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, 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.

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.

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.

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

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.

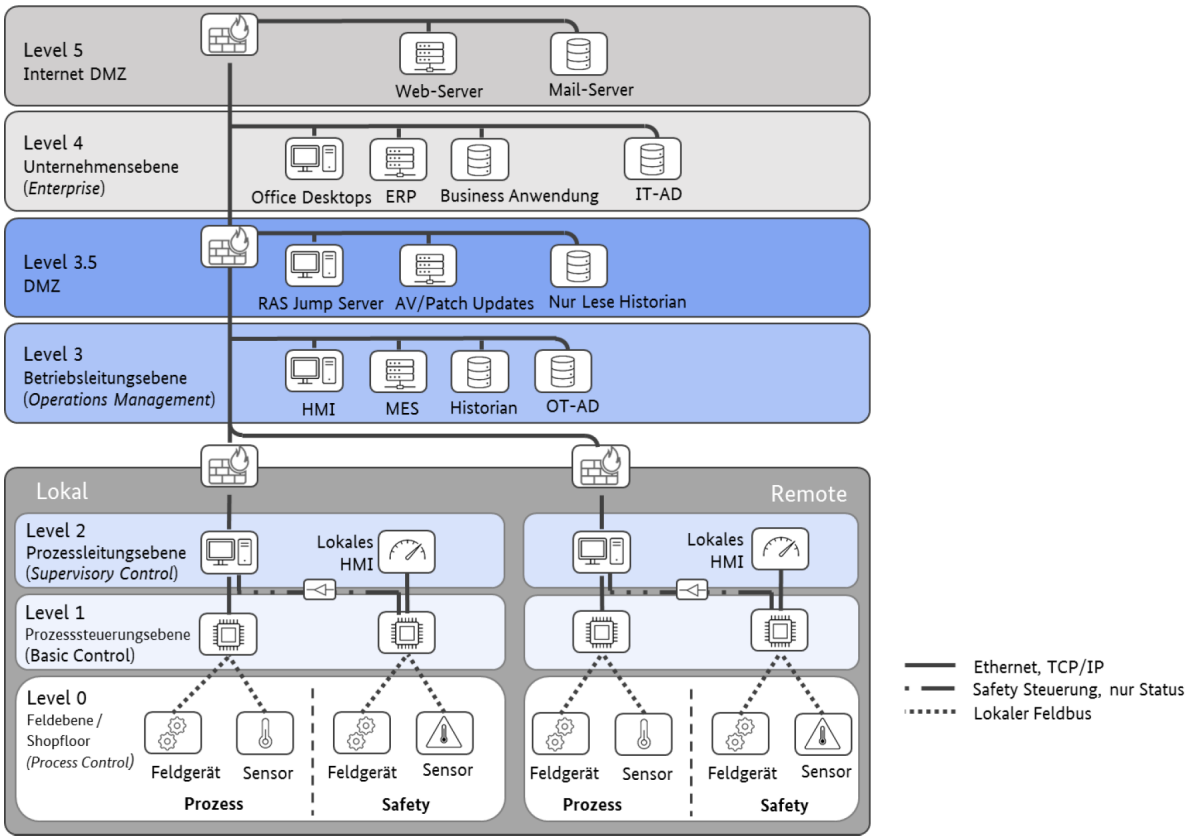

Bild 2.1. Beispiel Netzwerk nach Purdue/IEC 62443 Bildquelle: [4]

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 (das ICS) aus aufgebaut. 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].

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 Positionsgebers 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 "beliebigen" 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, über die Konfigurations- oder Diagnosedaten übertragen werden können (z. B. über HART) [8].

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.

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. 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

Feldgeräte als Einfallspunkt für Angriffe

Jedes Feldgerät, das in ein OT-Netzwerk bzw. ein Industrial Control System (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 an, so lassen sich in den meisten Fällen (rein analoge Geräte ohne zusätzliche Kommunikationsschnittstellen ausgenommen) 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 (verweis purdue Modell), zu kompromittieren, um anschließend manipulierte Befehle in das System einzuschleusen[7].

In der Praxis kann dies beispielsweise über missbrauchte Feldbus- oder Serviceprotokolle erfolgen. So wurde in [1] gezeigt, dass über manipulierte HART-Kommandos nicht nur Feldgeräte beeinflusst, sondern unter bestimmten Voraussetzungen auch weiterführende IT-Systeme, bis hin zur Unternehmensebene, erreicht werden können. 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, 7].

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 Zentrale Schutzziele für Feldgeräte

2.3 Stand der Technik

2.3.1 Stand der Technik bei nicht netzwerkfähigen Feldgeräten

2.3.2 Stand der Technik bei netzwerkfähigen Feldgeräten

2.4 Public-Key-Infrastrukturen und Zertifikate

2.4.1 Rolle von PKI in industriellen Kommunikationssystemen

2.4.2 Architektur industrieller PKI

2.4.3 Geräteidentitäten auf Basis von Zertifikaten

2.5 Regulatorische Anforderungen an Feldgeräte

2.5.1 IEC 62443-4-2

2.5.2 Cyber Resiliance Act

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] 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).

[8] 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).