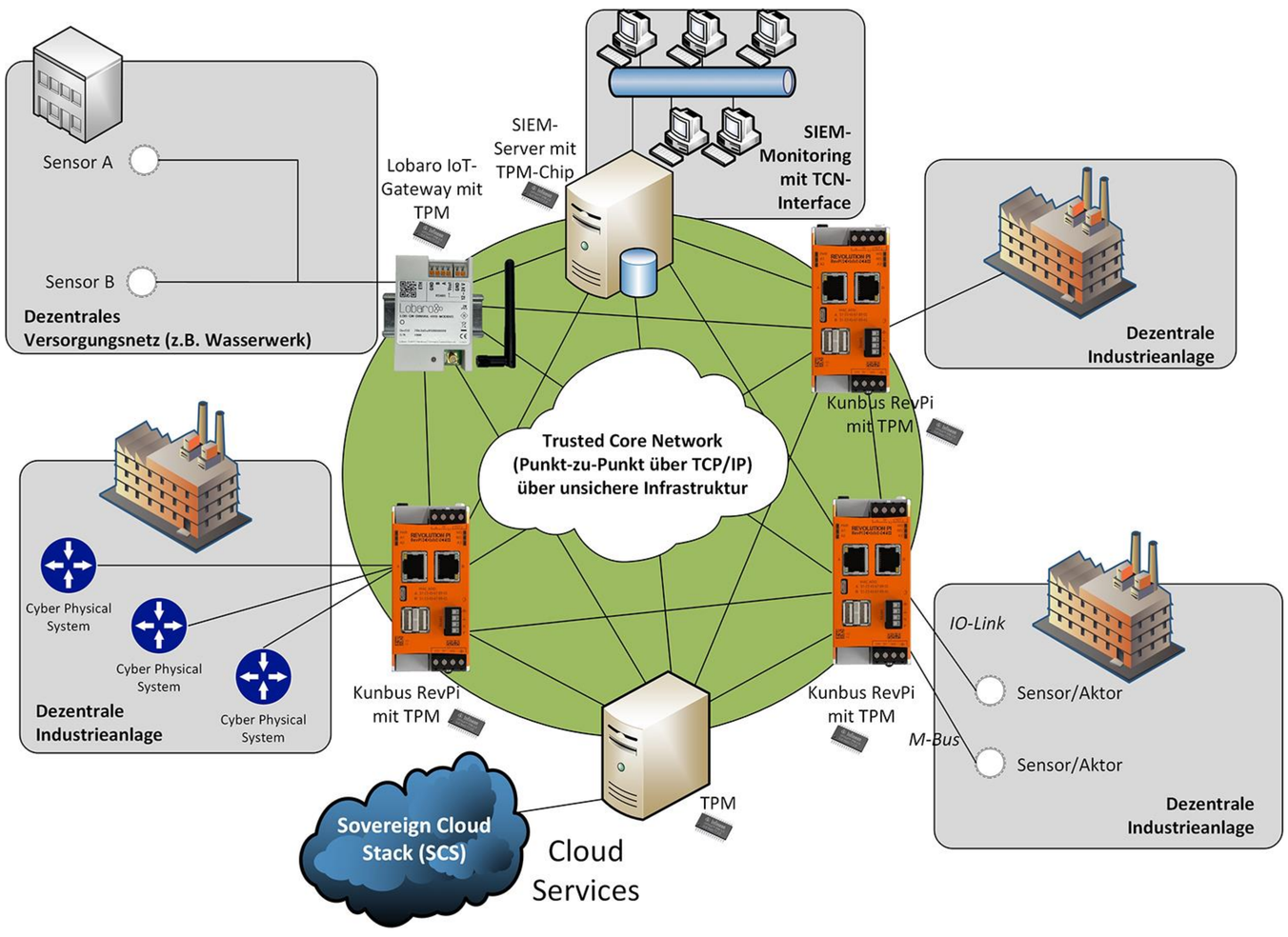
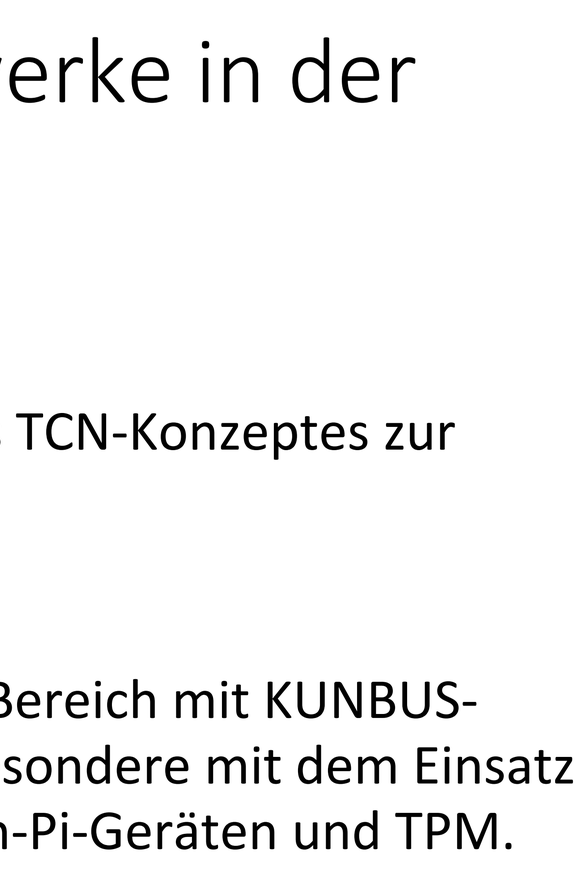
Mittelstandskonferenz 2023

KMU stärken durch digitale Innovationen





TRUSTnet — Vertrauenswürdige Netzwerke in der Industrie 4.0

Problemstellung und Motivation

Automatisierte Industrieanlagen sind zunehmend auf vernetzte Systeme angewiesen, welche potenzielle Sicherheitslücken aufweisen können. Die steigende Zahl von Cyberangriffen erhöht das Risiko, insbesondere für kritische Infrastrukturen, bei denen Ausfälle gravierende Folgen haben können. Ein Schlüssel zur Absicherung dieser Systeme liegt in der Verwendung von Vertrauens-ankern wie dem Trusted Platform Module (TPM) und der Device Identifier Composition Engine (DICE), die die Geräteintegrität der Endpunkte sicherstellen. SIEM-Systeme ermöglichen die Echtzeit-Überwachung.

Ziele

- Aufbau eines Trusted Core Network (TCN) mit integriertem SIEM-System.
- Einsatz von TPM- und DICE-basierter Remote Attestation (RA) zur Vertrauensbildung in Geräte.
- Einbindung von KUNBUS- und Lobaro-Geräten mit entsprechenden Sicherheitsprotokollen und -technologien.
- Anpassung des SIEM-Systems, um den Vertrauensstatus von Geräten im Netzwerk zu überprüfen.
- Simulation des TCN-Konzeptes zur Evaluierung.

Use Cases

- Industrial IoT-Bereich mit KUNBUS-Geräten, insbesondere mit dem Einsatz von Revolution-Pi-Geräten und TPM.
- Smart-Energy/Grid-Anwendungen mit Lobaro-Geräten ohne TPM mit DICE-Implementierung.

Projektkoordination
DECOIT® GmbH & Co. KG

Projektlaufzeit
1. April 2023 bis 31. März 2026

Kontakt
Prof. Dr. Kai-Oliver Detken
Fahrenheitstraße 9, 28359 Bremen
Tel.: +49 (0) 421/596064-01
E-Mail: detken@decoit.de

Förderkennzeichen
16KIS1786K, 16KIS1787-90

Akronym
TRUSTnet

Projektwebseite
www.trustnet-project.de

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Mittelstandskonferenz 2023

KMU stärken durch digitale Innovationen

TRUSTnet — Vertrauenswürdige Netzwerke in der Industrie 4.0

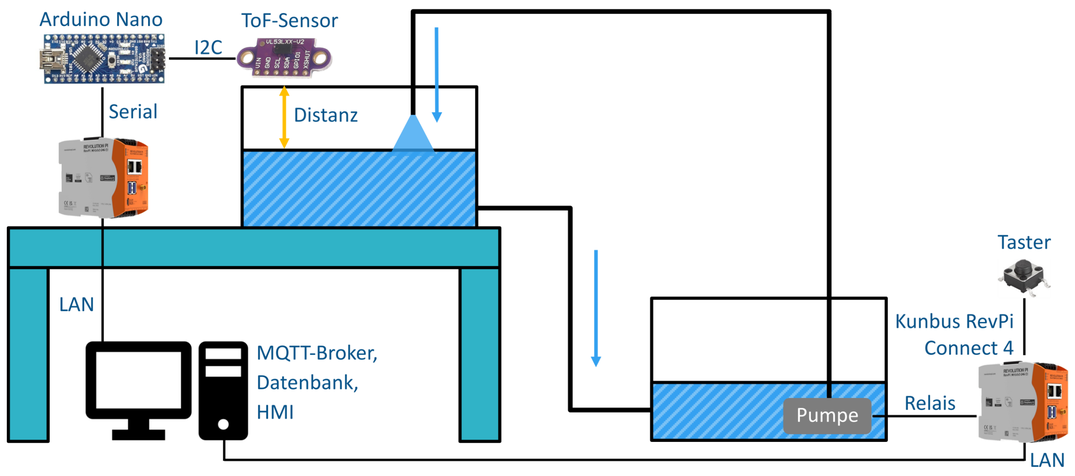
Lösungsansatz

- **Protokoll & Encoding:** Implementierung des Trusted Attestation Protokolls (TAP) der Trusted Computing Group (TCG) für eine effiziente TPM- und DICE-basierte RA. CoAP dient als Kommunikationsprotokoll, CBOR wird als Wire-Encoding verwendet.
- **SIEM-Integration:** Anbindung des SIEM-Systems ScanBox® der DECOIT® über eine speziell entwickelte API, die HTTP und JSON unterstützt. Dies ermöglicht eine nahtlose Integration und das Management des Vertrauensstatus von Geräten im Netzwerk.
- **Geräteintegration:** Integration von TPM in KUNBUS-Geräte (Revolution Pi) und mögliche Implementierung von DICE auf Lobaro-Geräten.
- **Architekturanpassung:** Einsatz der IETF-RATS-Architektur gemäß RFC 9334, einschließlich des Passport und Background Check Models, innerhalb der TCN-Architektur.
- **Protokollauswahl:** Abkehr von TNC zugunsten des fokussierten TAP, aufgrund festgestellter Inkompatibilitäten und überflüssiger Protokolle und Komponenten.

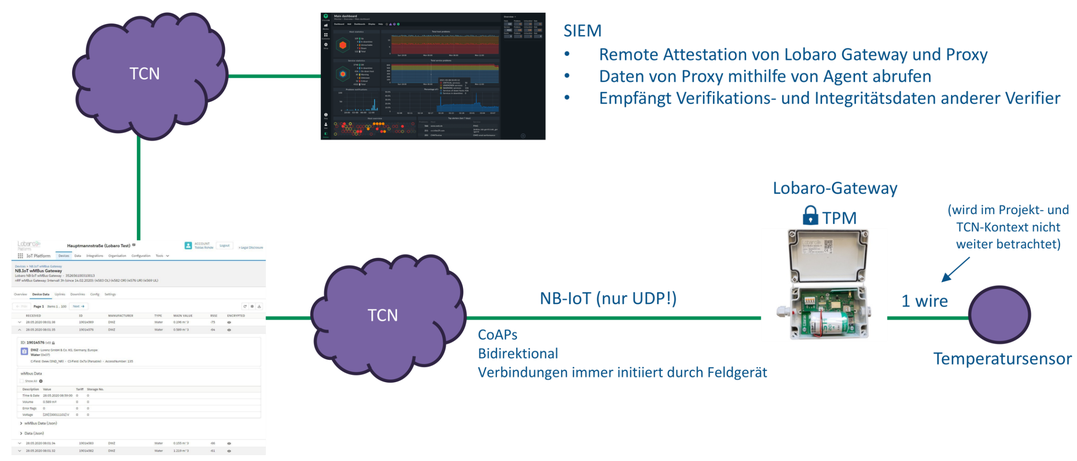
Bisherige Ergebnisse

- Abgeschlossene Bedrohungsanalyse.
- Fertiggestellte Architektur für das TRUSTnet mit SIEM-Systemen.
- Festgestellt, dass das Trusted Network Communication (TNC)-Protokoll inkompatibel zur ScanBox®-Architektur ist und viele nicht relevante Protokolle und Komponenten enthält.
- Bestimmung des TAP als bevorzugtes Protokoll zur Umsetzung von TPM- und DICE-basierter Remote Attestation.

Szenario Kunbus: Modell eines Pumpspeicherkraftwerks



Szenario Lobaro: Anbindung und Auswertung eines Sensors über Lobaro-Gateway



Backend/Cloudanwendung zur Datenaggregation und Kommunikation

DECOIT®
Fraunhofer SIT
HSB Hochschule Bremen City University of Applied Sciences
KUNBUS industrial communication
Lobaro Industrial IoT Solutions

Projektkoordination
DECOIT® GmbH & Co. KG

Projektlaufzeit
1. April 2023 bis 31. März 2026

Kontakt
Prof. Dr. Kai-Oliver Detken
Fahrenheitstraße 9, 28359 Bremen
Tel.: +49 (0) 421/596064-01
E-Mail: detken@decoit.de

Förderkennzeichen
16KIS1786K

Akronym
TRUSTnet

Projektwebseite
www.trustnet-project.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung