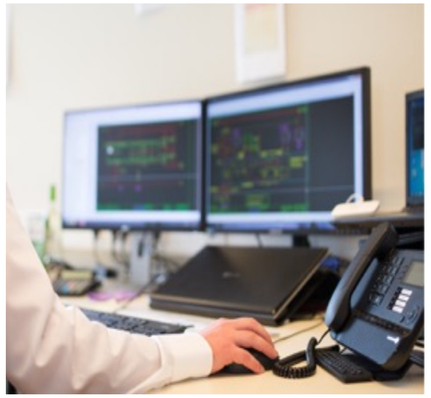


# ARENDAR
# Security by Design

INTERNET SECURITY DAYS 2017 ISD

AREND PROZESSAUTOMATION


Markus Jostock

**Arend Prozessautomation GmbH**
Am Kleinen Rotenberg 21
54516 Wittlich
Tel.: +49 6571 95579-0
Fax +49 6571 95579-28

info@arend-automation.de
www.arend-automation.de

# **AREND** bietet zukunftsweisende Automation für Industrie 4.0 aus einer Hand

Dr.-Ing. Markus Jostock
Leiter F&E

# ARENDAR

Industrieller Datensammler mit Sicherheitsmerkmalen zur zur Cloud-Anbindung von Maschinen

# ARENDAR

Edge-Computing
Plattform für
IoT Anwendungen
in Industrie 4.0

# ARENDAR

Entwicklung mit Secure Development Cycle auf Sicherheit ausgelegt

# Herausforderungen

# Aktuelle Marktsituation

Entweder auf **I/O** fokussiert

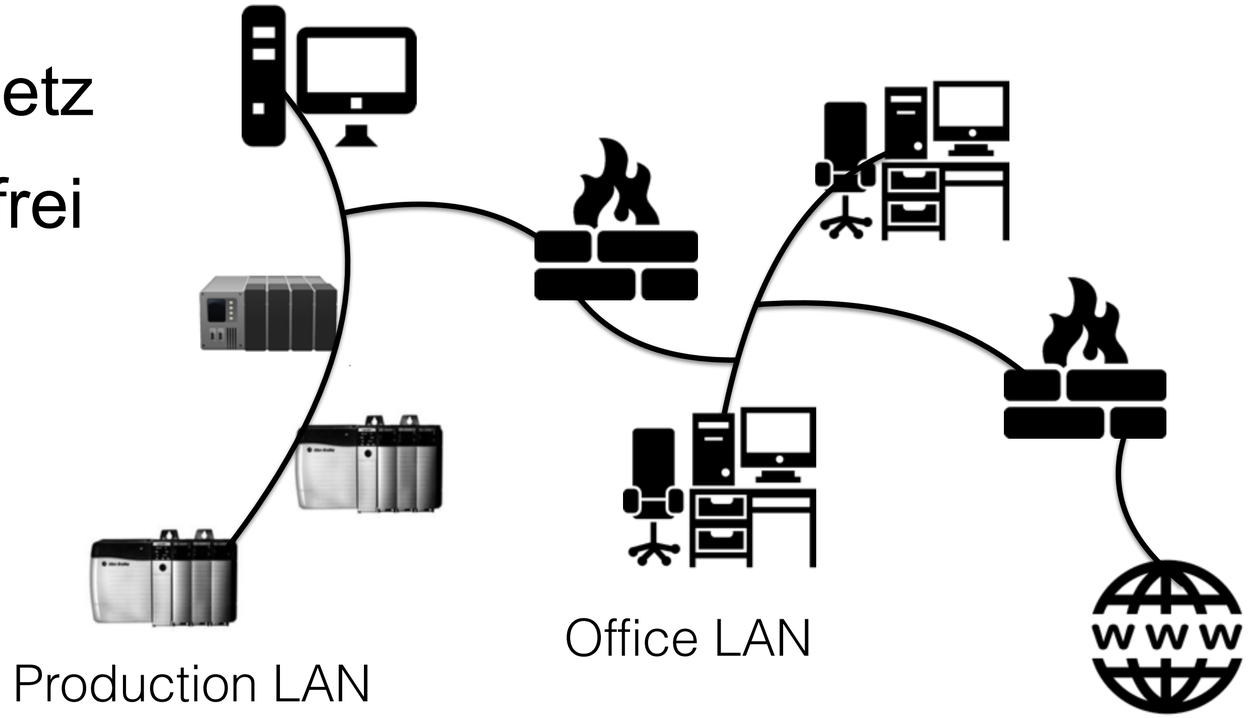
- kommt oft aus Echtzeit-Welt
- mit Steckkarten erweiterbar
- relativ hohe HW-Kosten
- keine HW-Verschlüsselung
- oft nur ein LAN I/F
- kaum Sicherheits-Funktionalität

Oder auf **Sicherheit** fokussiert

- kommt oft aus Firewall-Welt
- keine Maschinenanbindung
- nur Netzwerkschnittstelle(n)
- oft HW-basierter VPN Tunnel
- relativ hohe Kosten

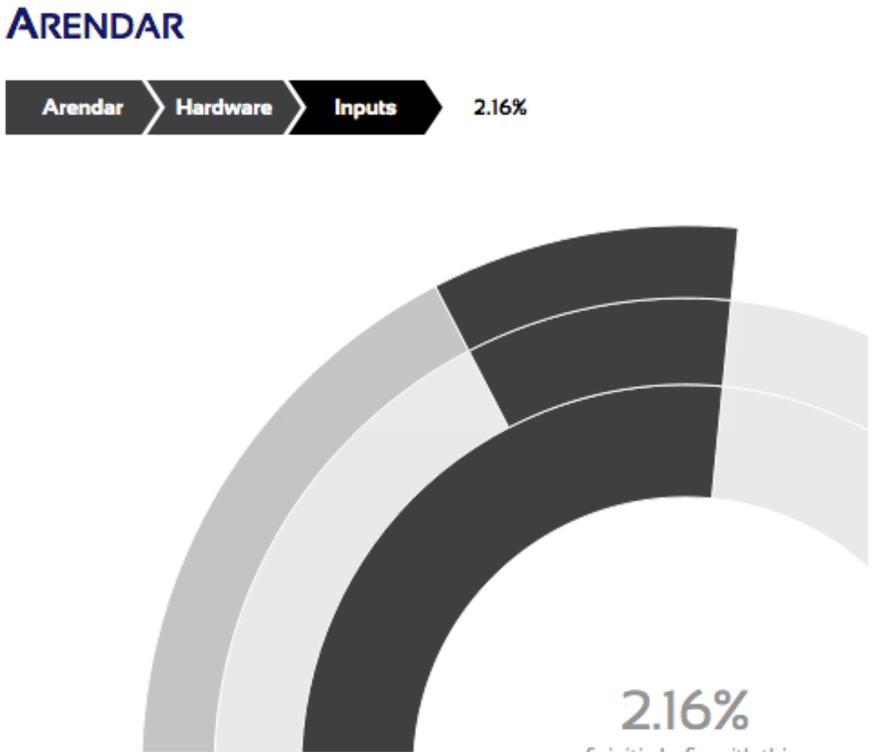
# Aktuelle Produktions-Situation

- Produktionsnetz getrennt von Office-Netz
- Alle Steuerungen im Produktionsnetz frei zugänglich
- Ausschließlich Perimeterschutz
- Verfügbarkeit ist dominantes Kriterium



# Entwicklung

# Einfache Bedienung




- Zukunftsweisende Bedienkonzepte
- Reiche Bedienoberfläche vorhanden
- Einfach an Maschine oder Anlage konfigurierbar

# Arend Secure Development Cycle

| Block | Nr. | Phase |
|---|---|---|
| | 0 | Schulung und Erkenntnis |
| Anforderungen | 1 | Projektbeginn |
| | 2 | Festlegen bewährter Design Methoden |
| | 3 | Risikobewertung für Sicherheit und Datenschutz |
| Entwurf | 4 | Angriffsoberflächenanalyse und -reduktion |
| | 5 | Bedrohungsmodellierung |
| | 6 | Dokumente und Tools für Nutzer |
| Implementierung | 7 | Sichere Programmierrichtlinien |
| Überprüfung | 8 | Sichere Testmethodik |
| | 9 | Feinschliff |
| | 10 | Abschließende Sicherheitsüberprüfung |
| Veröffentlichung | 11 | Vorfallreaktionsplan |
| | 12 | Produktveröffentlichung |
| | 13 | Vorfallreaktionausführung |

Angelegt an Microsoft Secure Development Cycle, aber angepasst an Besonderheit von Hardware-Software Co-Design

# Anwendung

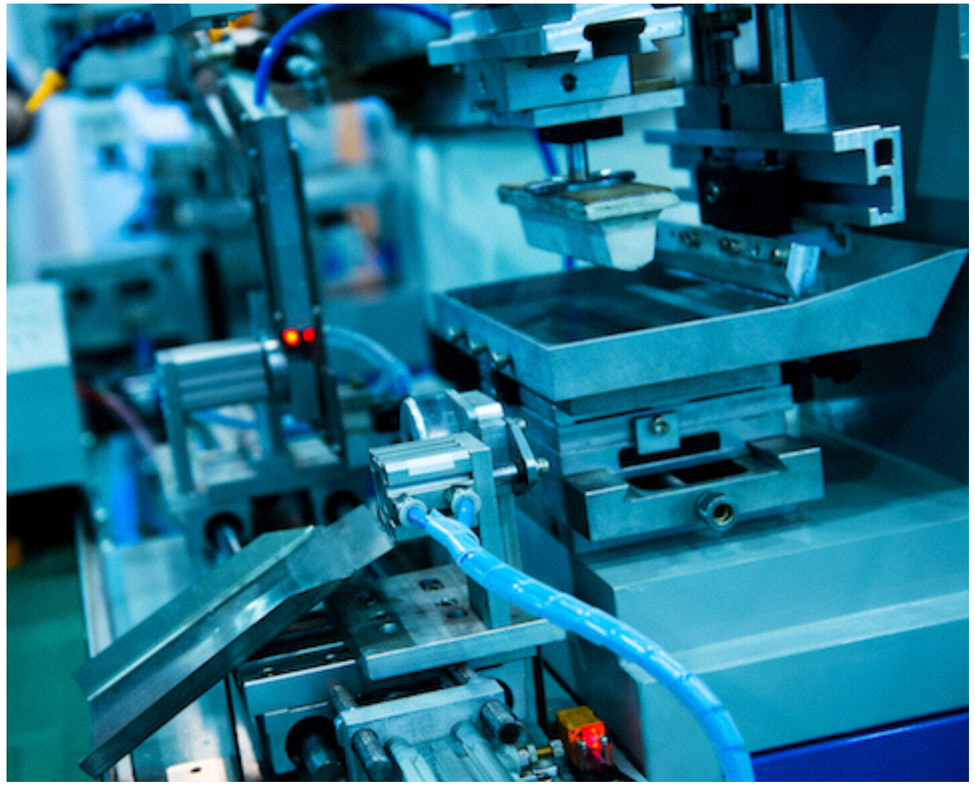
# Datenerfassung

- Einbau in Maschine oder Schaltschrank
- digitale und analoge **Ein**gänge (keine Aktuierung möglich)
- Seriell: TTY, RS-485
- Modbus, M-Bus für Meter/Zähler
- SPS-Anschluss z.B. via S7-Protokoll

# Datenerfassung

- jeder Digitaleingang liefert ein Datenobjekt mit
  - Hi/Lo Pegel
  - Zählwert
  - Taktzeit in ms
  - Zählfrequenz p.h.
- jeder Analogeingang liefert
  - aktueller Wert
  - Mittelwert über 1 Sekunde
  - Mittelwert über 10 Sekunden

# Edge Computing Plattform



- Eigene Logik implementierbar mit: Datenquelle, Datenpunkt, verschiedene Manipulatoren, Datensenke, Publish/Subscribe
- z.B. zur Generierung von Wartungsinformation aus Sensordaten
- perspektivisch: Implementierung eigener Algorithmen basierend auf API

# Cloud-Anbindung

Datenbereitstellung über verschiedene Protokolle:

- OPC-UA
- MQTT
- CoAP
- PPMP

# Gefährdung der Industrie durch IoT

- IoT-Geräte verbreiten sich rasend schnell (Industrie 4.0)
- Bedrohung durch Cyber-Angriffe auf vernetzte Systeme steigt
- Es wird sich ausschließlich auf Perimeter-Schutz verlassen
- Verfügbarkeit geht über Sicherheit

# Sicherheitsmerkmale

# Präsenz Detektion

- Bei sicherheitsrelevanten Konfigurationen wird Präsenz am Gerät verifiziert
- 3 Tasten an der Gehäusefront mit RGB-LEDs hinterleuchtet
- Tasten leuchten in unterschiedlichen, zufällig vergebenen Farben
- mehrere korrekte Bestätigungen an Fronttasten notwendig

# Detektion der Öffnung

- Eingebaute Photozelle auf Hauptplatine detektiert Gehäuseöffnung (eingebaut, noch nicht ausgewertet)

  → Schutz vor Innentätern separate Fragestellung

# Ausschließlich Kabelgebunden

- kein WLAN
- kein Bluetooth
- kein USB-Anschluss

- GSM Modul vorbereitet
  → z.B. für 2-Faktor Authorisierung

# 3 getrennte Netzwerkschnittstellen

- 1. LAN zum Internet
- 2. LAN zum Produktionsnetz für Datenerfassung aus Steuerungen und Produktionsmaschinen (z.B. mit S7-Stack)
- 3. LAN für direkten SPS-Anschluss **über Relais getrennt** und nur nach Authentifizierung zuschaltbar

# Keine Aktuierung

- Nur Signal**ein**gänge (bis auf zwei Solid State Relais z.B. für Lampen)
- **SPS Firewall** auf 2. LAN Schnittstelle.
  - ✦ Daten können nur gelesen, nicht geschrieben werden.
  - ✦ Datenzugriff auf bestimmte Variablen eingeschränkt

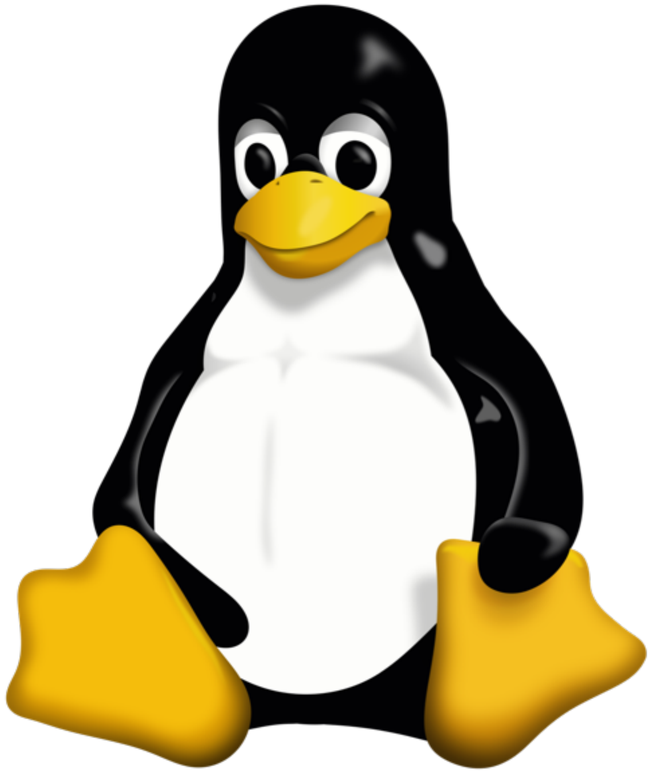
# Trusted Platform Modul 2.0 integriert

- Initialisierung (take ownership) mit frei definierbarem Passwort durch Arend
  → „Direct Anonymous Attestation“
- Erzeugt Root Key für alle abgeleiteten Schlüssel
- Erzeugt Storage Root Key
  nur neu generierbar via „take ownership“
- Erzeugt Storage Key
- Private Keys nicht auslesbar

# TPM Anwendung

- Erzeugung von asymmetrischen (RSA-2048, ECC) und symmetrischen Schlüsseln (AES-256)
- Datenverschlüsselung
- Erstellung von Signaturen und Hash-Werten (SHA-256)
- Generierung von Signaturen und Signaturprüfung
- Erzeugung einer sicheren und vertrauenswürdigen ID (Random Modul)

# Linux Betriebssystem

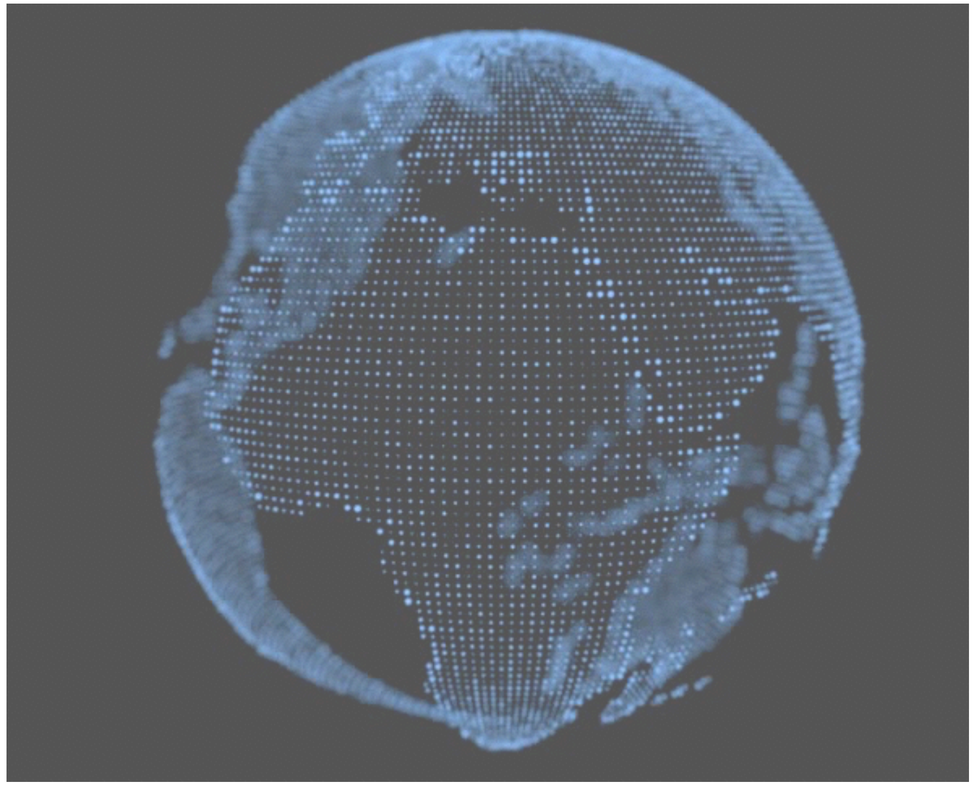


- Boot-Prozess überprüft RSA-signierten Kernelsignatur vor jedem Systemstart.
- Kein Start unsignierter Programme verhindert Einschleusen von Malware und Botnetz Infektion
- Verwendung von **SMACK** (Simplified Mandatory Access Control Kernel) mit extended attributes im Kernel aktiviert
- Labelling und dazugehöriges Regelwerk für Berechtigungen von Objekten und Prozessen zur Einschränkung von Systemrechten

# TPM Anwendung

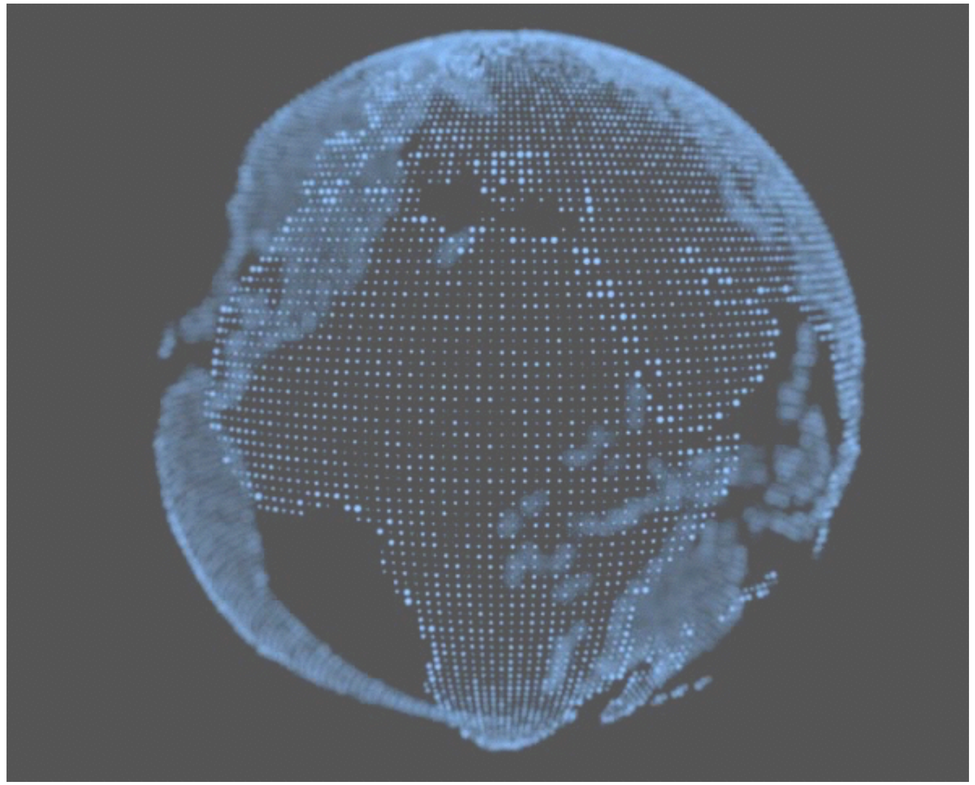
- Eindeutige ID zur Identifizierung des Geräts
- Aufspielen nur von korrekt signierten Patches möglich
- Aufbau verschlüsselter Kommunikation
- Verschlüsselte Ablage von Konfigurationsdaten und Prozessdaten auf lokalem Datenträger

# Web Kommunikation



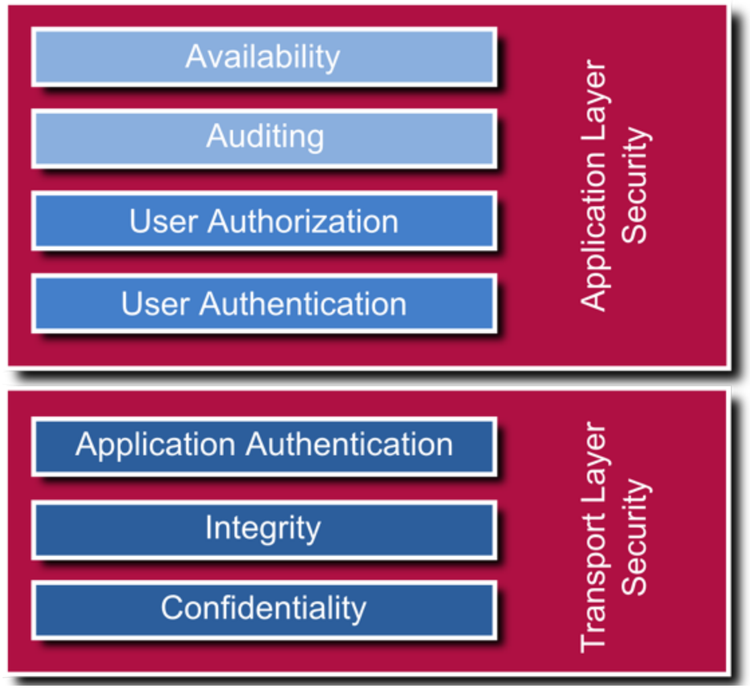
- Webserver nur über HTTPS erreichbar
- Eigene Implementierung eines Webservers mit WSS (web secure socket)
- Transportverschlüsselung via TLS/SSL

# Web Kommunikation



- Anfragen für Updates gehen nur von ARENDAR auf Arend Server
- Zugriff auf zuschaltbare 3. LAN Schnittstelle nur nach Aufbau einer VPN-Verbindung (openVPN)
- Via VPN eingeschränkter Zugriff auf Systemressourcen

# OPC-UA Stack




Quelle: ascolab.com

- Stack implementiert auf LAN1 (Internet) und LAN2 (Produktionsnetz)
- Sicherheit im Protokoll-Stack vorgesehen
- Basiert auf X.509 Zertifikaten

# Sicherheit und MQTT

Stark erhöhter Protokoll-Overhead für kleine Datenmengen

| Anzahl Bytes pro Übertragung | | | | |
|---|---|---|---|---|
| | **Quality 0** (at most once) | **Quality 1** (at least once) | **Quality 2** (exactly once) | **Faktor** |
| **ohne Verschl.** | 72 | 78 | 86 | 1 |
| **TLS-PSK** | 1172 | 1224 | 1331 | 16 |
| **TLS/SSL** | 3742 | 3777 | 3843 | 48 |

# DIN Spec 27070

Referenzarchitektur eines Security Gateways zum Austausch von Industriedaten und Dienste

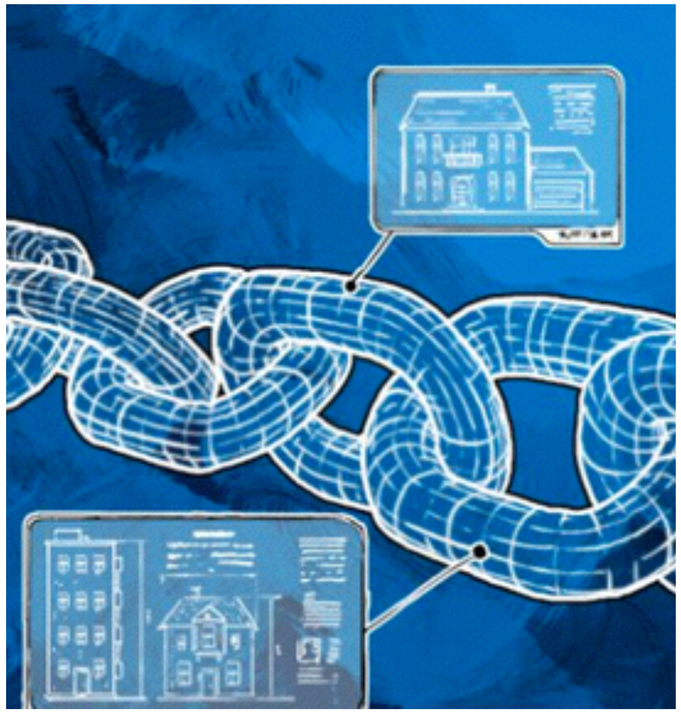
- Sicherheitsprofile
- Isolation
- Attestation
- Autorisierung
- sichere Kommunikation

# Weitere Entwicklung

# Zertifizierungen

- Konzeptvorstellung am BSI ist erfolgt
- Common Criteria Zertifizierung angestrebt
- TÜV SÜD Sec-IT GmbH Zertifizierung angestrebt

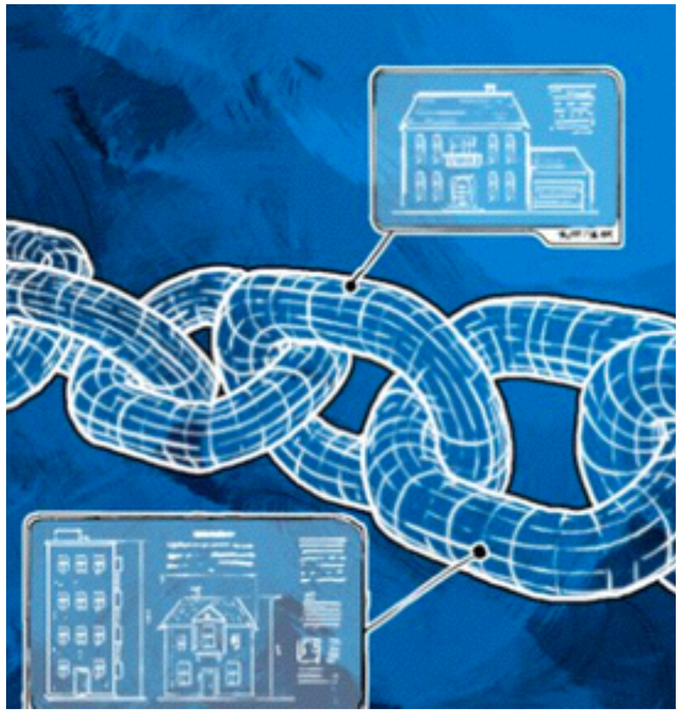
# Blockchain Technologie



Implementierung einer privaten Blockchain

- Dokumentation von Maschinennutzung über Blockchain Technologie
- Dokumentation von Patches und Updates
- Smart Contracts zur Freischaltung von Leistungsmerkmalen in Maschinen

# Blockchain Forschung



Forschungsprojekte

- Sichere Blockchain-Implementierung auf „Lightweight“-Plattformen mit reduzierter Rechnerleistung und limitiertem Speicher
- Sichere Blockchain Transaktionen bei extrem limitierter Bandbreite (z.B. ausschließlich SMS Versand/Empfang)

# Zusammenfassung

# Der ARENDAR

## Machine Connectivity

- Erfassung von Relaiszuständen und Signalen, Zählfrequenzen und Zeitstempel
- Analogsensoren
- RS485, Modbus, M-Bus
- SPS-Anbindung

## Edge Computing

- Offene Programmierschnittstelle (API)
- Integration eigener und kundenspezifischer Applikationen
- Raum für eigene Datenverarbeitung

## Future Technologies

- Blockchain
- Smart Contracts
- Pay Per Use
- Machine Currency

## Cyber Security DIN27070

- TPM2.0 Kryptoprozessor mit SHA-1, SHA-256, RSA, ECC, Hashing und sicherem Schlüsselspeicher
- Sicheres Linux mit SMACK & U-Boot
- getrennte LAN-Schnittstellen für Web & Produktion
- Präsenznachweis am Gerät

## Cloud Connectivity

- HTTPS / WSS
- OPC-UA
- MQTT / PPMP / CoAP

- optional: GSM / NFC u.a.

# ARENDAR
# Security by Design

INTERNET SECURITY DAYS 2017 ISD

AREND PROZESSAUTOMATION

Vielen Dank für Ihre Aufmerksamkeit!