BG ETEM
Energie Textil Elektro
Medienerzeugnisse

Herausforderung Digitalisierung: Safety related security

Dipl.-Ing. **Björn Kasper**

Berufsgenossenschaft Energie Textil Elektro Medienerzeugnisse (BG ETEM)

Prüflabor Dresden

07. September 2021

Fachtagung „Digitalisierung der Arbeitswelt“, DGUV Congress Dresden

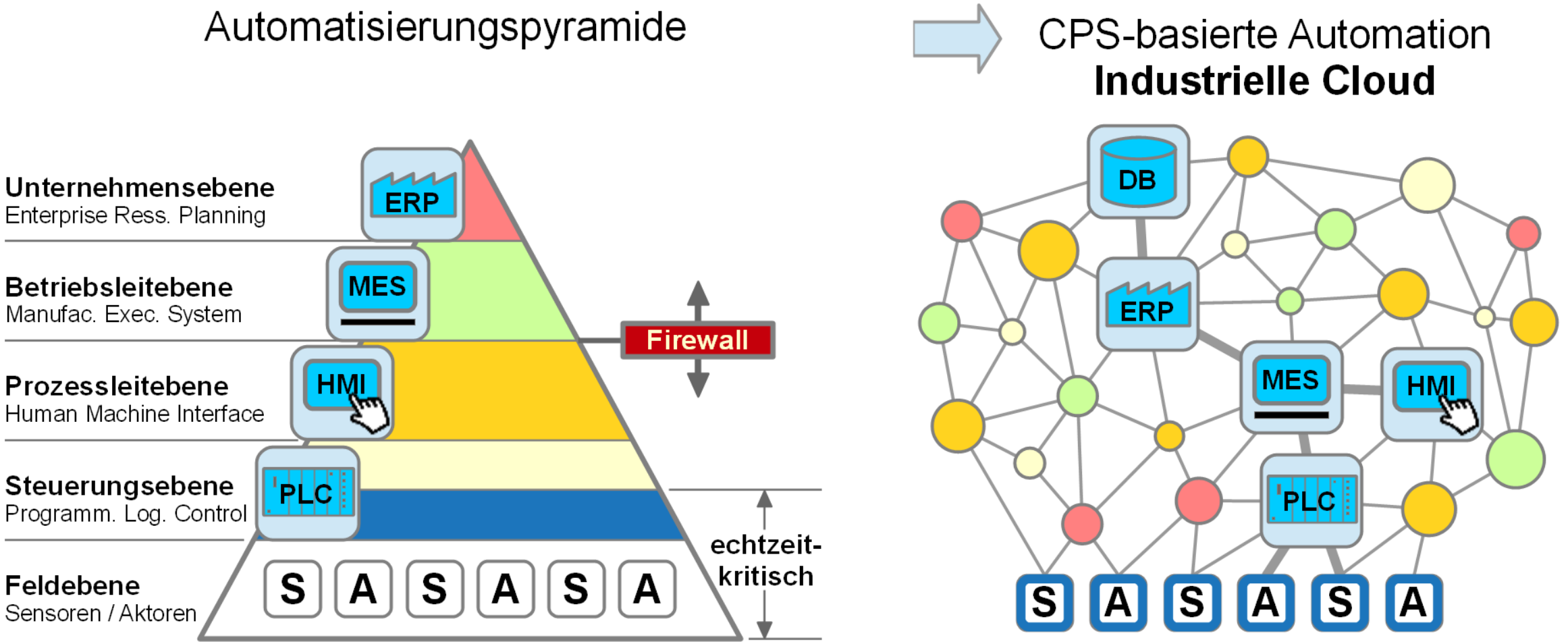
Digitalisierung: Durchgängig vernetzte Maschinen & Anlagen

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

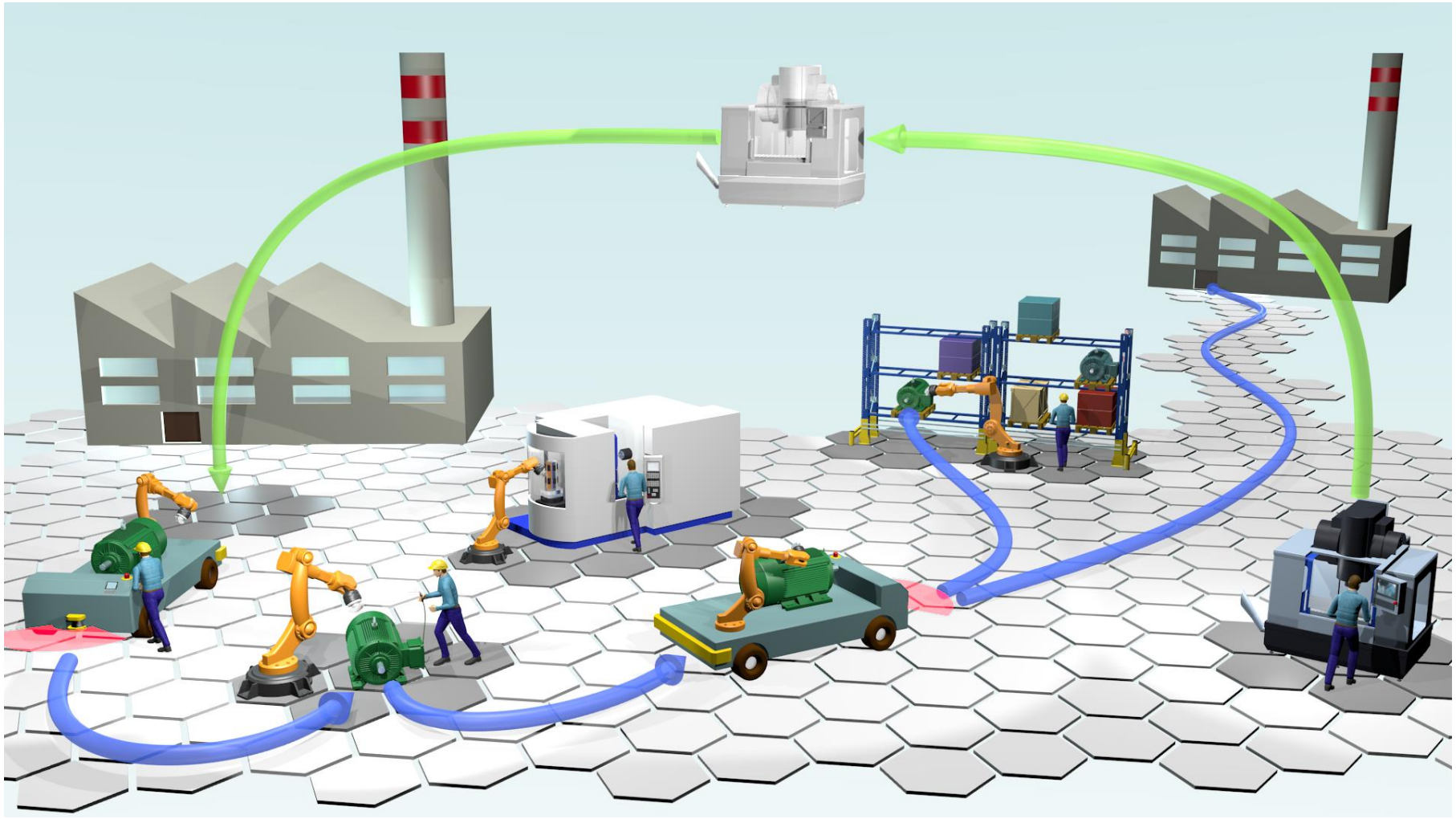
⇒ Komplexität ⇑ + Transparenz & Nachvollziehbarkeit für Beschäftigte ⇓

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



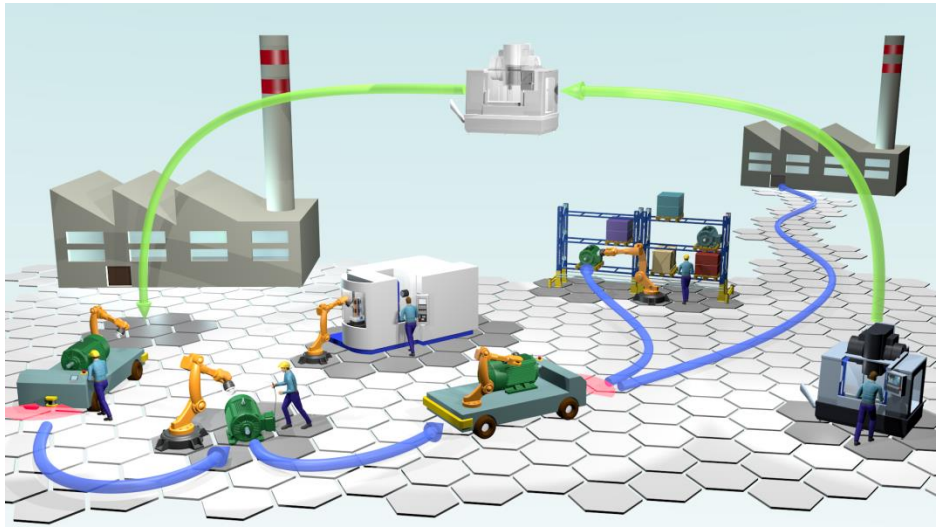
Blau: **Modularisierung** der Produktion durch z. B. vernetzte Fertigungsinseln
Grün: **Wandelbarkeit** der Produktion: Produkt steuert Fertigungsprozess

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

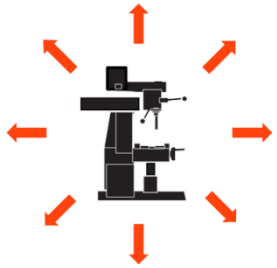
Sicherheitstechnik vernetzter Maschinen & Anlagen

Sicherheitstechnik:

- Technische & organisatorische Maßnahmen zur Erreichung der Sicherheit

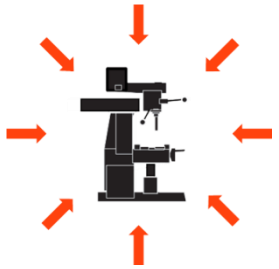
Safety (= Produkt- / Betriebssicherheit):

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



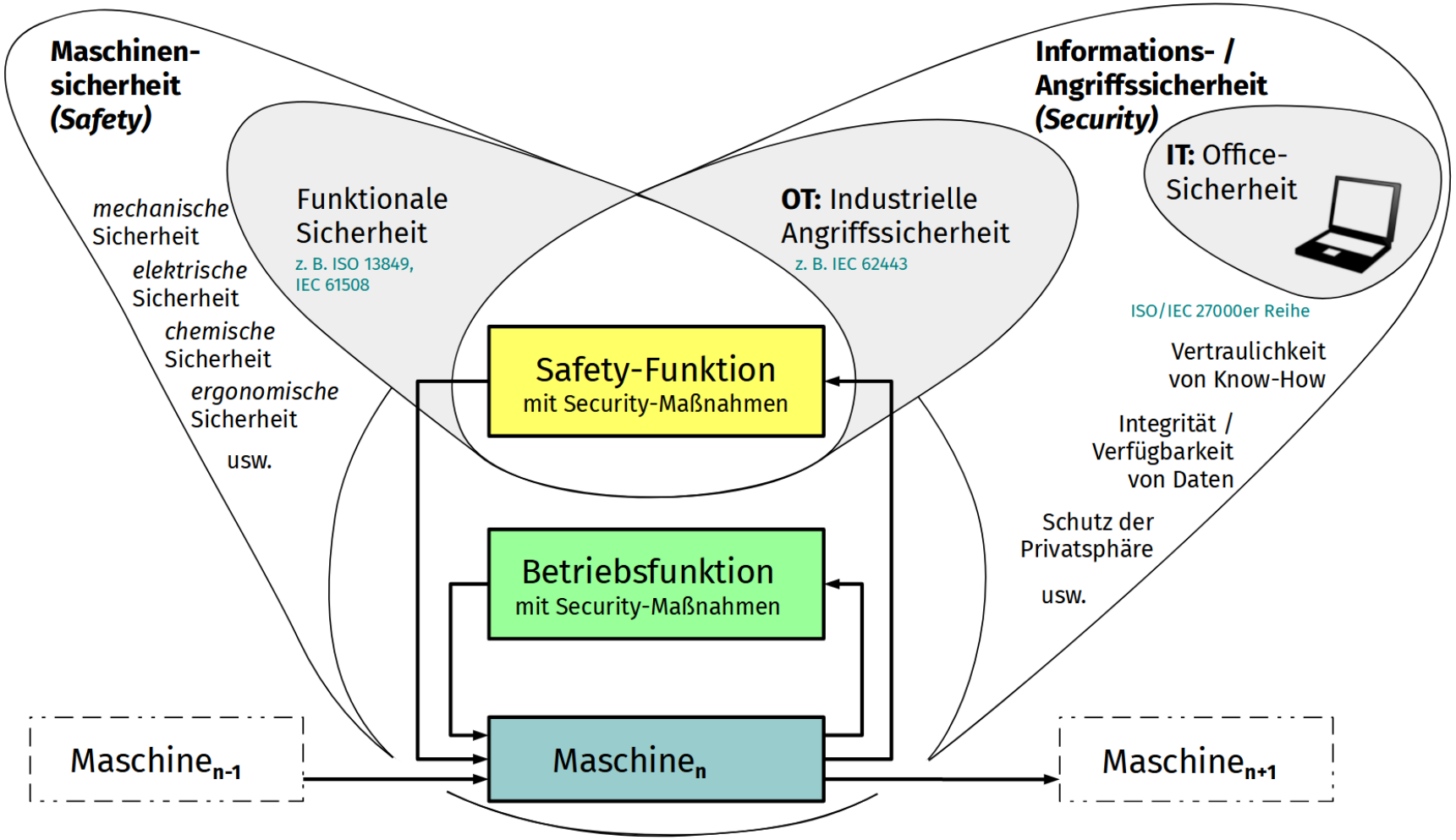
Industrial Security (= Angriffs- / Manipulationssicherheit):

- 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



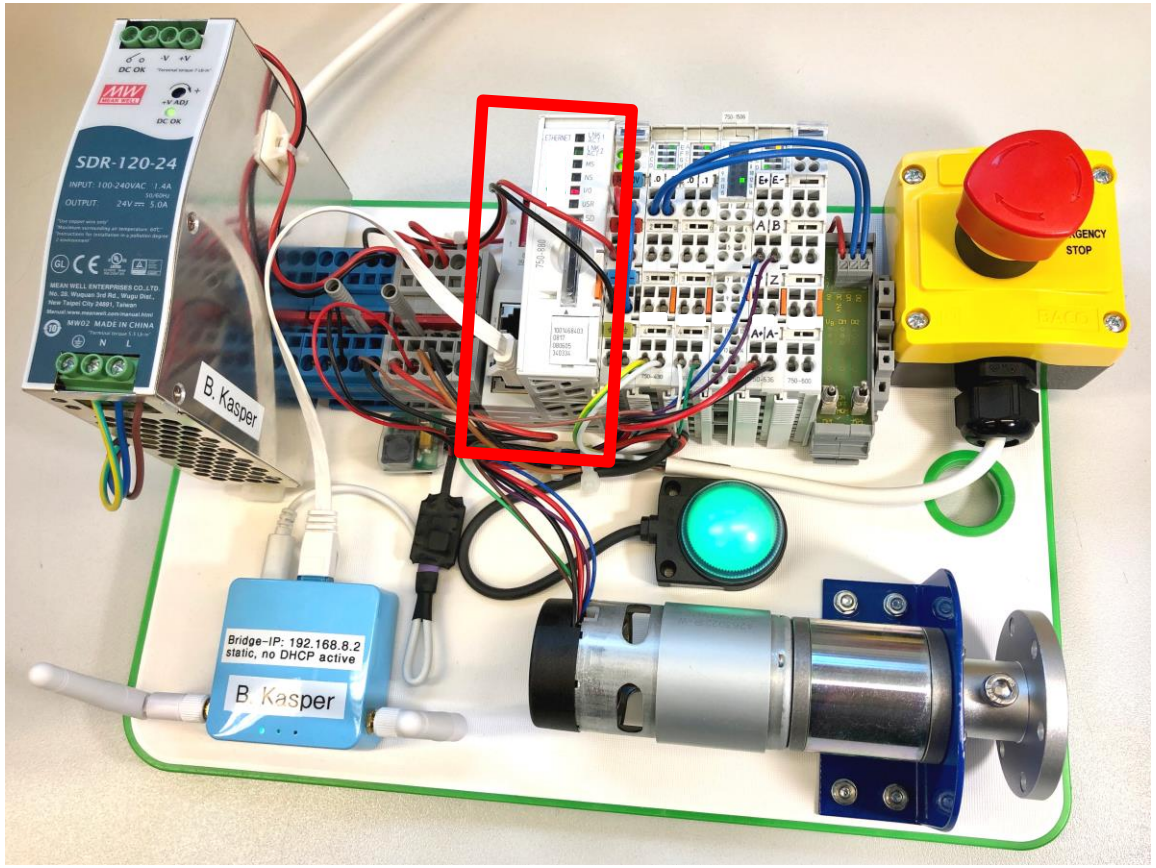
Quelle: Kasper, Lizenz: CC BY-SA 4.0

Betriebs- und Sicherheitsfunktionen von Maschinen und Anlagen

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

Beispielhaftes Prüfobjekt (1)

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



Quelle: Kasper, Lizenz: CC BY-SA 4.0

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

- im Auslieferungszustand **keine** Sec.-Maßnahmen aktiv!
- HTTP, FTP, SNMP: keine Verschlüsselung
- schwache Authentifizierung (login "admin" + password „feldbus“)
- 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 des Motor-Treibers
- etc.

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

Beispielhaftes Prüfobjekt (2)

7.5.4 MODBUS-Konfigurationsregister

Über die Konfigurationsregister lassen sich die Eigenschaften er-
mitteln und teilweise verändern.

MODBUS Configuration Register for FC3, FC4, FC6 and FC16

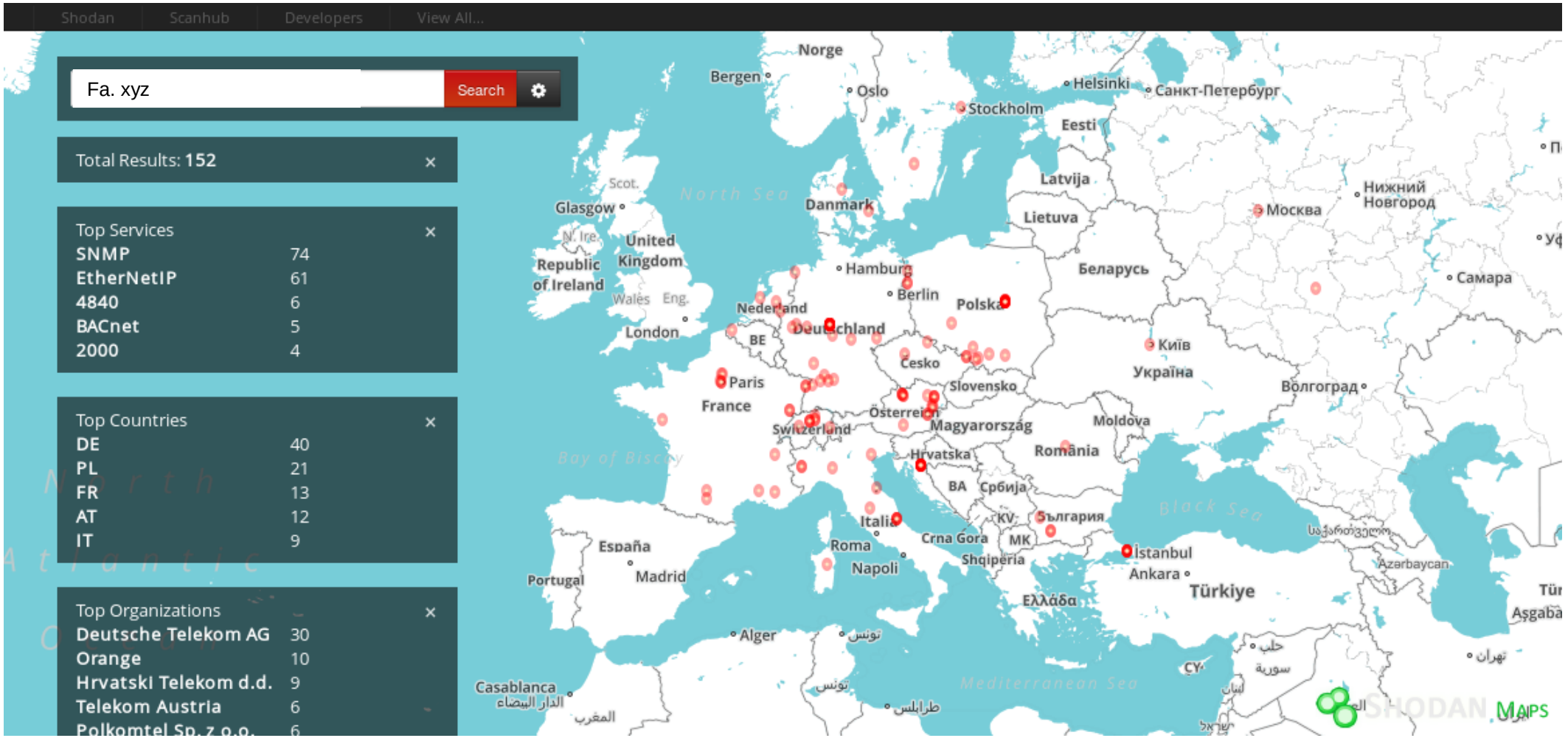
MODBUSAddress [dec]	[hex]	Length [Word]	Access	Description
8256	0x2040	1	W	Software Reset (write 0x55AA or 0xAA55)
8257	0x2041	1	W	Format Flash-
8258	0x2042	1	W	Extract file system
8259	0x2043	1	W	Werkseinstellungen

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 " xyz › Ethernet Settings" => "Dateisystem zurücksetzen"

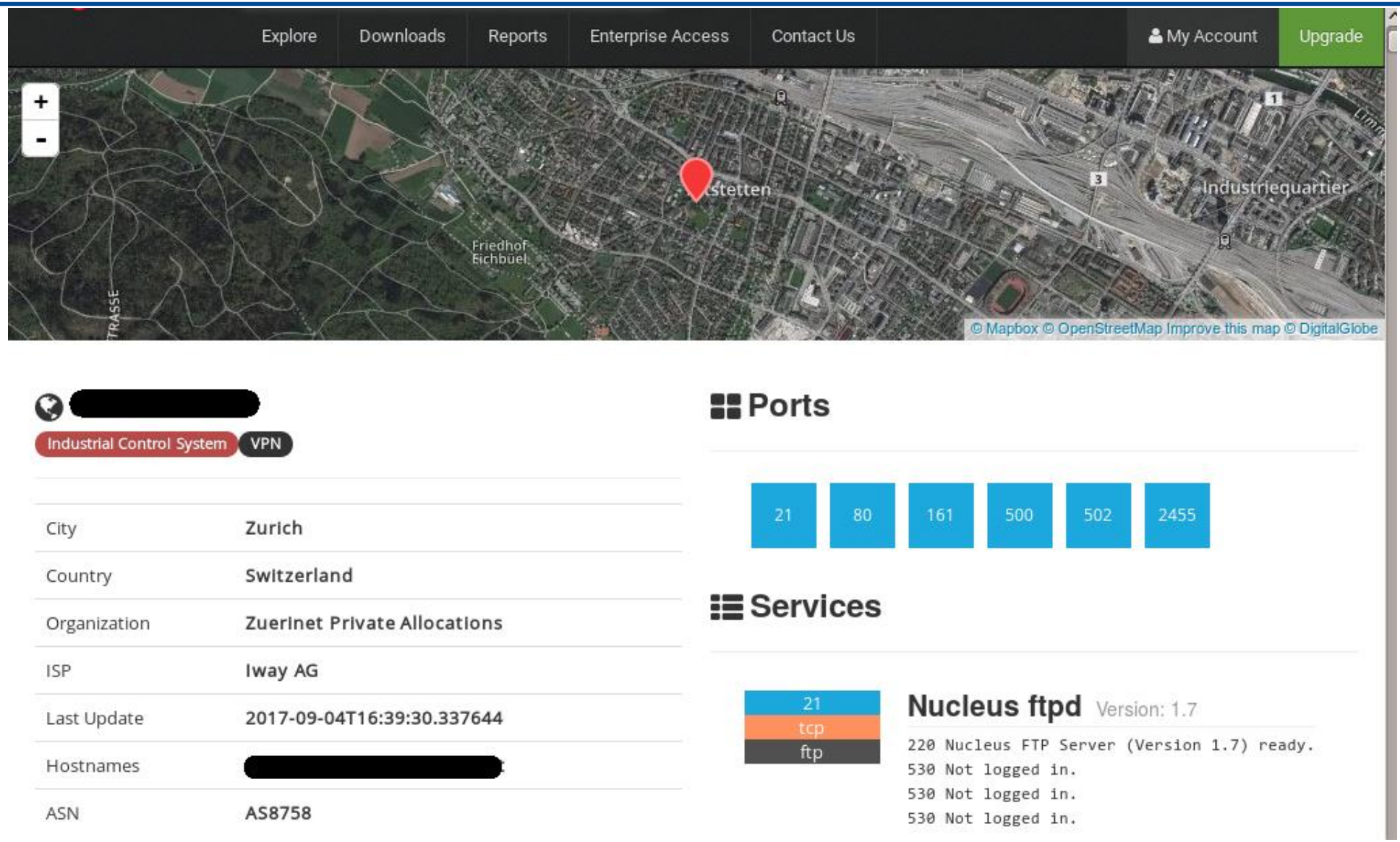
Relevanz-Überprüfung



Quelle: Kasper, Lizenz: CC BY-SA 4.0

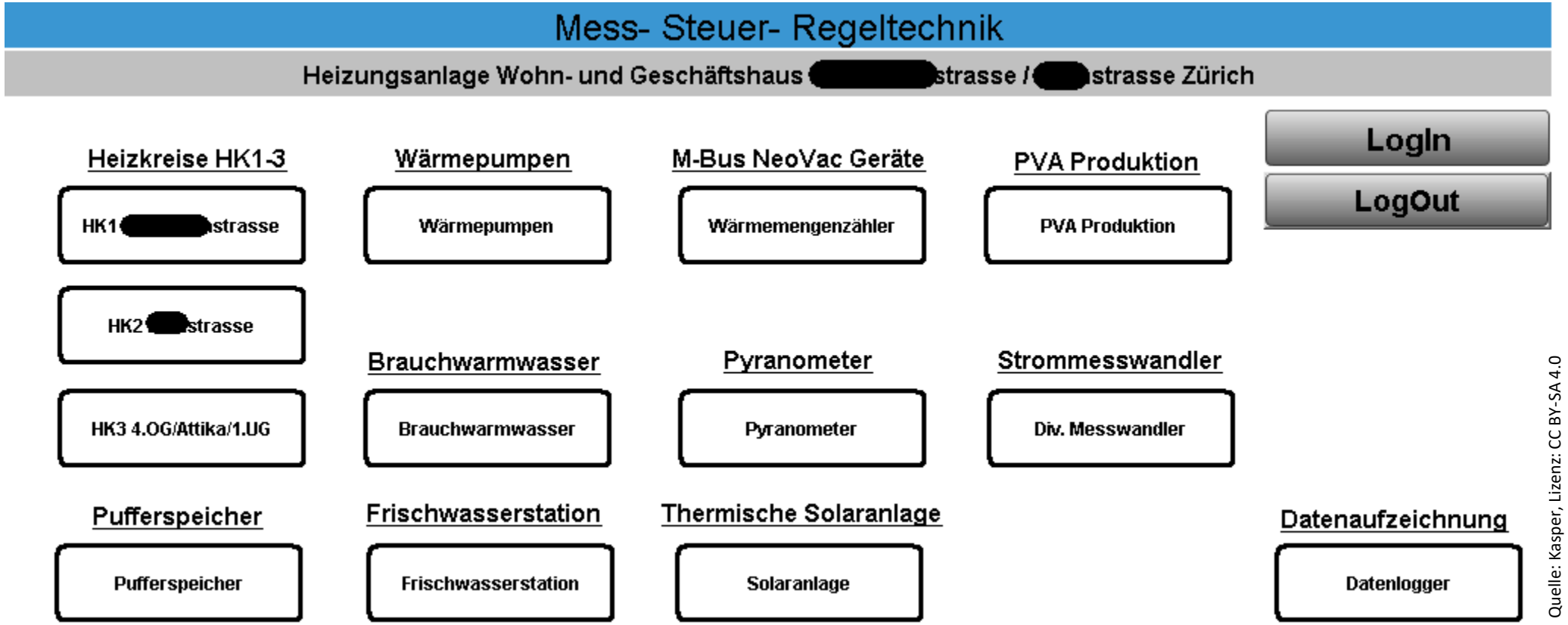
Weltweite Verbreitung angreifbarer Feldbus-Controller, Bsp. xyz
(URL: https://www.shodan.io)

Bsp: über Internet angreifbare Hausautomation (1)

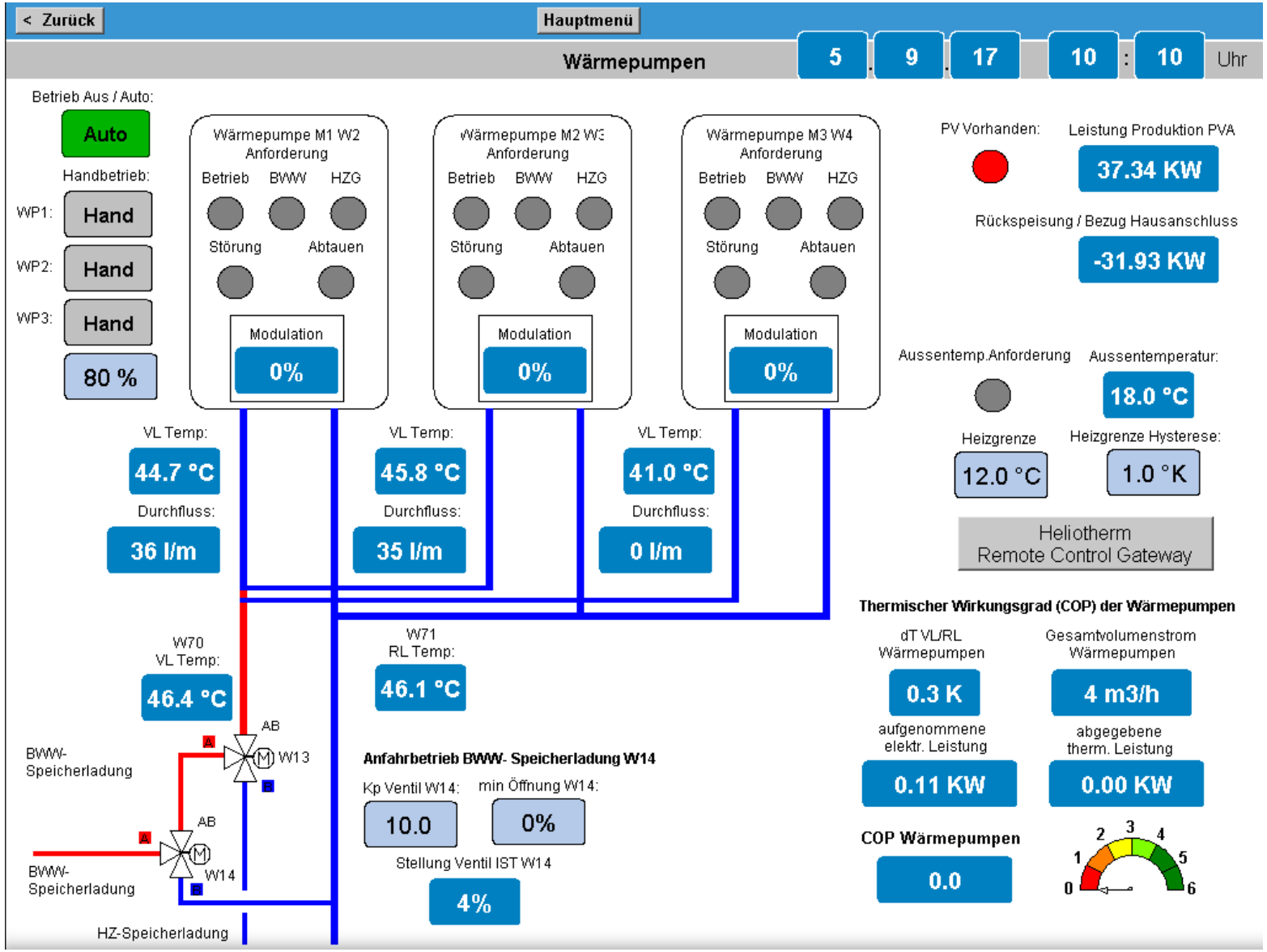


Quelle: Kasper, Lizenz: CC BY-SA 4.0

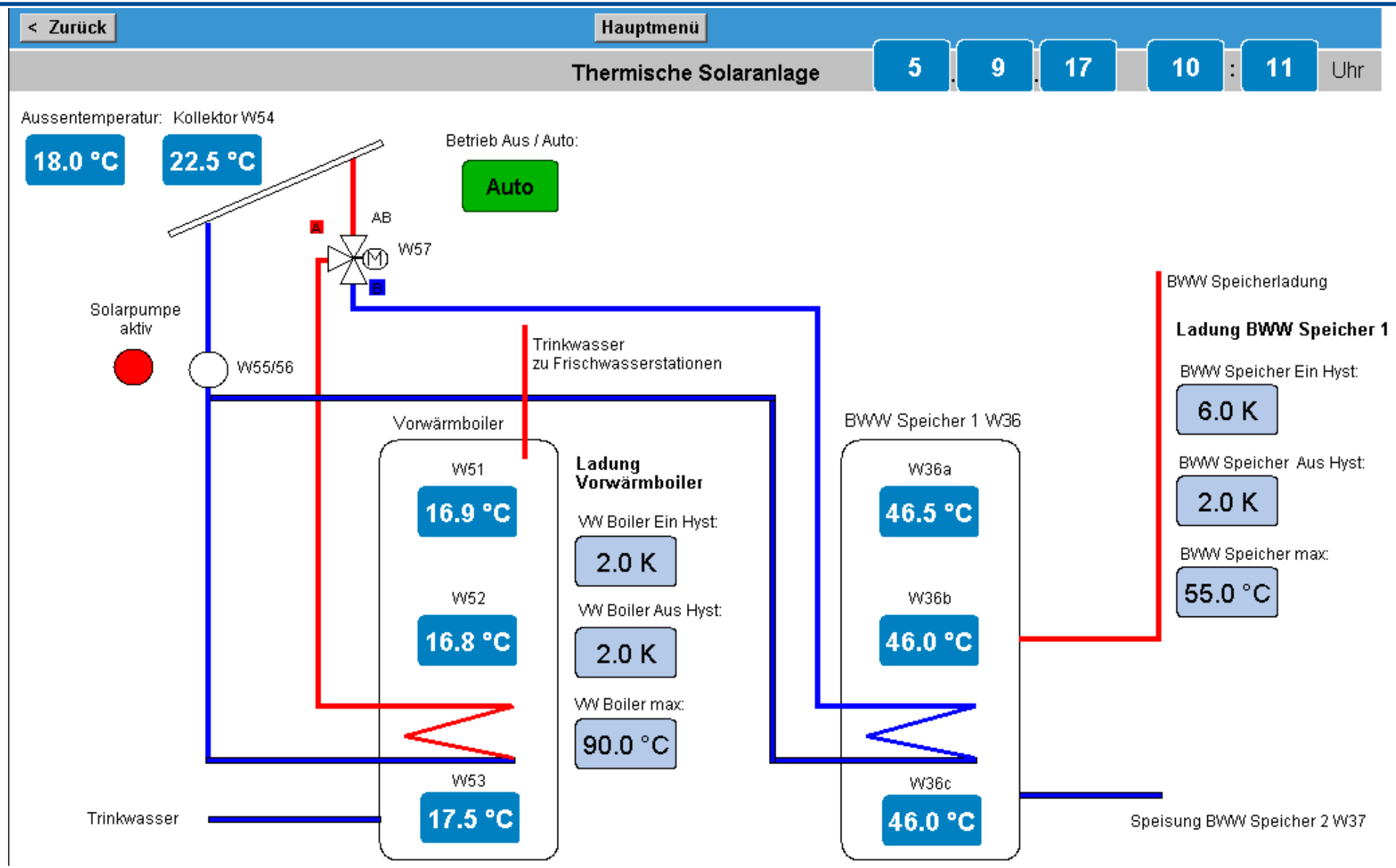
Bsp: über Internet angreifbare Hausautomation (2)



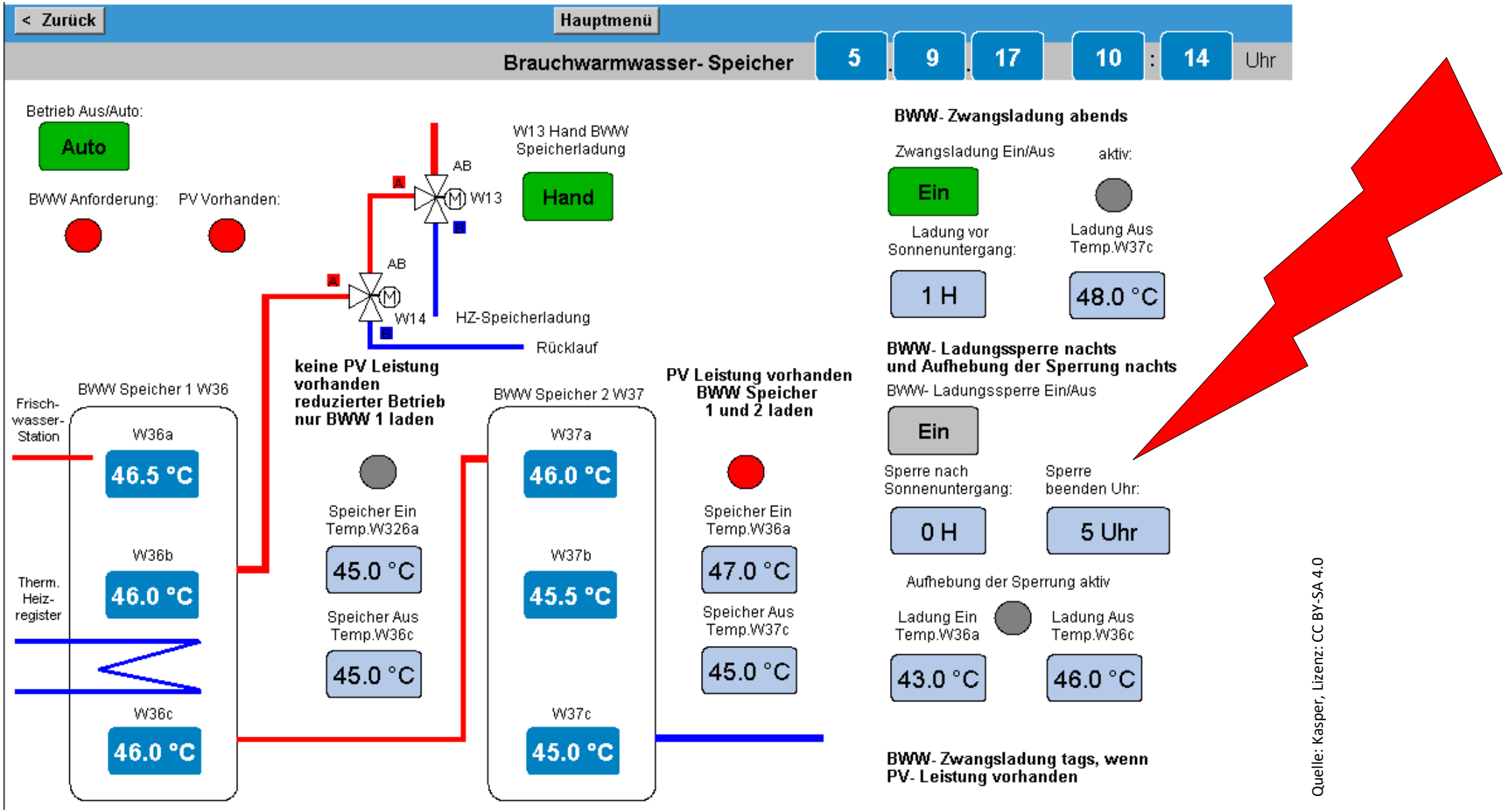
Bsp: über Internet angreifbare Hausautomation (3)



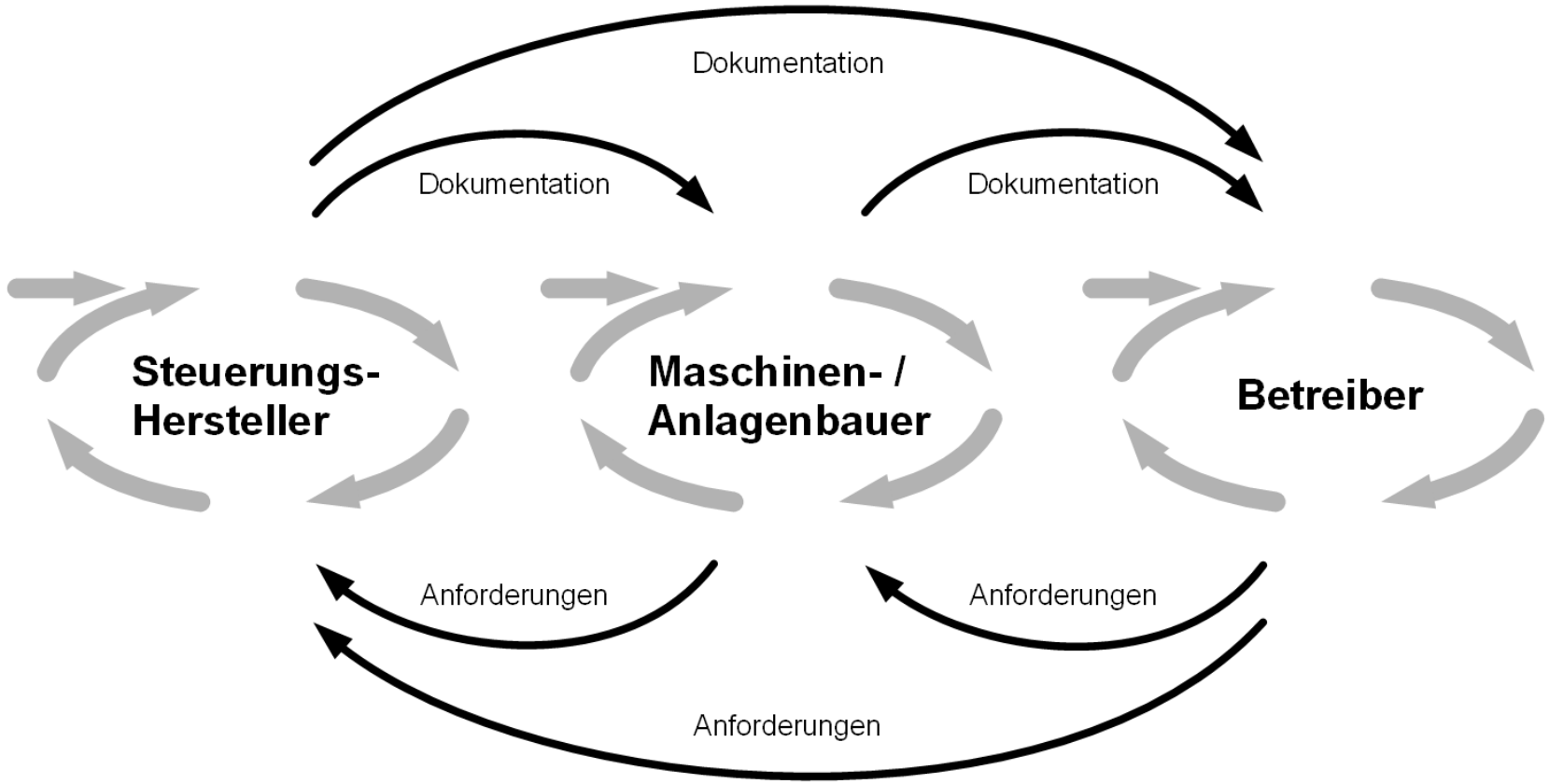
Bsp: über Internet angreifbare Hausautomation (4)



Bsp: über Internet angreifbare Hausautomation (5)

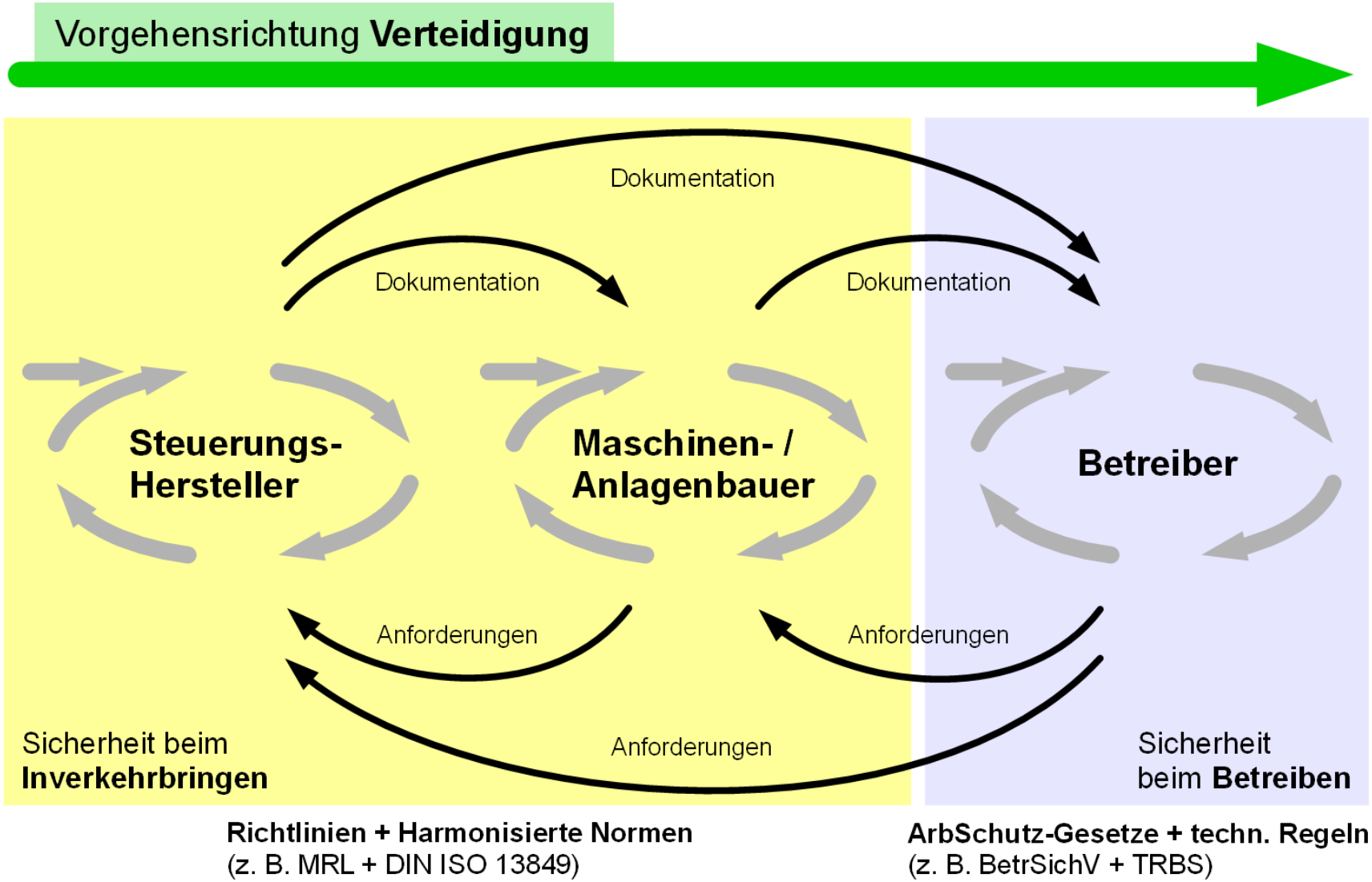


Vorschlag: Rollenbasierte Risikobeurteilung (1)

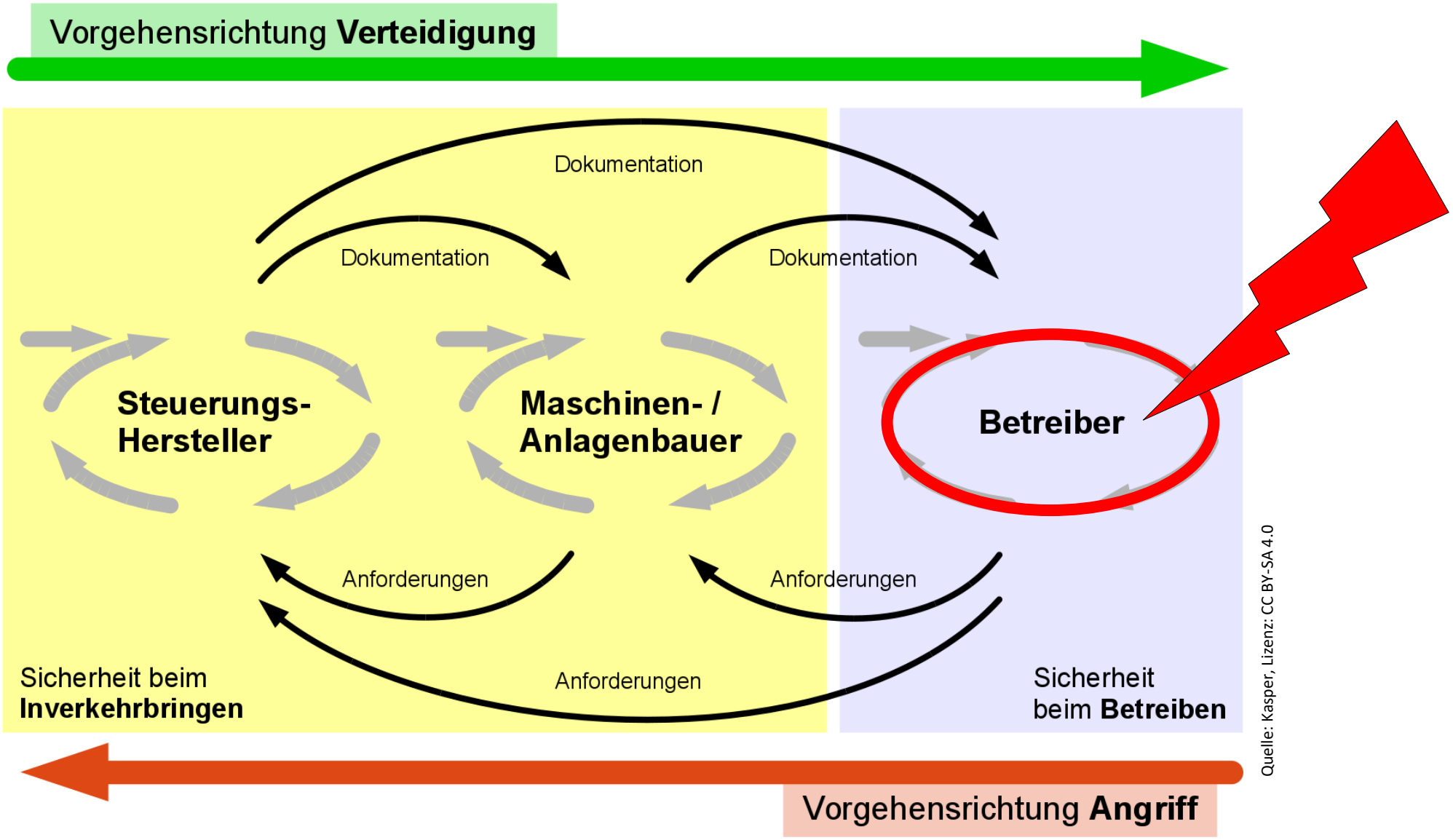


Rollenverteilung bei der Security-Risikobeurteilung (angelehnt an VDI/VDE 2182-1:2011-01)

Vorschlag: Rollenbasierte Risikobeurteilung (2)



Vorschlag: Rollenbasierte Risikobeurteilung (3)



Zusammenfassung

Anlass:

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

Folgen:

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

Maßnahmen (Auswahl; siehe u. a. IEC 62443)**:**

- Fachkompetenz (extern) einholen, Asset-Inventarisierung + -Management, Überblick über vorhandene Netzwerkstrukturen und -kommunikationspartner ...
- Grundlegende Fragestellungen: Benötigen Maschinen / Steuerungskomponenten zwingend Internetzugriff? Wenn ja: für welche Funktionen + wie lange (z. B. Ferndiagnose)?
- Rollenbasierte Risiko- bzw. Gefährdungsbeurteilung (z. B. Betreiber stellt klare sicherheitstechnische Anforderungen + Hersteller liefert detaillierte Dokumentation und bietet fachliche Unterstützung)

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
- 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