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 [3].

In ►Bild 2.1 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.

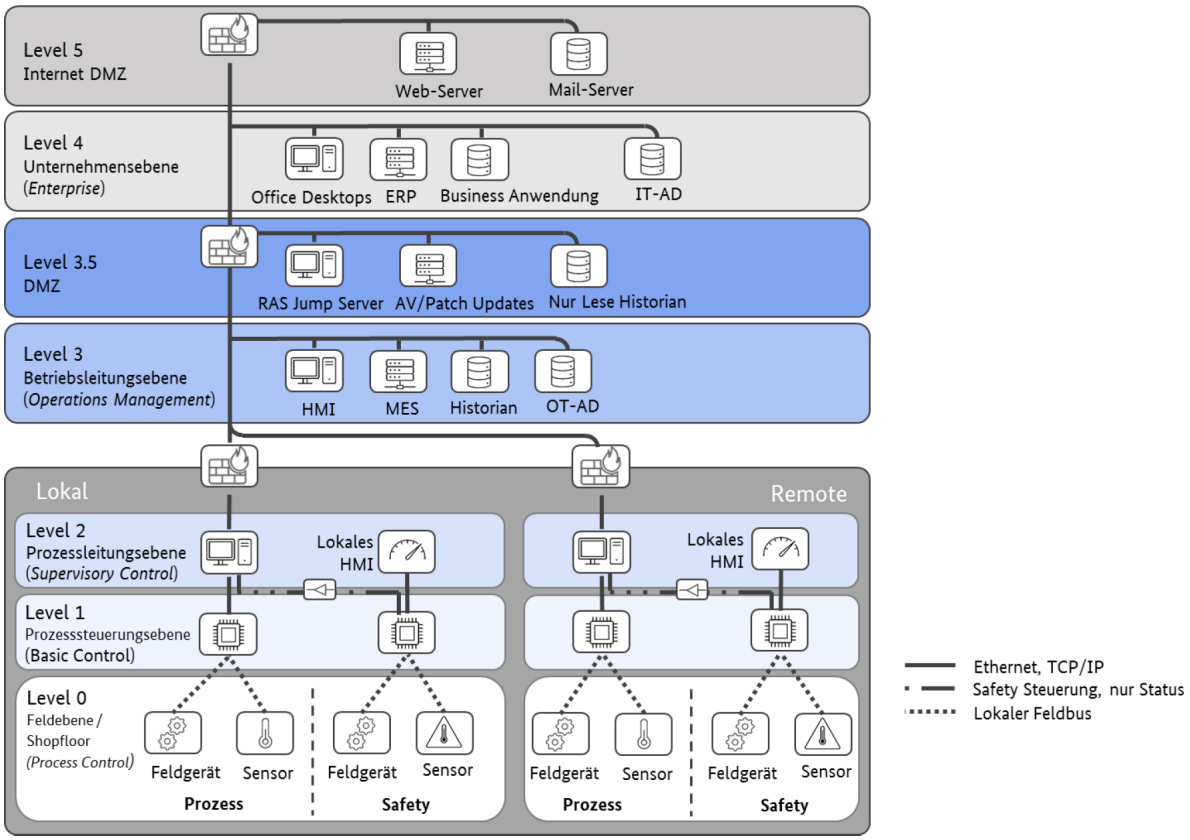

Bild 2.1. Beispiel Netzwerk nach Purdue/IEC 62443 Bildquelle: [4]

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 [3].

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 [3].

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) [11].

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.[3].

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-Kanal zur Übertragung von Messwerten an übergeordnete Steuerungen sowie der Control-Kanal, über den Parametrierung, Konfiguration oder Diagnose erfolgt.

Ein Angriff über den Control-Kanal zielt darauf ab, eine Systemkomponente aus einer höheren Kommunikationsschicht, zu kompromittieren, um anschließend manipulierte Befehle in das System einzuschleusen[10].

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-Kanal 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. [6, 10].

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 [3]. 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 [5]. 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 [3]. 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 [3].

[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.

Kann eine Anforderung nicht allein durch die Komponente erfüllt werden, sind ergänzende Maßnahmen auf Systemebene erforderlich; entsprechende Kompensationsmaßnahmen sind vom Hersteller zu dokumentieren [9].

Ist ein Produkt nach dieser Norm zertifiziert, so wird ein Zertifikat von einer unabhängigen Prüfstelle ausgestellt, die das entsprechende Security-Level angibt. In [14] 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 [12].

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 [8].

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 [7].

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 [11]. 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 [12]. 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 basiert auf dem Konzept der Informationssicherheit. Sie umfasst Maßnahmen und Strategien, die darauf abzielen, Systeme, Daten und Kommunikation vor unbefugtem Zugriff, Manipulation und Ausfall zu schützen. Informationssicherheit bildet dabei die Grundlage um sichere Feldgeräte, und somit sichere Anlagen zu entwickeln.

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)

Während in IT-Systemen die Geheimhaltung oft oberste Priorität hat, stehen in OT-Systemen die Integrität und Verfügbarkeit im Vordergrund. Hier sind Integrität und Verfügbarkeit von kritischerer Bedeutung. Dies liegt darin begründet , dass in OT-System ein Systemausfall oder die Manipulation von Daten unmittelbare Auswirkungen auf physische Prozesse haben kann und die Geheimhaltung von Daten, eine geringere Bedeutung hat[13].

kritischerer -> Komisches Wort

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 Örganisation"hinzugefügt, das verdeutlicht, das diese Anforderungen mittels organisatorischer Maßnahmen umgesetzt werden müssen.

das liegt darin begründet, hört sich komisch an

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

Die Zuordnung in Schutzziel macht keinen Sinn

Tabelle sauber beschrieben in Latex einfügen.

Bild 2.2. Mapping der Anforderungen -> DELETE

Da sich diese Thesis mit dem sicheren Verbindungsaufbau bei nicht netzwerkfähigen Geräten befasst, werden die Schutzziele, die durch organisatorische Maßnahmen gewährleistet werden nicht weiter betrachtet. Generell gilt, dass nur Anforderungen durch das in der Thesis entwickelte Protokoll umgesetzt werden können, die auch kryptographisch umsetzbar sind. So kann beispielsweise ein Angriff auf die Verfügbarkeit eines Gerätes nicht verhindert werden, wenn ein Angreifer das Gerät physisch zerstört.

Näher auf die Schutzziele eingehen oder passt das so?

2.4 Stand der Technik

2.4.1 Stand der Technik bei nicht netzwerkfähigen Feldgeräten

2.4.2 Stand der Technik bei netzwerkfähigen Feldgeräten

2.5 Public-Key-Infrastrukturen und Zertifikate

2.5.1 Rolle von PKI in industriellen Kommunikationssystemen

2.5.2 Architektur industrieller PKI

2.5.3 Geräteidentitäten auf Basis von Zertifikaten

3 Bedrohungsmodell

Literaturverzeichnis

[1] Alexander, B. *HART as an attack vector: From current loop to application layer, presented*. DEF CON Russia, 2014 (siehe S. 11).

[2] Babel, W. *Systemintegration in Industrie 4.0 und IoT: Vom Ethernet bis hin zum Internet und OPC UA*. 1st ed. 2024. Wiesbaden: Springer Vieweg, 2024. 1 S. ISBN: 978-3-658-42987-4. DOI: 10.1007/978-3-658-42987-4 (siehe S. 8, 9).

[3] BSI - Bundesamt für Sicherheit in der Informationstechnik. *ICS Security Kompendium V2.0*. 23. Apr. 2024. (Online - zuletzt aufgerufen am 30. 01. 2026) (siehe S. 8, 10, 12).

[4] Deutschland, Hrsg. *IT-Grundschutz-Kompendium*. 6. Edition. Köln: Reguvis, 2023. ISBN: 978-3-8462-0906-6 (siehe S. 8).

[5] Di Pinto, A., Dragoni, Y. ; Carcano, A. *TRITON: The First ICS Cyber Attack on Safety Instrumen Systems*. 2018 (siehe S. 12).

[6] 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) (siehe S. 11).

[7] European Commission. Joint Research Centre. ; European Union Agency for Cybersecurity. *Cyber resilience act requirements standards mapping: Joint Research Centre & ENISA joint analysis.* LU: Publications Office, 2024. DOI: 10.2760/905934. URL: https://data.europa.eu/doi/10.2760/905934 (online - zuletzt aufgerufen am 11. 02. 2026) (siehe S. 14).

[8] 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)*. Legislative Body: OP_DATPRO. 20. Nov. 2024. URL: http://data.europa.eu/eli/reg/2024/2847/2024-11-20 (online - zuletzt aufgerufen am 11. 02. 2026) (siehe S. 14).

[9] *IEC 62443-4-2:2019, IT-Sicherheit für industrielle Automatisierungssysteme Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)*. 2019 (siehe S. 13).

[10] 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) (siehe S. 11).

[11] Niemann, K.-H. ; Merklin, S. „OT-Sicherheitsanforderungen für Ethernet-APL-Feldgeräte : Technologischer Wandel kann zu besserem Schutz führen“. 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) (siehe S. 10, 14).

[12] Niemann, K.-H., Waldeck, B. ; Eßlinger, T. „PROFINET– Zukünftige OT-Security-Anforderungen : Was fordern NIS2, CER, CRA und IEC 62443“. 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) (siehe S. 13, 14).

[13] 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*. NIST SP 800-82r3. Gaithersburg, MD: National Institute of Standards ; Technology (U.S.), 28. 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) (siehe S. 15).

[14] TÜV NORD. *VEGAPULS 6X IEC 62443-4-2:2017 Zertikfat*. 3. 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) (siehe S. 13).