



ABSICHERUNG VON IOT-GERÄTEN – DAMIT DAS LICHT NICHT AUSGEHT

ZD.B Themenplattform Cybersecurity – Best Practice IoT Security

16.6.2021 Dr. Manuel Sojer, Dr. Christian Schläger

MASCHINENFABRIK REINHAUSEN AUF EINEN BLICK

Global führend in Nischen der elektrischen Energietechnik

- | Gegründet 1868, Marke seit 1901
- | In der fünften Generation mehrheitlich in Familieneigentum
- | Weltmarktführer u.a. im Schalten von Transformatoren
- | 3.600 Mitarbeiter, 70% davon in Deutschland
- | 90% der Produktion in Deutschland
- | 40 Tochtergesellschaften und 4 Beteiligungsgesellschaften
- | Konzernumsatz 730 Millionen EUR, höchstes erhältliches Rating (AAA)



>50%

des weltweiten Stromverbrauchs
fließt über unsere Produkte

>80%

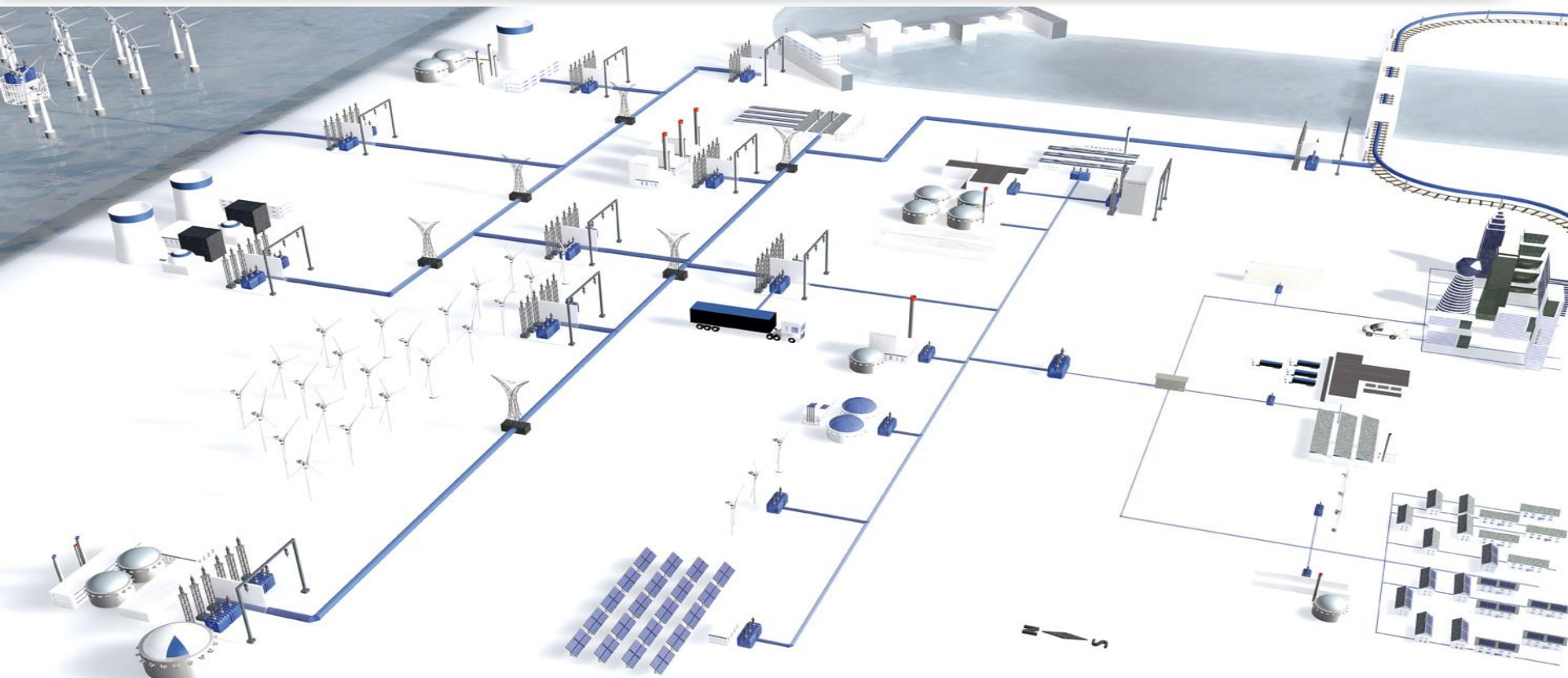
aller Produkte noch in Betrieb,
der älteste OILTAP seit 1950

Build38 – Mobile App Security for the Real World

- Gegründet 2018, venture-backed durch starke Investoren wie Caixa Capital Risc oder eCAPITAL
- Spin-off der Giesecke+Devrient
- Basis in München mit Büros und Entwicklungszentren in Barcelona und Singapore
- 100+ Millionen Nutzer über 6 Industrien werden weltweit durch uns unterstützt und geschützt
- Gewinner der PwC Cybersecurity Solution des Jahres 2020 und des Deutschen IT Security Pitch 2019
- Deep-Tech Unternehmen mit 75% Entwickleranteil



STROMNETZE „TICKEN“ IN SPANNUNGSEBENEN, DIE DURCH TRANSFORMATOREN VERBUNDEN WERDEN



TRANSFORMATOREN IM ÜBERTRAGUNGSNETZ REGELN SEIT 100 JAHREN DIE SPANNUNG MIT LASTSTUFENSCHALTERN



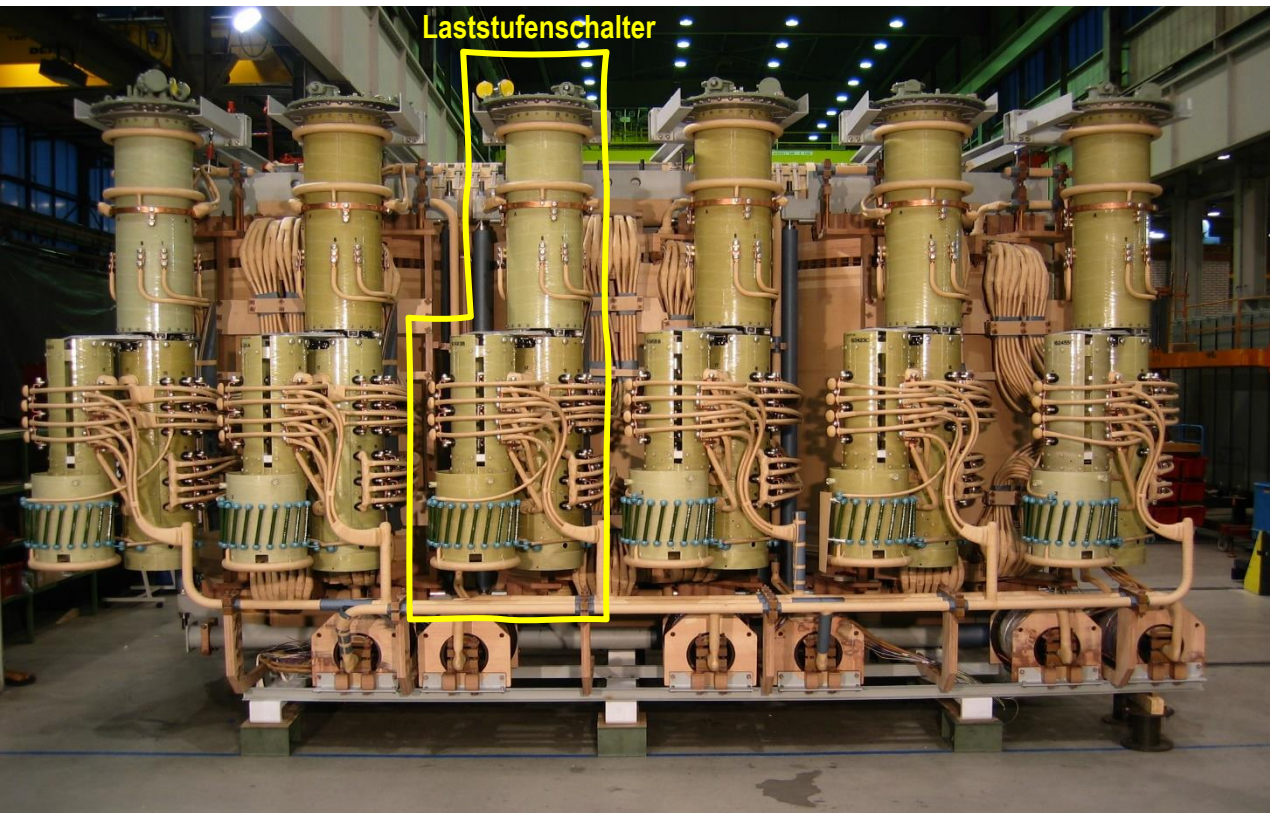
Umspannwerke als „geschlossene“ Systeme

- | Begrenzte Anzahl (~400 in DE)
- | Gut gegen physischen Zugriff geschützt
- | Kontinuierliche Überwachung
- | Dedizierte Kommunikationsnetze für SCADA
- | Teure Geräte mit eigenen, physischen HMIs für Inbetriebnahme, Parametrierung, Fehlerinteraktion etc.

DIE ENERGIEWENDE STELLT DIE STROMNETZE AUF DEN KOPF – SPANNUNGSREGELUNG AUCH IM VERTEILUNGSNETZ HILFT



FÜR DAS VERTEILUNGSNETZ MUSS DIE TECHNIK NEU GEDACHT WERDEN...



...INSBESONDERE AUCH DIE SICHERHEIT

Im Verteilungsnetz wird der Transformator IoT-Device

- | Kein Budget für physisches HMI und Gerät ggf. schlecht bedienbar bei großer Zahl (~650.000 in DE)
- | Häufig keine datentechnische Anbindung

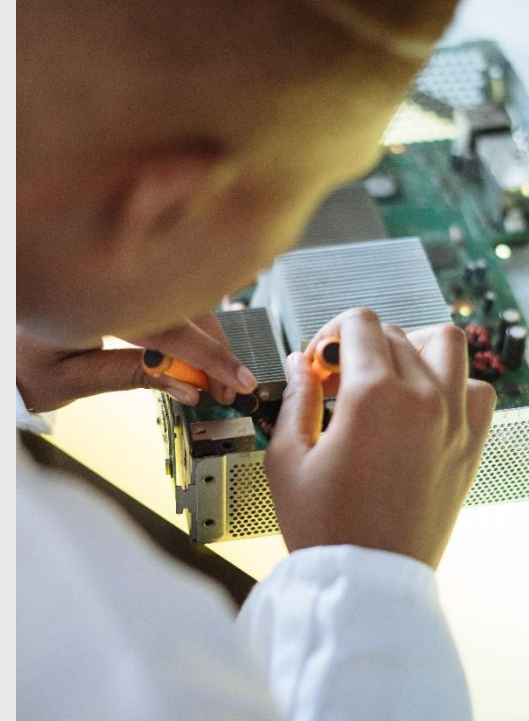
→ Handy-App mit Funkkommunikation als HMI

- | Sichere Verbindung zwischen Handy und Transformator
- | Zuverlässige und nachverfolgbare Authentifizierung und Autorisierung von Verbindungsanfragen (im „schlimmsten“ Fall ohne Internetverbindung)
- | Berechtigungsmanagement über verschiedene, eindeutig identifizierbare Nutzer und Zeitfenster
- | Besitzerwechsel des Transformators
- | Zuverlässiges Verhalten der Handy-App

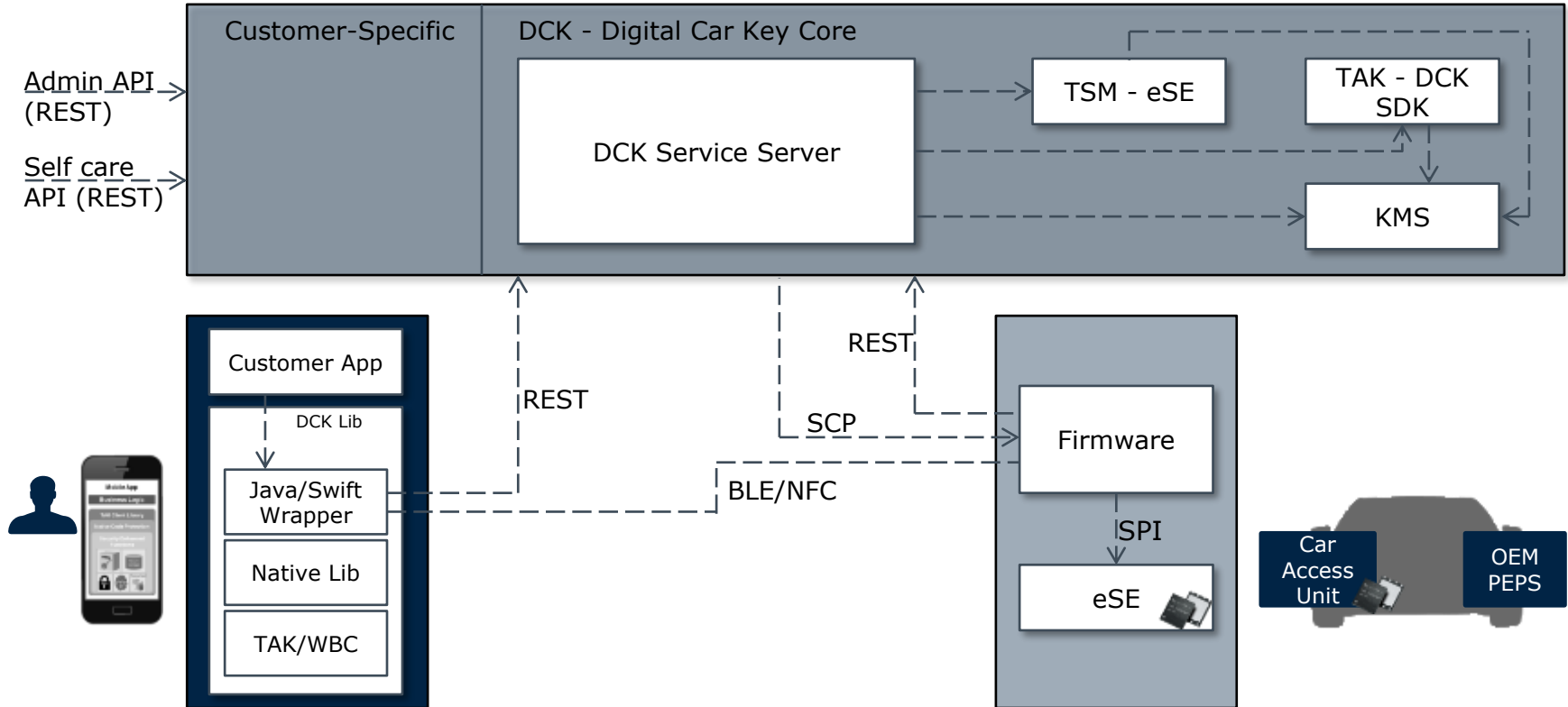


Die zentrale Herausforderung im IIoT Bereich ist die verlässliche Verbindung und die Arbeit mit vertrauenswürdigen Identitäten

- Bei Industriemaschinen und Apps treffen Welten aufeinander
- Kernproblem der IIoT ist das Verlassen der eigenen, definierten Umgebung - die Maschine muss in der Lage sein zu erkennen:
 - darf ich für dich arbeiten und
 - darfst du mir Befehle erteilen
- Grundlegende IT Sicherheitsfragen muss auch die IIoT beantworten:
 - Vertrauen wir der Verbindung?
 - Vertrauen wir dem Nutzer?
 - Sind die übermittelten Daten valide?
- Nutzung in einer kritischen Infrastruktur und Safety machen den Einsatz von allgemeinen Software Kits / App Kits unmöglich

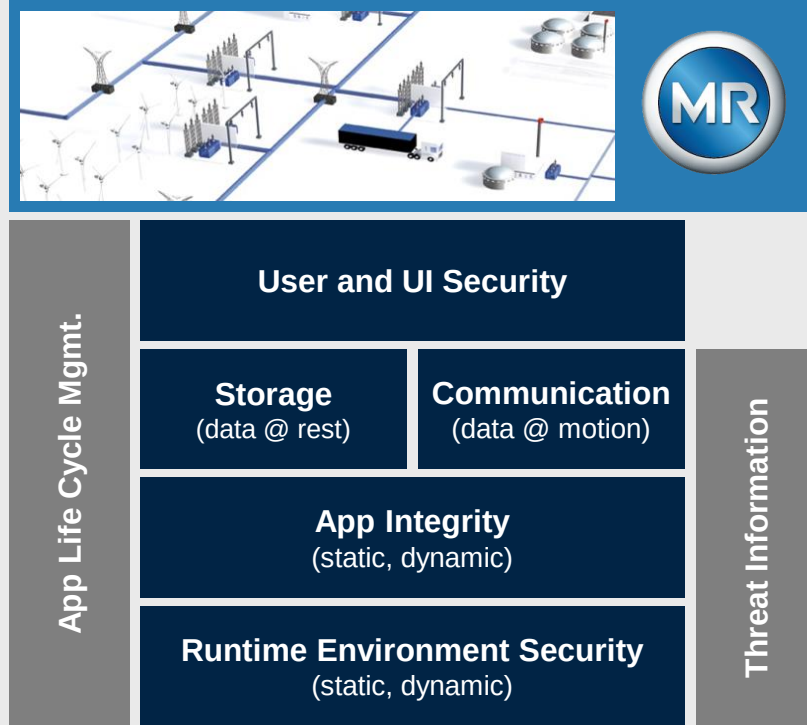


Beispiel Digitaler Autoschlüssel – auch nur ein IIoT Device



Build38 verbindet Welten und garantiert Verlässlichkeit

- Kernfunktionen der App werden über SDK schnell eingebunden
- KritIS Sicherheit by Design
- Spezifische Funktionen und Use Cases kommen on-top
- SDK für App wird ständig aktuell gehalten (durch Build38) und stört die Maschinenentwicklung nicht
- Zusatzfunktionen wie Threat Intelligence und Signatur ergänzen Geschäftsmodelle



Build38 SaaS Service

Lösungsarchitektur ist Referenz für Industrielle IoT: Fokus auf Verbindung, Rechtevergabe und Vertrauen

pre

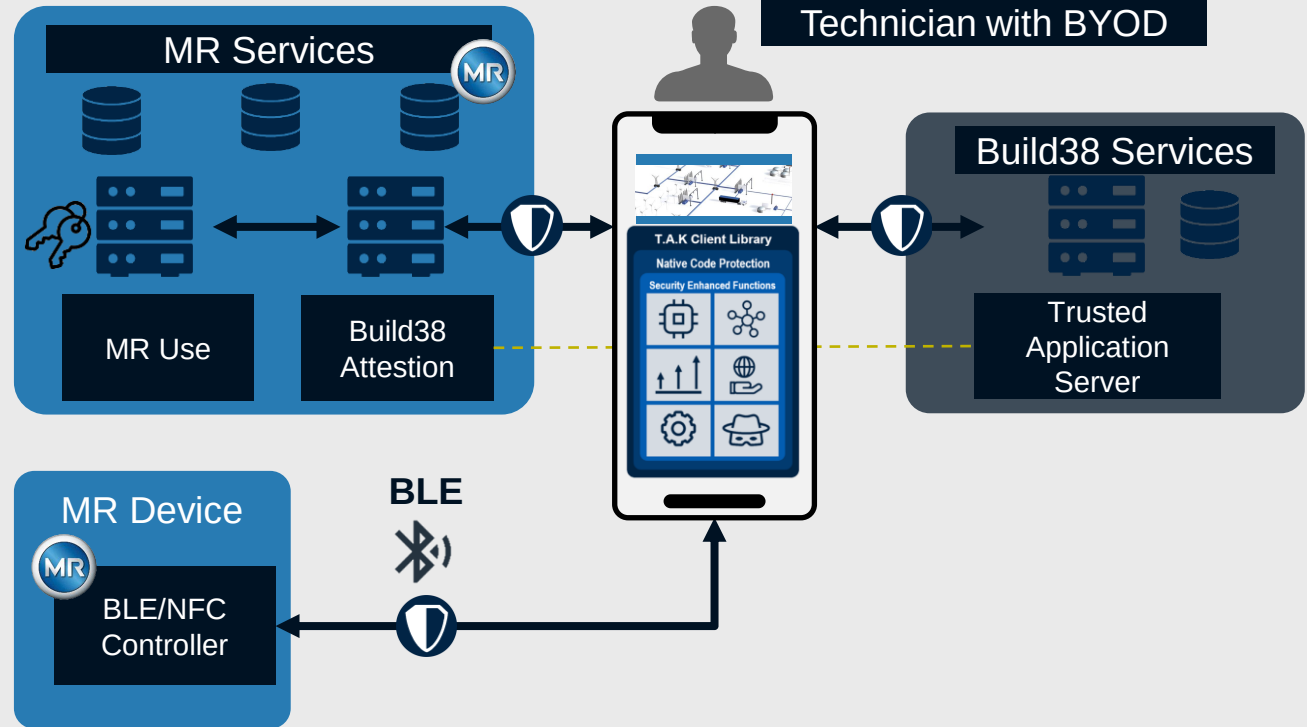
1. Techniker installiert App aus dem App Store
2. Identifizierung und Autorisierung – Zuweisung von Schaltern

FIELD

3. Verbindung zwischen Gerät und App (BLE)
4. Gerät lädt aktuelle FW / Updates
5. Gerät sendet Usage Daten

post

6. Gerät wird konfiguriert
7. Gerätedaten werden ausgewertet



Mehr erfahren:



www.build38.com



Mobile App Security for the Real World

Build38 GmbH

Tal 12 | 80331 München



Link zum Whitepaper

<https://build38.com/whiterpaper-build38-product/>



Link zur Case Study DCK

<https://build38.com/case-study-digital-car-key/>



Link zum Blog

<https://build38.com/blog/>



meet us



Dr. Christian Schläger
Managing Director & Co-Founder



+49 172 680 7769



christian@build38.com



www.build38.com

THE POWER BEHIND POWER.

www.reinhausen.com

