# 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 Vertrauensankern wie dem Trusted Platform Module (TPM) und der Device Identifier Composition Engine (DICE), die die Geräteintegrität der Endpunkte sicherstellen. Diese kann zudem durch SIEM-Systeme in Echtzeit überwacht werden.

**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-Geräten („Rich Devices“) und Lobaro-Geräten („Constrained Devices“) mit entsprechenden Sicherheitsprotokollen und -technologien.
- Anpassung des SIEM-Systems, um den Vertrauensstatus von Geräten im Netzwerk zu überprüfen.
- Simulation des TCN-Konzeptes zur Evaluierung von Robustheit und Stabilität.

**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 mit DICE-Implementierung.

**Lösungsansatz**

- **Protokoll & Encoding:** Implementierung des Trusted Attestation Protokolls (TAP) der Trusted Computing Group (TCG) sowie des Trusted Neighborhood Discovery (TND) Protokolls für eine effiziente TPM- und DICE-basierte Peer-to-Peer RA. CoAP dient als Kommunikationsprotokoll, CBOR und JSON werden als Wire-Encoding verwendet. Abkehr von Trusted Network Connect (TNC) aufgrund festgestellter Inkompatibilitäten und überflüssiger Komplexität sowie Redundanz zu den anderen eingesetzten Protokollen.
- **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 Connect 4) 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.

**Bisherige Ergebnisse**

- Abgeschlossene Bedrohungsanalyse.
- Fertiggestellte Architektur für das TRUSTnet TCN-Szenario mit SIEM-Systemen.
- Bereitstellung der Hardwareplattformen.
- 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.
- Implementierung erster Komponenten des TCN-Konnektors.
- Modellaufbau in der Simulation begonnen.
- Demonstrator für Secure- und Measured Boot auf der Raspberry-Pi-4-Plattform umgesetzt.


**Projektkoordination**
DECOIT® GmbH & Co. KG

**Projektlaufzeit**
1. April 2023 bis 31. März 2026

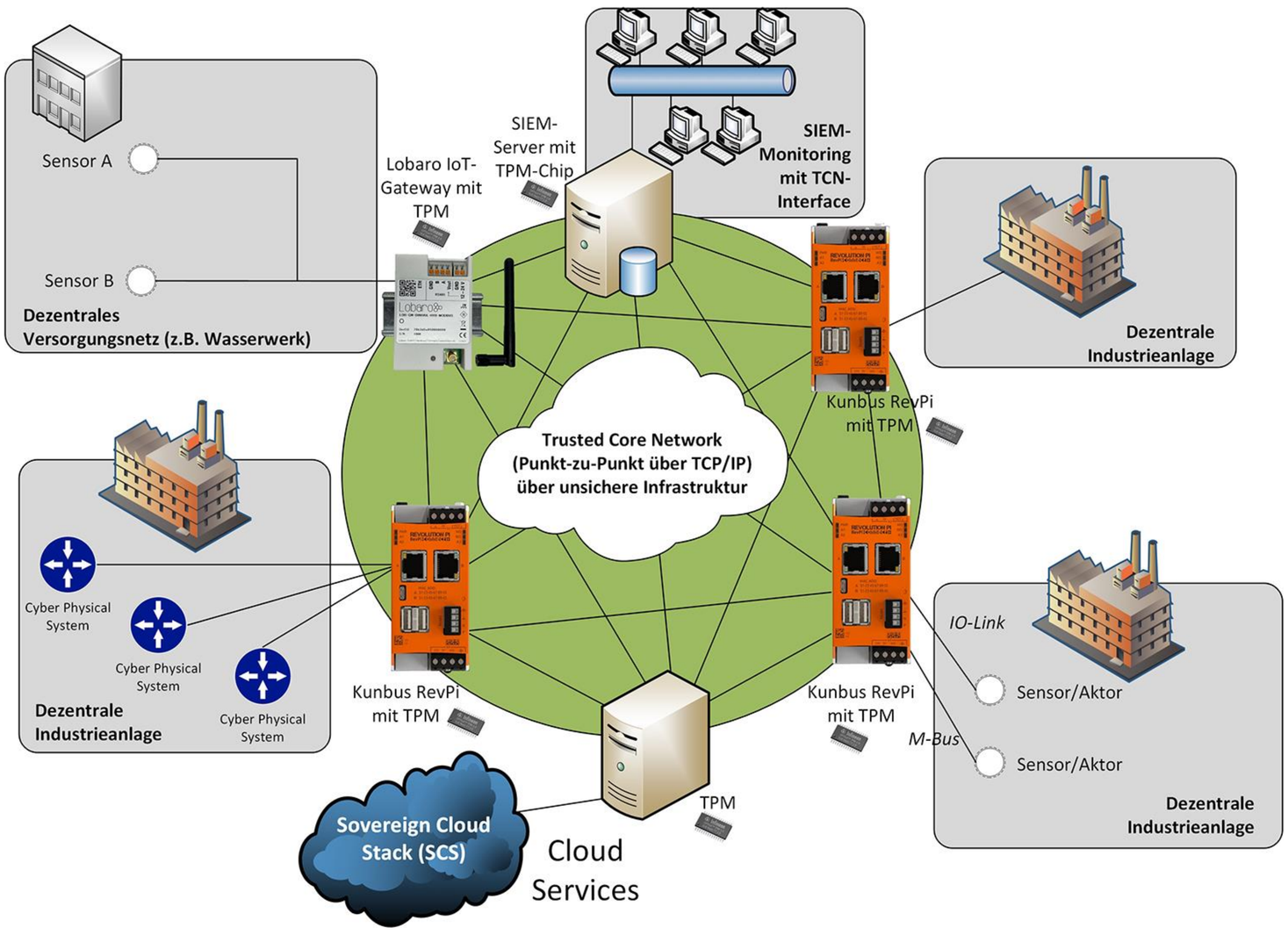
**Kontakt**
Prof. Dr. Kai-Oliver Detken
Fahrenheitstraße 9, 28359 Bremen
Tel.: +49 (0) 421/596064-01
E-Mail: detken@decoit.de



**Förderkennzeichen**
16KIS1786K

**Akronym**
TRUSTnet


**Projektwebseite**
www.trustnet-project.de





GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung