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.

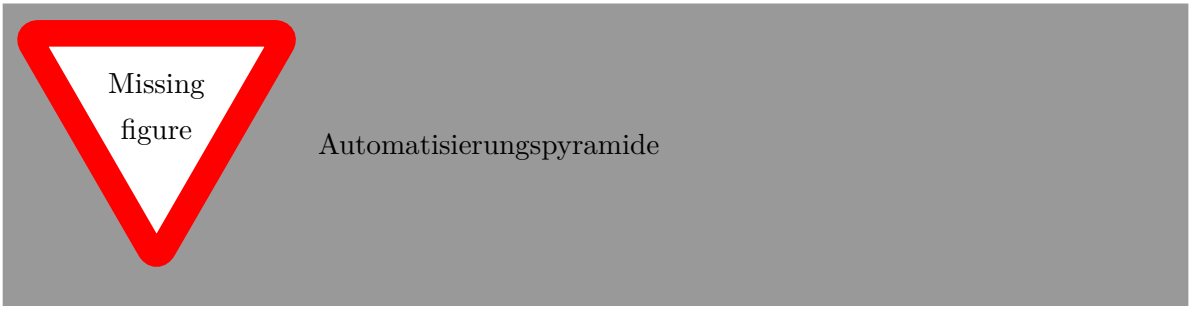
Abschnitt einfügen was Netzwerk-Stack ist

.

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 AUtomatisierungspymide



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 stellen Prozessinformationen auf der Feldebene bereit und kommunizieren dabei typischerweise über Signale und Protokolle, die historisch für Robustheit, einfache Verdrahtung und lange Lebensdauern ausgelegt wurden.

Zitat

Im Folgenden werden die wichtigsten Kanäle beschrieben.

4-20-mA-Stromschleife: Der klassische Übertragungsweg in der Prozessindustrie ist die 4-20-mA-Stromschleife. Das Feldgerät kodiert den Messwert als Strom im definierten Bereich, wobei 4 mA typischerweise den unteren Messbereich (oder einen definierten Grundzustand) repräsentieren und 20 mA den oberen Messbereich. Die Übertragung ist kontinuierlich und sehr störsicher; sie erlaubt zudem in vielen Ausführungen, das Feldgerät aus derselben Zweidrahtschleife zu versorgen. Funktional handelt es sich hierbei um einen rein analogen Kanal: Er liefert primär den Messwert (oder bei Aktoren eine Stellvorgabe) und besitzt ohne zusätzliche Maßnahmen weder Adressierung noch Sitzungs- oder Teilnehmerkonzepte. Aus Systemsicht ist die Stromschleife daher ein sehr einfacher, aber zentraler Kommunikationskanal zwischen Feldebene und Steuerung.

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.