherten Daten, sowie zur Etablierung eines strukturierten Schwachstellenmanagement [10].

In der Praxis kann dies über bereits etablierte Normen und Sicherheitsstandards realisiert werden. Mappings, welche CRA-Anforderungen mit bestehenden Normen und Sicherheitspraktiken in Beziehung setzen, unterstützen eine pragmatische Umsetzung und erleichtern die Ableitung konkreter Entwicklungs- und Nachweispflichten. Da viele CRA-Zielrichtungen (z. B. systematische Risikoanalyse, sichere Produktentwicklung, Schutz zentraler Sicherheitsziele) inhaltlich mit Anforderungen der IEC 62443-Familie kompatibel sind, können Hersteller, die ihre Produktentwicklung bereits an dieser Normenreihe ausrichten, wesentliche CRA-Anforderungen konsistent abdecken [9].

Eine besondere Herausforderung stellen Feldgeräte dar, die nicht ethernetbasiert sind, wie sie z. B. häufig in der Prozessindustrie vorkommen. Solche Geräte verfügen häufig nur über eingeschränkte oder gar keine kryptographischen Schutzmechanismen, da ihre Rechenleistung, Energieversorgung oder Protokolleigenschaften dies nicht vorsehen. Ihre Messwerte werden entweder analog oder über ältere Feldbus-Mechanismen übertragen, und es nicht zu erwarten, dass diese Feldbusse in Zukunft mit Sicherheitsfunktionen ausgestattet werden [14]. Da diese Geräte jedoch digitale Elemente wie Firmware, digitale Parametrierung, Diagnosedaten oder Konfigurationsschnittstellen besitzen, fallen auch diese Geräte unter die Anforderungen des CRA. Für Hersteller ergibt sich daraus die zentrale Frage, wie CRA-relevante Vorgaben bei begrenzten Kommunikations- und Sicherheitsressourcen technisch sinnvoll umgesetzt und nachvollziehbar begründet werden können.

Da die Anforderungen aus dem CRA für neue Produkte erst ab Dezember 2027 greift, liegen derzeit nur begrenzte praktische Erfahrungen zur konkreten Ausgestaltung der Konformitätsprozesse bei Feldgeräten vor [15]. Vor diesem Hintergrund ist die in dieser Arbeit vorgenommene Untersuchung besonders relevant. Sie adressiert die Frage, wie auch nicht ethernetbasierte Feldgeräte kryptographisch gestützte Sicherheitsmaßnahmen und belastbare Schutzkonzepte umsetzen können, um zukünftige regulatorische Anforderungen und Nachweiserwartungen zu erfüllen.

3.3 Zentrale Schutzziele für Feldgeräte

Die Sicherheit moderner IT- und OT-Systeme stützt sich unter anderem auf das Konzept der Informationssicherheit. Dieses umfasst Maßnahmen und Strategien, die darauf abzielen, Systeme, Daten und Kommunikation vor unbefugtem Zugriff, Manipulation und Ausfällen zu schützen Informationssicherheit bildet eine wesentliche Grundlage für die Entwicklung sicherer Feldgeräte und damit auch für den Aufbau zuverlässiger und sicherer Anlagen.

Ein zentrales Element der Informationssicherheit sind sogenannte Schutzziele. Diese beschreiben, welche sicherheitsrelevanten Eigenschaften eines Systems oder einer Komponente erhalten bleiben müssen, um einen sicheren Betrieb zu gewährleisten. Für Feldgeräte, die in sicherheitskritischen Umgebungen eingesetzt werden, sind Schutzziele von besonderer Bedeutung, da sie die Grundlage für den Schutz vor Angriffen und die Gewährleistung eines zuverlässigen Betriebs bilden.

Die CIA-Triade und deren Anwendung in OT-Systemen Die CIA-Triade ist ein zentrales Konzept der Informationssicherheit und definiert drei grundlegende Schutzziele:

- Geheimhaltung (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

Sie dient als Grundlage für die Bewertung und den Schutz von IT- und OT-Systemen.

Während in IT-Systemen die Geheimhaltung oft oberste Priorität hat, stehen in OT-Systemen die Integrität und Verfügbarkeit im Vordergrund. Dies liegt daran, dass ein Systemausfall oder die Manipulation von Daten direkte Auswirkungen auf physische Prozesse haben kann. Die Vertraulichkeit von Daten spielt hier im Vergleich eine geringere Rolle [19].

Die Normenreihe IEC 62443-4-2 konkretisiert diese Schutzziele auf Komponentenebene und definiert sieben Foundational Requirements (FR), die als normative Schutzziele interpretiert werden können. Diese Anforderungen adressieren zentrale Sicherheitsaspekte wie Authentifikation, Zugriffskontrolle und Integrität und bieten einen klaren Rahmen für die Entwicklung sicherer Feldgeräte. Es wurde auch noch das Schutzziel *Organisation* hinzugefügt, das verdeutlicht, das diese Anforderungen mittels organisatorischer Maßnahmen umgesetzt werden müssen.

Die Zuordnung in Schutzziel macht keinen Sinn

Da sich diese Thesis mit dem sicheren Verbindungsaufbau bei Feldgeräten ohne Netzwerkschnittstelle befasst, werden Anforderungen, die ausschließlich durch organisatorische oder bauliche Maßnahmen in der Umgebung umgesetzt werden können, im weiteren Verlauf nicht vertieft. Für die Eingrenzung des Untersuchungsumfangs werden die aus IEC 62443-4-2 abgeleiteten Anforderungen danach unterschieden, ob sie durch den Kommunikationsmechanismus adressierbar sind oder außerhalb des Einflussbereichs eines Protokolls liegen. Daraus ergibt sich eine Einteilung in drei Klassen, nach [15]:

1. Anforderungen, die für das betrachtete Feldgerätprofil nicht relevant sind (z. B. Notstromversorgung, Schutz der Zonengrenze).

Tabelle sauber beschrieben in Latex einfügen.

IEC	Schutzziel	Erklärung	Beispiel
1. Identifizierung und Authenfikation	Integrität	Alle Nutzer müssen sich identifizieren und authentifizieren, bevor Zugriff auf das System gewährt wird	Zertifkate
2. Nutzungskontrolle	Integrität	Rollenbasierter Zugriff Jedem Nutzer werden entsprechende Berechtigungen zugewiesen	Benutzerkonten
3. Systemintegrität	Integrität	Die Integrität der Komponente muss sichergestellt werden	Physischer Zugriffsschutz Individuelle Sitzungskennungen
4. Vertraulichkeit der Daten	Geheimhaltung	Schutz von Informationen bei Speicherung und Übertragung	Zugriffsschutz Verschlüsselung
5. eingeschränkter Datenfluss,	Organisation	Einteilung einer Anlage in verschiedene Zonen	Zugriff auf IT-Netz unterbinden
6. rechtzeitige Reaktion auf sicherheitsrelevante Ereignisse und	Organisation	Sicherheitsverletzungen werden dokumentiert	Ereignisprotokoll
7. Verfügbarkeit der Ressourcen	Verfügbarkeit	Verfügbarkeit der Komponente wird sichergestellt	Physischer Zugrifssschutz Untebinden mehrer Sessions

Bild 3.2. Mapping der Anforderungen -> DELETE

2. Anforderungen, die unmittelbar durch kryptografische Mechanismen auf der Kommunikationsstrecke umgesetzt werden können (z. B. Integritätsschutz und Vertraulichkeit der übertragenen Daten).

3. Anforderungen, die sicherheitsrelevant sind, deren Umsetzung jedoch primär von der Geräteplattform abhängt (z. B. Integrität beim Software-Update, Integrität des Boot-Prozesses).

Die vorliegende Arbeit fokussiert daher auf Klasse 2, da nur diese Anforderungen direkt durch den Verbindungsaufbau, die Authentisierung und die Aushandlung von Sitzungsschlüsseln auf Protokollebene beeinflussbar sind. Angriffe auf die Verfügbarkeit, die durch physischen Zugriff oder Zerstörung des Geräts entstehen, können durch ein Kommunikationsprotokoll hingegen nicht verhindert werden.

3.4 Stand der Technik

3.4.1 Stand der Technik bei nicht netzwerkfähigen Feldgeräten

Wie in Abschnitt **??** abgegrenzt, fokussiert diese Arbeit auf Anforderungen der Kommunikationssicherheit (Klasse 2 der Anforderungen), also auf kryptografische Mechanismen zur Authentisierung sowie zum Integritäts- und optional Vertraulichkeitsschutz der übertragenen Daten. Für nicht netzwerkfähige Feldgeräte sehen die zugehörigen Feldbusstandards solche Mechanismen typischerweise nicht vor. Keiner der gängigen Feldbusse, weder HART, PROFIBUS PA, OPC noch MODBUS unterstützt Sicherheitsfunktionen in Bezug auf Integrität, Verschlüsselung oder Authentifizierung auf Protokollebene. Auch ist nicht davon auszugehen, dass sich dies in absehbarer Zeit ändern wird [3][14]. In der Praxis werden die fehlenden Protokollmechanismen daher überwiegend durch Maßnahmen der Umgebung (Klasse 1) sowie durch gerätespezifische Härtungsmaßnahmen (Klasse 3) kompensiert.

Die Ursachen für das Fehlen protokollseitiger Sicherheitsmechanismen sind vielfältig und historisch gewachsen.

Physischer Schutz und Air-Gaps Die folgenden Maßnahmen adressieren primär Anforderungen der Klasse 1, da sie außerhalb des Einflussbereichs eines Feldbusprotokolls liegen und durch Anlagenbetrieb und Umgebung umgesetzt werden. ICS-Anlagen befinden sich in der Regel in physisch abgesicherten Bereichen, die durch Zäune, Mauern oder vergleichbare Barrieren geschützt sind. Der Zugang zu den Feldgeräten ist dabei auf das vor Ort tätige Betriebspersonal sowie auf externe Dienstleister, etwa für Inbetriebnahme oder Wartung, beschränkt [14]. Zusätzlich wurden insbesondere ältere Anlagen häufig physisch von anderen Netzwerken isoliert, um sie vor Cyberangriffen zu schützen. Da sich die Geräte in einem abgeschotteten Bereich befanden und nicht von außen erreichbar waren, wurde lange Zeit argumentiert, dass dieser Schutz ausreichend sei [4].

Diese sogenannten *Air-Gaps*, also die vollständige Trennung von IT und OT, erreichen in der Praxis jedoch selten das angestrebte Schutzniveau. Häufig ist trotz der physischen Trennung ein Datenaustausch zwischen den Netzen notwendig oder gewünscht, und genau diese Schnittstellen können von Angreifern ausgenutzt werden, um die Isolation zu überwinden [4]. Darüber hinaus ist eine vollständige Trennung der OT von der IT heute nur noch in Ausnahmefällen und bei besonders hohem Schutzbedarf umsetzbar. Mehrstufige Produktionsprozesse, deren systemübergreifende Steuerung sowie regulatorische Vorgaben erfordern zunehmend eine Vernetzung der OT, auch über Organisationsgrenzen hinweg. Verstärkt wird diese Entwicklung durch den Trend zur Optimierung von Fertigungsprozessen im Kontext von Industrie 4.0 [5].

Selbst bei ausreichender Absicherung der OT und einem physischen Zugangsschutz bestehen weiterhin Risiken, da Angreifer mit internem Zugriff auf das Automatisierungsnetzwerk oder mit direktem Zugang zum Feldgerät gezielt Schwachstellen ausnutzen könnten. Eine Studie von Bitkom zeigt, dass interne Bedrohungen eine erhebliche Gefahr darstellen: 62 % der Angriffe auf deutsche Unternehmen gehen von aktuellen oder ehemaligen Mitarbeitern aus [20]. Mit entsprechendem Zugang wäre es beispielsweise möglich, ein Feldgerät unbemerkt durch ein manipuliertes Gerät auszutauschen.

Darüber hinaus gibt es Einsatzszenarien, in denen ein flächendeckender physischer Schutz nicht realisierbar ist. Auch wenn das Feldgerät selbst und zugehörige Komponenten wie Gateways vor unbefugtem Zugriff geschützt sind, können Verbindungsleitungen, insbesondere bei größeren Distanzen, ungeschützt verlaufen. Ein charakteristisches Beispiel ist die Füllstandsmessung an einem Stausee oder Überlaufbecken, wo die Messleitungen über längere Strecken außerhalb kontrollierten Bereichs verlaufen können.

Technische Einschränkungen Neben den physischen Schutzmaßnahmen spielen auch technische Limitierungen eine wesentliche Rolle für das Fehlen protokollseitiger Sicherheitsmechanismen der Klasse 2.

Viele der heute eingesetzten Feldgeräte stammen aus einer Zeit, in der Cybersicherheitsbedrohungen noch nicht in dem heutigen Ausmaß existierten. Diese Legacy-Systeme verfügen weder über die erforderliche Hardware noch über die Softwareunterstützung, um moderne Sicherheitsverfahren umzusetzen. Da Anlagen im OT-Umfeld häufig über mehrere Jahrzehnte

betrieben werden, ist eine große installierte Basis solcher Geräte nach wie vor im Einsatz [19].

Kryptografische Verfahren, insbesondere asymmetrische Algorithmen, sind ohne dedizierte Krypto-Peripherie vergleichsweise rechenintensiv. Zusätzlicher Rechenaufwand aufgrund Berechnung kryptographischer Operationen würde die verfügbare Verarbeitungszeit zusätzlich beanspruchen und steht damit in direktem Konflikt mit den begrenzten Ressourcen der Feldgeräte [13].

Kryptographische Operationen, stehen zudem auch im Konflikt mit dem Energieverbrauch der Fedlgeräte. Nicht netzwerkfähige Feldgeräte sind häufig für besonders robuste und energieeffiziente Betriebsbedingungen ausgelegt. Bei 2-Draht-Geräten muss die gesamte Elektronik aus dem begrenzten Energiehaushalt der 4 mA–20 mA-Stromschleife versorgt werden. Abzüglich Toleranzen und Reserven stehen dabei lediglich ca. 3,5 mA für die interne Elektronik zur Verfügung [12]. Mikrocontroller werden daher häufig mit niedrigen Taktraten betrieben und die verfügbaren Ressourcen auf das für Messwerterfassung, Signalverarbeitung, Diagnose und Kommunikation notwendige Minimum optimiert. Zwischen Verarbeitungsdauer, Energieverbrauch und Sicherheitsniveau muss somit stets ein Kompromiss gefunden werden. In der Konsequenz wurden Sicherheitsmechanismen in vielen Feldgeräten entweder gar nicht vorgesehen oder auf einfache Schutzfunktionen wie Schreibschutz, PIN-basierte Sperren oder rein organisatorische Maßnahmen beschränkt [4].

Einordnung nach IEC 62443 und kompensierende Maßnahmen In der IEC-62443-Familie werden Sicherheitsanforderungen für Komponenten im Kontext eines übergreifenden Zonen- und Leitungsmodells betrachtet, das dem Prinzip einer Defense in Depth Strategie folgt, indem mehrere Schutzschichten kombiniert werden (z. B. organisatorische Maßnahmen, physischer Schutz, Netzwerksegmentierung und Komponentenhärtung). Für nicht netzwerkfähige Feldgeräte zeigt sich dabei ein typisches Bild: Anforderungen der Klasse 1 dominieren den Betriebsschutz, plattformspezifische Maßnahmen der Klasse 3 sind je nach Gerätegeneration teilweise vorhanden, während die protokollseitige Absicherung der Kommunikation (Klasse 2) auf dem Feldbus in der Regel fehlt. Insbesondere Security Level 2 wird in vielen Industriepublikationen als das niedrigste Niveau eingeordnet, ab dem Schutz gegen vorsätzlichen Missbrauch adressiert wird [15]. Dies verdeutlicht die Lücke zwischen klassischen Feldgeräteprotokollen ohne integrierte Security-Funktionen und den Anforderungen, die bei gezielten Angriffen typischerweise relevant werden.

Praxisbeispiel: Security-Umsetzung bei einem nicht netzwerkfähigen Feldgerät Am Beispiel eines 2-Draht-Feldgeräts (VEGAPULS 6X mit 4 … 20 mA/HART) zeigt sich, dass Sicherheitsfunktionen in der Praxis stark auf lokale Schutzmechanismen und organisatorische Maßnahmen verteilt werden. Die zugehörige Security Guideline [22] weist explizit darauf hin, dass das standardisierte HART-Protokoll keinen ausreichenden Schutz gegen Datenmanipulation und Spionage bietet und deshalb nur in einer Umgebung mit Schutzniveau entsprechend SL1 bzw. bei sichergestelltem physischem Zugriffsschutz auf die Signalleitungen betrieben werden soll. Damit werden zentrale Risiken durch Maßnahmen der Klasse 1 (physischer Zugriffsschutz, Betriebsvorgaben) adressiert und um ausgewählte geräteinterne Funktionen der Klasse 3 ergänzt. Für Schnittstellen und den Gerätezugang werden daher Maßnahmen wie

Zugriffsschutz per Passwort, Deaktivierung ungenutzter Kommunikationskanäle sowie physische Sicherungen (z. B. Verplombung) gefordert. Geräteseitig werden zudem Funktionen wie Firmware-Integritätsprüfungen, Ereignisspeicher und Ressourcenmanagement als Sicherheitsfunktionen genannt. Diese Maßnahmen erhöhen die Härtung des Geräts, ersetzen jedoch keinen kryptografisch geschützten Kommunikationskanal auf dem Feldbus.

Verbleibende Lücken auf Protokollebene Aus Sicht der Schutzziele Vertraulichkeit und Integrität verbleibt bei nicht netzwerkfähigen Feldgeräten insbesondere eine Lücke in den Anforderungen der Klasse 2, also in der Ende-zu-Ende-Absicherung der Kommunikation.

Während Integrität im Feldbuskontext häufig nur über einfache Prüfsummen oder CRC-Mechanismen adressiert wird, existieren typischerweise keine Verfahren zur kryptografischen Authentifizierung von Geräten, keine aushandelbaren Sitzungsschlüssel und keine Verschlüsselung der Nutzdaten auf der Leitung. Damit kann ein Angreifer mit physischem Zugriff auf die Signalleitung Daten mitlesen oder manipulieren, ohne durch das Protokoll selbst zuverlässig detektiert oder ausgeschlossen zu werden. Genau an dieser Stelle setzt die vorliegende Arbeit an, indem eine gerätebasierte Identität über Zertifikate und ein sicherer Verbindungsaufbau auch für nicht IP-basierte Kommunikationskanäle konzipiert und umgesetzt wird.

Kryptografie als Option auf modernen Feldgeräten Obwohl die Feldbusprotokolle nicht IP-basierter Geräte die Anforderungen der Klasse 2 weiterhin kaum adressieren, haben sich die technischen Rahmenbedingungen für Feldgeräte in den letzten Jahren deutlich verschoben. Moderne Mikrocontroller integrieren dedizierte Krypto-Peripherie bzw. Hardwarebeschleuniger, sodass kryptografische Verfahren nicht mehr zwangsläufig im Widerspruch zu den typischen Restriktionen (begrenzte Rechenleistung, enger Energiehaushalt, zeitliche Anforderungen) stehen. Hierbei werden kryptographische Primitive, in speziell dafür entwickelten Hardwareblöcken berechnet, wodurch einerseits der Przoessor entlastet wird und die kryptographischen Berechnungen deutlich schneller und effizienter berechnet werden [18].

Definition Kryptografische Primitive raussuchen

Beispielhafte Messungen auf einem STM32U3 verdeutlichen die Größenordnung: Für AES-128-GCM erreicht die Hardware[2] etwa 9,17 $\mathrm{MB\,s^{-1}}$, während eine Software-Implementierung auf demselben Controller bei etwa 0,76 $\mathrm{MB\,s^{-1}}$ liegt. Für SHA-256 wurden 45,87 $\mathrm{MB\,s^{-1}}$ (Hardware) gegenüber 1,355 $\mathrm{MB\,s^{-1}}$ (Software) gemessen [16]. Das entspricht einer Beschleunigung um etwa den Faktor 12 bzw. 34, während der Energieverbrauch nur leicht steigt .

Messungen hinzufügen, oder darauf verweisen

Parallel zu dieser Entwicklung im Bereich Hardware, stehen aber auch für Berechnung in Software optimierte Verfahren zur Verfügung, etwa *Curve25519* für Schlüsselaustausch und Signaturen, sowie *ChaCha* als schnelle Alternative für symmetrische Verschlüsselung [17].

Ergänzend dazu werden Secure Elements oder vergleichbare geschützte Ausführungsumgebungen eingesetzt, wenn langfristige Schlüssel und Identitäten auch gegen Softwarefehler und physische Angriffe abgesichert werden müssen. Sie trennen Schlüsselmaterial und sicherheitskritische Operationen (z. B. Signaturen oder Schlüsselaustausch) vom Mikrocontroller, sodass private Schlüssel idealerweise weder im Klartext im Hauptspeicher erscheinen noch durch die Applikation direkt verarbeitet werden. Je nach Plattform ist dies als separater Baustein oder als integrierte Sicherheitsfunktion des Mikrocontrollers realisiert. Diese Baugruppen bringen

[2]Hardware bezieht sich auf den HW-Beschleuniger und Software auf die Berechnung mittels CyclonePRO-Softwarebibliothek auf dem Mikrocontroller

noch weitere Funktionen wie sichere Schlüsselerzeugung, zertifizierte Entropiequellen, Anti-Tampering- und sichere Bootmechanismen mit sich [18].

Damit wird es möglich, die Anforderungen der Klasse 2 auch für nicht netzwerkfähige Feldgeräte auf Applikations- und Protokollebene nachzurüsten, ohne die Randbedingungen energieoptimierter Hardware grundsätzlich zu verletzen. Diese Entwicklung bildet die Grundlage für die nachfolgenden Kapitel, in denen ein entsprechender Ansatz konzipiert und auf die Randbedingungen nicht netzwerkfähiger Feldgeräte angepasst wird.

3.4.2 Stand der Technik bei netzwerkfähigen Feldgeräten

Wie in Abschnitt **??** abgegrenzt, fokussiert diese Arbeit auf Anforderungen der Kommunikationssicherheit (Klasse 2), also auf kryptografische Mechanismen für Authentisierung sowie Integritäts- und optional Vertraulichkeitsschutz. Bei ethernetbasierten Feldgeräten sind diese Mechanismen grundsätzlich verfügbar, da sich die Kommunikation entweder direkt durch Security-Erweiterungen der Feldbusprotokolle absichern lässt oder über etablierte Sicherheitsprotokolle wie TLS abgebildet werden kann. Der Stand der Technik ist damit nicht durch das Fehlen geeigneter Konzepte geprägt, sondern durch deren praktische Anwendung im Feld.

Die zunehmende Vernetzung der OT führt dazu, dass Ethernet-Technologien immer weiter in Richtung Feldgeräte verschoben werden. Single Pair Ethernet (SPE) bildet hierfür die physikalische Grundlage auf nur einem Adernpaar. Ethernet-APL ist darauf aufbauend eine prozessindustrielle Ausprägung, die zusätzliche Randbedingungen adressiert, insbesondere die Zweidrahtanbindung mit Energieversorgung, lange Leitungslängen und Konzepte für den Einsatz in explosionsgefährdeten Bereichen. Damit entsteht technisch die Möglichkeit, ethernetbasierte Kommunikationsprotokolle inklusive ihrer Security-Mechanismen bis zum Messumformer zu führen [8].

Unabhängig von der konkreten Protokollfamilie folgt Kommunikationssicherheit im Ethernet-Umfeld typischerweise einem wiederkehrenden Muster. Zunächst werden die Kommunikationspartner beim Verbindungsaufbau authentisiert, häufig auf Basis von X.509-Zertifikaten und einer Vertrauenskette. Anschließend werden symmetrische Sitzungsschlüssel abgeleitet, da diese für die laufende Datenübertragung deutlich effizienter sind als asymmetrische Verfahren. Auf dieser Grundlage werden Nachrichten gegen Manipulation geschützt (Integrität und Authentizität) und optional verschlüsselt (Vertraulichkeit). Die Schlüssellebensdauer wird durch Rekeying oder erneuten Verbindungsaufbau begrenzt [15]. Genau dieses Muster ist für die spätere Übertragung auf nicht IP-basierte Kanäle relevant.

PROFINET ist ein geeignetes Beispiel, um die Umsetzung von Klasse 2 in einem etablierten Feldbuskontext zu zeigen. Im Rahmen von PROFINET Security werden Security Classes definiert, die schrittweise Fähigkeiten von Robustheit bis zu kryptografisch geschützter Kommunikation abdecken. Security Class 1 adressiert vor allem Härtung und Robustness-Aspekte, etwa durch verbesserte Management- und Discovery-Mechanismen sowie die Möglichkeit, Gerätebeschreibungsdateien kryptografisch abzusichern, um Manipulationen in Engineering-Prozessen zu erschweren. Security Class 2 zielt auf Integrität und Authentizität der Kommunikation, sodass unbemerkte Manipulationen der PROFINET-IO-Daten verhindert werden sollen. Security Class 3 ergänzt zusätzlich den Vertraulichkeitsschutz, um ein Mitlesen und Interpretieren der Daten zu erschweren, sofern dies im jeweiligen Anwendungsfall erforderlich ist. Beim Verbindungsaufbau authentisieren sich beide Endpunkte gegenseitig über X.509-Zertifikate,

und es werden symmetrische Schlüssel für die nachfolgende Kommunikation abgeleitet. Diese Schlüssel werden im Betrieb regelmäßig erneuert, um die Auswirkungen einer möglichen Schlüsselkompromittierung zeitlich zu begrenzen. Damit zeigt PROFINET Security exemplarisch, wie Klasse 2 Anforderungen direkt auf Protokollebene adressiert werden können, ohne dass die Wirksamkeit allein auf Segmentierung oder physische Maßnahmen ausgelagert wird [23].

Ethernetbasierte Feldgeräte zeigen, dass kryptografisch abgesicherte Verbindungen auf Kommunikationsschnittstellen heute grundsätzlich realisierbar sind und in Spezifikationen bereits vorgesehen werden. Die wesentlichen Bausteine sind dabei Authentisierung über Geräteidentitäten, Ableitung symmetrischer Sitzungsschlüssel und deren Nutzung für Integritäts- und optional Vertraulichkeitsschutz. Nicht netzwerkfähige Feldgeräte besitzen diese Bausteine auf ihrer Kommunikationsschnittstelle typischerweise nicht. Die nachfolgenden Kapitel greifen daher das etablierte Muster aus dem Ethernet-Umfeld auf und übertragen es auf nicht IP-basierte Kanäle, angepasst an deren Ressourcen- und Betriebsrandbedingungen.

3.5 Public-Key-Infrastrukturen und Zertifikate

3.5.1 Geräteidentitäten und PKI als Grundlage für sichere Verbindungsaufbauten

Für kryptografisch abgesicherte Kommunikationsbeziehungen (Klasse 2) ist eine belastbare Geräteidentität eine zentrale Voraussetzung. In modernen Sicherheitsarchitekturen wird diese Identität typischerweise über X.509-Zertifikate abgebildet, die einen öffentlichen Schlüssel kryptografisch an ein Subjekt binden und von einer vertrauenswürdigen Zertifizierungsstelle signiert werden. Auf dieser Basis kann ein Kommunikationspartner die Echtheit des Gegenübers prüfen und anschließend Sitzungsschlüssel für einen effizienten Integritäts- und optional Vertraulichkeitsschutz ableiten.

Root of Trust und Validierung von Zertifikatsketten Die Vertrauensentscheidung in einer PKI basiert auf einem Root of Trust, der typischerweise als Trust Anchor im Truststore der prüfenden Instanz hinterlegt ist. Die Validierung eines End-Entity-Zertifikats erfolgt dann entlang der Zertifikatskette, indem jede Signatur mit dem öffentlichen Schlüssel des jeweils ausstellenden Zertifikats geprüft wird. Vereinfacht ergibt sich dabei folgende Prüfreihenfolge:

1. Die Signatur des Geräte- (End-Entity-) Zertifikats wird mit dem öffentlichen Schlüssel der ausstellenden Issuing-CA geprüft.

2. Die Signatur der Issuing-CA wird mit dem öffentlichen Schlüssel der übergeordneten CA (Intermediate oder Root) geprüft.

3. Für ein selbstsigniertes Root-Zertifikat kann die Signatur formal mit dem eigenen öffentlichen Schlüssel geprüft werden.

4. Entscheidend ist anschließend die Vertrauensentscheidung: Die Kette gilt nur dann als vertrauenswürdig, wenn das Root-Zertifikat als Trust Anchor im Truststore des prüfenden Kommunikationspartners hinterlegt ist.

Damit wird klar, dass nicht die Selbstsignatur der Root-CA Vertrauen erzeugt, sondern die sichere Verteilung und Hinterlegung des Trust Anchors.

Secure Device Identity nach IEEE 802.1AR (DevID) Der IEEE-Standard zu Secure Device Identifiers beschreibt DevIDs als eindeutige, kryptografisch gebundene Geräteidentitäten und unterscheidet dabei Initial Device Identifiers (IDevID) und Local Device Identifiers (LDevID). Ein DevID besteht aus einem RFC-5280-konformen X.509-Zertifikat, einem zugehörigen privaten Schlüssel (DevID secret) sowie der Zertifikatskette bis zu einem Vertrauensanker. Damit ist eine DevID nicht nur ein Identifier, sondern ein vollständiges Credential, mit dem ein Gerät seine Identität in Authentisierungsprotokollen nachweisen kann.

Die sichere Bindung an das Gerät erfolgt dadurch, dass der private Schlüssel in einem DevID-Modul geschützt gespeichert wird und ausschließlich für kryptografische Operationen genutzt werden kann. Unter einem DevID-Modul wird dabei die Kombination aus geschützter Schlüsselablage und einer Schnittstelle verstanden, die Signieroperationen ausführt, ohne den privaten Schlüssel preiszugeben. Das Gerät weist seine Identität nach, indem es Signaturoperationen mit dem DevID secret ausführt und damit den Besitz des privaten Schlüssels beweist. Dieses Prinzip der Besitzprüfung ist entscheidend, da nur so eine Nachahmung des Geräts durch Dritte verhindert wird.

Die IDevID wird vom Hersteller vor Auslieferung bereitgestellt, ist global eindeutig und gegen Modifikation geschützt. Zusätzlich kann das Gerät eine oder mehrere LDevIDs unterstützen, die durch den Betreiber erzeugt und verwaltet werden. LDevIDs erleichtern die Einbindung in eine lokale Sicherheitsinfrastruktur, da sie eine betriebsspezifische Identität bereitstellen können, ohne die herstellerseitige Grundidentität zu ersetzen. Je nach Betriebsmodell kann eine LDevID mit einem neu erzeugten Schlüssel arbeiten oder auf einem bestehenden Schlüssel aufsetzen, sofern dies durch die Sicherheitsrichtlinie zugelassen ist.

X.509-PKI nach RFC 5280 RFC 5280 beschreibt das Profil der X.509-Zertifikate und den grundlegenden PKI-Mechanismus im Internet. Zertifikate binden öffentliche Schlüssel an Subjekte und werden von einer Zertifizierungsstelle signiert, wodurch sich ein prüfbarer Vertrauensnachweis ergibt. Da ein Kommunikationspartner nur eine begrenzte Menge an vertrauenswürdigen CA-Schlüsseln im Voraus besitzt, wird die Vertrauensprüfung typischerweise über Zertifikatsketten realisiert. Dabei wird ein End-Entity-Zertifikat über eine oder mehrere Zwischenzertifizierungsstellen bis zu einem Trust Anchor validiert. Zertifikate können zudem vor Ablauf ihrer Gültigkeit ungültig werden, etwa durch Schlüsselkompromittierung oder organisatorische Änderungen. RFC 5280 beschreibt hierfür Widerrufsmechanismen wie Certificate Revocation Lists (CRLs), die es erlauben, kompromittierte oder nicht mehr gültige Zertifikate vorzeitig aus dem Vertrauensmodell zu entfernen.

Im DevID-Kontext ist relevant, dass IDevIDs typischerweise sehr lange Gültigkeitszeiten besitzen, um Gerätelebensdauern nicht künstlich zu begrenzen. Gleichzeitig bleibt die Vertrauensprüfung von der Qualität der PKI und der Integrität der Trust-Anchor-Verteilung abhängig. Der IEEE-Standard benennt hierzu Risiken wie kompromittierte Signierschlüssel in der Hersteller-PKI, fehlerhafte Trust-Anchor-Listen oder die Offenlegung des DevID secret als kritische Angriffspunkte.

CSR als Schnittstelle zwischen Gerät und PKI (PKCS#10, RFC 2986) Für die Ausstellung eines Gerätezertifikats wird in der Praxis häufig ein Certificate Signing Request verwendet. RFC 2986 (PKCS#10) definiert den CSR als signierte Datenstruktur, die den Subject Name, den öffentlichen Schlüssel und optionale Attribute enthält. Die Signatur über die Request-Information dient als Nachweis, dass der Antragsteller den zugehörigen privaten Schlüssel besitzt.

Der Ablauf ist in Abbildung **??** dargestellt. Zunächst erzeugt das Gerät ein Schlüsselpaar und erstellt daraus einen CSR, der neben dem öffentlichen Schlüssel auch Metadaten enthalten kann (z. B. Seriennummer oder Geräteattribute). Anschließend wird der CSR vom Gerät mit dem privaten Schlüssel signiert und an eine RA übermittelt. Die RA prüft den Antrag gemäß den lokalen Richtlinien und leitet ihn im Erfolgsfall an die CA weiter. Die CA stellt daraufhin ein X.509-Zertifikat aus, signiert dieses und liefert es über die RA an das Gerät zurück. Das Gerät speichert das Zertifikat zusammen mit der notwendigen Zertifikatskette und kann es anschließend verwenden, um seine Identität in Authentisierungsprotokollen nachzuweisen.

Ablauf CSR

Bezug zur Arbeit Die beschriebenen Konzepte bilden ein etabliertes Fundament für sichere Verbindungsaufbauten: Ein Gerät besitzt eine kryptografische Identität (DevID), weist diese durch Besitz des privaten Schlüssels nach und nutzt darauf aufbauend eine PKI-gestützte Vertrauenskette zur Authentisierung. Darauf aufbauend können Sitzungsschlüssel abgeleitet werden, um Kommunikationsdaten effizient gegen Manipulation zu schützen und optional zu verschlüsseln. Im weiteren Verlauf der Arbeit werden diese Bausteine aufgegriffen und auf nicht IP-basierte Kommunikationskanäle übertragen, wobei insbesondere die Bereitstellung einer herstellerseitigen IDevID als zentraler Baustein dient.

4 Bedrohungsmodell

Literaturverzeichnis

[1] Alexander, B. *HART as an attack vector: From current loop to application layer, presented*. Techn. Ber. DEF CON Russia, 2014.

[2] Babel, W. *Systemintegration in Industrie 4.0 und IoT: Vom Ethernet bis hin zum Internet und OPC UA*. ger. 1st ed. 2024. Wiesbaden: Springer Vieweg, 2024. ISBN: 978-3-658-42987-4. DOI: 10.1007/978-3-658-42987-4.

[3] BSI - Bundesamt für Sicherheit in der Informationstechnik. *ICS-Security-Kompendium, Testempfehlungen und Anforderungen für Hersteller von Komponenten*. Nov. 2014. (Online - zuletzt aufgerufen am 13. 02. 2026).

[4] BSI - Bundesamt für Sicherheit in der Informationstechnik. *ICS Security Kompendium V2.0*. Apr. 2024. (Online - zuletzt aufgerufen am 30. 01. 2026).

[5] Deutschland, Hrsg. *IT-Grundschutz-Kompendium*. ger. 6. Edition. Köln: Reguvis, 2023. ISBN: 978-3-8462-0906-6.

[6] Di Pinto, A., Dragoni, Y. ; Carcano, A. *TRITON: The First ICS Cyber Attack on Safety Instrumen Systems*. 2018.

[7] Elnour, M., Noorizadeh, M., Shakerpour, M., Meskin, N., Khan, K. ; Jain, R. „A Machine Learning Based Framework for Real-Time Detection and Mitigation of Sensor False Data Injection Cyber-Physical Attacks in Industrial Control Systems“. In: *IEEE Access* 11 (2023), S. 86977–86998. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2023.3303015. URL: https://ieeexplore.ieee.org/document/10210375/ (online - zuletzt aufgerufen am 11. 02. 2026).

[8] Ethernet-APL. *Ethernet - To the Field*. Juni 2021. URL: https://www.ethernet-apl.org/wp-content/uploads/2022/08/Ethernet-APL_Ethernet-To-The-Field_EN_FINAL_June-2021.pdf?utm_source=chatgpt.com (online - zuletzt aufgerufen am 14. 02. 2026).

[9] European Commission. Joint Research Centre. ; European Union Agency for Cybersecurity. *Cyber resilience act requirements standards mapping: Joint Research Centre & ENISA joint analysis*. eng. LU: Publications Office, 2024. DOI: 10.2760/905934. URL: https://data.europa.eu/doi/10.2760/905934 (online - zuletzt aufgerufen am 11. 02. 2026).

[10] European Parliament. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)*. en. Legislative Body: OP_DATPRO. Nov. 2024. URL: http://data.europa.eu/eli/reg/2024/2847/2024-11-20 (online - zuletzt aufgerufen am 11. 02. 2026).

[11] *IEC 62443-4-2:2019, IT-Sicherheit für industrielle Automatisierungssysteme Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)*. 2019.

[12] Johnson, T. ; Brychta, M. *Power Limitations of Loop- Powered Smart Transmitters, MS-2475*. Technical Article MS-2475. Analog Devices, Inc., 2013. (Online - zuletzt aufgerufen am 02. 02. 2026).

[13] McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M. ; Karri, R. „The Cybersecurity Landscape in Industrial Control Systems“. In: *Proceedings of the IEEE* 104.5 (Mai 2016), S. 1039–1057. ISSN: 0018-9219, 1558-2256. DOI: 10.1109/JPROC.2015.2512235. URL: http://ieeexplore.ieee.org/document/7434576/ (online - zuletzt aufgerufen am 11. 02. 2026).

[14] Niemann, K.-H. ; Merklin, S. „OT-Sicherheitsanforderungen für Ethernet-APL-Feldgeräte : Technologischer Wandel kann zu besserem Schutz führen“. de. In: (2022). Artwork Size: 611 KB, 9 pages Medium: application/pdf, 611 KB, 9 pages. ISSN: 2625-4212. DOI: 10.25968/OPUS-2320. URL: https://serwiss.bib.hs-hannover.de/2320 (online - zuletzt aufgerufen am 05. 02. 2026).

[15] Niemann, K.-H., Waldeck, B. ; Eßlinger, T. „PROFINET– Zukünftige OT-Security-Anforderungen : Was fordern NIS2, CER, CRA und IEC 62443“. de. In: (2025). Artwork Size: 721 KB, 8 pages Medium: application/pdf, 721 KB, 8 pages. ISSN: 2190-4111. DOI: 10.25968/OPUS-3710. URL: https://serwiss.bib.hs-hannover.de/3710 (online - zuletzt aufgerufen am 11. 02. 2026).

[16] Oryx Embedded. *Benchmark Results for STM32U3 Crypto*. URL: https://www.oryx-embedded.com/benchmark/st/crypto-stm32u3.html (online - zuletzt aufgerufen am 03. 02. 2026).

[17] Paar, C., Pelzl, J. ; Güneysu, T. *Understanding cryptography: from established symmetric and asymmetric ciphers to post-quantum algorithms*. eng. Second edition. Berlin: Springer, 2024. ISBN: 978-3-662-69006-2 978-3-662-69007-9.

[18] STMicroelectronics. *DS14830, STM32u385XX Datasheet Rev.2*. Feb. 2025. URL: https://www.st.com/resource/en/datasheet/stm32u385cg.pdf (online - zuletzt aufgerufen am 12. 12. 2025).

[19] Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A. ; Thompson, M. *Guide to Operational Technology (OT) security*. Techn. Ber. NIST SP 800-82r3. Gaithersburg, MD: National Institute of Standards ; Technology (U.S.), Sep. 2023, NIST SP 800–82r3. DOI: 10.6028/NIST.SP.800-82r3. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf (online - zuletzt aufgerufen am 05. 02. 2026).

[20] Streim, A. ; Kuhlenkamp, F. *Spionage, Sabotage, Datendiebstahl: Deutscher Wirtschaft entsteht jährlich ein Schaden von 55 Milliarden Euro*. Techn. Ber. Bitkom e.V., Juli 2017. URL: https://www.bitkom.org/print/pdf/node/10630 (online - zuletzt aufgerufen am 13. 02. 2026).

[21] TÜV NORD. *VEGAPULS 6X IEC 62443-4-2:2017 Zertikfat*. Feb. 2023. URL: https://www.vega.com/api/sitecore/DocumentDownload/Handler?documentContainerId=1008756&languageId=2&fileExtension=pdf&softwareVersion=&documentGroupId=1020307&version=03-02-2023 (online - zuletzt aufgerufen am 12. 02. 2026).

[22] VEGA Grieshaber KG. *IT-Sicherheitsrichtlinien VEGAPULS 6X, Document ID: 1007792.* URL: https://www.vega.com/api/sitecore/DocumentDownload/Handler?documentContainerId=1008754&languageId=1&fileExtension=pdf&softwareVersion=&documentGroupId=1007792&version=06-03-2023 (online - zuletzt aufgerufen am 12. 02. 2026).

[23] Walz, A., Niemann, K.-H., Göppert, J., Fischer, K., Merklin, S., Ziegler, D. ; Sikora, A. „PROFINET Security: A Look on Selected Concepts for Secure Communication in the Automation Domain“. en. In: (2023). Artwork Size: 297 KB, 6 pages Medium: application/pdf, 297 KB, 6 pages. ISSN: 2378-363X. DOI: 10.25968/OPUS-2934. URL: https://serwiss.bib.hs-hannover.de/2934 (online - zuletzt aufgerufen am 14. 02. 2026).