salzburgresearch

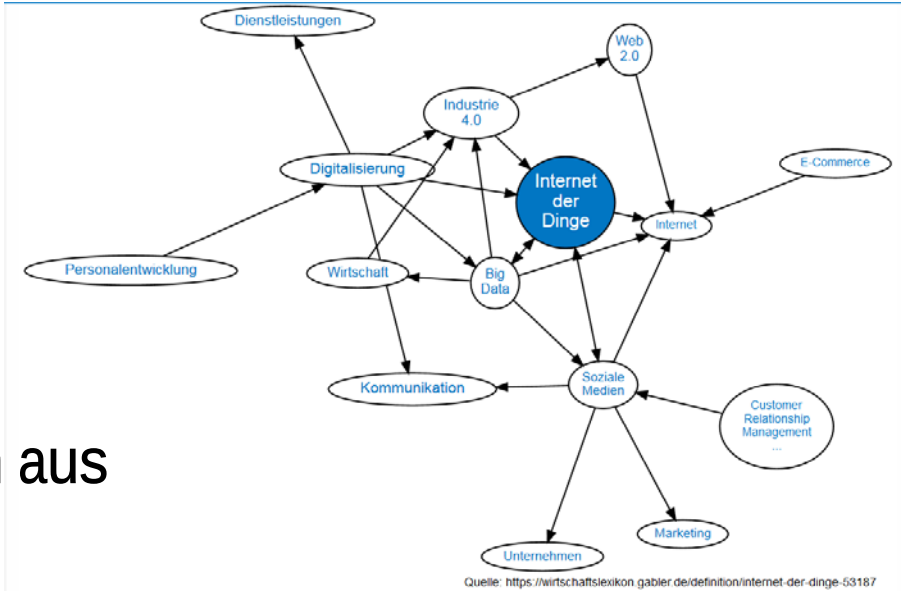
Industrial IoT – Für Sicherheit braucht es mehr als Security

DI (FH) DI Peter Dorfinger

Internet der Dinge – Internet of Things (IoT)

- Definition Gabler Wirtschaftslexikon
  - IoT bezeichnet die **Vernetzung von Gegenständen** mit dem **Internet**, damit diese **Gegenstände selbstständig** über das Internet **kommunizieren** und so verschiedene **Aufgaben für den Besitzer erledigen** können. Der Anwendungsbereich erstreckt sich dabei von einer allg. Informationsversorgung über automatische Bestellungen bis hin zu **Warn- und Notfallfunktionen**.

- Definition Austrian Standards
  - Das Internet der Dinge bezeichnet die **Verknüpfung** eindeutig identifizierbarer **physischer Objekte** mit einer **virtuellen Repräsentation** innerhalb einer **Internet**-ähnlichen Struktur.

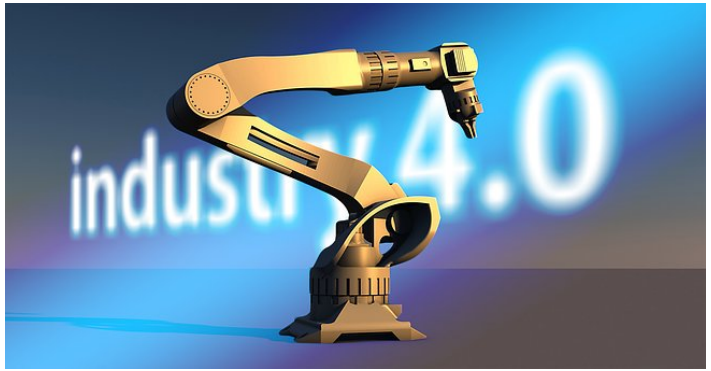


Quelle: https://wirtschaftslexikon.gabler.de/definition/internet-der-dinge-53187

=> Dinge tauschen Informationen aus

Industrial IoT

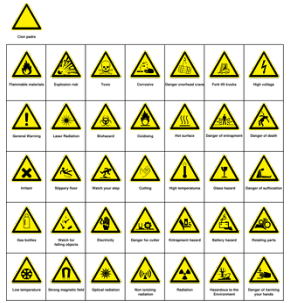
- Das Internet der Dinge in der Industrie



Sicherheit

Sicherheit

Security & Safety



Safety Integrity Level - SIL

- IEC 61508/IEC61511
- Funktionale Sicherheit
- Ermittlung des potentiellen Risikos für Geräte und Personen im Falle einer Fehlfunktion
- Zuverlässigkeit von Sicherheitsfunktionen
- 4 Stufen von 1 (Niedrigste) bis 4 (Höchste)

Drahtlose Bedienterminals mit Not-AUS

- Mehr Komfort für Operator durch Flexibilität
- Volle Prozesskontrolle
- Eingeschränkter Bereich wo sich Operator aufhalten darf
- Not-AUS am mobilen Terminal

Image source: Siemens, SIMATIC HMI Mobile Panels wireless.

Drahtlose Verbindungen Probleme in Bezug auf SIL

- Störungen der drahtlosen Signale von extern
- Störungen der drahtlosen Signale durch Produktionsabläufe
- Zuverlässigkeit der drahtlosen Verbindung
- Bereiche mit ausreichender/unzureichender Netzabdeckung
- Gezielter Angriff auf die drahtlose Signalausbreitung

Drahtloser Not-AUS SIL zertifiziert

- Drahtlose Verbindung wird als nicht zuverlässige Black Box betrachtet
- Zyklischer Informationsaustausch zwischen Maschine und Not-AUS
- Wenn Not-AUS nicht antwortet, kann nicht sichergestellt werden dass er nicht gedrückt wurde

=> MASCHINE STOPT!

Zuverlässige drahtlose Netze von Vorteil

- Aktuell sehr wichtiges Forschungsfeld
- Vor allem soll 5G zuverlässige drahtlose Netze anbieten
- Kontrolle der Zuverlässigkeit ist unerlässlich
- Kontrolle durch Unabhängige ist besser als Vertrauen

Zuverlässigkeit ist der Schlüssel

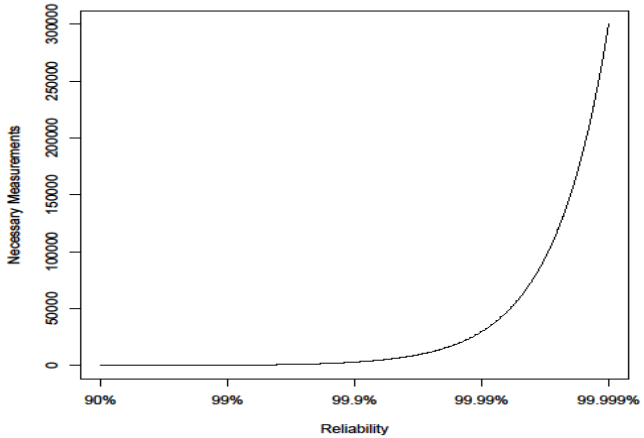
- **Zuverlässigkeit**: Rate (oder Anteil oder Wahrscheinlichkeit) an empfangenen Paketen
  - korrekt und
  - rechtzeitig

- Gründe für verringerte Zuverlässigkeit
  - Zustand des drahtlosen Kanals
    - Objekte auf der Sichtlinie (Maschinen, Autos, Pflanzen)
    - Reflektionen
    - Interferenz (aus dem gleichen oder anderen Frequenzbändern)
  - Antenne (Richtung, Änderung der Kapazität durch Objekte in der Nähe)
  - Mechanisch (Temperatur, Vibrationen, Metallstaub)
  - Wetter (Regen in der Luft, Wasseransammlung auf Oberflächen und in Vertiefungen)
  - Softwarestack
    - Medienzugriff, Zeitablaufsteuerung, Kontroll-/Kreuzverkehr
    - Übertragungswiederholungsprotokoll, Ratenkontrolle
  - Hardware, Herstellung, gefälschte Bausteine, Single Event Upsets
  - Sicherheitsfeatures, Angriffe, Störer
  - Nicht alle sind bekannt ➔ Ende-zu-Ende Tests nötig

Messung der Zuverlässigkeit

Bestimmen von 99,999 % Zuverlässigkeit (<1 von 100 000 fehlerhaft)

- 300 000 (unabhängige) Messungen benötigt
  - Untere Grenze des 95% Konfidenzintervalls > 99.999%
  - P(Unzuverlässigkeit detektiert | Unzuverlässigkeit gegeben) > 95%
    - Für 99.999% Konfidenz ~1 100 000 Messungen nötig
- Je 100 cm² (10 cm Kohärenz-Distanz → 100 Punkte pro 1 m²; in 3D: 1000 pro 1 m³)
- Je 500 kHz Bandbreite (Kohärenz-Bandbreite)

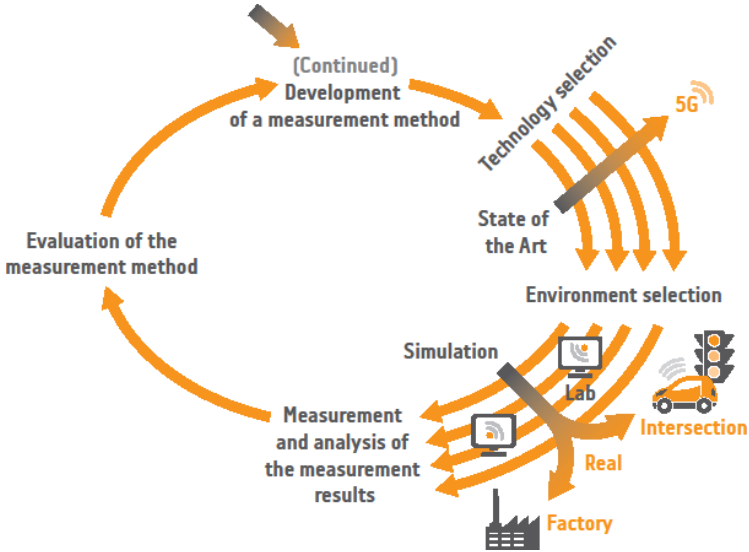


→ Explosion der Anzahl nötiger Messungen

→ Ausnutzung der Korrelation über Raum / Zeit / Frequenz nötig

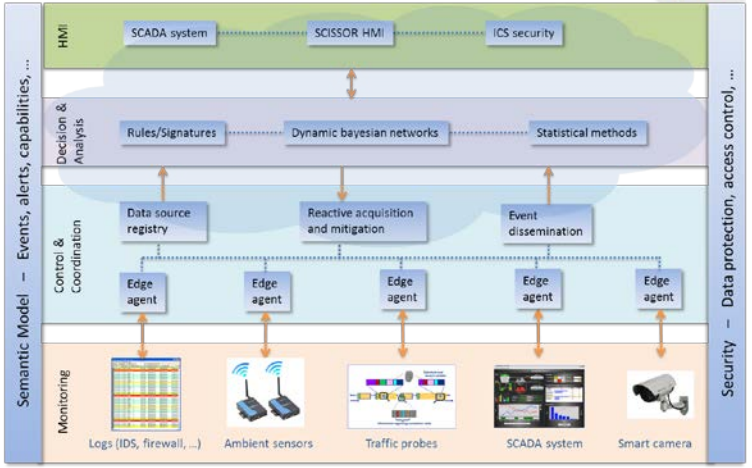
Zuverlässigkeitsmessungen

- Wir entwickeln Methoden zur Messung der Zuverlässigkeit von drahtlosen Netzwerken
- Monitoring der Umgebung um Änderungen die Einfluss auf die Kommunikation haben könnten frühzeitig zu identifizieren
- Keine teure Messhardware soll verwendet werden
- Auf Basis der Messungen soll die zukünftige Zuverlässigkeit vorhergesagt werden
- Prüfung durch unabhängiges Institut



Zusammenspiel Security / Safety

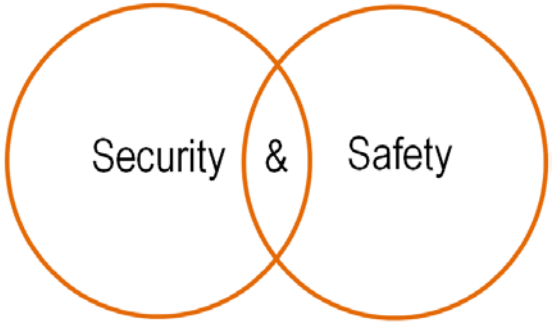
- Fallbeispiel Stuxnet
  - Angriff auf iranische Atomzentrifugen
  - Geschwindigkeit der Zentrifugen manipuliert
  - Anzeige der Geschwindigkeit ebenfalls manipuliert
  - Obwohl SIL zertifiziert gab es Schäden an den Atomzentrifugen



- Abhilfe hätte hier wieder ein unabhängiges Monitoring-System bieten können

- Ohne Security keine Safety, aber mit Security noch lange keine Safety

=> Sicherheit braucht Beides



salzburgresearch

Fragen?

DI (FH) DI Peter Dorfinger

Salzburg Research Forschungsgesellschaft m.b.H.
Jakob-Haringer-Straße 5/3 | Salzburg, Austria

Tel. +43 662 2288-452 | Fax +43 662 2288-222

peter.dorfinger@salzburgresearch.at