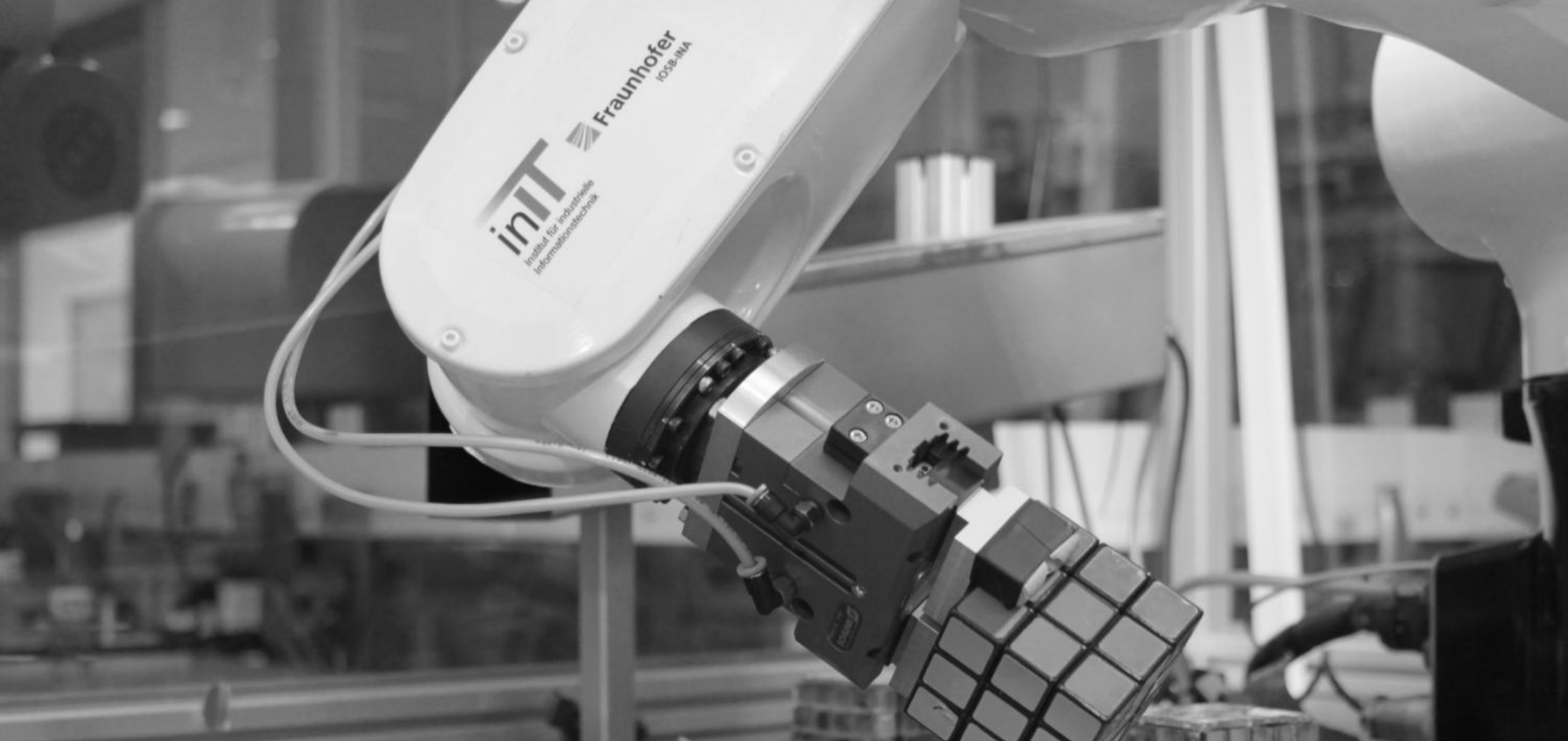


Automatische Evaluierung von Anforderungen bezüglich der Informationssicherheit für das zukünftige industrielle Netzwerkmanagement

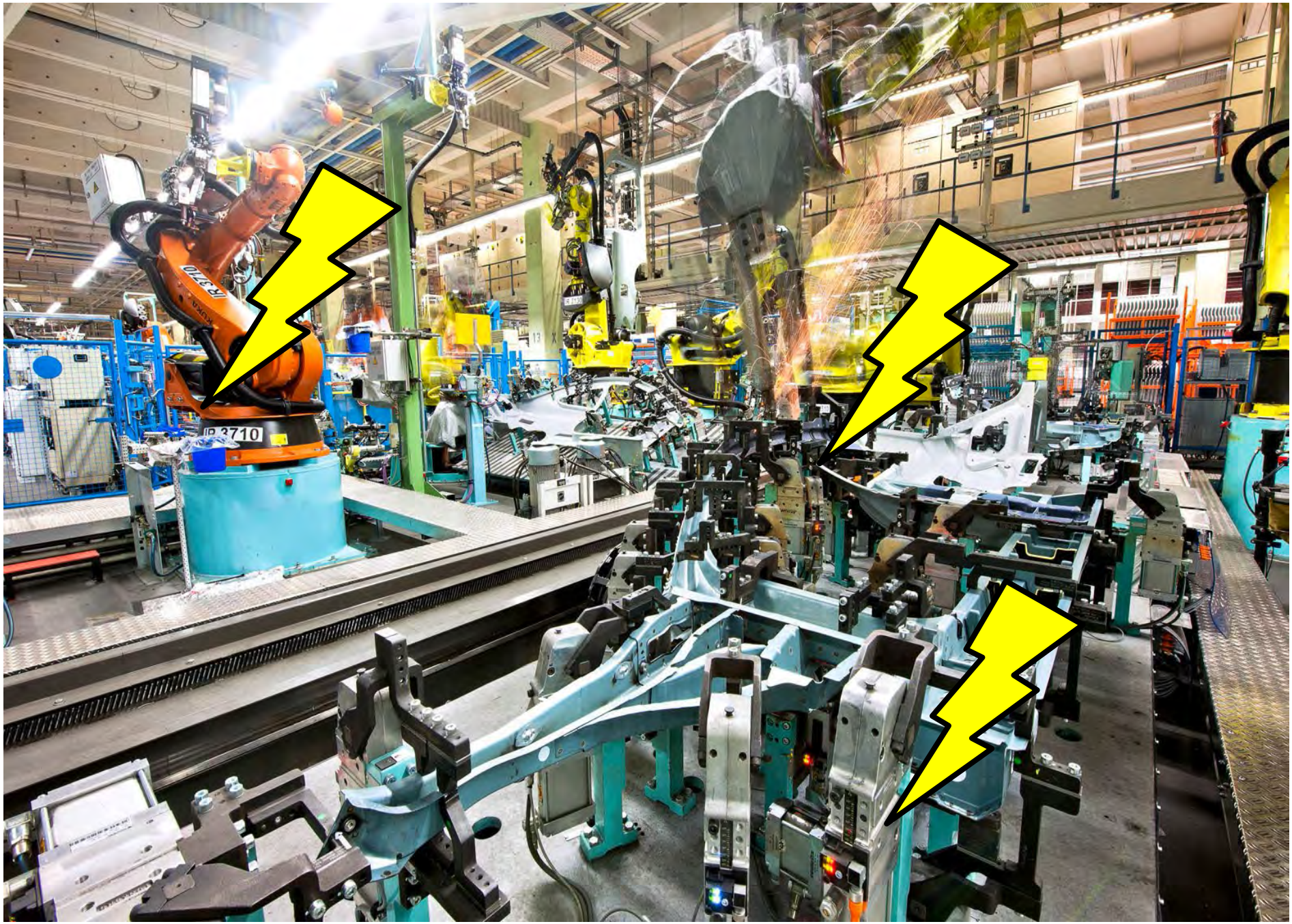
Marco Ehrlich, Henning Trsek & Jürgen Jasperneite

inIT

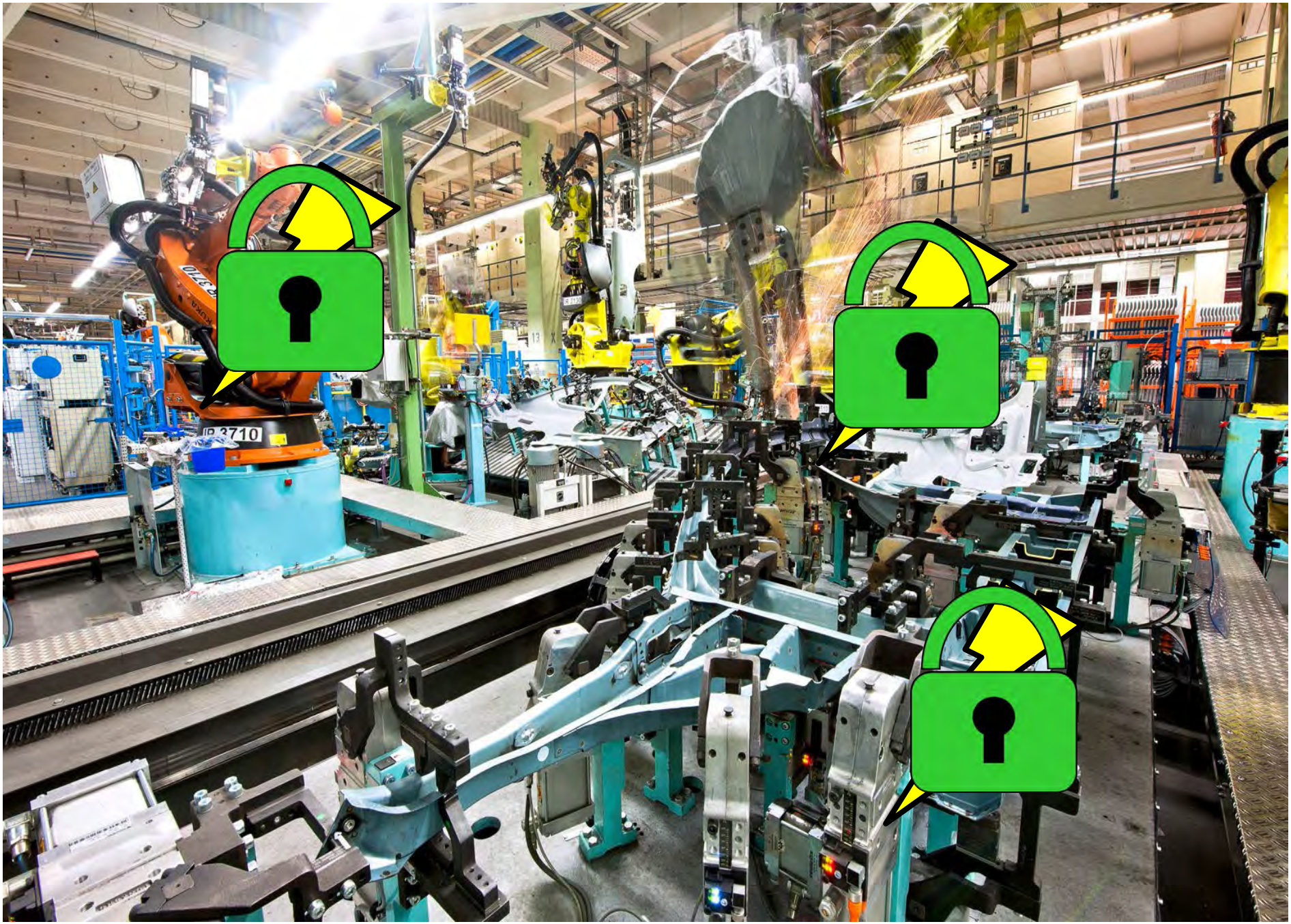
rt-solutions.de
experts you can trust.

Fraunhofer
IOSB-INA

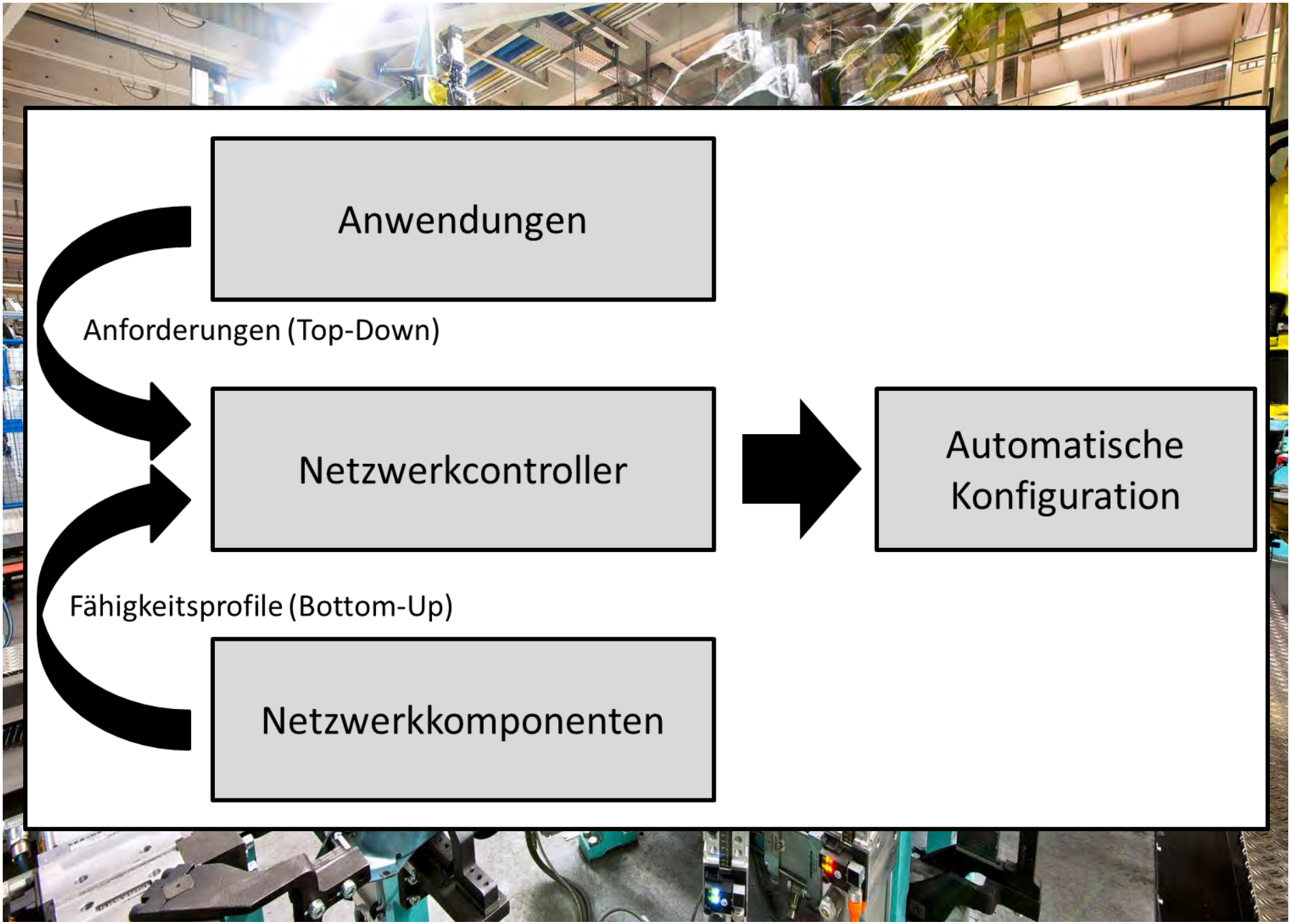
© Daimler AG



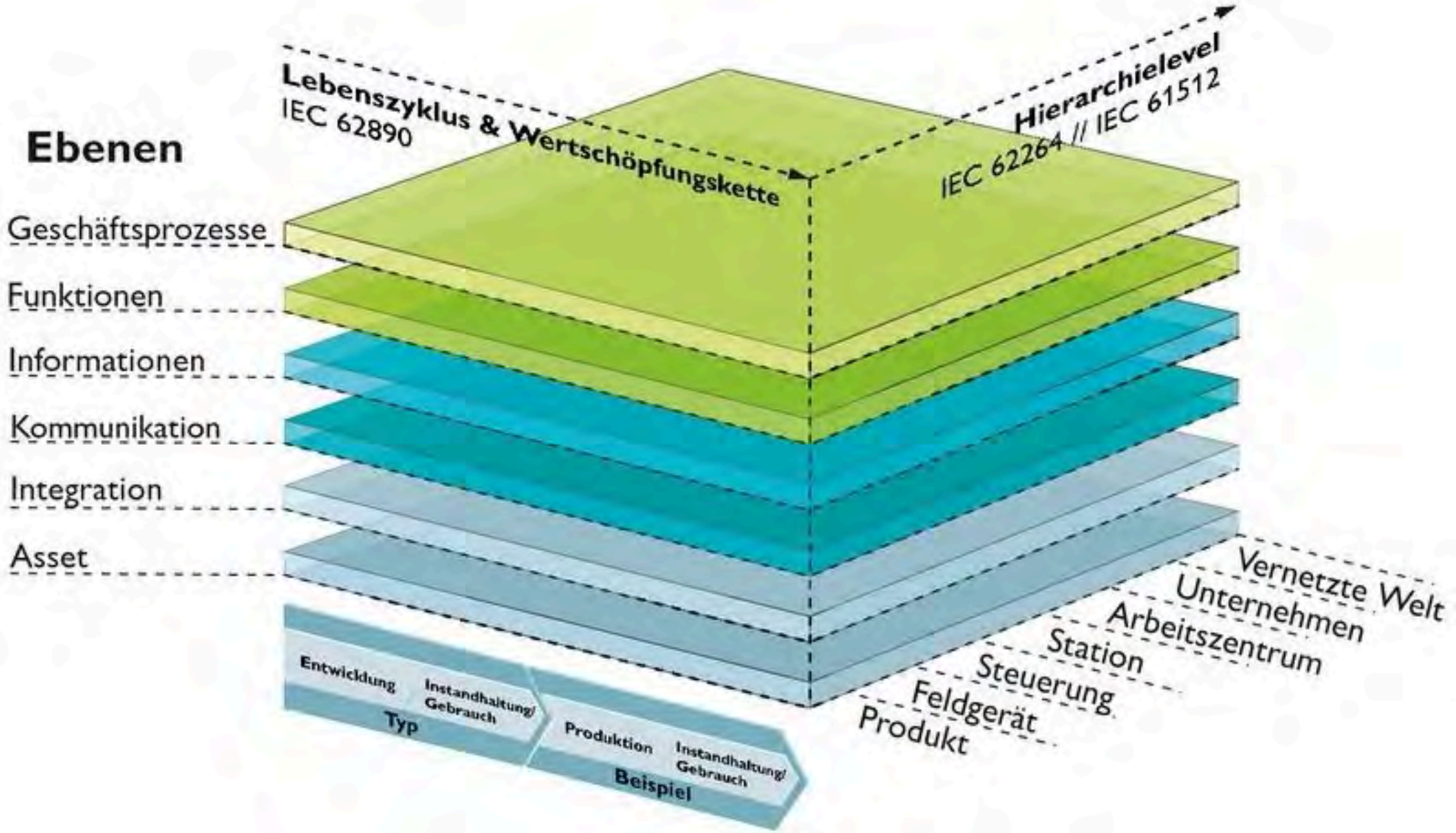
© Daimler AG



© Daimler AG

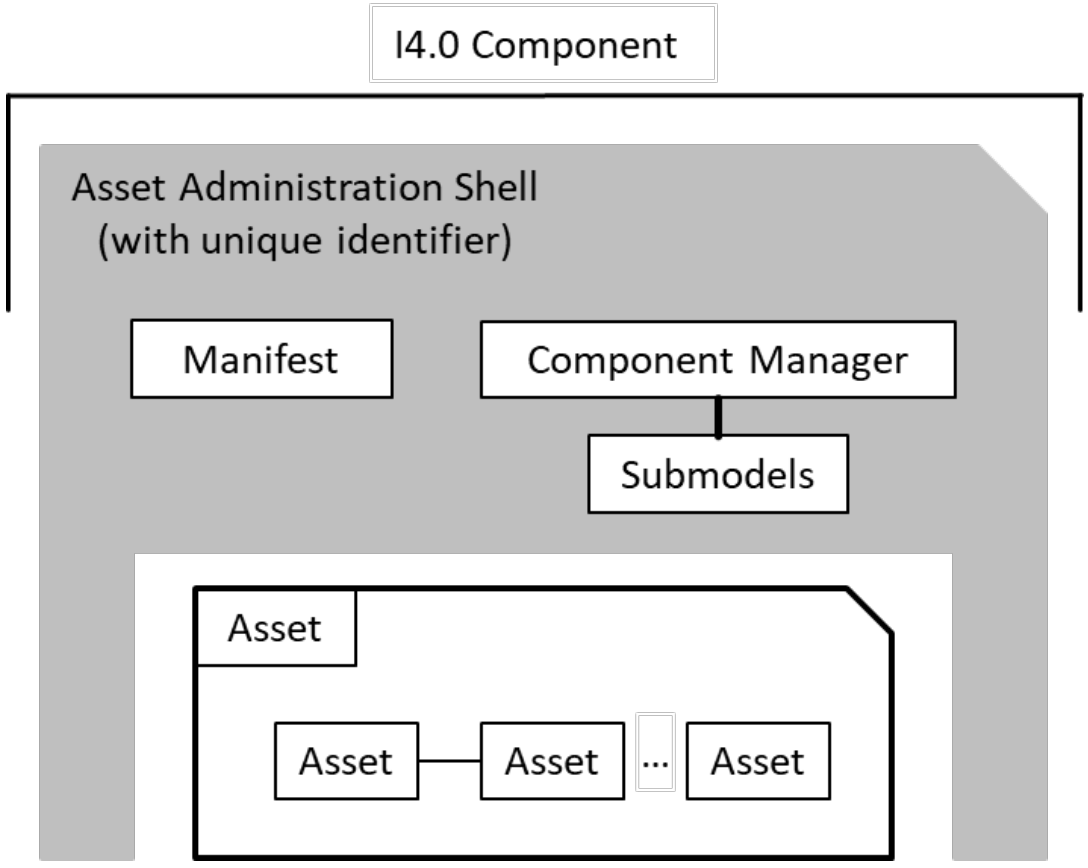

Anwendungen
Anforderungen (Top-Down)
Netzwerkcontroller
Automatische Konfiguration
Fähigkeitsprofile (Bottom-Up)
Netzwerkkomponenten

REFERENZARCHITEKTURMODELL INDUSTRIE 4.0



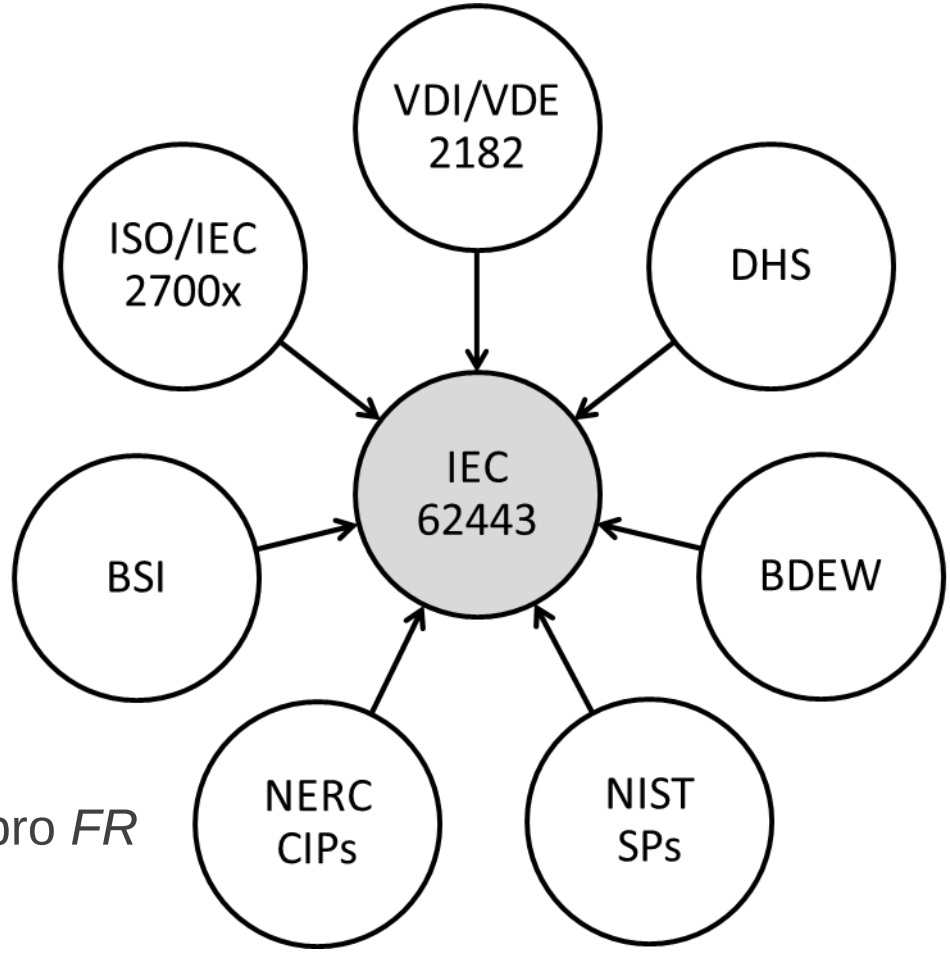
INDUSTRIE 4.0 VERWALTUNGSSCHALE - ASSET ADMINISTRATION SHELL (AAS)

- Implementierung eines “Digitalen Zwillings” aus den RAMI4.0 Entwicklungen
- Assets sind eindeutig identifizierbar und haben einen Wert für das Unternehmen
  - Hardware
  - Software
  - Ideen & Konzepte
  - Internes Wissen
- *I4.0 Component = Asset + AAS*
- Zusammensetzung der AAS
  - *Manifest*
  - *Component Manager*
  - *Submodels*



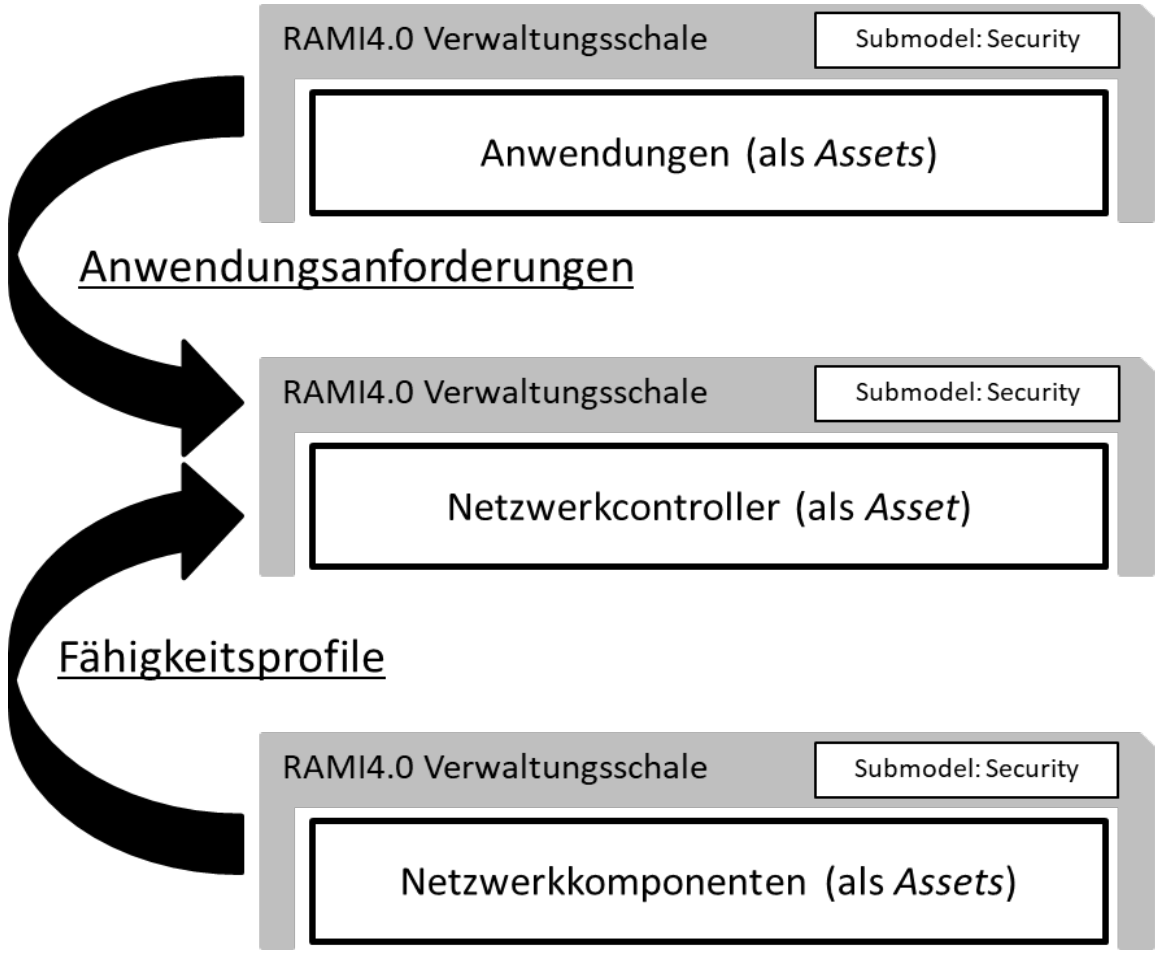
IEC 62443 STANDARD

- Standard für die Nutzung in *Industrial Automation and Control Systems (IACSs)*
- 4 *Security Levels (SLs)*
  - Basierend auf Motivation & Ressourcen
  - *Capability / Target / Achieved*
- Zusicherung der allgemeinen Schutzziele
  - Verfügbarkeit *(Availability)*
  - Integrität *(Integrity)*
  - Vertraulichkeit *(Confidentiality)*
- 7 *Foundational Requirements (FRs)*
- Verschiedene *System Requirements (SRs)* pro *FR*



UNIFIED SECURITY MODELLING METRIC (USMM)

- Erste konzeptionelle Versuche
  - Verwaltungsschale
  - Submodel Security
  - IEC 62443 Standard
- Bereits evaluierte Beispiele
  - OPC UA Server
  - AR Anwendung
- Aktueller Forschungsstand
  - Informationsmodellierung
  - Automatischer Vergleich
  - Skalierbarkeit der Lösung
  - Weitere Anwendungsfälle



INDUSTRIELLE ANWENDUNGSFÄLLE ALS BASIS FÜR DIE EVALUIERUNG

- *Standard OPC UA Server Profile* (als de-facto Industrie 4.0 Standard):
- *Augmented Reality (AR)* Anwendung:

OPC UA	**SL**	**FR**	**SL**	**Augmented Reality Worker**
User Identity Tokens *Application Instance Certificates* *Software Certificates*	4	1	2	Identifikation und Authentifizierung Nur Lesezugriff auf die Prozessdaten
User Identity Tokens Rechte- und Benutzerverwaltung	3	2	3	Absicherung gegen Rechteeskalation Benutzer- und Rechteverwaltung
Sym. Verschlüsselung *(HmacSha1)* Asym. Verschlüsselung *(RsaSha1)*	2	3	2	Integrität der Prozessdaten Ressourcenbeschränkte Verschlüsselung
Sym. Verschlüsselung *(Aes128)* Asym. Verschlüsselung *(Rsa15)*	2	4	2	Vertraulichkeit der Prozessdaten Ressourcenbeschränkte Verschlüsselung
Application Instance Certificates *Software Certificates*	3	5	3	Management von Funkverbindungen Daten zur Positionslokalisierung
Nicht vorhanden bzw. bewertbar	1	6	1	Nicht vorhanden bzw. bewertbar
Message Flooding Minimierung	2	7	1	Verfügbarkeit von Prozessdaten Keine Echtzeit QoS Anforderungen

EVALUIERUNG DER MODELLIERUNG - 1

Eigenschaften	Bewertung	Begründung der Evaluierung
Granularität	✓	Vier verschiedene *Security Levels* können benutzt werden
Verfügbarkeit	(✓)	Sieben *Foundational Requirements* sind vorhanden
Kosteneffizienz	(✓)	Ressourcensparende und einfache Berechnungen
Lokalisierung	✗	Modellierung der Informationssicherheit ist subjektiv
Validierung	✗	Konzepte zur internen Überprüfung fehlen noch
Flexibilität	✓	Dynamisch anpassbar während der Laufzeit
Automatisierung	✗	Manuelle Eingabe von Expertenwissen wird benötigt
Maschinenlesbarkeit	✓	Die Modellierung basiert auf quantitaitiven Bewertungen
Zukunftssicherheit	✓	Die Lösung ist technologie- und protokollunabhängig

EVALUIERUNG DER MODELLIERUNG - 2

FR	Bewertung	Begründung der Evaluierung
1	(✓)	+ Passt nur zur Modellierung von Fähigkeitsprofilen − Muss für Anwendungen ohnehin immer gegeben sein
2	(✓)	+ Passt nur zur Modellierung von Fähigkeitsprofilen − Muss für Anwendungen ohnehin immer gegeben sein
3	✓	+ Deckt das Schutzziel der Integrität ab + Für Fähigkeitsprofile und Anwendungsanforderungen nutzbar
4	✓	+ Deckt das Schutzziel der Vertraulichkeit ab + Für Fähigkeitsprofile und Anwendungsanforderungen nutzbar
5	✗	− Die Definition der zones und *conduits* ist nicht anwendbar − Für Fähigkeitsprofile und Anwendungsanforderungen nicht nutzbar
6	✓	+ Deckt das Schutzziel der Verfügbarkeit ab + Zusätzliche *SRs* werden zur Verfeinerung benötigt
7	✗	− *Distributed Denial of Service (DDoS)* Bezug ist zu spezifisch − Deckt das Schutzziel der Verfügbarkeit nicht ab

ZUSAMMENFASSUNG & AUSBLICK

- Heterogene und hybride (drahtlos & drahtgebunden) Kommunikationssysteme
- Die Digitalisierung der Industrie bringt Chancen aber auch Herausforderungen
- Manuelle Konfiguration durch Experten aus der jeweiligen Domäne wird benötigt
- Das Netzwerkmanagement sollte im Bereich *Security* automatisiert werden
- Verfügbare Standards sind manuell, statisch und ressourcenintensiv
- Die RAMI4.0 Verwaltungsschale (AAS) und der IEC 62443 Standard als Startpunkt
- Definition und Spezifikation des *Submodel Security* muss weiter entwickelt werden

Vielen Dank für die Aufmerksamkeit!

M.Sc. Marco Ehrlich
marco.ehrlich@hs-owl.de