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

1 Grundlagen

1.1 Stand der Technik bei nicht netzwerkfähigen Feldgeräten

Beschreibun des Kapitels einfügen

1.1.1 Einordnung und Begriffsdefinition

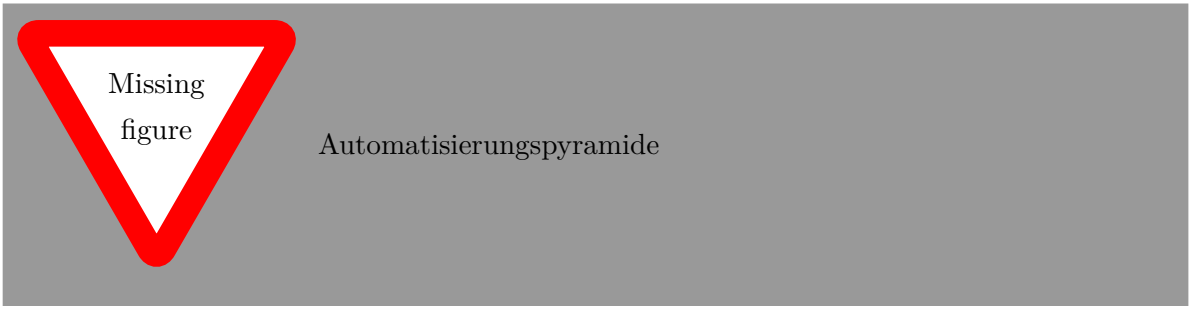
Im Rahmen dieser Arbeit werden unter nicht-netzwerkfähigen Geräten solche Feldgeräte verstanden, die entweder ausschließlich einen kontinuierlichen Messwert bereitstellen oder zwar mit einer Steuerungs- oder Leitebene kommunizieren, selbst jedoch keinen eigenen Netzwerk- oder IP-Stack implementieren.

Abschnitt einfügen was Netzwerk-Stack ist

Typische Vertreter dieser Geräteklasse sind klassische Prozessfeldgeräte wie Druck-, Temperatur-, Durchfluss- oder Füllstandssensoren sowie Grenz- und Näherungsschalter. Sie sind üblicherweise über 4-20-mA-Stromschleifen, über HART oder über feldbusbasierte Systeme wie PROFIBUS-PA oder vergleichbare Feldbusse an eine übergeordnete Steuerung angebunden. In der Automatisierungspyramide sind diese Geräte der Feldebene (Level 0) zuzuordnen, wie in Abbildung dargestellt.

insert ref

Was ist die AUtomatisierungspyramide



Automatisierungspyramide

Sie erfassen physikalische Größen direkt im Prozess oder wirken unmittelbar auf diesen ein und bilden damit die Schnittstelle zwischen physikalischer Anlage und digitaler Steuerung.

Zu den nicht-netzwerkfähigen Geräten im Sinne dieser Arbeit zählen ebenfalls Feldgeräte, die keine direkte Verbindung zu einer übergeordneten Steuerung besitzen, sondern deren Messwerte ausschließlich lokal bereitgestellt werden, beispielsweise über ein angeschlossenes Anzeige- oder Bediengerät. In solchen Fällen wird der Messwert ausschließlich von einem Menschen abgelesen, ohne dass das Feldgerät selbst Teil eines automatisierten Kommunikationssystems ist.

Feldgeräte, die über Feldbusse kommunizieren, sind damit zwar grundsätzlich kommunikationsfähig, jedoch nicht im Sinne eines autonomen Netzwerkteilnehmers. Die Kommunikation erfolgt typischerweise entweder über Punkt-zu-Punkt-Verbindungen (z. B. klassische 4-20-mA-Schleifen) oder über Feldbusse, bei denen mehrere Feldgeräte gemeinsam an einem Bussegment betrieben werden. Solche Segmente sind elektrisch und logisch klar abgegrenzt und werden

über definierte Kopplungspunkte, etwa Ein-/Ausgangskarten oder Gateway-Module, an die darüberliegenden Steuerungs- oder Leitebenen angebunden.

Aus Sicht des einzelnen Feldgeräts bleibt die Kommunikationsschnittstelle dabei stets auf ein analoges Signal (4-20 mA) und/oder ein nicht-IP-basiertes Feldprotokoll beschränkt. Die Anbindung in IP-basierte Automatisierungs- oder IT-Netze erfolgt ausschließlich indirekt über die vorgelagerte Infrastruktur. Genau diese strukturelle Eigenschaft unterscheidet nicht-netzwerkfähige Feldgeräte grundlegend von modernen IoT- oder IIoT-Geräten und bildet die Ausgangsbasis für die Betrachtung sicherer Kommunikation und sicheren Onboardings in dieser Arbeit.

1.1.2 Kommunikation bei nicht netzwerkfähigen Feldgeräten

Nicht netzwerkfähige Feldgeräte kommunizieren in der Praxis über vergleichsweise einfache, feldnahe Übertragungsmechanismen, die historisch auf Robustheit, deterministisches Verhalten und lange Lebensdauern ausgelegt sind. Im Unterschied zu IP-basierten Endgeräten treten sie nicht als eigenständige Netzwerkteilnehmer auf, sondern sind aus Sicht der höheren Ebenen typischerweise über Kopplungskomponenten (z. B. Ein-/Ausgangskarten, Remote-I/O oder Gateways) angebunden.

Was noch?

1.1.3 Onboarding und Geräteidentität

Im Folgenden wird beschrieben, wie nicht netzwerkfähige Feldgeräte heute in Anlagen aufgenommen (Onboarding) und im Betrieb eindeutig zugeordnet werden.

In der Praxis beginnt das Onboarding eines Feldgeräts meist mit der Zuordnung zwischen dem physischen Gerät und einer Messstelle bzw. einem Anlagentag. Dazu werden typischerweise Typenschildinformationen (Hersteller, Typbezeichnung, Seriennummer) mit den Planungsunterlagen abgeglichen. Diese Informationen werden dann im Asset Management System abgelegt. Dort wird die physische Messstelle (z. B. Tag-Nummer) manuell mit Geräteinformationen verknüpft. Dadurch können die Feldgeräte in Zukunt lokalisiert und identifiziert werden, sowie das Austauschen von Geräten, bzwdas Aktualisieren von Geräten (z. B. neue Firmware) koordiniert werden. [3]. Diese Informationen die eine Identifikation unterstützen sollen, sind dabei aber nicht kryptografisch gesichert, sondern dienen lediglich der Identifikation und sicherstellung, dass das Gerät äußerlich dem entspricht, das man erwartet.

Da die Identität nicht netzwerkfähiger Feldgeräte hauptsächlich organisatorisch, und nicht kryptografisch, abgesichert ist, muss auch organisatorisch sichergestellt werden, dass es keinen unbefugten Zutritt zur Anlage bzw. zum Gerät gibt. Wenn kryptografisch nicht sichergestellt werden kann, ob ein Gerät evt. unautorisiert getauscht bzw. manipuliert wurde, muss es organisatorisch sichergestellt werden. Dafür werden physische Schutzmaßnahmen angewendet. Zutrittskontrollen (Wer darf an die Anlage, Schaltschränke, Klemmenkästen), Zäune, verschlossene Technikräume oder Schränke. NIST SP 800-82 nennt physische und organisatorische Kontrollen als integralen Bestandteil eines OT-Sicherheitsprogramms, u. a. weil viele Angriffe und Fehlhandlungen in OT erst durch physischen Zugriff möglich werden [3]. In der Praxis wird damit ein erheblicher Teil der Verantwortung für die Sicherstellung der Geräteintegrität und -identität auf Betreiberprozesse und physische Zugriffskontrolle verlagert.

Die beschriebenen Verfahren sind in der industriellen Praxis etabliert, haben jedoch systematische Grenzen. Insbesondere liefern Nameplate/Seriennummer, Dokumentationsabgleich und konfigurierbare Kennzeichen (z. B. Tag-Felder) keinen kryptografischen Beweis dafür, dass die Kommunikationsbeziehung tatsächlich mit dem erwarteten physischen Gerät endet. Konfigurierbare Identifikationsattribute können prinzipiell geändert oder nachgeahmt werden.

Zudem adressieren rein physische Schutzmaßnahmen Insider-Bedrohungen nur begrenzt: Personen mit berechtigtem Zugang können Geräte tauschen, manipulieren oder Parameter verändern, ohne dass dies zwangsläufig erkannt wird. OT-Sicherheitsleitfäden behandeln solche Risiken unter anderem durch Forderungen nach kontrollierten Änderungen, Protokollierung und klaren Rollen/Prozessen, weisen aber zugleich darauf hin, dass organisatorische Maßnahmen allein keinen technischen Herkunftsnachweis des Geräts liefern [3]. Für nicht netzwerkfähige Feldgeräte ergibt sich daraus eine Lücke zwischen praktischer Zuordnung (Asset-Verwaltung) und technischer, beweisbarer Geräteauthentizität. Weiterhin gibt es auch Einsatzbereiche, die nicht physisch schützbar sind, da sie öffentlich zugänglich sind. Beispielsweise Sensoren, die im Bereich Wastewater, also z.B. Kanalisation, eingesetzt werden.

1.1.4 Warum gibt es keine Kryptografie?

Dieses Kapitel ordnet ein, weshalb kryptografisch abgesicherte Kommunikation in nicht netzwerkfähigen Feldgeräten historisch nur eingeschränkt umgesetzt wurde und welche Entwicklungen diese Situation heute verändern.

Nicht netzwerkfähige Feldgeräte sind häufig für besonders robuste und energieeffiziente Betriebsbedingungen ausgelegt. Bei loop-versorgten 2-Draht-Geräten muss die gesamte Elektronik aus dem begrenzten Energiehaushalt der 4 mA–20 mA-Stromschleife betrieben werden. Abzüglich Toleranzen und Puffer, stehen 4...20mA Geräten ein Strom von ca. 3,5 mA zur Verfügung [**johnson_power_2013.**] Daraus resultiert, dass Mikrocontroller in Feldgeräten oft mit niedrigen Taktraten betrieben werden und die verfügbaren Ressourcen auf das für Messwerterfassung, Signalverarbeitung, Diagnose und Kommunikation notwendige Minimum optimiert sind.

Kryptografische Verfahren, insbesondere asymmetrische Verfahren sowie moderne, authentifizierte Verschlüsselung, sind in reiner Softwareausführung vergleichsweise rechenintensiv. In ressourcenbeschränkten Feldgeräten führt dies typischerweise zu langen Ausführungszeiten und erhöhtem Energieverbrauch. Für den Anlagenbetrieb kann dies problematisch sein, da zusätzliche Latenzen im Kommunikations- oder Parametrierpfad auftreten und gleichzeitig der ohnehin knappe Leistungsrahmen belastet wird. In der Konsequenz wurden Sicherheitsmechanismen in vielen Feldgerätekategorien entweder gar nicht vorgesehen oder auf einfache Schutzfunktionen (z. B. Schreibschutz, PIN/Lock, organisatorische Prozesse) beschränkt [1].

Diese Situation wird durch die lange Nutzungsdauer industrieller Feldgeräte zusätzlich verstärkt. Feldgeräte verbleiben häufig über Zeiträume von 10 bis 15 Jahren (oder länger) im Betrieb. Gerätewechsel sind kostenintensiv, erfordern Stillstände und sind durch Zertifizierungen, und qualitätssichernde Prozesse gebremst. Dadurch existiert eine große installierte Basis an Legacy-Geräten, deren Hardwareplattformen nicht für moderne Kryptografie ausgelegt wurden. Selbst wenn neue Sicherheitsanforderungen entstehen, setzen sie sich in der Feldebene daher nur langsam durch [1].

In den letzten Jahren hat sich die Hardwarelandschaft jedoch deutlich weiterentwickelt. Moderne Mikrocontroller für Industrie- und Embedded-Anwendungen integrieren zunehmend dedizierte Krypto-Beschleuniger, etwa für AES, SHA und elliptische Kurvenverfahren (ECC). Ergänzend werden Sicherheitsfunktionen wie geschützte Schlüsselspeicher, sichere Bootketten, TrustZone-basierte Isolierung, manipulationsresistente Speicherbereiche oder externe Secure-Elemente verfügbar. Dadurch verlagern sich rechenintensive kryptografische Primitive in spezialisierte Hardwareblöcke, die sowohl schneller als auch energieeffizienter arbeiten als reine Softwareimplementierungen. Beispielhafte Messungen für einen STM32U3-Mikrocontroller zeigen diesen Effekt deutlich: Für AES-128 im Galois/Counter Mode (GCM) wird in der dedizierten Krypto-Hardware ein Datendurchsatz von etwa 9,17 $\mathrm{MB\,s^{-1}}$ erreicht, während eine reine Software-Implementierung auf demselben Controller lediglich etwa 0,76 $\mathrm{MB\,s^{-1}}$ erzielt. Für SHA-256 liegen die gemessenen Durchsätze bei 45,87 $\mathrm{MB\,s^{-1}}$ in Hardware gegenüber 1,355 $\mathrm{MB\,s^{-1}}$ in Software [2]. Somit ist die Verarbeitung in Hardware ca. 12- bzw. 34-mal schneller als in Software. Während diese Werte natürlich von Controller, Krypo-Peripherie und Implementierung des Algorithmus abhängen, zeigen sie doch deutlich, um welche Größenordnung die Aktionen beschleunigt werden können.

Aus Systemsicht hat dies zwei Konsequenzen. Erstens wird Kryptografie unter den Randbedingungen der Feldebene überhaupt erst praktikabel, weil Energie- und Laufzeitkosten pro Operation sinken. Zweitens eröffnen sich dadurch neue Architekturoptionen: Auch ohne vollwertigen IP-Stack kann ein Gerät kryptografische Operationen, Schlüsselableitung und geschützte Datenübertragung realisieren, sofern ein zuverlässiger Byte-Transportkanal vorhanden ist. Damit werden auf IP basierende Konzepte prinzipiell auch über serielle oder proprietäre Feldschnittstellen denkbar, vorausgesetzt Protokollaufbau und Nachrichtenformate werden an die beschränkten Ressourcen angepasst.

Trotz der verbesserten Hardwarebasis bleibt eine wesentliche Lücke bestehen: Für viele nicht-IP-basierte Feldkommunikationswege existiert kein breit etablierter Standard, der eine kryptografisch eindeutige Geräteidentifikation bietet. Das obwohl mittlerweile durch entsrpechende HW, die Möglichkeit kryptografische Operationen in akzeptabler Zeit durchzuführen, da ist.

2 Bedrohungsmodell

Hallo ich bin Bedrohungsmodell.

Und Hier kann ich Sachen hinzufügen.

Test nach Tabelle. Hallo, ich schreibe jetzt in VScode.

Das ist ein doppeltes Enter. Das ist ein Enter mit zwei leerzeichen nach dem Punkt.

Literaturverzeichnis

[1] BSI - Bundesamt für Sicherheit in der Informationstechnik. *ICS Security Kompendium V2.0*. 23. Apr. 2024. (Online - zuletzt aufgerufen am 30. 01. 2026) (siehe S. 5).

[2] 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) (siehe S. 6).

[3] 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. 4, 5).