Weiterentwicklung sicherheitstechnischer Analyse- und Bewertungsmethoden für die Industrie 4.0

Dipl.-Ing. Björn Kasper
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, FG 2.4
Arbeitstätten, Maschinen- und Betriebssicherheit, Dresden

23. März 2017

Agenda

- **Kurzüberblick Industrie 4.0**
  - Paradigmen
  - Komponenten / Technologien
  - Modelle
- **Sicherheitstechnische Aspekte**
  - Sicherheitstechnische Methoden heute
  - Weiterentwicklung für morgen?
- **Ausblick**
- **Fragen & Diskussion**

I4.0: Zentrale Paradigmen (1)

- Cyber-physisches Produktionssystem (CPPS)
  - Verknüpfung realer (physischer) Objekte und Prozesse in industrieller Produktion
  - starke (globale) Vernetzung untereinander[1]

- Dezentrale Intelligenz / Steuerung
  - Modularisierung und Dezentralisierung von Steuerungs- und Software-Komponenten
  - auftragsbezogene **Rekombination** der Module zur Laufzeit der Maschine bzw. Anlage
  - Ziel: **Individualisierung** der Produktion $\Rightarrow$ **Prosumer**
  - klassische **Automatisierungspyramide** $\Rightarrow$ Dezentralisierung auf Basis CPS[2] $\Rightarrow$ **industrielle Clouds**

[1] vgl. Geisberger und Broy 2012, zitiert in VDI / VDE 2013
[2] Cyber-physische Systeme

I4.0: Zentrale Paradigmen (2)

- Vertikale und horizontale Integration
  - *vertikale Integration:* Kommunikation zwischen Leitstandebene und dem Produkt über die Steuerungsebene
  - *horizontale Integration:* Informationsaustausch zwischen Automatisierungsstrukturen der gleichen Ebene (z. B. Maschine-zu-Maschine-Kommunikation)

- Betrachtung gesamter **Produktlebenszyklus**
  - durchgängiges **digitales Engineering** erforderlich
  - Erweiterung der Konzepte *virtuelle Fabrik* um die Dimension "Zeit" $\Rightarrow$ *digitale Fabrik*[3]

[3] vgl. D. Siepman, "Industrie 4.0 – Grundlagen und Gesamtzusammenhang", in *Einfuehrung und Umsetzung von Industrie 4.0*. Februar 2016

I4.0: Technologische Basis-Komponenten (1)

- dezentrale Datenerfassung, -Speicherung und -Verarbeitung
  - dezentrale Daten (z. B. Prozessdaten im Feld) dezentral *erfassen*, *speichern* (z. B. in Datenbanken) und verarbeiten (z. B. Prozesssteuerung und -regelung aus der Cloud / Analyse großer, verteilter Datenbestände)
  - eingebettete Systeme werden zu dezentralen Steuerungs- und Regelungskonzepten vernetzt

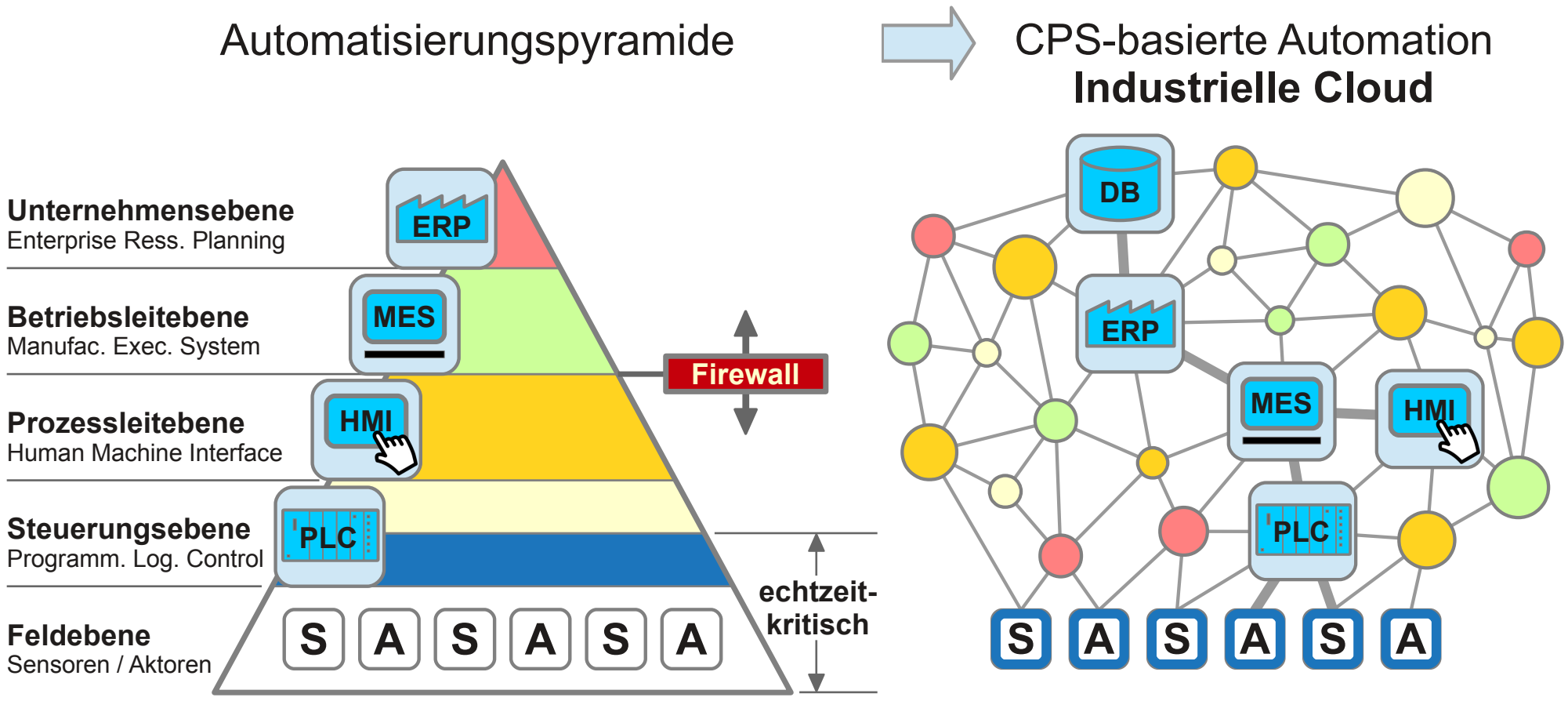
- Maschine-zu-Maschine-Kommunikation (M2M-Kommunikation)
  - heute: *echtzeitfähige* (sicherheitsgerichtete), überwiegend kabelgebundene Feldbusse (bzgl. Medien, Protokolle)
  - zunehmende Nutzung *nicht-echtzeitfähiger* (nicht-sicherheitsgerichteter), *funkbasierter* Kommunikationstechnik als Übertragungsmedium $\Rightarrow$ wie können Anforderungen an Echtzeit, Safety/Security zukünftig erfüllt werden?

I4.0: Technologische Basis-Komponenten (2)

- Mensch-Maschine-Interaktion (MMI)
  - Erkenntnis: “menschenleere Fabrik” bleibt Illusion (vgl. CIM[4])
    $\Rightarrow$ Mensch muss in Fertigung integriert werden!
  - Kollaborationen zw. Mensch & Technik $\Rightarrow$ **Arbeitsschutz**?
  - zur Laufzeit veränderliche Produktions-Prozesse (auftragsbezogene Rekombination von Anlagen)
    $\Rightarrow$ starker Anstieg der Komplexität $\Rightarrow$ Erfassbarkeit / Beherrschbarkeit durch Menschen? $\Rightarrow$ Fehlbedienungen / Fehlentscheidungen wahrscheinlich!
  - unterstützende Technologien: *Virtual Reality (VR)* vs. *Augmented Reality (AR)*

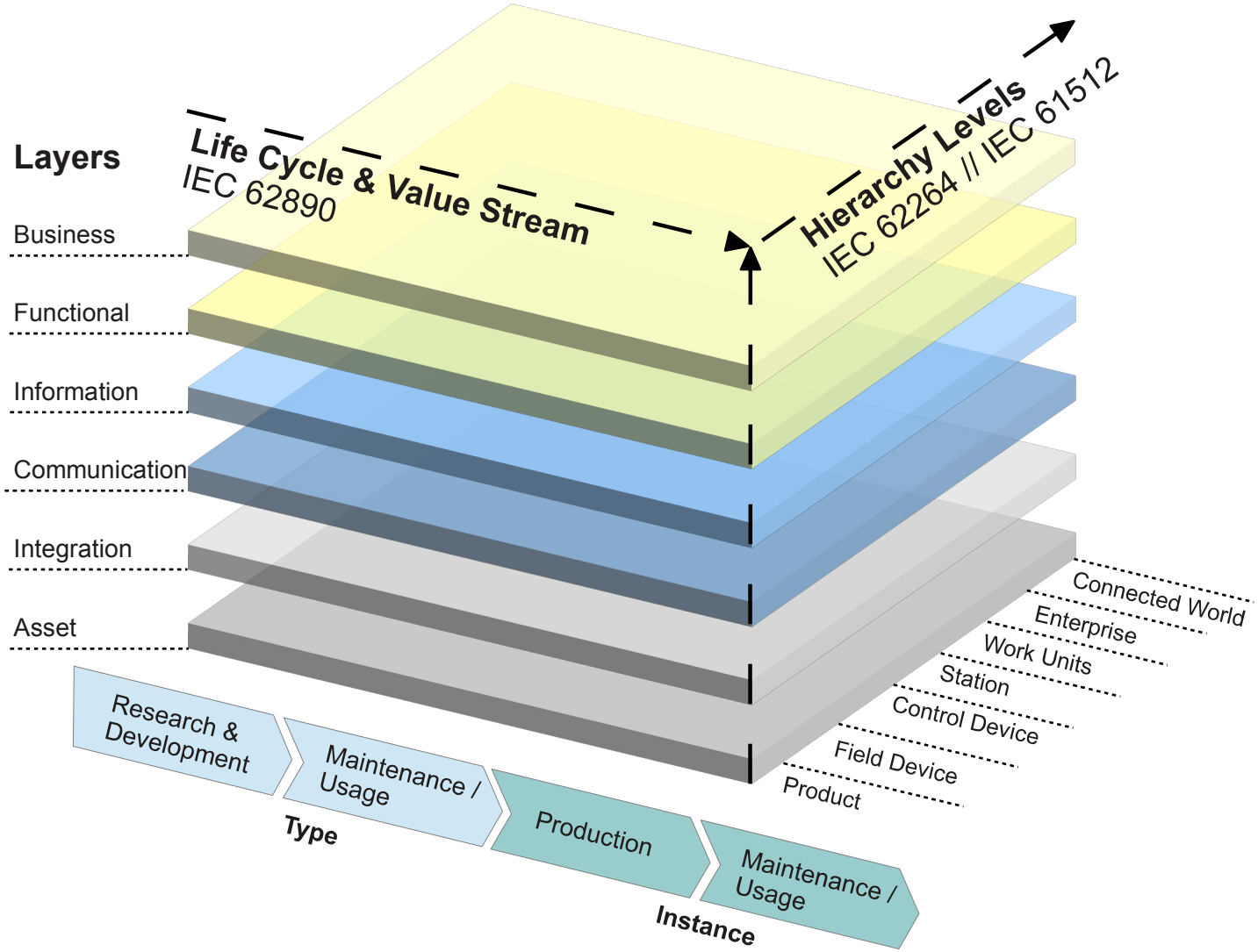
[4] Computer-integrated manufacturing

I4.0: Modell-Weiterentwicklung – CPS-Cloud (1)



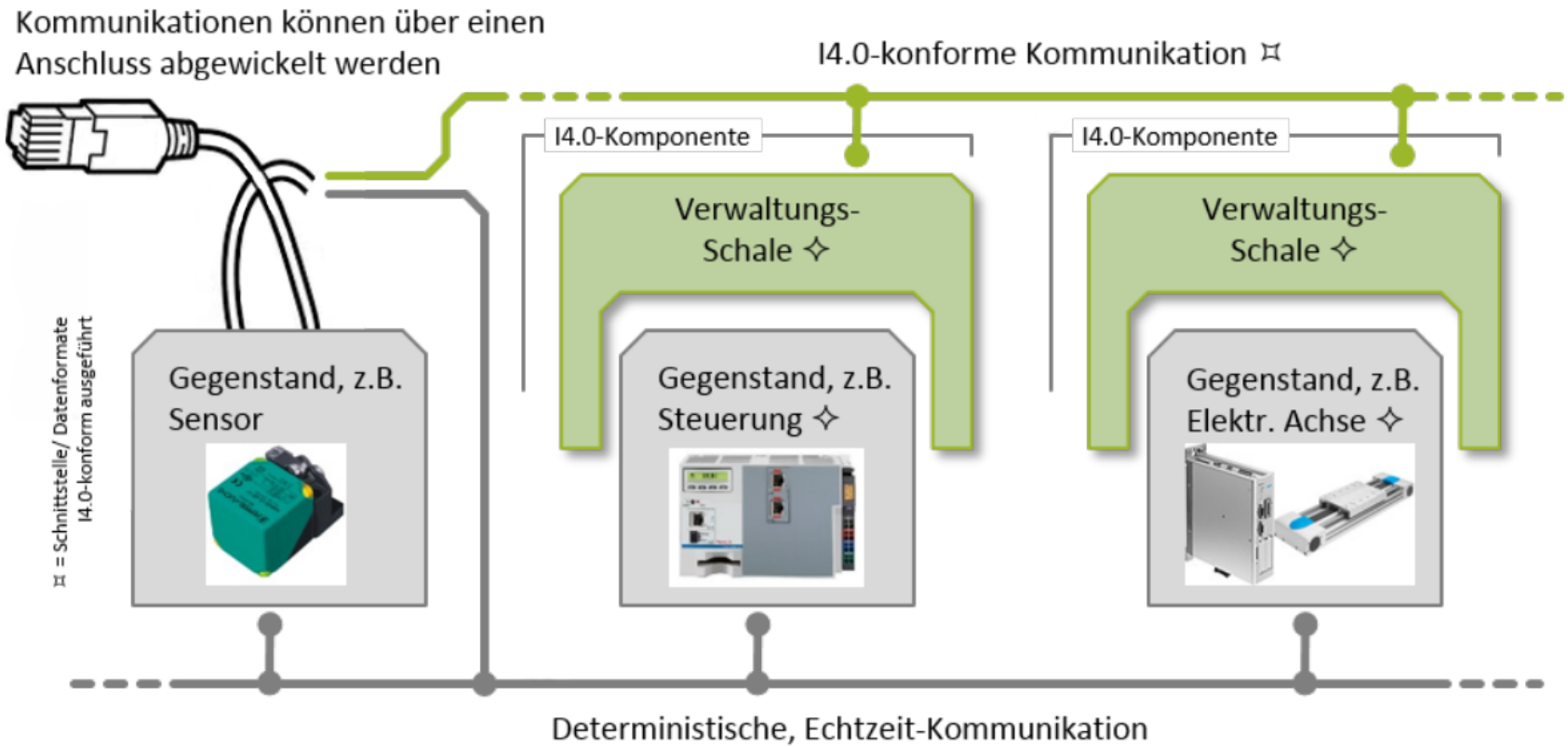
(vgl. VDI/VDE "Thesen und Handlungsfelder - Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation". April 2013)

I4.0: Modell-Weiterentwicklung – RAMI 4.0 (2)



RAMI 4.0: Referenzarchitektur-Modell für Industrie 4.0 – **makroskopische** Sicht (vgl. DIN SPEC 91345:2016-04)

I4.0: Modell-Weiterentwicklung – RAMI 4.0 (3)



RAMI 4.0: I4.0-Komponente mit Verwaltungsschale – **mikroskopische** Sicht (Quelle: DIN SPEC 91345:2016-04)

Sicherheitstechnische Aspekte – Begriffe (1)

Sicherheit und Sicherheitstechnik

- **Sicherheitstechnik**: techn. & organisat. Maßnahmen zur Erreichung der Sicherheit
- **Sicherheit**: formale Unterscheidung von 2 Aspekten[a]
  - Produkt- / Betriebssicherheit: ***Safety***
  - Angriffs- / Manipulationssicherheit: ***Security***

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

[a] vgl. Arbeitskreis Industrie 4.0 "Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0", Abschnitt 5.4 "Sicherheit als erfolgskritischer Faktor für Industrie 4.0". April 2013

Sicherheitstechnische Aspekte – Begriffe (2)

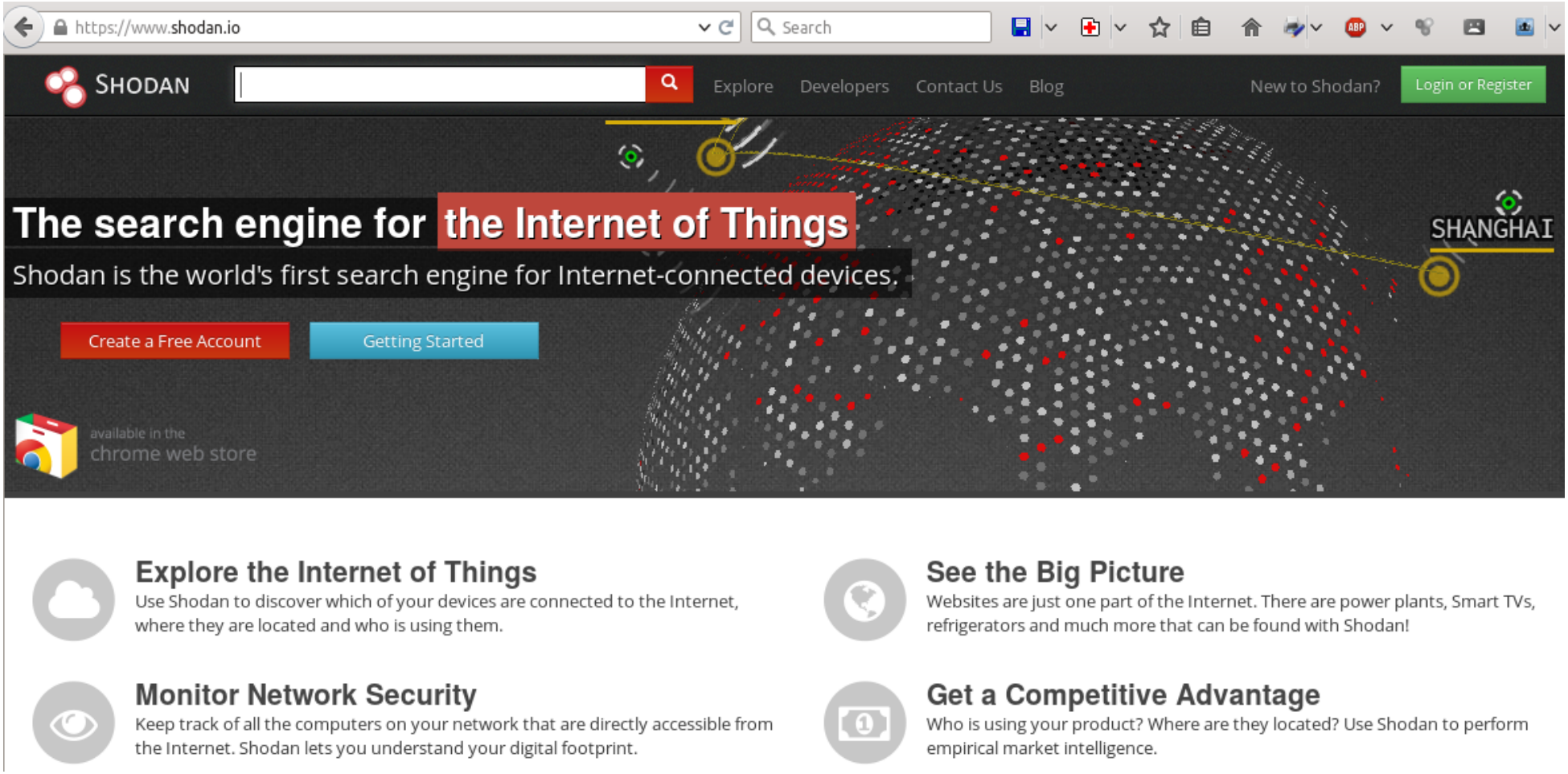
Safety (= Produkt- / Betriebssicherheit):

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

Industrial Security (= Angriffs- / Manipulationssicherheit):

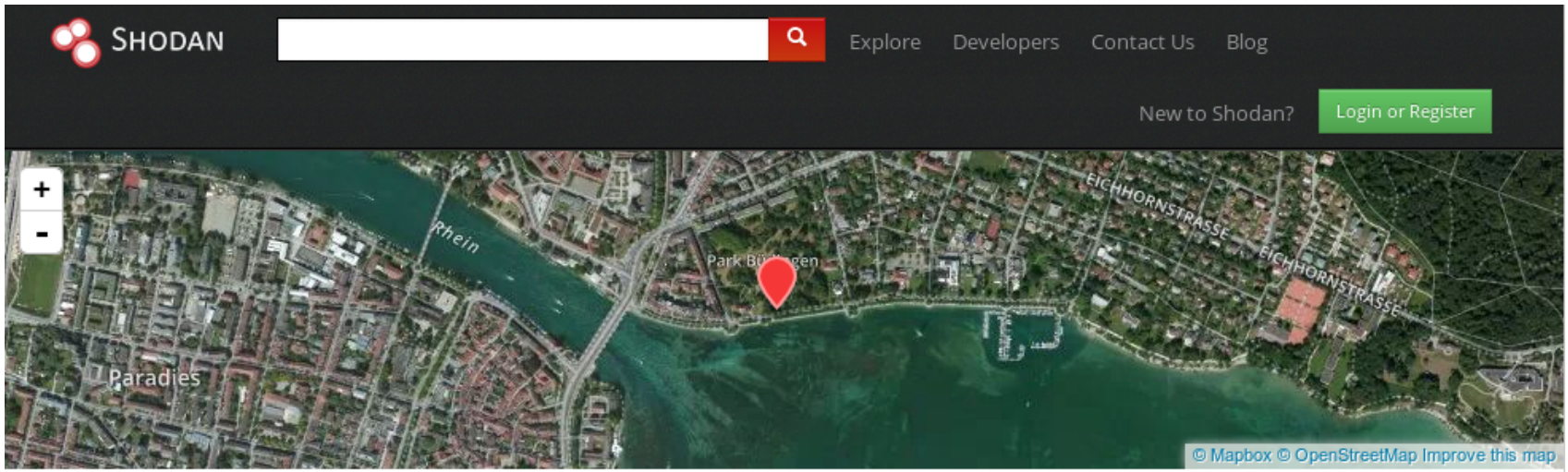
- Wirkungsrichtung: **Umgebung** ⇒ **System** (Funk.-Sich.)
- Schutzziele: Daten und Dienste schützen
- neben "Internetsicherheit" ⇒ **Maschinen-Sicherheit** + verkettete Maschinen- / Anlagen-Sicherheit (z. B. Taktstraßen)

Sicherheitstechnische Aspekte – Beispiel IoT (1)



Auffinden von mit dem Internet verbundener, unsicherer Maschinen und Anlagen (Bildquelle: https://www.shodan.io)

Sicherheitstechnische Aspekte – Beispiel IoT (2)



[redacted]

Standortdetails

City	Konstanz
Country	Germany
Organization	Universitaet Konstanz
ISP	Universitaet Konstanz
Last Update	2014-10-15T05:25:43.606228
ASN	AS553

Ports

Suche: Werkzeugmaschinen-Steuerung

102 5900

Services

Steuerungsdetails

102 [redacted]

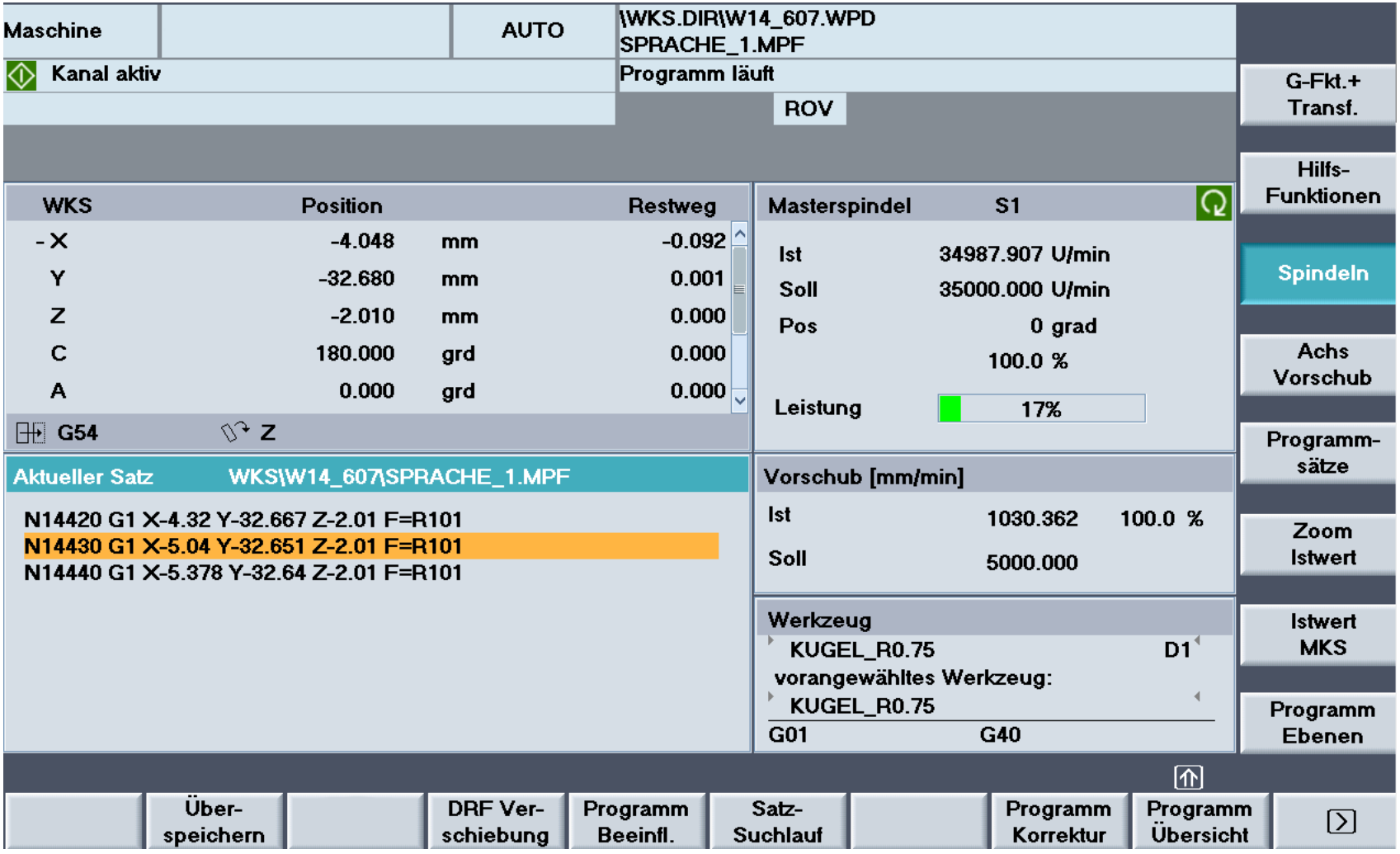
```
Module type: CP xxxyyy
PLC name:
Module: v.0.2
Basic Firmware: v.2.1.0
Module name: [redacted]
Basic Hardware: [redacted]
```


baua:

Sicherheitstechnische Aspekte – Beispiel IoT (3)

(Bildquelle: http://www.uni-konstanz.de/wisswerk/Aktuelles/ultrasonic.php)

Sicherheitstechnische Aspekte – Beispiel IoT (4)



Per VNC vollständig bedienbares HMI der entfernten Maschine (Bildquelle: https://support.automation.siemens.com)

I4.0: Rekonfiguration ⇒ Re-Validierung? (1)

Safety: Stand heute

- **Voraussetzung zur Anwendung** heutiger Safety-Methoden: *definierte* Anlagen mit variablen aber klar *definierten* Prozessen ⇒ *deterministische / probabilistische* Systeme
- nach IBN und Safety-Abnahme: keine Veränderung der Maschine *ohne* erneute (Teil-)Abnahme zulässig
- System-Änderungen **zur Laufzeit** sind **nicht** zulässig! (vgl. **IEC 61508-3:1998/2010**, 7.8 "Softwaremodifikation" und Tab. A.2-6 "Dynamische Rekonfiguration")

⇒ **I4.0-Konzepte** mit heutigen Methoden **nicht umsetzbar**, da Voraussetzungen zur Anwendung verletzt!

I4.0: Rekonfiguration ⇒ Re-Validierung? (2)

Safety: Zukünftige I4.0-Konzepte

- auftragsbezogen, sich selbst konfigurierende Anlagen
- flexible Vernetzung zur Laufzeit ⇒ *Systeme aus Systemen*
- Gesamtstruktur + Gesamtverhalten bei Entwurf der Einzelsysteme nur schwer vorhersagbar (Dynamik)
  ⇒ Verletzung der Deterministik und Vorhersagbarkeit
  ⇒ Widerspruch zur heutigen Sicherheitsnachweisführung!

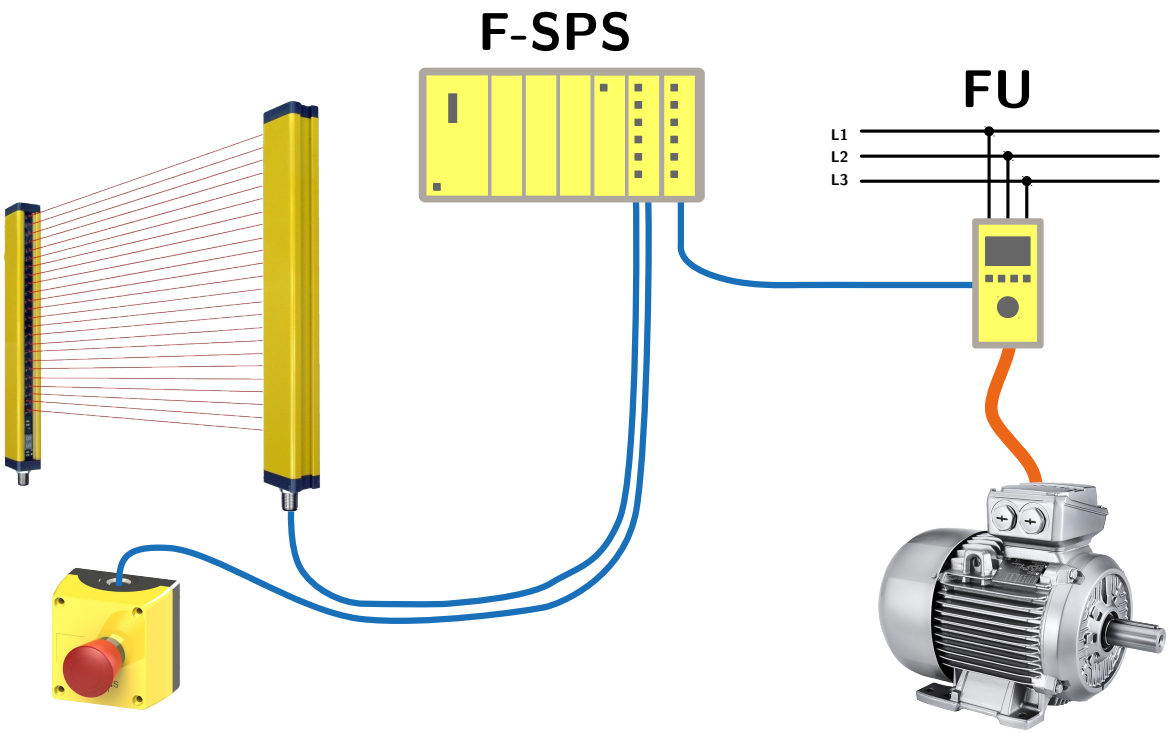
Berücksichtigung von Safety *UND* Security

- heute: getrennte Zuständigkeiten für beide Aspekte
- "Nachbesserung" von Security während oder nach IBN
- sehr unterschiedliches Methodenwerk:
  - *Safety:* keine Modifikationen nach Abnahme **zulässig**
  - *Security:* kontinuierliche Anpassung an Stand der Technik **notwendig** (z. B. Reaktion auf neue Bedrohungen)

I4.0: Aut.-Strukturen und sitechn. Methoden (1)

Safety-Strukturen heute: statisch

überwiegend **zentrale Safety-Strukturen**; nach Safety-Abnahme **statisch** (zur Laufzeit in ihrer Struktur unveränderlich)

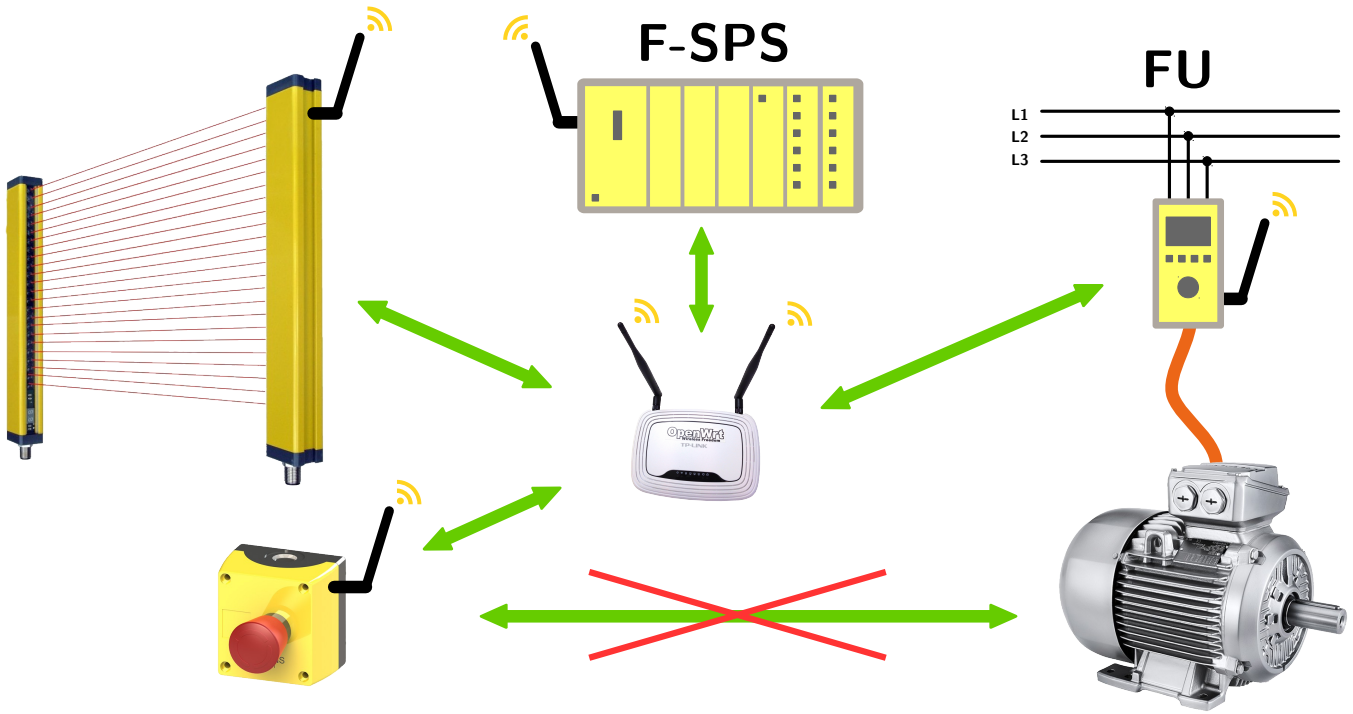


Sicherheitsfunktion "Sicherer Betriebshalt (SOS)" nach DIN EN 61800-5-2

I4.0: Aut.-Strukturen und sitechn. Methoden (2)

Safety-Strukturen morgen: dynamisch

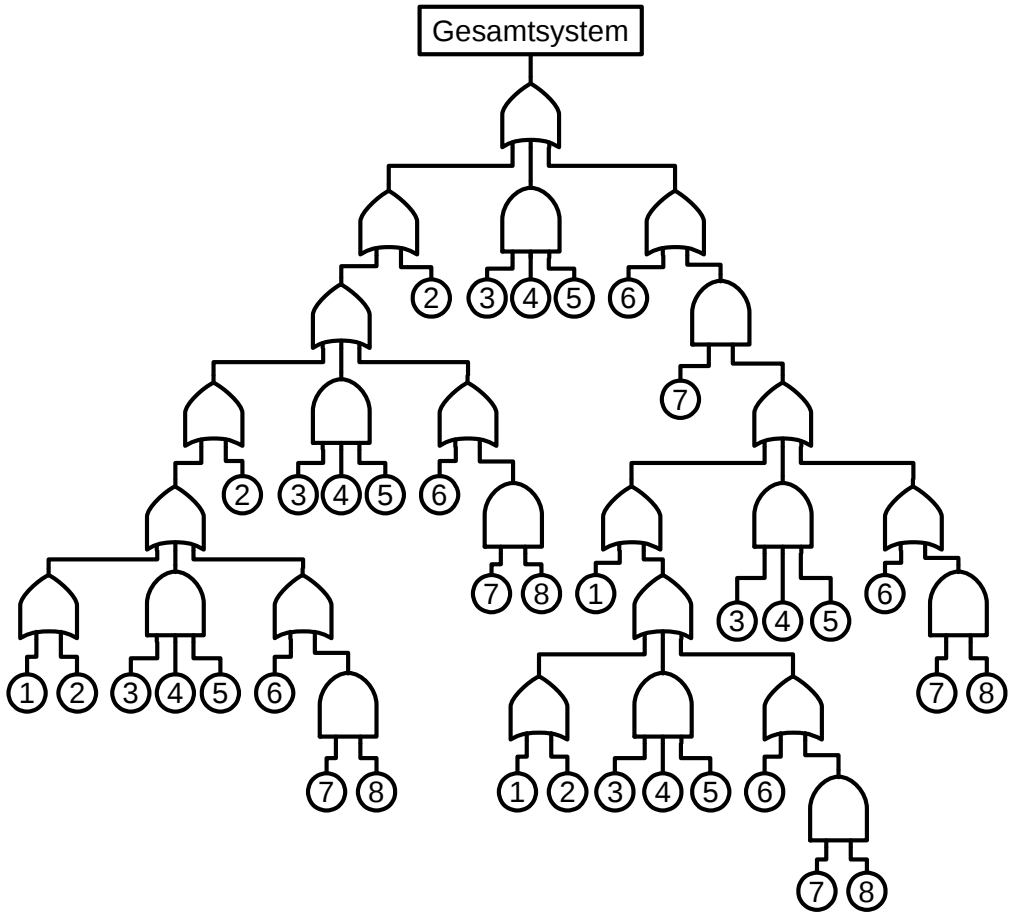
dezentrale Safety-Strukturen; zur Laufzeit in ihrer Struktur veränderlich **dynamisch** (auftragsbezogene Rekombination)



Dezentrale Sicherheitsfunktionen auf Basis funkbasierter, sicherheitsgerichteter industrieller Kommunikationstechnik (IKT) ⇒ **System aus Systemen**

I4.0: Aut.-Strukturen und sitechn. Methoden (3)

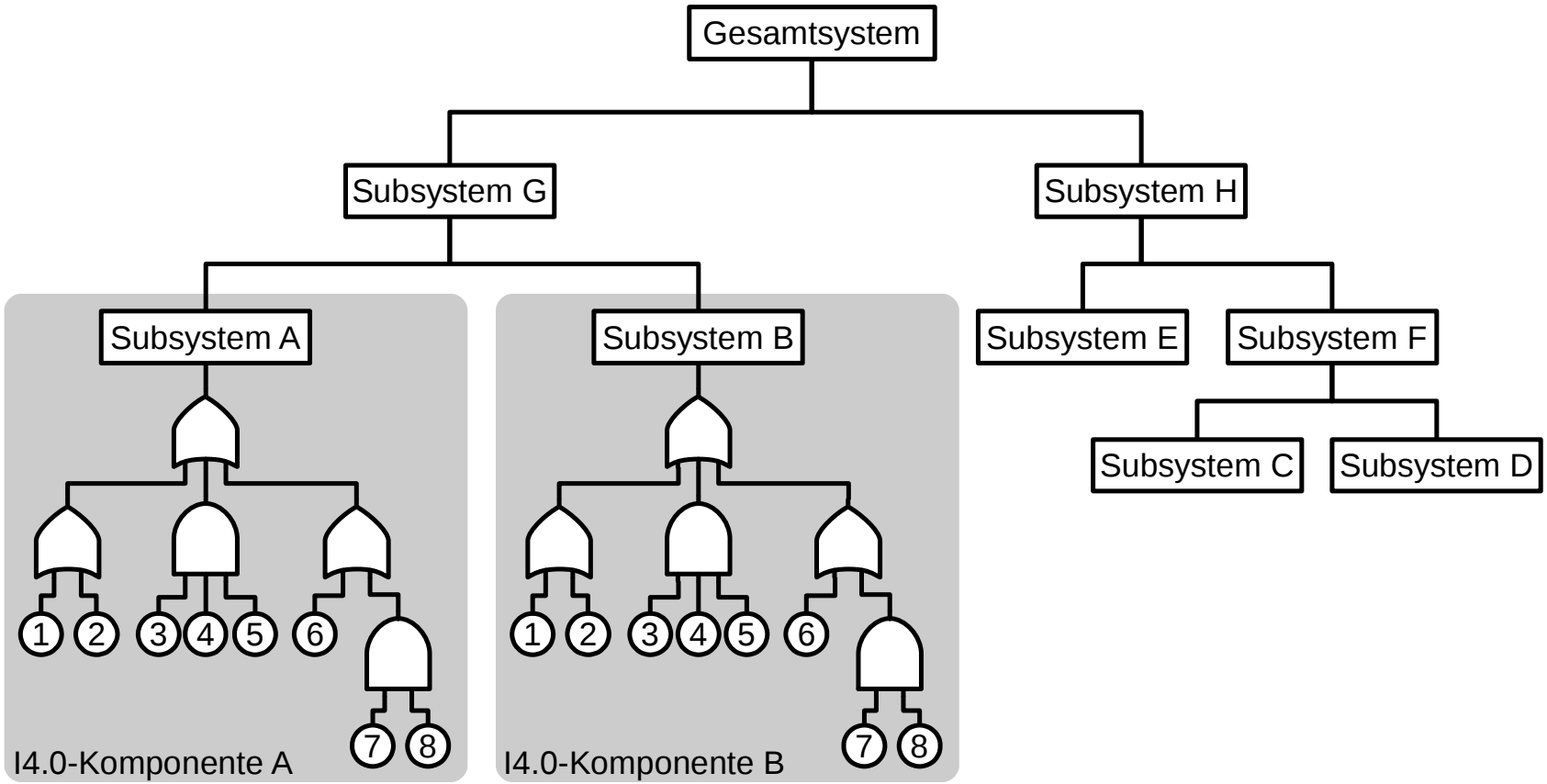
Safety-Methoden heute: statisch-manuell



Zentrale (manuelle) Validierungsmethoden (hier: FTA) während System-Entwurf und -Abnahme ⇒ Reaktionen auf Änderungen zur Laufzeit nicht möglich

I4.0: Aut.-Strukturen und sitechn. Methoden (4)

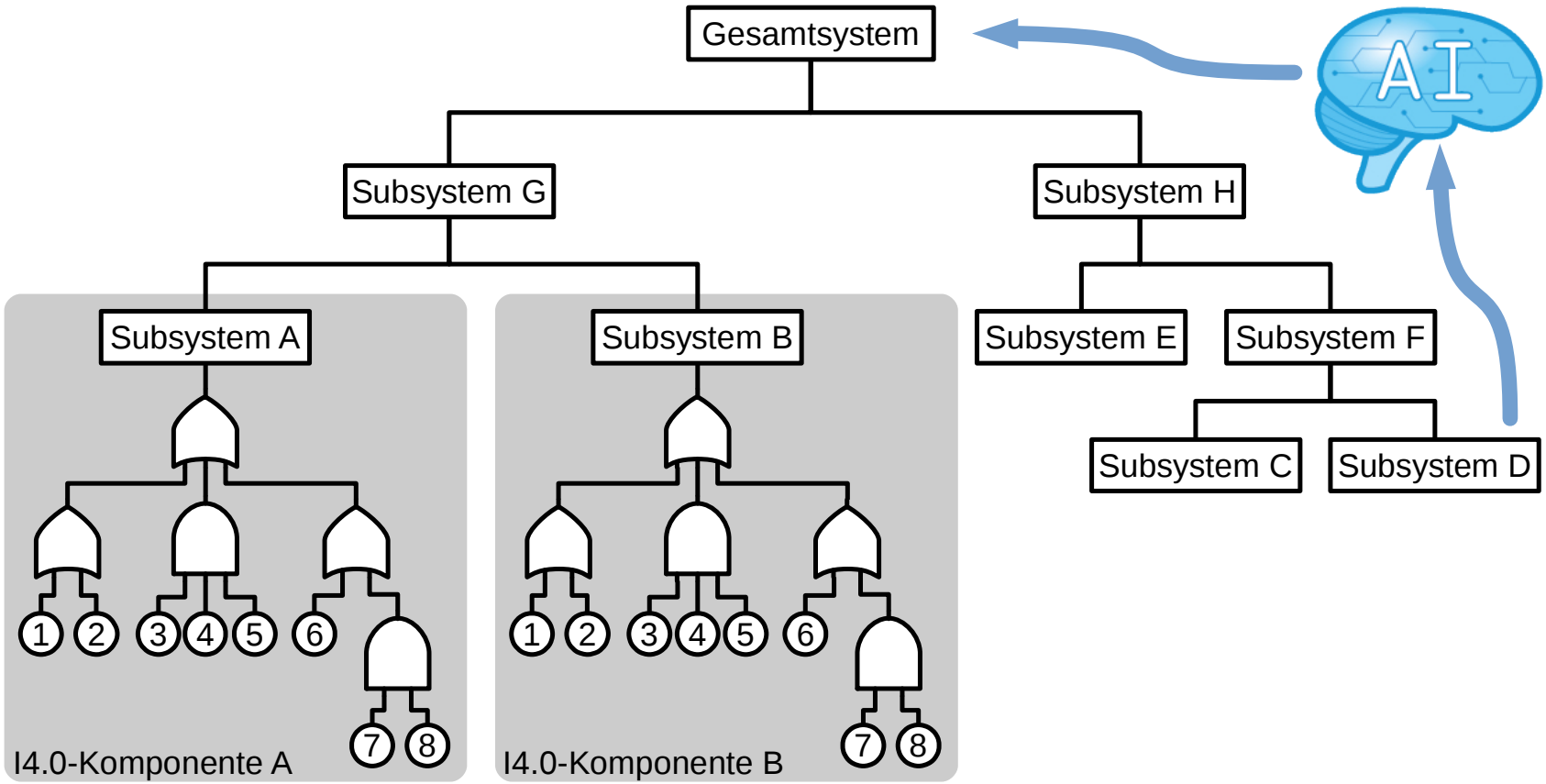
Safety-Methoden morgen: statisch-regelbasiert



Dezentrale Validierungsmethoden (hier: *modularisierte FTA*) ⇒ Reaktionen auf Änderungen zur Laufzeit sind möglich ⇒ Abbildung *System aus Systemen*

I4.0: Aut.-Strukturen und sitechn. Methoden (5)

Safety-Methoden morgen: statisch-regelbasiert + dynamisch-lernfähig(?)



stat.-regelb. Methoden werden **ergänzt** durch dyn.-lernf. (aber **nicht ersetzt**!)
⇒ Reaktionen auf (zum Zeitpkt. Systementw. unbek.) Fehlerzustände möglich

I4.0: Aut.-Strukturen und sitechn. Methoden (6)

Gegenüberstellung **statischer** und **dynamischer** Steuerungsstrukturen sowie der entsprechenden Analyse- und Bewertungsmethoden

	heute	**Industrie 4.0**	
Steuerungs-**Strukturen** / -**Topologien** (inkl. Safety-Konzept)	**statisch** (nach Abnahme der Anlage *unveränderlich*)	**dynamisch** (zur Laufzeit *veränderlich*; auftragsbezogene Rekombination / Rekonfiguration der Anlage)	
Analyse- und Bewertungs-**Methoden** (Sicherheitsnachweis)	**statisch-manuell** (während Design- u. Inbetriebnahme *einmalig u. überw. manuell* durchgeführt)	*erforderlich:* **statisch-regelbasiert** (regelbasierte, modularisierte Methoden *zur Laufzeit* ausgeführt)	*optimal:* **statisch-regelbasiert + dynamisch-lernfähig** (statisch-regelbasierte Methoden ergänzt durch dynamisch-lernfähige Methoden)

Stand Normung bzgl. *dynamisch-lernfähiger Methoden*:

vgl. **IEC 61508-3:1998/2010**, Tab. A.2-5: Einsatz **künstlicher Intelligenz** (+ Fehlerkorrektur) sind **nicht** zulässig! $\Rightarrow$ kategorischer Ausschluss von Methoden $\hat{=}$ aktueller Stand der Technik? $\Rightarrow$ Neubewertung?

Ausblick (1)

Forschung ($\Rightarrow$ BAuA)

- Weiterentwicklung + Modularisierung heutiger (manueller) statisch-regelbasierter / dynamisch-lernfähiger Safety-Methoden $\Rightarrow$ Validierung zur Laufzeit nach Rekombination möglich
- aktive Beteiligung vieler Interessensgruppen an Methoden-Weiterentwicklung gewünscht $\Rightarrow$ *Open Source*-Prozess
- Ergebnisse: quelloffene *Prinziplösungen* (Software-Bibliotheken)

Ausblick (2)

Entwicklung

- Steuerungs-Hersteller portieren Software-Methoden (Prinziplösungen) auf eigene Steuerungs-Architektur
- Weiterentwicklung zu industriell einsetzbarem, sicheren Produkt

Normung ($\Rightarrow$ BAuA)

- Vorstellung der Forschungs- und Entwicklungsergebnisse in relevanten Normungsgremien
- Ziel: Aufnahme weiterentwickelter Methoden in *strategische* und *inhaltliche* Normungsarbeit

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!