BG ETEM
Energie Textil Elektro
Medienerzeugnisse

Digitalisierung: Safety related security im betrieblichen Arbeitsschutz

Dipl.-Ing. **Björn Kasper**

Berufsgenossenschaft Energie Textil Elektro Medienerzeugnisse (BG ETEM),

Prüf- und Zertifizierungsstelle Elektrotechnik, Prüflabor Dresden

17. Oktober 2022

SiFa-Tagung Oktober 2022, Dresden

BG ETEM Vorstellung Prüf- und Zertifizierungsstelle Elektrotechnik (1)

Die Prüf- und Zertifizierungsstelle Elektrotechnik ist angesiedelt
im **Fachbereich Energie Textil Elektro Medienerzeugnisse (ETEM)**
der **Deutschen Gesetzlichen Unfallversicherung (DGUV)**
und bietet folgende Leistungen:

Prüfungen:

- Prüfungen und Messungen an elektrotechnischen Erzeugnissen, Maschinen und Anlagen
- Überprüfung der elektromagnetischen Verträglichkeit (EMV)
- Prüfung von Lasereinrichtungen nach DIN EN 60825-1/VDE 0837

Zertifizierungen:

- Zertifizierung von Produkten nach EU-/EG-Richtlinien (Maschinenrichtlinie, Niederspannungsrichtlinie und PSA-Richtlinie) und Produktsicherheitsgesetz (ProdSG)

Kalibrierungen von Messgeräten**:**

- für ***elektrische Messgrößen*** (Gleich-, Wechselspannung, Gleich-, Wechselstromstärke, Gleichstromwiderstand, Frequenz)
- ***thermodynamische Messgrößen*** (direktanzeigende Thermometer)

BG ETEM Vorstellung Prüf- und Zertifizierungsstelle Elektrotechnik (2)

Die Prüf- und Zertifizierungsstelle Elektrotechnik ist angesiedelt
im **Fachbereich Energie Textil Elektro Medienerzeugnisse (ETEM)**
der **Deutschen Gesetzlichen Unfallversicherung (DGUV)**
und bietet folgende Leistungen:

Unterstützung des **DGUV-Fachbereichs ETEM** u.a. durch:

- Mängeluntersuchungen
- Sonderprüfungen von neuartigen Arbeitsmitteln und Arbeitsverfahren

Unterstützung der **Präventionsabteilung** durch:

- Untersuchungen bei Unfällen
- Schulungen, Vorträge bei Fachtagungen und regelmäßige BG ETEM-Seminare, z.B.:
    - 163 (ehem. ET8) „Sichere und fachgerechte Prüfung elektrischer Anlagen, Betriebsmittel und Maschinen“
    - 266 (ehem. MT4) „Konstruktion nach EU-Richtlinien“

Vorstellung Prüf- und Zertifizierungsstelle Elektrotechnik (3)

Kontakt:
Fachbereich ETEM
Prüf- und Zertifizierungsstelle Elektrotechnik
im DGUV Test

Gustav-Heinemann-Ufer 130
50968 Köln

Pruefstelle-et@bgetem.de

www.bgetem.de
Webcode: pruefstelle-et

Standort Köln (Hauptverwaltung BG ETEM)

Standort Dresden (Bezirksverwaltung BG ETEM)

BetrSichV: Gefährdungsbeurteilung Elektrosicherheit (1)

Gerät / Anlage	Gefährdungen	Maßnahmen
 Steckdosenadapter mit Schalter	• Elektrischer Schlag • Brand	• Prüfung nach DGUV Vorschrift 3 (ehem. BGV A3-Prüfung)
 Funksteckdose (433 MHz)	• Elektrischer Schlag • Brand • Unerwartetes Schalten aufgrund Manipulation der Funk-Schaltbefehle	• Prüfung nach DGUV Vorschrift 3 (ehem. BGV A3-Prüfung) • ??

BetrSichV: Gefährdungsbeurteilung Elektrosicherheit (2)

Gerät / Anlage

WLAN-Steckdose, sog. Smart Plug
(mit Steuerung über Cloud und App)

Gefährdungen

- Elektrischer Schlag
- Brand

- Unerwartetes Schalten aufgrund:
  - Manipulation Funk-Kommunikation
  - Manipulation Schaltbefehle
  - Manipulation Firmware Smart Plug
  - Manipulation Smartphone App
  - Manipulation Router / Gateway
  - Manipulation Schaltlogik in Cloud
  - …

- Kompromittierung Firmennetzwerke:
  - Scannen anderer Netze
  - Manipulation Funk-Kommunikation
  - Einbau von Hintertüren
  - …

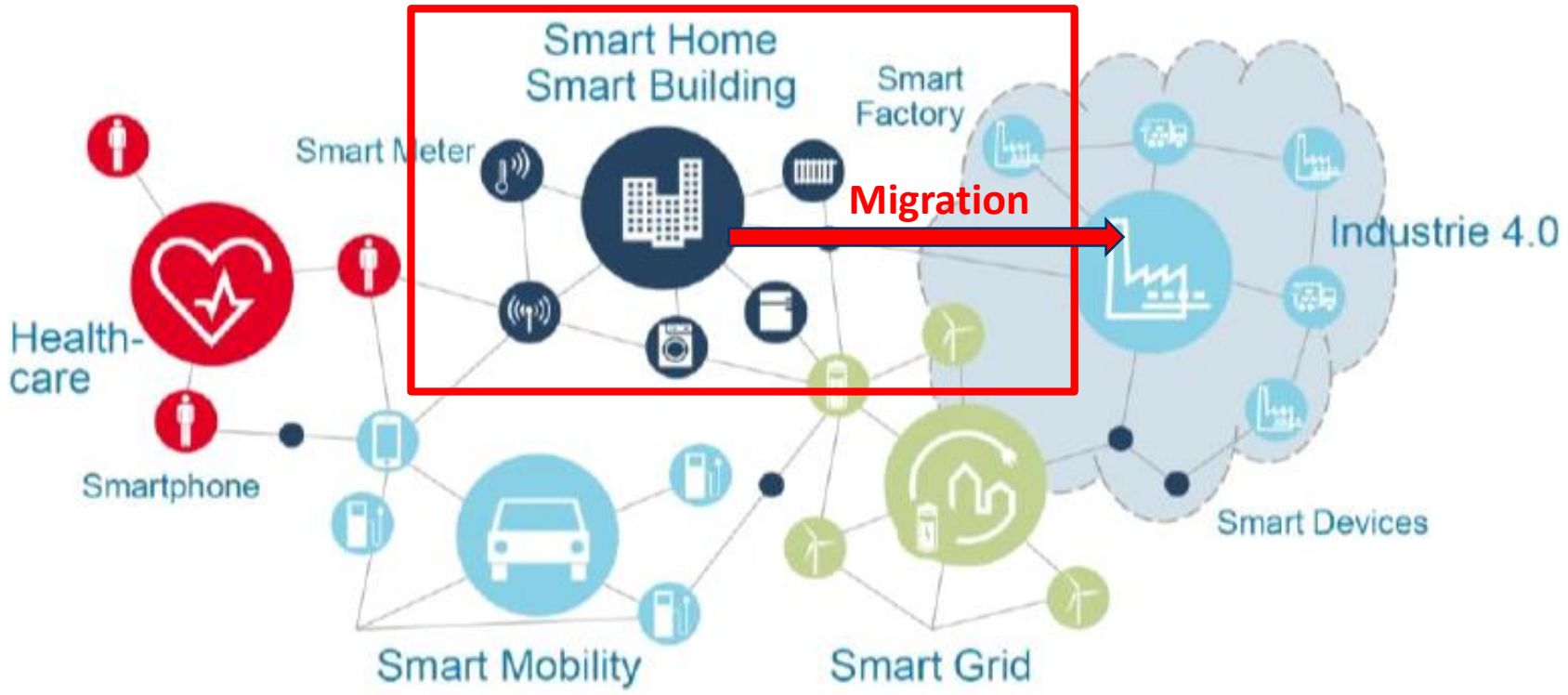
Maßnahmen

- Prüfung nach DGUV Vorschrift 3
  (ehem. BGV A3-Prüfung)

??

??

Digitalisierung: Migrationsprodukte im Betriebsumfeld

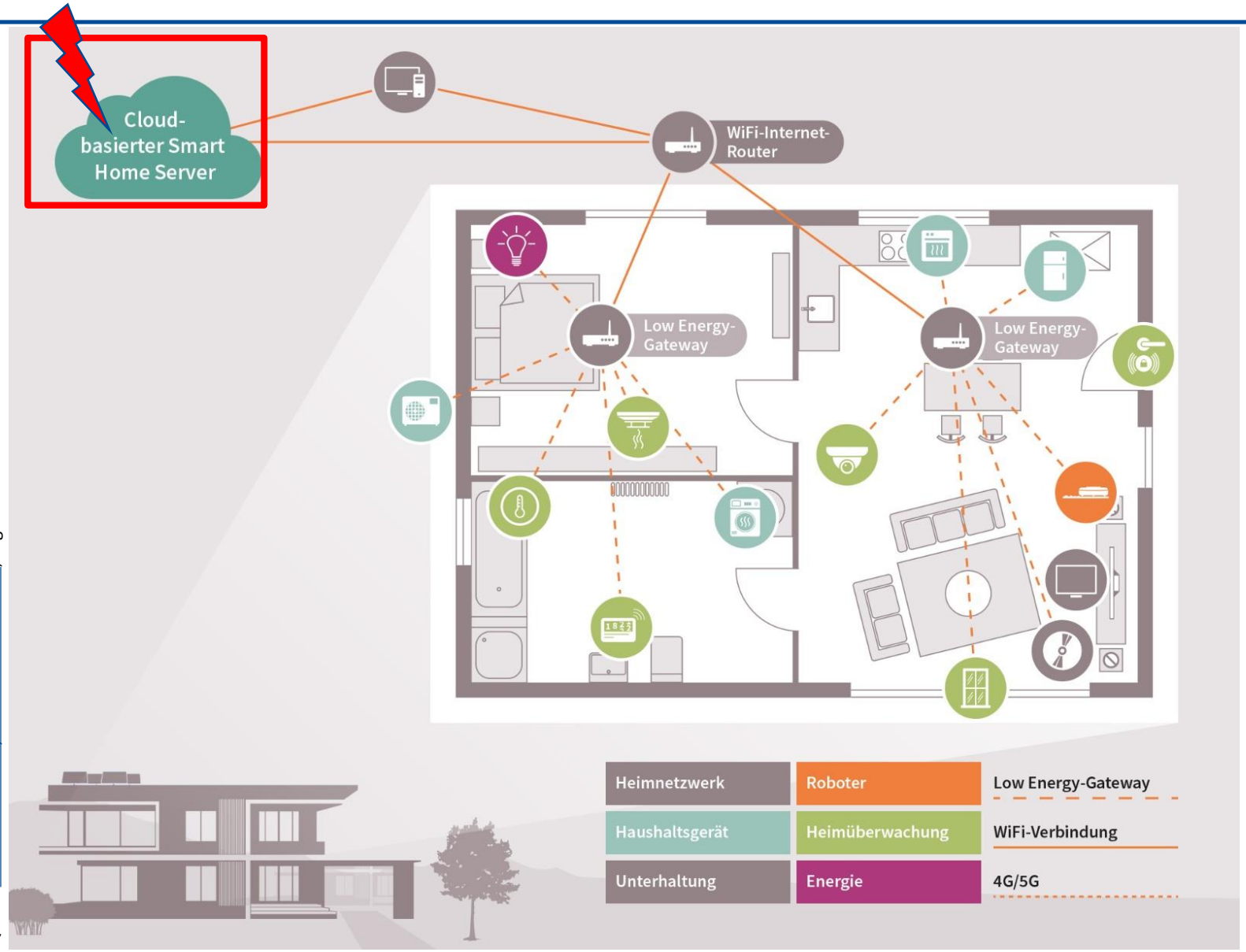


Quelle: VDMA Forum Industrie 4.0

- **Migrationsprodukte**: Smart-Home-Automation wird z.T. im betrieblichen Arbeitsumfeld genutzt
- Neben Datenschutz & Know-How-Schutz können auch **Safety**-Aspekte relevant werden
- Smart-Home-Produkte genügen oft nicht den erhöhten Industrie-Anforderungen (u.a. mechanische Robustheit, Elektrosicherheit, EMV und insb. **Security**)

⇒ **Unsachgemäßer Einsatz stellt erhebliche Angriffsfläche für Unternehmen dar!**

Smart Home: IoT-Struktur als Angriffsvektor



Quelle: Smart Home: Alles, was Sie wissen sollten, abgerufen am 29.09.2022

Sicherheit der Funkkommunikation:

Verschlüsselung möglich
(z.B. WPA2 bei WLAN)

Verschlüsselung kaum möglich, da verbindungsloser Low Energy-Funk und/oder bekannte schwere **Sicherheitslücken**
(z.B. ZigBee*, Z-Wave**)

***ZigBee**:
- Deepsec: ZigBee macht Smart Home zum offenen Haus
- Sicherheitspatch: Philips-Hue-Lampe als Sprungbrett in Netzwerke

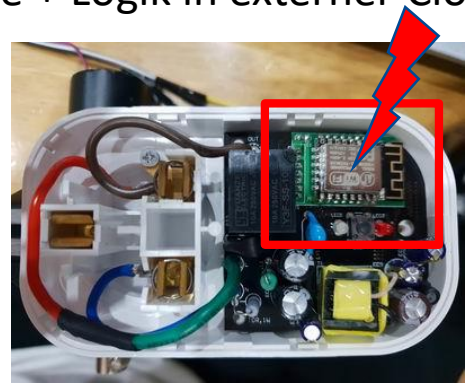
****Z-Wave**:
- Z-Shave: Angreifer könnten Funkstandard Z-Wave ausspionieren
- Z-Wave-Alarmanlagen mit einfachsten Mitteln zu knacken

Smart Home: IoT-Geräte als Angriffsvektor

- Unsichere Kommunikationsprotokolle (HTTP, FTP, Telnet, …)
- Bekannte Standard-„Passwörter“
- Mangelhafte embedded Firmware mit massiven Bugs
- „hard coded“ Passwörter
- Mangelhafte Update-Mechanismen
- Logik in externer Cloud mit zweifelhafter Sicherheit
- …

Bsp.: **WLAN-Kameras***
=> unsichere Protokolle + Standard-„Passwörter“

Bsp.: **WLAN-Steckdosen****
=> Unsichere Firmware + Logik in externer Cloud



OS-Firmware flashen

TASMOTA

Substituieren?

***Unsichere Passwörter**:
- Passwort-Petze
- IP-Kameras machen das Zuhause oft unsicherer
- Default Camera Passwords

****Tuya-Firmware**:
- Heise-Artikel: Der Tuya-Smart-Home-Hack
- 35C3-Vortrag: Smart Home - Smart Hack

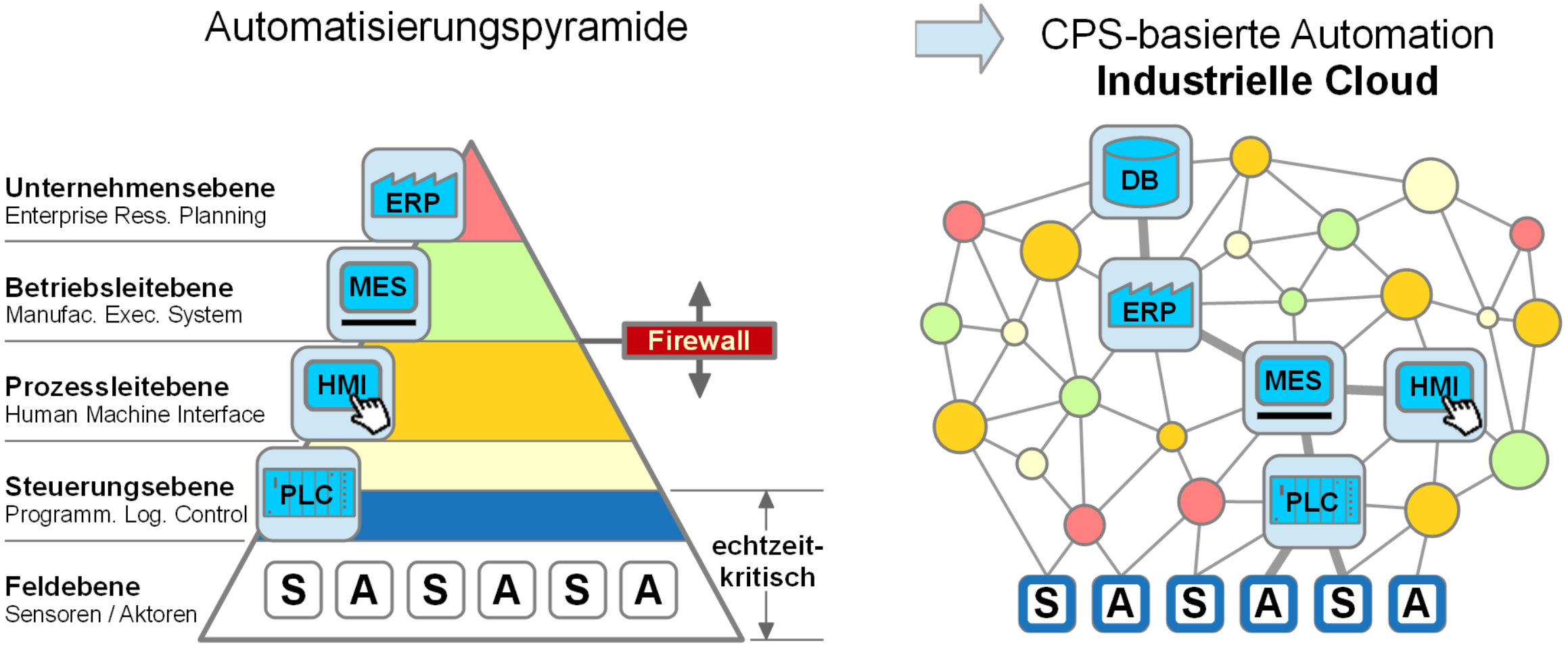
Digitalisierung: Durchgängig vernetzte Maschinen & Anlagen

Quelle: VDMA Forum Industrie 4.0

- Durchgängige Automatisierung und Vernetzung kompletter Wertschöpfungsketten
- Mitführung von Produktionsdaten über gesamten Lebenszyklus ⇒ Vermeiden medialer Brüche
- Zusammenwirken von Natur-, Ingenieurs- und Geisteswissenschaften + deren wiss. Methoden

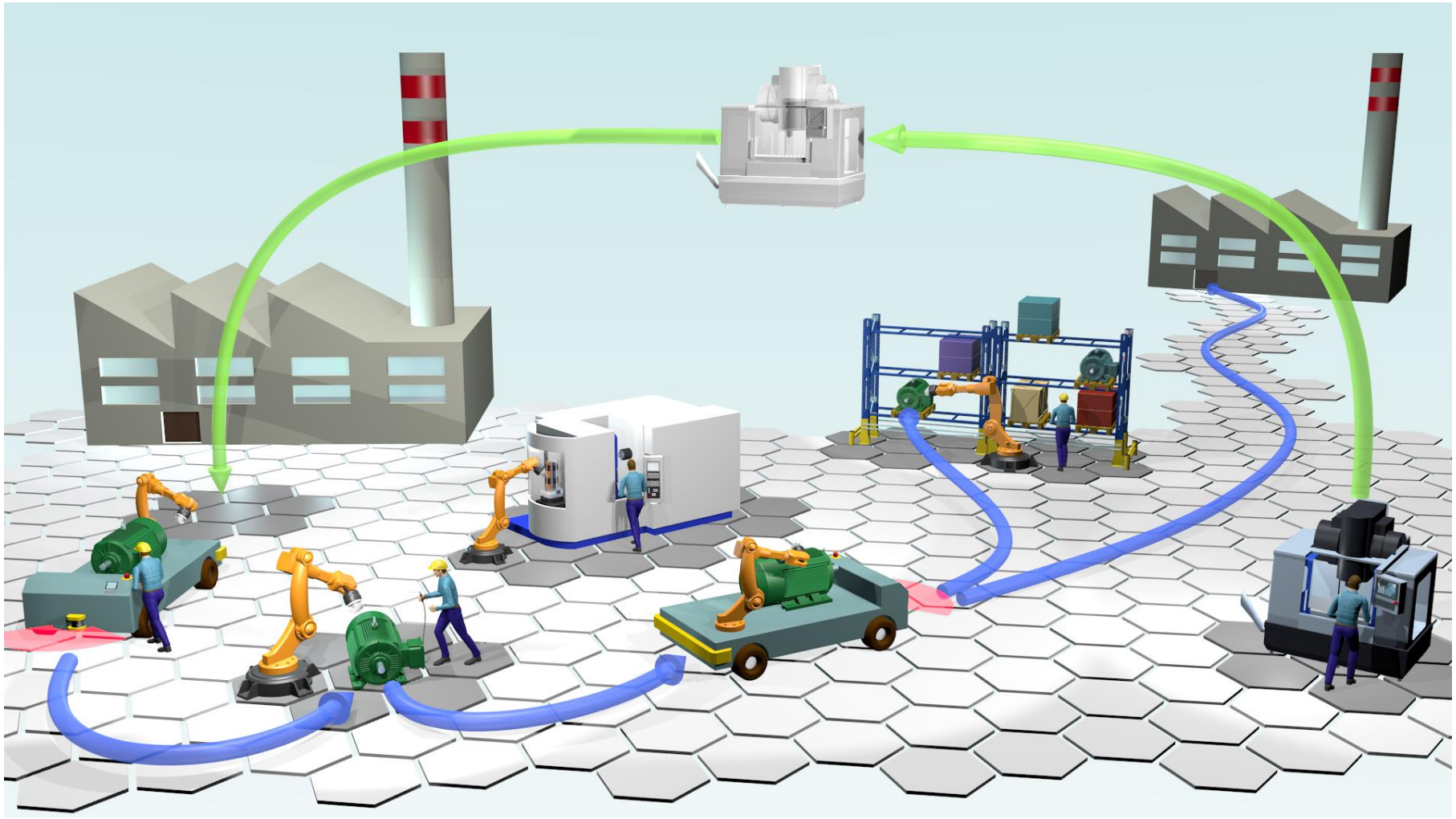
⇒ Komplexität ⇑ + Transparenz & Nachvollziehbarkeit für Beschäftigte ⇓

Vernetzte Maschinen & Anlagen: heute und morgen?



(vgl. VDI/VDE "Thesen und Handlungsfelder - Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation". April 2013)

Warum?: Wandelbarkeit durch Modularisierung ⇒ Industrie 4.0



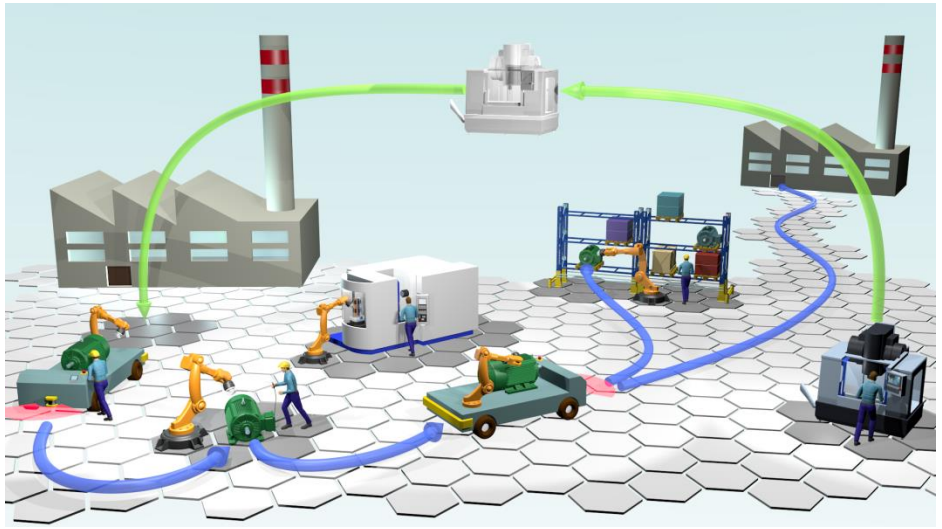
Blau: **Modularisierung** der Produktion durch z. B. vernetzte Fertigungsinseln
Grün: **Wandelbarkeit** der Produktion: Produkt steuert Fertigungsprozess

I4.0: Paradigmenwechsel in Fertigungs- u. Produktionstechnik

Quelle: Bossard Smart Factory Logistics

Heute:
Flexibilisierung
durch Varianten-Fertigung

Funkbasierte **Vernetzung** von Anlagenteilen



Quelle: Kasper, Lizenz: CC BY-SA 4.0

Morgen: **Wandelbarkeit** durch Modularisierung von vernetzten Fertigungsinseln

Industrie 4.0: modulare, intelligente, digital vernetzte „cyber-physische“ Systeme verbunden mit dynamischer Rekombinierbarkeit ⇒ Wandelbarkeit

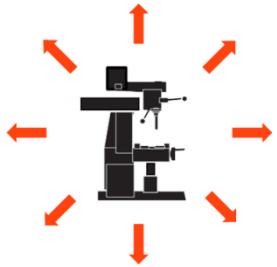
Sicherheitstechnik vernetzter Maschinen & Anlagen

Sicherheitstechnik:

- Technische & organisatorische Maßnahmen zur Erreichung der Sicherheit

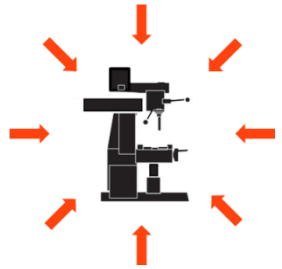
Safety (= Produkt- / Betriebssicherheit):

- Wirkungsrichtung: System ⇒ Umgebung
- Abwesenheit unvertretbarer Risiken für Menschen und Umgebung durch Herstellung / Betrieb des Systems



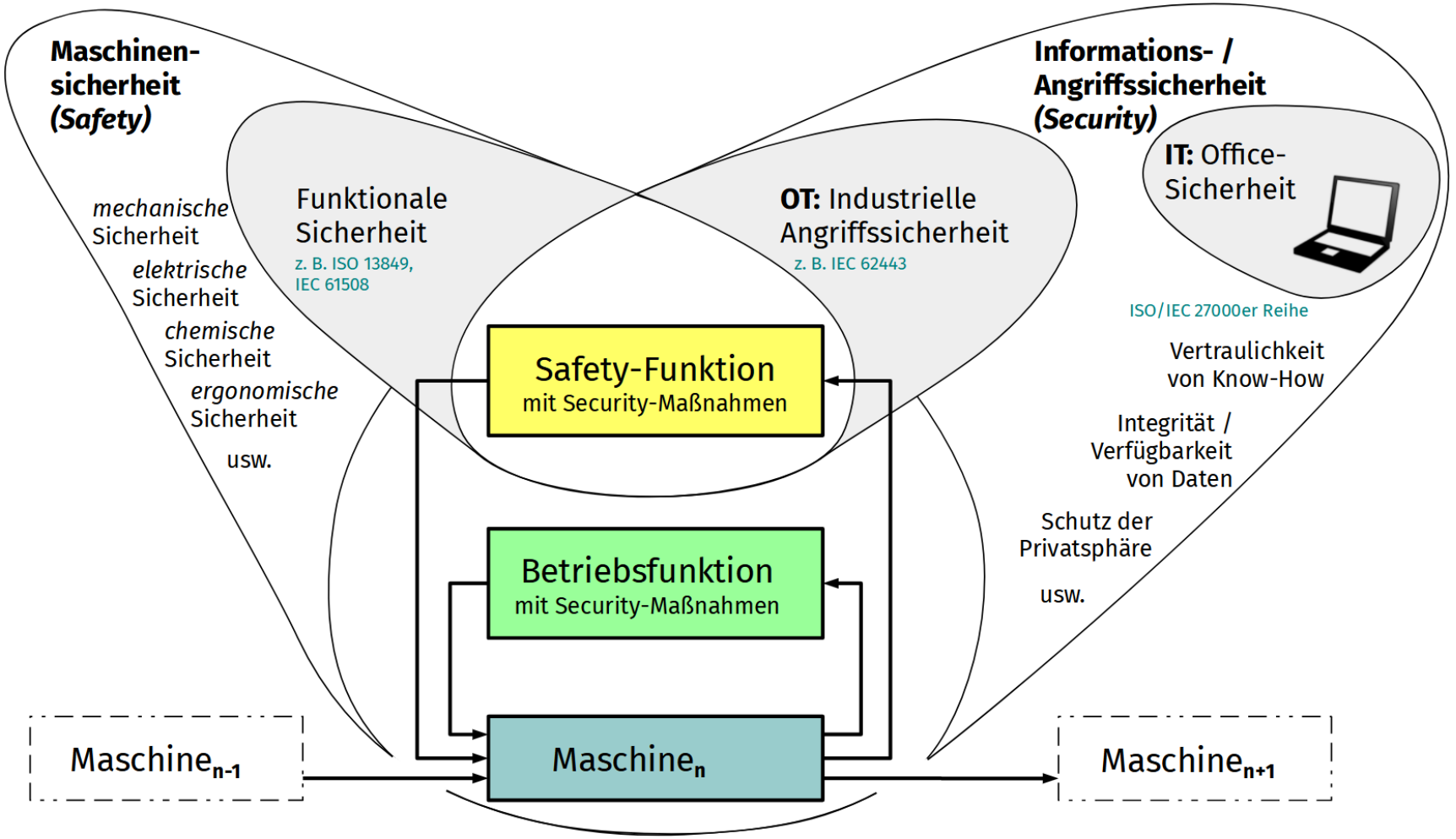
Industrial Security (= Angriffs- / Manipulationssicherheit):

- Wirkungsrichtung: Umgebung ⇒ System (Funk.-Sich.)
- Schutzziele: Daten und Dienste schützen
- neben „Internetsicherheit“ (**IT-Security**) ⇒ Maschinen- / Anlagen-Sicherheit (**OT-Security**)



⇒ Können sich gegenseitig beeinflussen: aus Security-relevanten Bedrohungen können Risiken für Safety entstehen (sog. „**safety related security aspects**“)

Schutzziele von Safety & Security



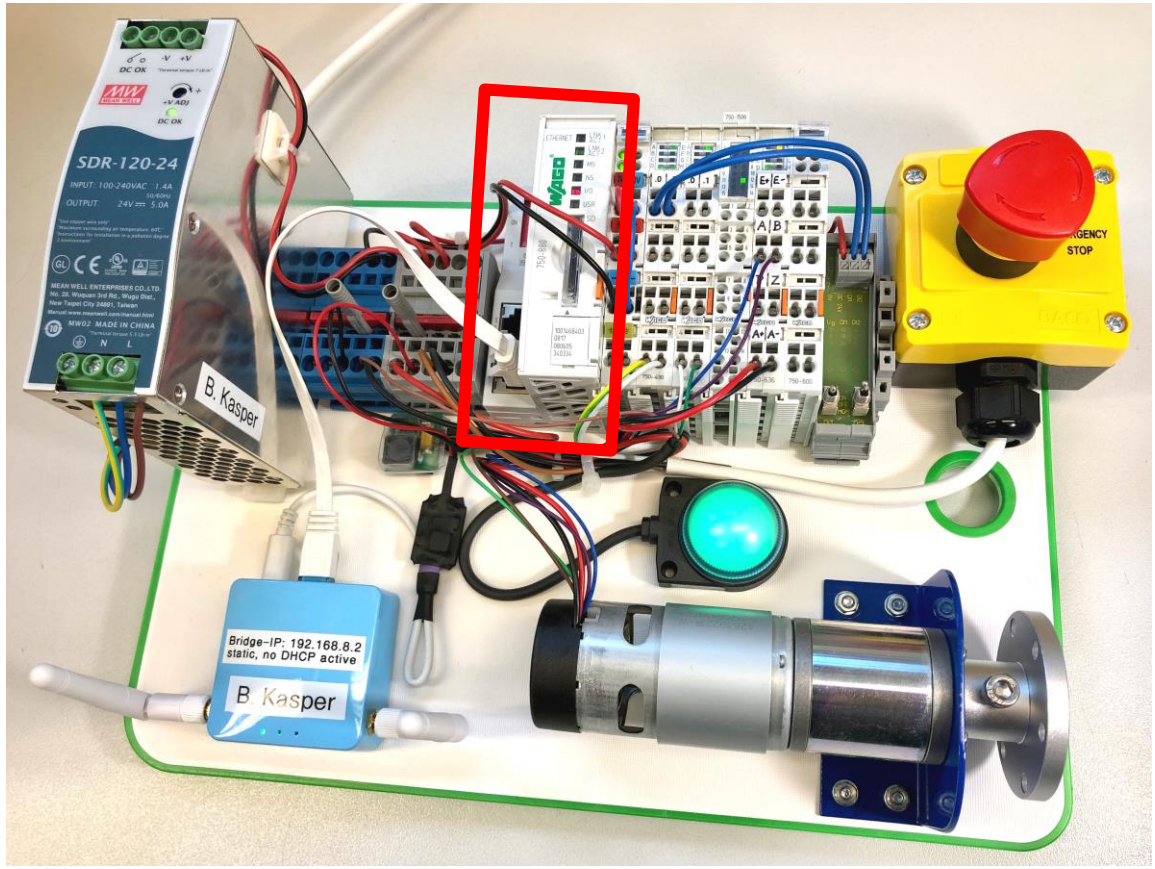
Quelle: Kasper, Lizenz: CC BY-SA 4.0

Betriebs- und Sicherheitsfunktionen von Maschinen und Anlagen

⇒ **Ziel: Risikobeurteilung als kombinierten Prozess etablieren!**

Beispielhaftes Prüfobjekt (1)

Programmierbarer Feldbus-Controller
(für Ethernet IP + Modbus TCP)



Bekannte **Safety-related Security-Bugs:**

- im Auslieferungszustand **keine** Sec.-Maßnahmen aktiv!
- HTTP, FTP, SNMP: keine Verschlüsselung
- schwache Authentifizierung (login "admin" + password "wago")
- Java-basiertes Web-HMI: unsicher + veraltet
  ⇒ Nicht per Update zu beheben!
- Modbus-TCP komplett offen + sehr leicht angreifbar
- Ext. Zugriff auf sicherheitsrelevante Funktionen im Zustand ‚RUN'
- Keine Lebenzeichenüberwachung der Motor-Treiber-Karte über Rückwandbus
- …

⇒ oft **keine Änderung** durch Hersteller / Betreiber (Unkenntnis?, mangelndes Problembewusstsein?)

Beispielhaftes Prüfobjekt (2)

7.5.4 MODBUS-Konfigurationsregister des 750-88x

Über die Konfigurationsregister lassen sich die Eigenschaften des 750-88x ermitteln und teilweise verändern.

750-88x: MODBUS Configuration Register for FC3, FC4, FC6 and FC16

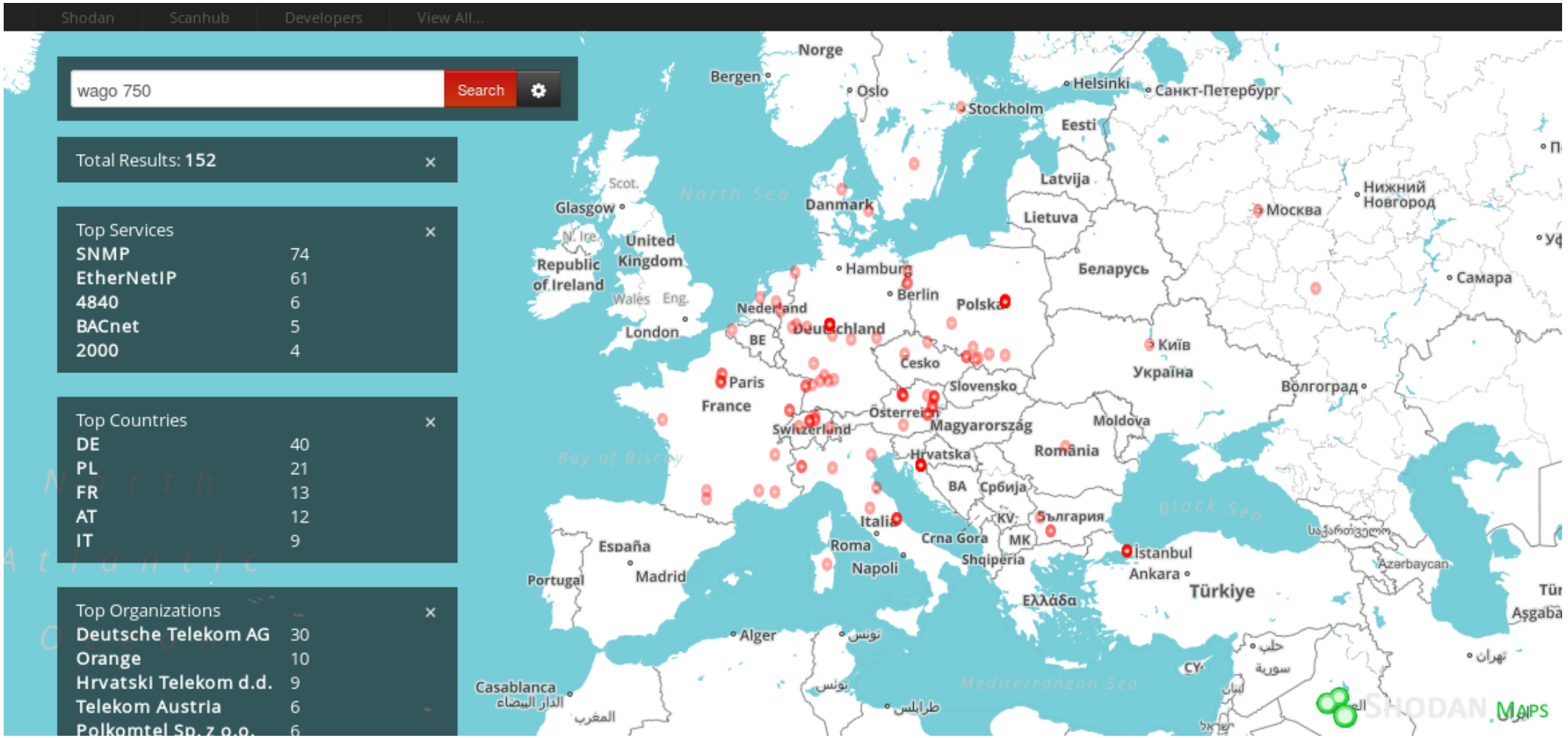
MODBUS Address [dec]	MODBUS Address [hex]	Length [Word]	Access	Description
8256	0x2040	1	W	Software Reset (write 0x55AA or 0xAA55)
8257	0x2041	1	W	Format Flash-
8258	0x2042	1	W	Extract file system
8259	0x2043	1	W	Werkseinstellungen

bk 19.08.2017, 19:28:29
Adressbereiche können über WBM=>Modbus geblockt werden.

bk 19.08.2017, 19:19:25
Achtung:
Diese Aktion löscht auch das interne Dateisystem (Webserver + Konfigurationen sind weg)!!! => I/O-LED blinkt rot

bk 19.08.2017, 19:19:28
Dateisystem wiederherstellen mit dem Tool "Wago Ethernet Settings" => "Dateisystem zurücksetzen"

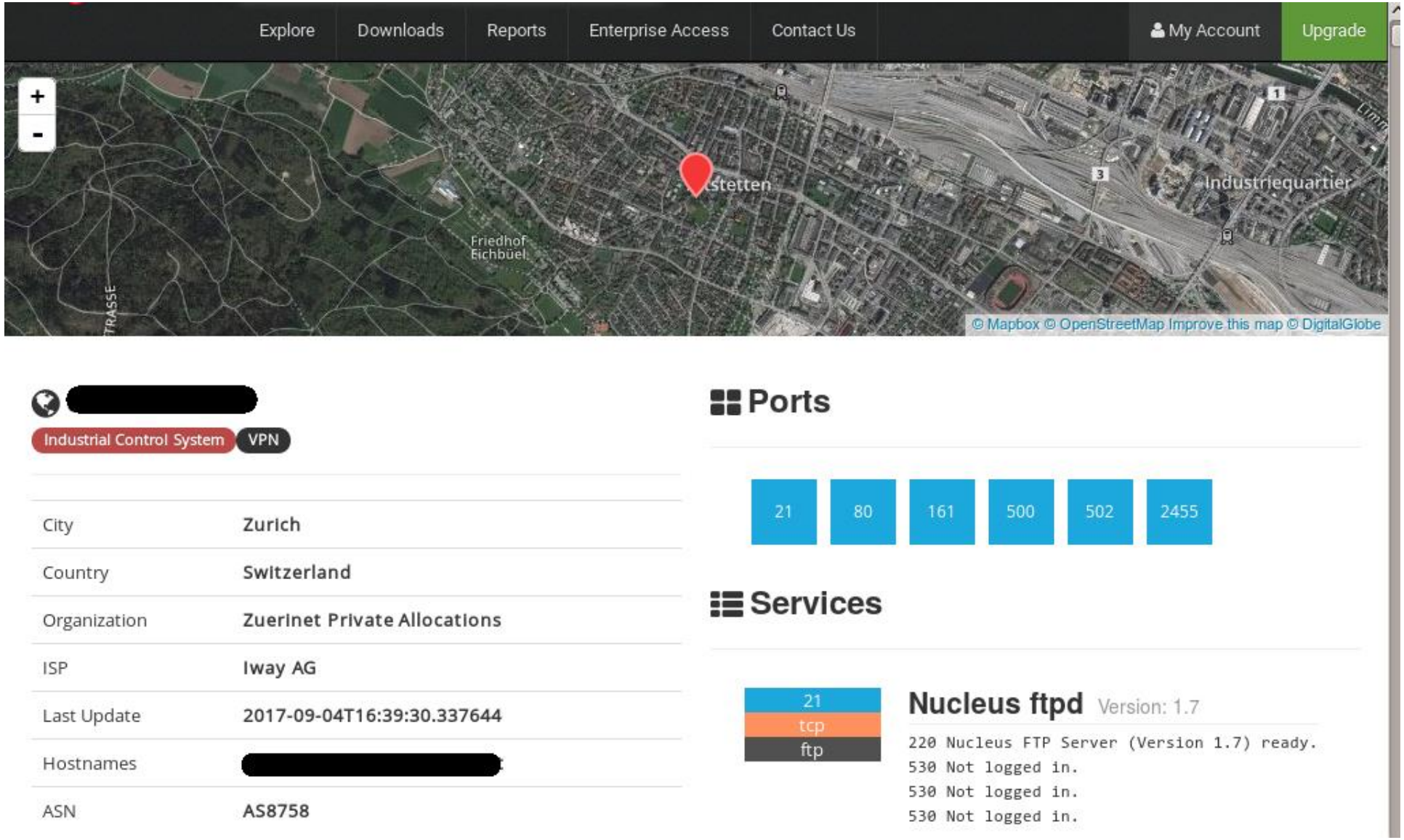
Relevanz-Überprüfung



Quelle: Kasper, Lizenz: CC BY-SA 4.0

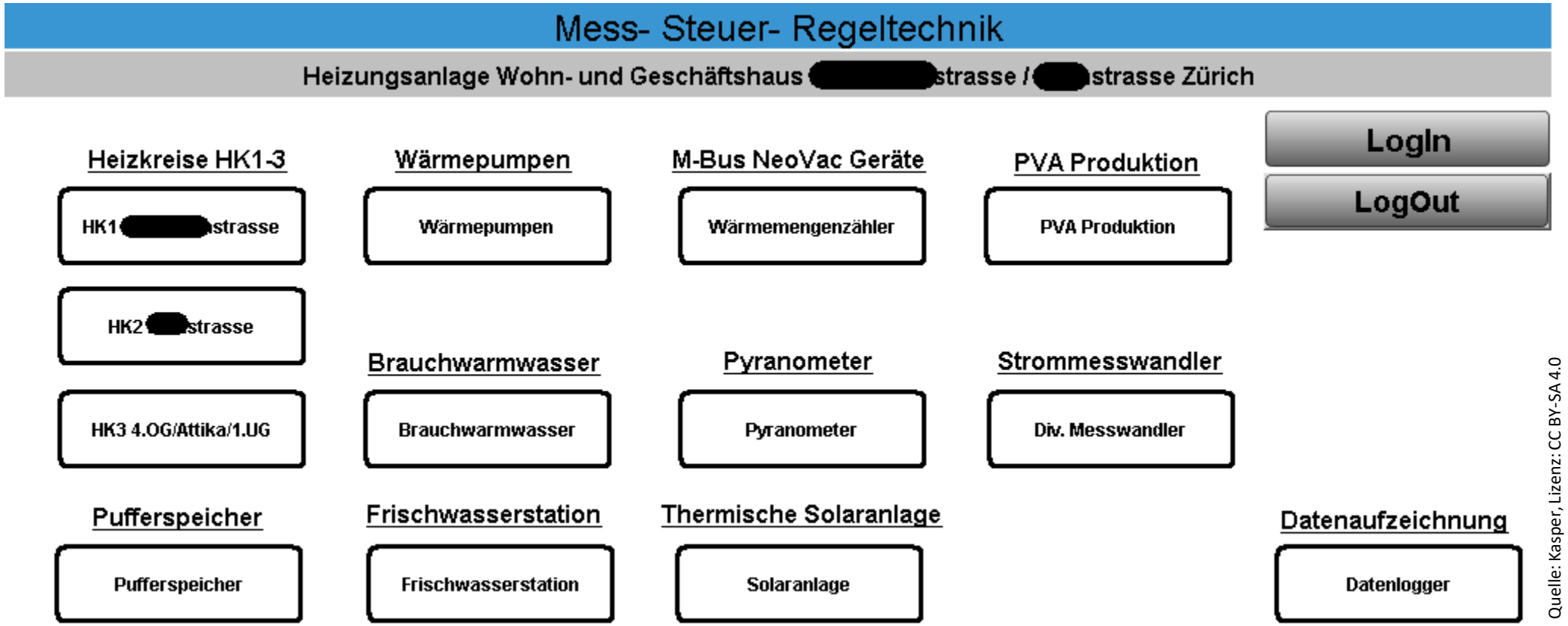
Weltweite Verbreitung angreifbarer Feldbus-Controller, Bsp. Wago 750
(URL: https://www.shodan.io)

Bsp: über Internet angreifbare Hausautomation (1)

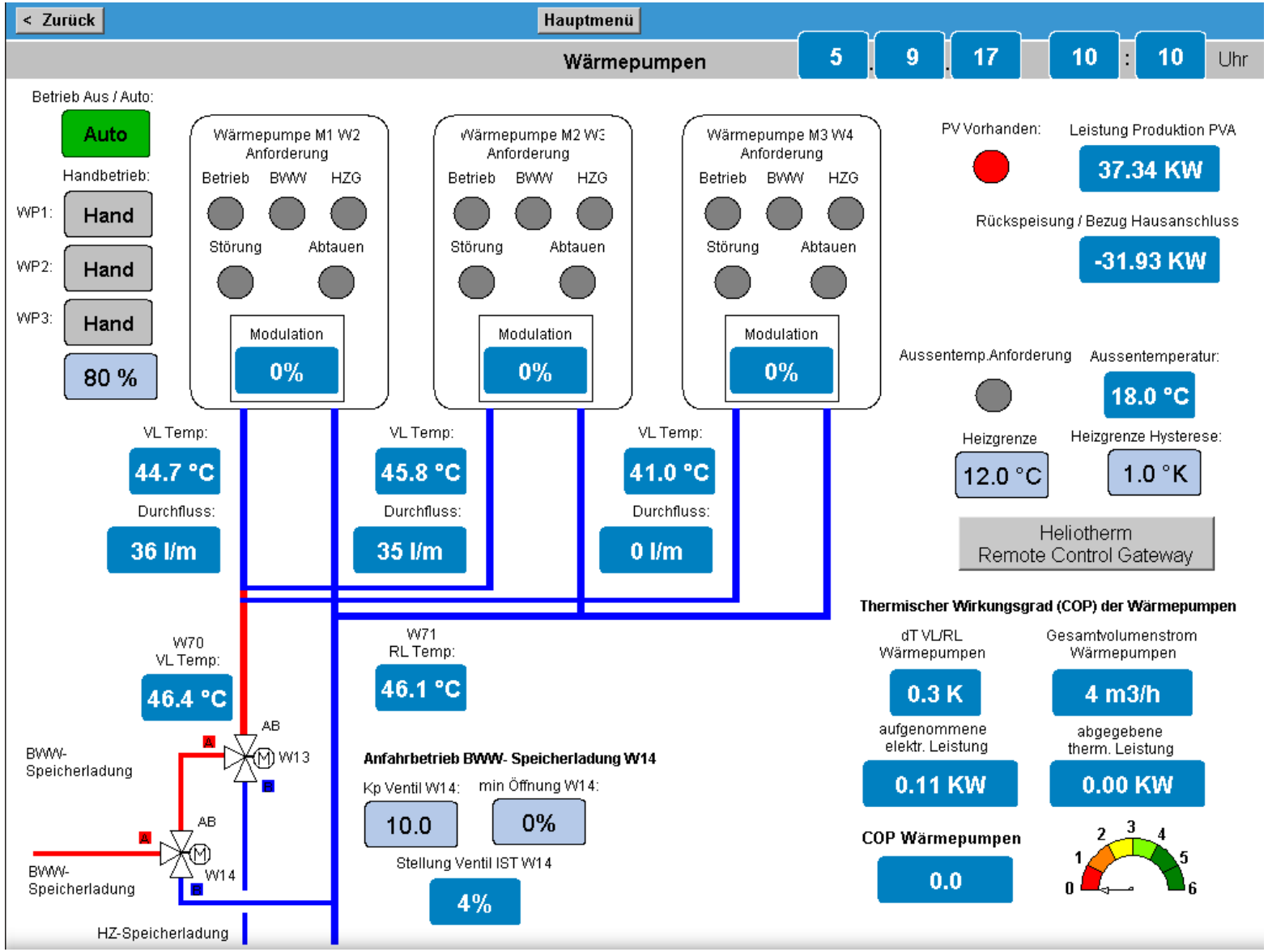


Quelle: Kasper, Lizenz: CC BY-SA 4.0

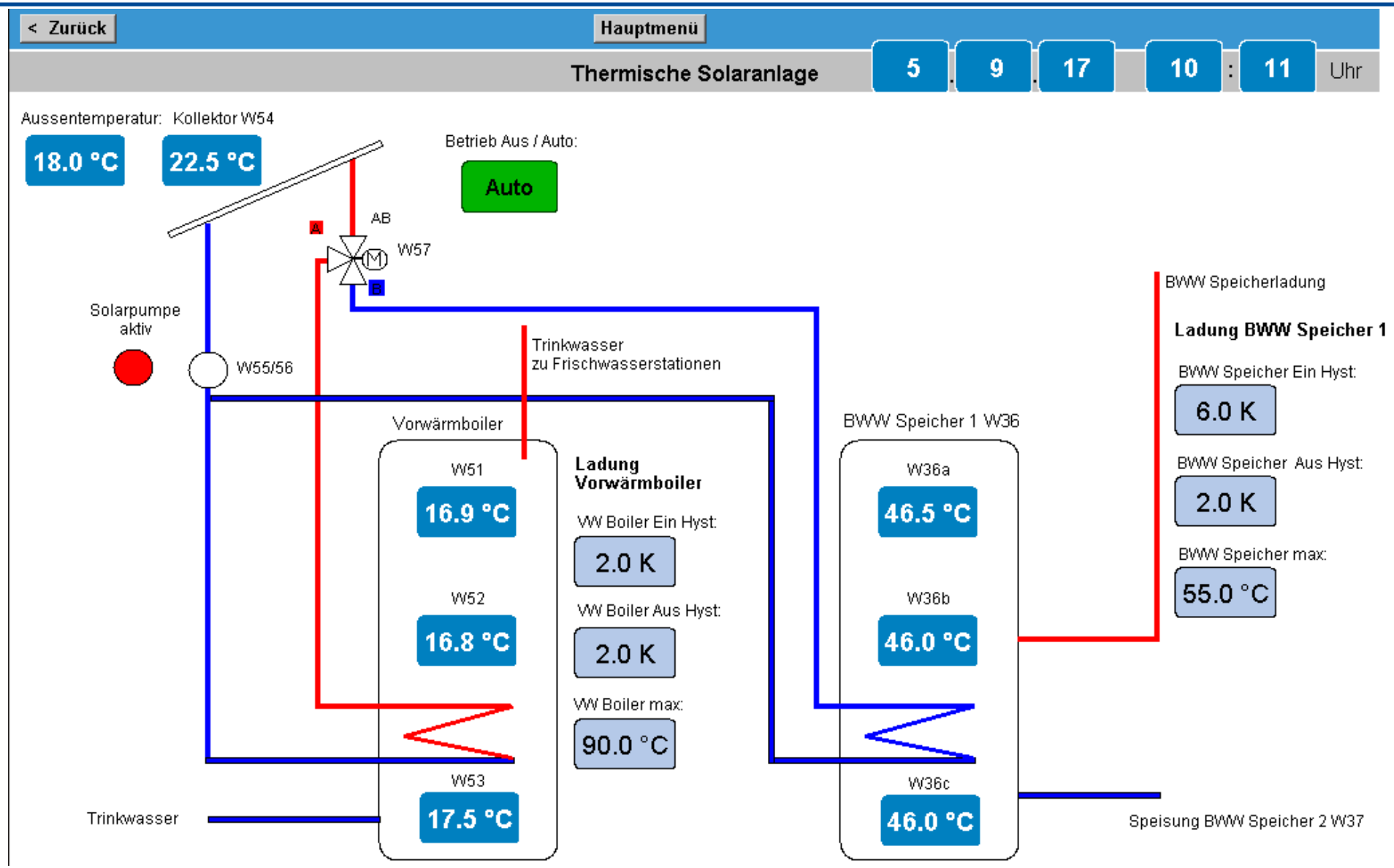
Bsp: über Internet angreifbare Hausautomation (2)



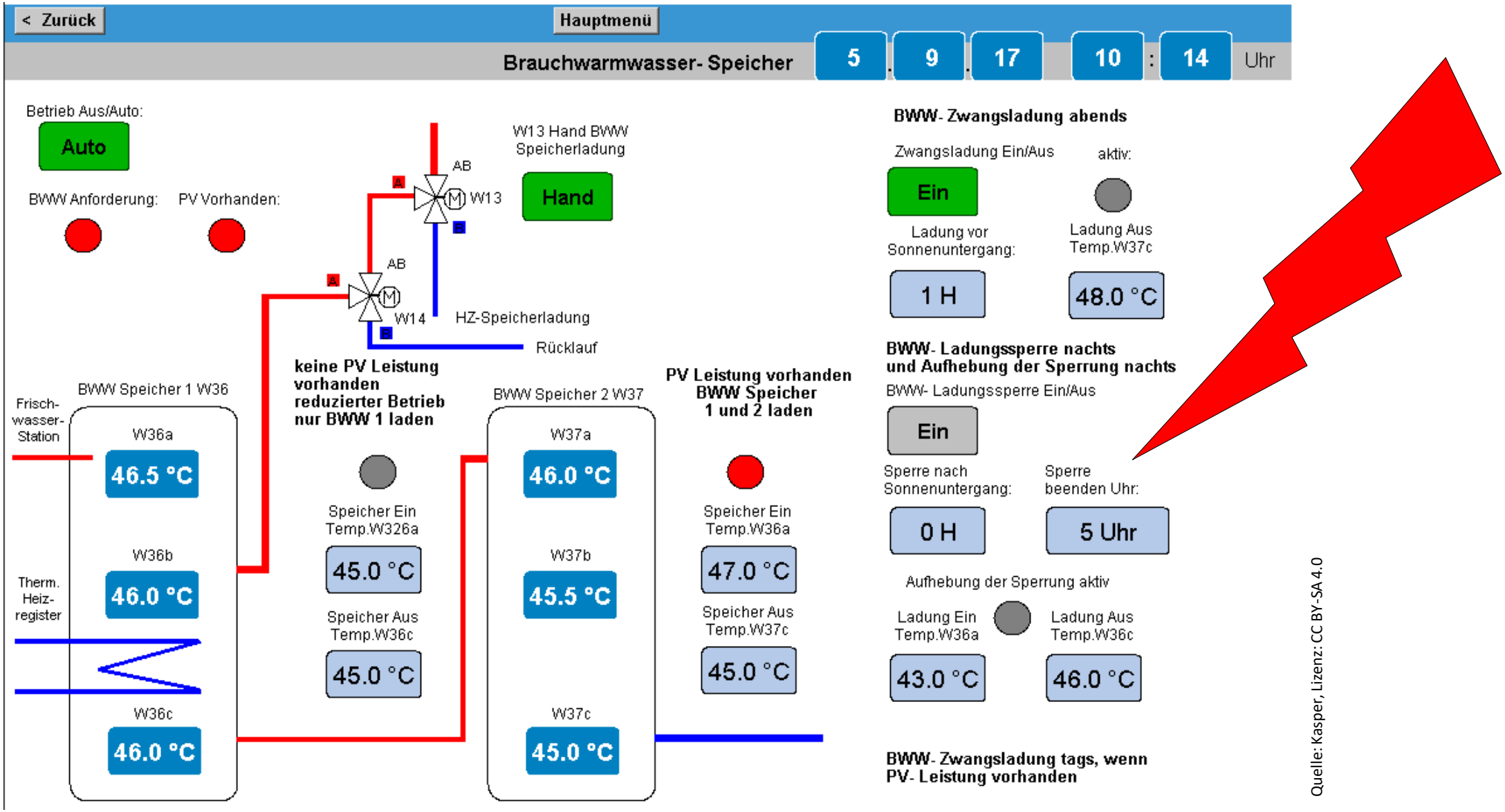
Bsp: über Internet angreifbare Hausautomation (3)



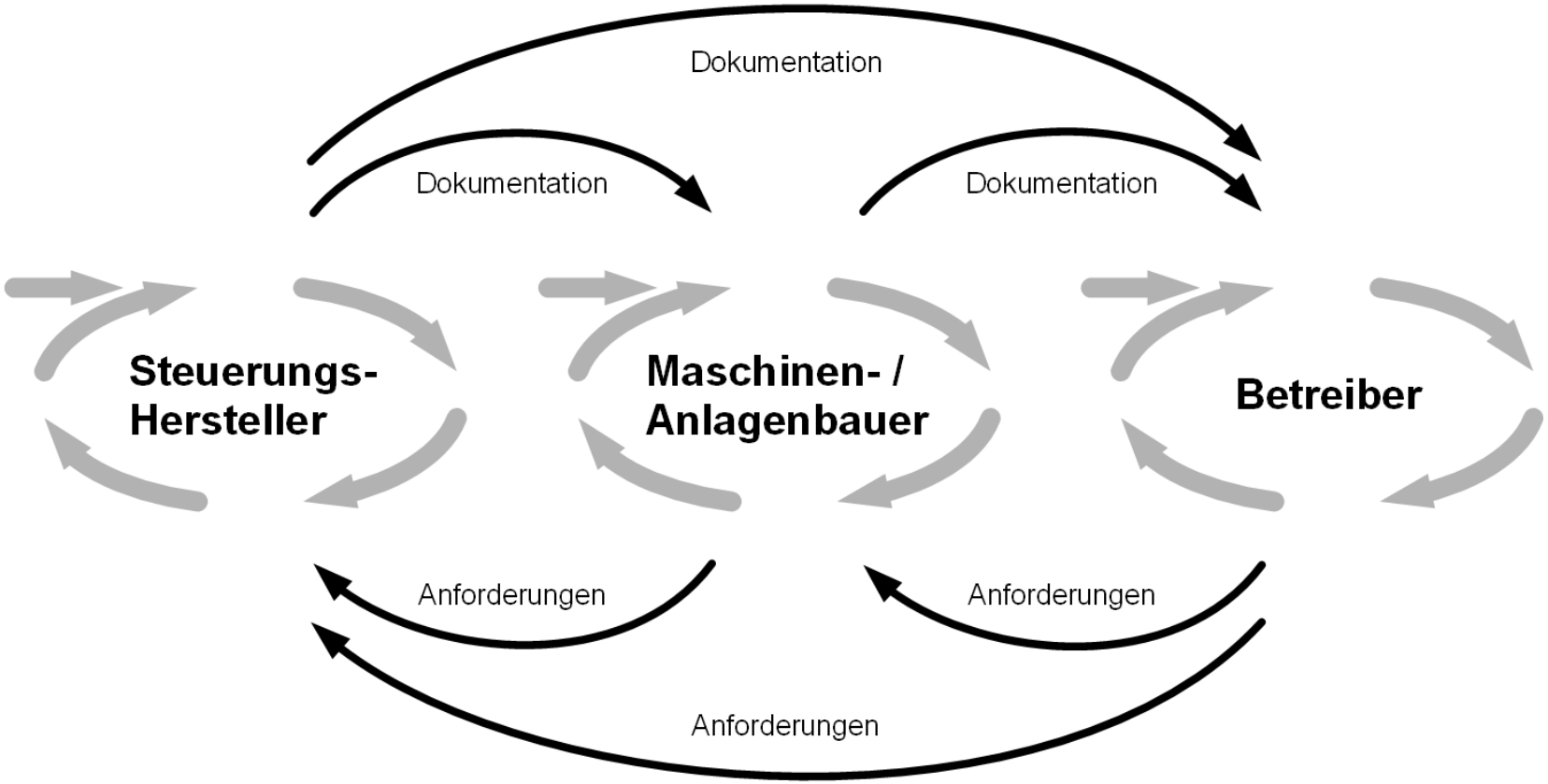
Bsp: über Internet angreifbare Hausautomation (4)



Bsp: über Internet angreifbare Hausautomation (5)

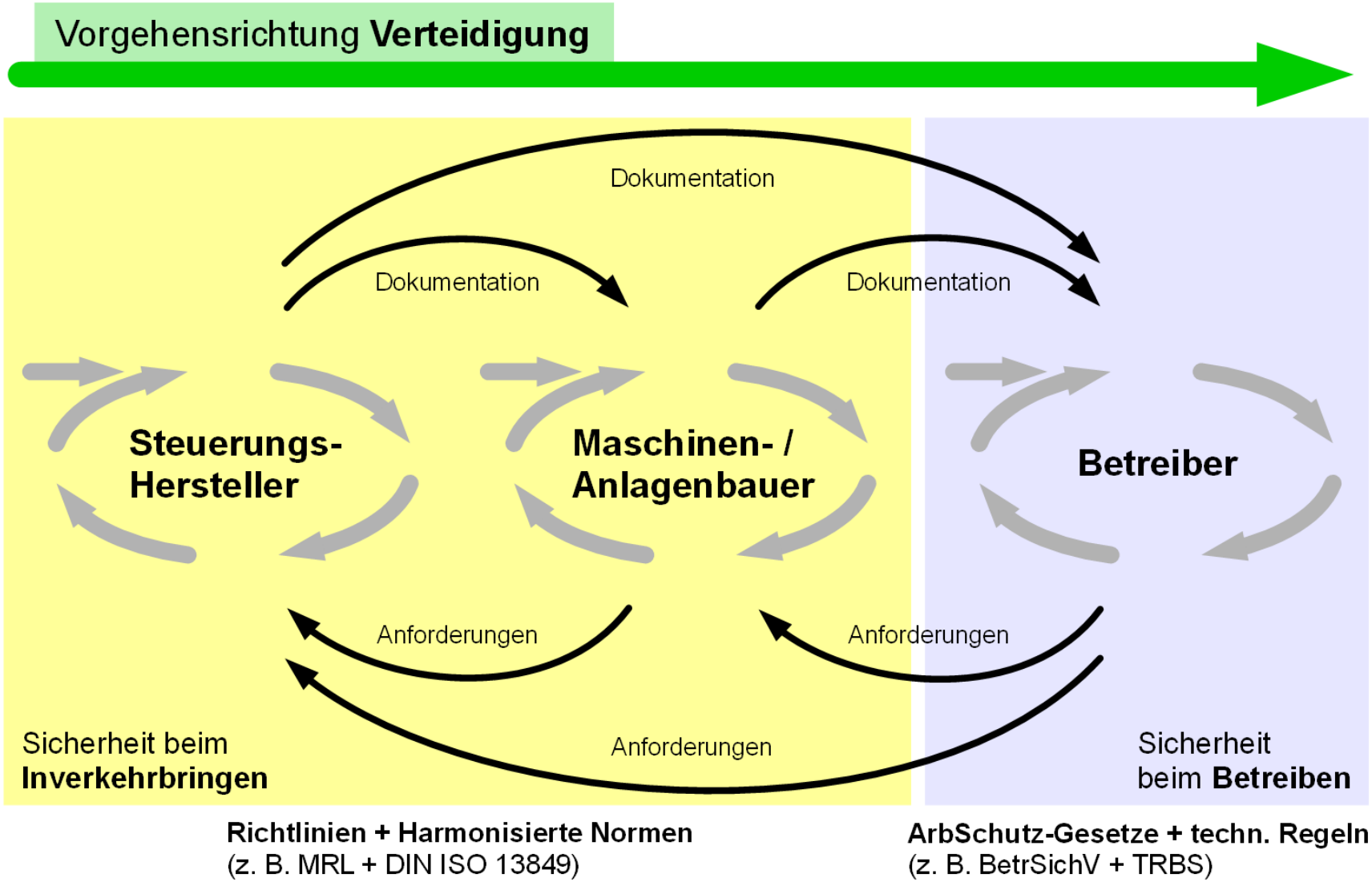


Empfehlung: Rollenbasierte Risikobeurteilung (1)

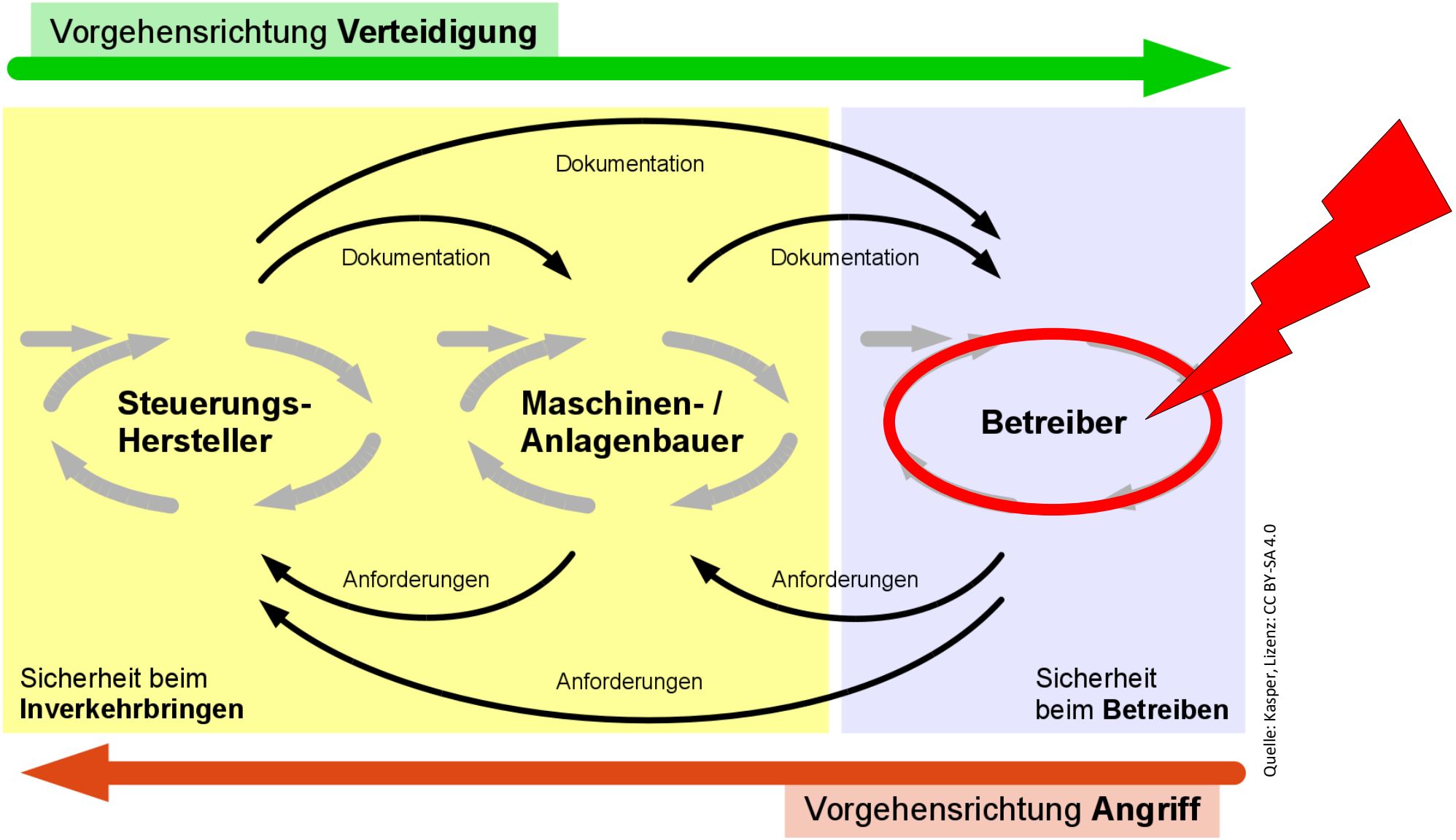


Rollenverteilung bei der Security-Risikobeurteilung (angelehnt an VDI/VDE 2182-1:2011-01)

Empfehlung: Rollenbasierte Risikobeurteilung (2)



Empfehlung: Rollenbasierte Risikobeurteilung (3)



Zusammenfassung

Anlass:

- Hoher Vernetzungsgrad von Geräten / Maschinen untereinander
- Etliche Funktionen setzen Internetzugang voraus (z.B. Ferndiagnose, Fernzugriff, Updates, Schaltlogik)

Folgen:

- Geräte / Maschinen werden oft zu leichtfertig und oft ohne notwendige u. angemessene Security-Schutzmaßnahmen ins Internet gebracht
- Technisch leichter Zugriff auf Geräte / Maschinen sowie angrenzende Firmennetzwerke möglich
- Unsichtbare Lebensgefahr für Mitarbeiter (+ wirtschaftlicher Schaden für Unternehmen)

Maßnahmen (Auswahl)**:**

- Grundlegende Fragestellungen: Benötigt Gerät / Maschine zwingend Internetzugriff? Wenn ja: für welche Funktionen + wie lange?; Alternativen möglich?
- Rollenbasierte Risiko- bzw. Gefährdungsbeurteilung (z. B. Betreiber stellt klare sicherheitstechnische Anforderungen + Hersteller liefert detaillierte Dokumentation und bietet fachliche Unterstützung)
- Asset-Inventarisierung, Überblick Netzwerkstrukturen und -kommunikationspartner, ...

Vielen Dank für Ihre Aufmerksamkeit!

- B. Kasper. *Safety related Security am Beispiel einer angreifbaren Werkzeugmaschine - Analyse der Angriffsvektoren und deren Auswirkungen auf die funktionale Maschinen-Sicherheit*. 2020 DOI: https://doi.org/10.13140/RG.2.2.28172.33929/1
- B. Kasper. 2019. Industrie 4.0: *Technologieentwicklung und sicherheitstechnische Bewertung von Anwendungsszenarien*. 1. Auflage. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin 2019. DOI: https://doi.org/10.21934/baua:bericht20190204
- B. Kasper und S. Voss. *Neue Anforderungen an die Sicherheitsnachweisführung von Maschinen und Anlagen im Kontext von Industrie 4.0*, sicher ist sicher, 09.18, 368-371, 2018 https://www.baua.de/DE/Angebote/Publikationen/Aufsaetze/artikel2093.html

Kontakt:
Dipl.-Ing. Björn Kasper
Berufsgenossenschaft Energie Textil Elektro Medienerzeugnisse (BG ETEM), Prüflabor Dresden
kasper.bjoern@bgetem.de