WANN IST EINE COBOT-ANWENDUNG SICHER?

Safety und Security in der Anwendung

Dr.-Ing. Christian Henke

Hannover | 26. April 2022

ROBOTICS KONGRESS

Deutsche Messe
Technology Academy

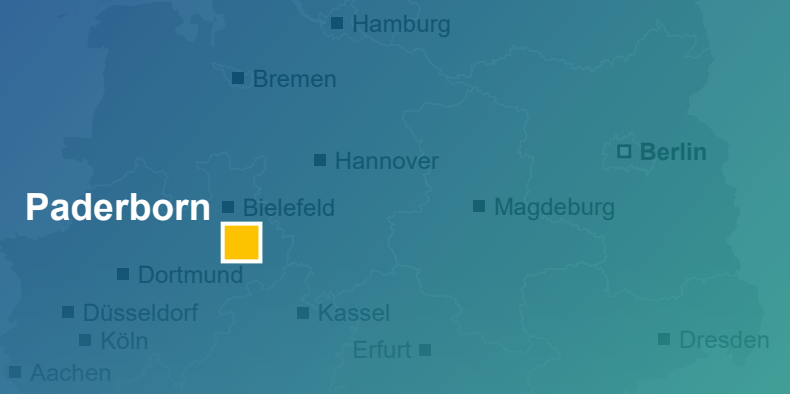
Fraunhofer IEM

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Gefördert durch:
Fraunhofer

Fraunhofer IEM

Standort, Mitarbeiter und Direktorium



An der Zukunftsmeile 1 in Paderborn

> 130 Mitarbeiterinnen und Mitarbeiter

Forschungsbereiche

Scientific Automation
PROF. TRÄCHTLER

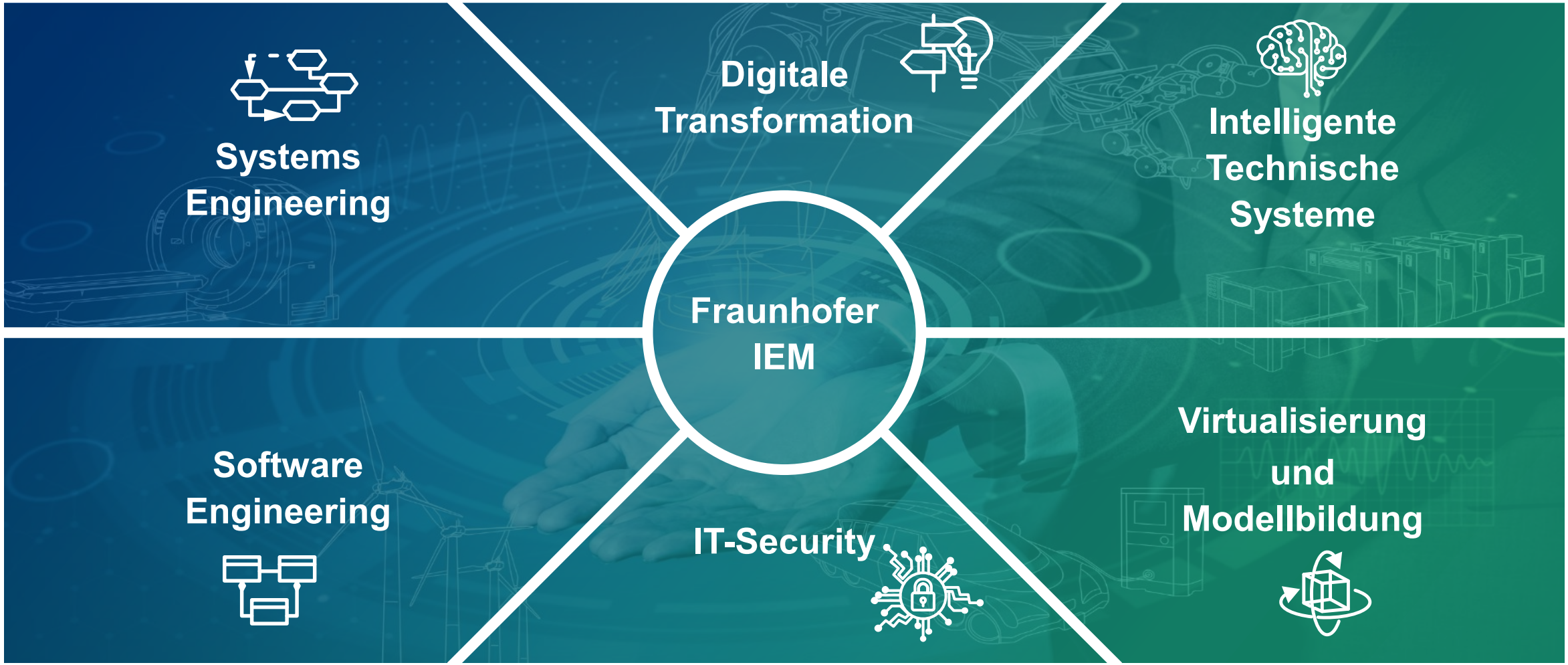
Produktentstehung
PROF. DUMITRESCU

Software Engineering & IT Security
PROF. BODDEN

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer
IEM

Kernkompetenzen
des Fraunhofer IEM



Forschungsbereich Scientific Automation

Unsere Schwerpunkte

Automatisierungstechnik

- Modulare Steuerungsarchitekturen
- Steuerungsvernetzung
- Datenanalyse und Machine Learning
- Antriebs- und Steuerungsoptimierung

Robotik

- Mensch-Roboter-Kollaboration
- Sensorgeführte Roboter
- Roboterprüfstande
- Schweißrobotik
- 3D-Bauteilvermessung

Intelligente Regelungen

- Self-X-Fähigkeiten, z.B. Selbstdiagnose, -heilung oder -konfiguration
- Model Predictive Control
- Sebstkorrigierende Fertigungsprozesse

Robotics Lab

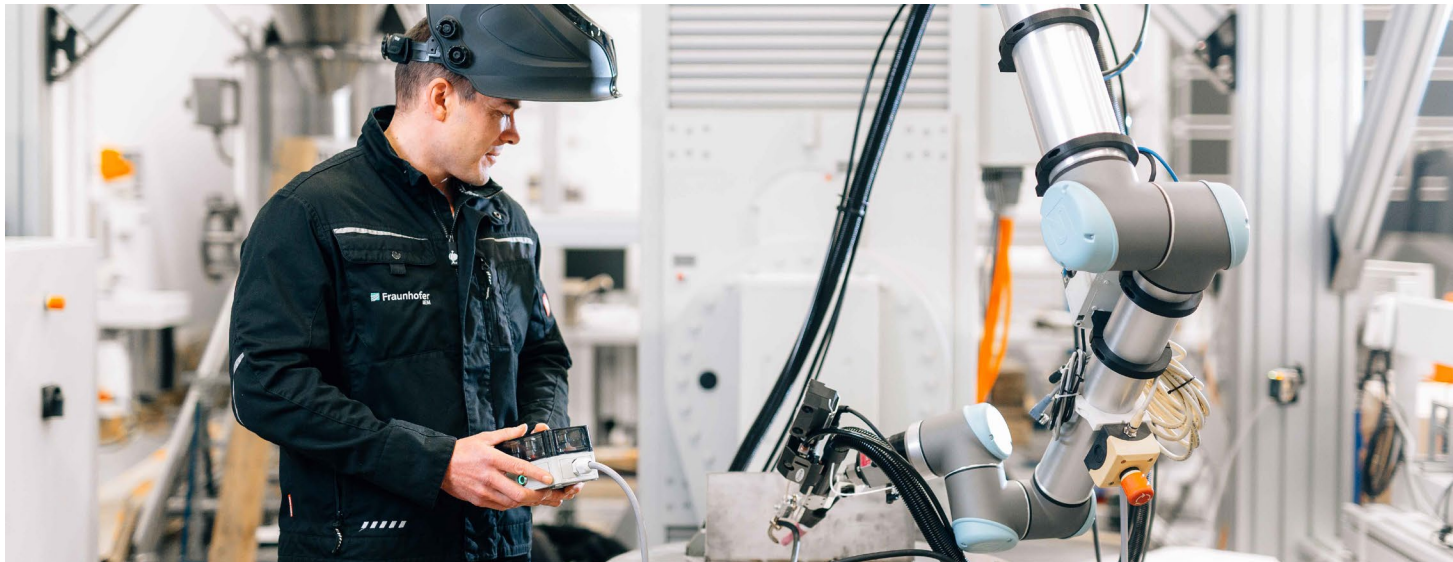
Fertigungsautomatisierung bei Losgröße 1

Entwicklungen am Fraunhofer IEM

- **Entwicklung roboterbasierter kollaborativer Schweißsysteme**
  - Automatische Nahterkennung und -verfolgung
  - Ausrichtung auf „High Mix, Low Volume“-Fertigung
  - Qualitätserhöhung der resultierenden Schweißnähte durch selbstlernende Ansätze und Selbstoptimierung

Technische Arbeitsziele

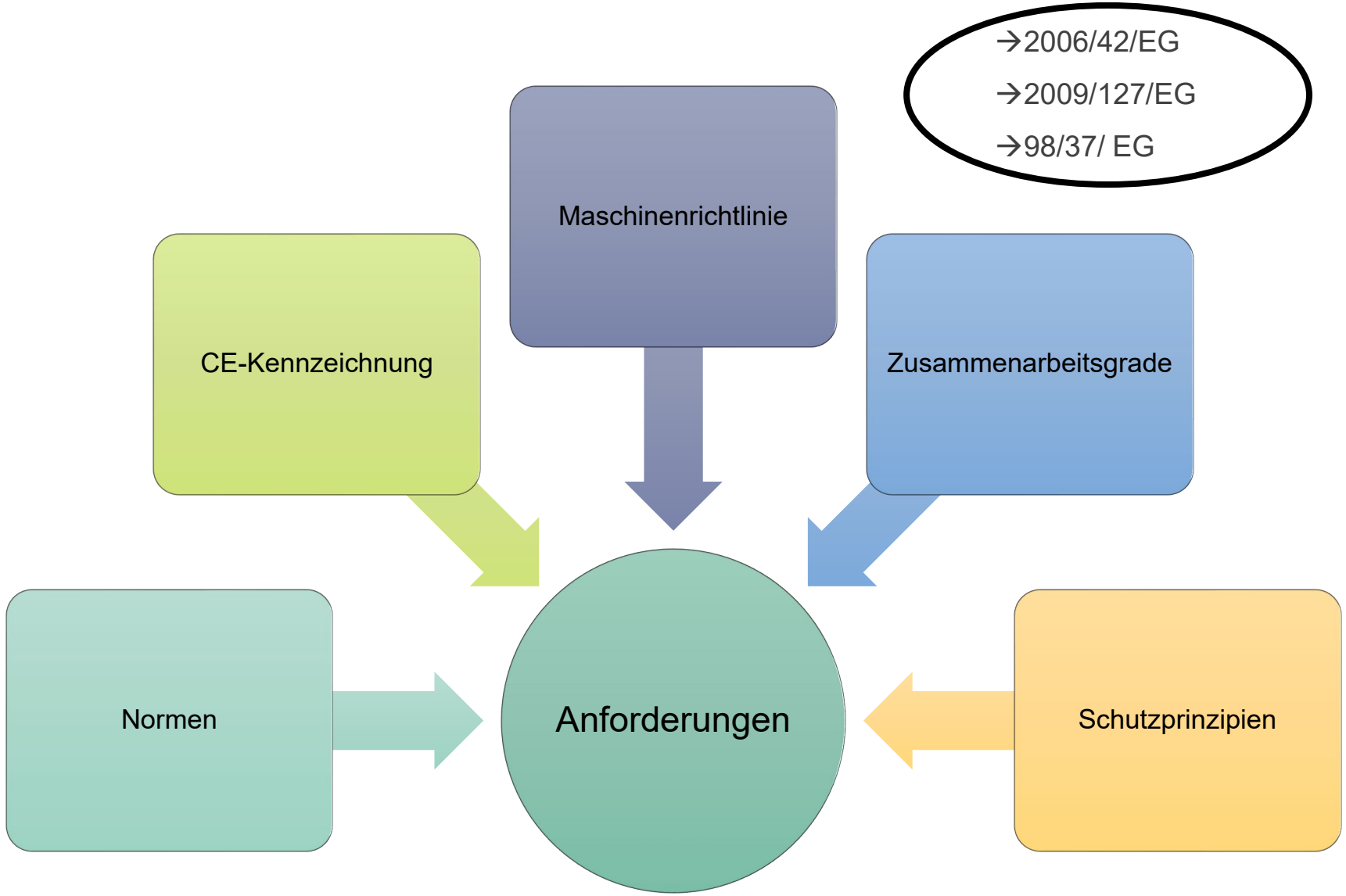
1. Flexible Adaption des Schweißsystems auf unterschiedliche Werkstücke **ohne roboter- oder anlagenspezifische Programmierung → Low-/No-Code-Lösungen**
2. Erhöhung der **Bewegungsmöglichkeiten des Schweißsystems**
3. Automatische Überwachung und **Optimierung der Nahtgüte**



Sicherheit bei der Mensch-Roboter-Kollaboration

Anforderungen

- → DIN EN 61508
- → ISO 1200
- → ISO 10218-1
- → DIN EN ISO 11161
- → ISO 21434
- → ISO 62443
- → UNECE WP29
- → ISO/TS 15066:2016



Safety- und Security Aspekte für Cyber-Physische Systeme (CPS)

Ausgangssituation und Handlungsbedarf

Entwicklung und Anwendungsfelder

Ausgangssituation

- Gestiegene Komplexität und Vernetzung von Robotersystemen erfordern **Gewährleistung und Nachweis** von Safety und Security
- Safety und Security beeinflussen sich wechselseitig: **frühe, integrierte Betrachtung** nötig
- Normen fordern die Gewährleistung von Safety und Security, welche in der Praxis jedoch oft getrennt betrachtet werden
- In der Folge werden Konflikte und Synergien zwischen Safety- und Security-Maßnahmen erst spät erkannt

Handlungsbedarf

- Frühe, werkzeugunterstützte Erkennung von Konflikten und Synergien zwischen Safety und Security

Quelle: medium.com

Zunehmende Herausforderungen für Safety & Security

Beispiel: Cyber-Physische Systeme

- Zusammenziehen von Funktionalität auf eine zentrale IPC mit viel Rechenpower
- Alle nötigen Informationen an einem Ort
- Reduzierte Kommunikationszeiten

Wechselwirkung!
Ziel: Konflikte erkennen, Synergien nutzen.

Safety-Herausforderungen

- Trennung von Funktionen mit hoher Kritikalität von weniger kritischen
- Single Point of Failure:
  Fail Operational statt Safe State nötig

Security-Herausforderungen

- Große Angriffsfläche (Cloud/Apps,Sensoren, Kameras, …)
- Segmentierung / Defense in Depth
- Safety-Eigenschaften nicht verletzen

Safety & Security

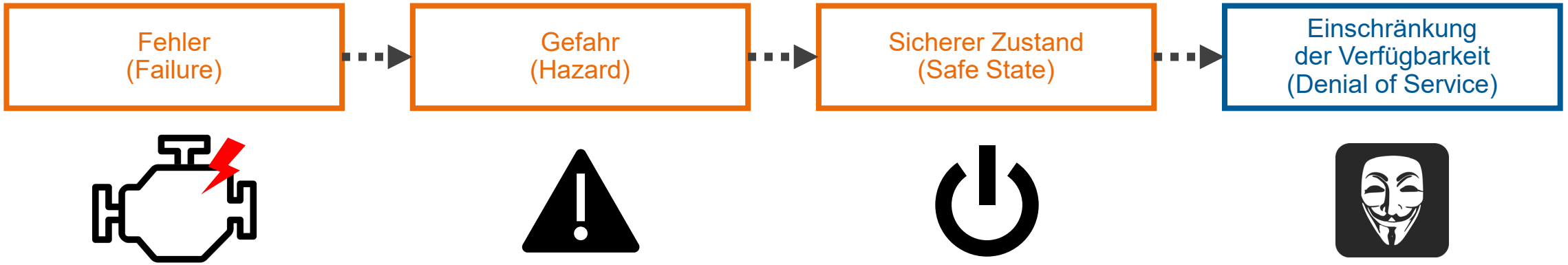
Denkweisen: Gefahrenanalyse vs. Bedrohungsanalyse

Safety (Betriebssicherheit)

Risiko von **Gefahren (Hazards)** ausgehend von systematischen und zufälligen **Fehlern** reduzieren

- Safety-Gewährleistung und Nachweis sind Pflicht
- Existierende Standards (z.B. IEC 61508, ISO 26262)
- Etablierte Methoden (z.B. FMEA, FTA, …)
- Früh in der Entwicklung

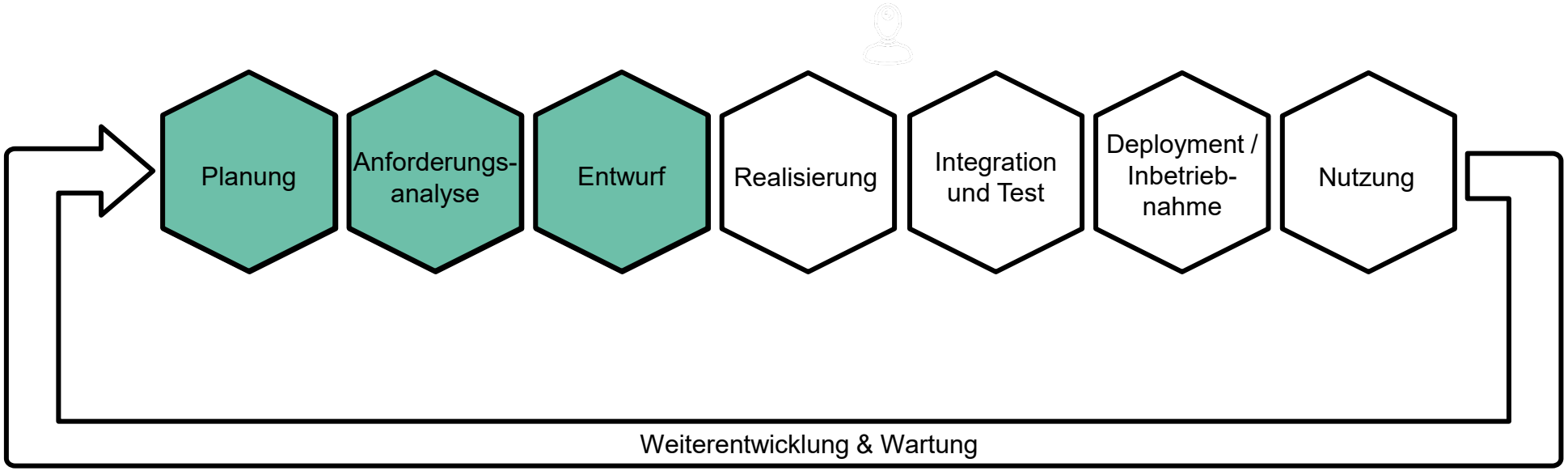
- Welche Reaktion ist angemessen oder notwendig?
- Kann der Fehler unter Umständen gefahrlos ignoriert werden?
- Fehlende Methoden und Werkzeuge zur **integrierten** Betrachtung von Safety und Security vom Beginn einer Systementwicklung
- **Ziel:** Analyse der gegenseitigen Einflüsse, um ganzheitliche Sicherheit entlang des Systemlebenszyklus zu garantieren (**Safety- und Security-by-Design**)



Failure Mode and Effects Analysis (FMEA) [IEC06b]
Fault Tree Analysis (FTA) [IEC06a]

Klassischer Entwicklungsprozess nach VDI2221

Differenzierte Safety/Security-Maßnahmen entlang des gesamten Entwicklungsprozesses

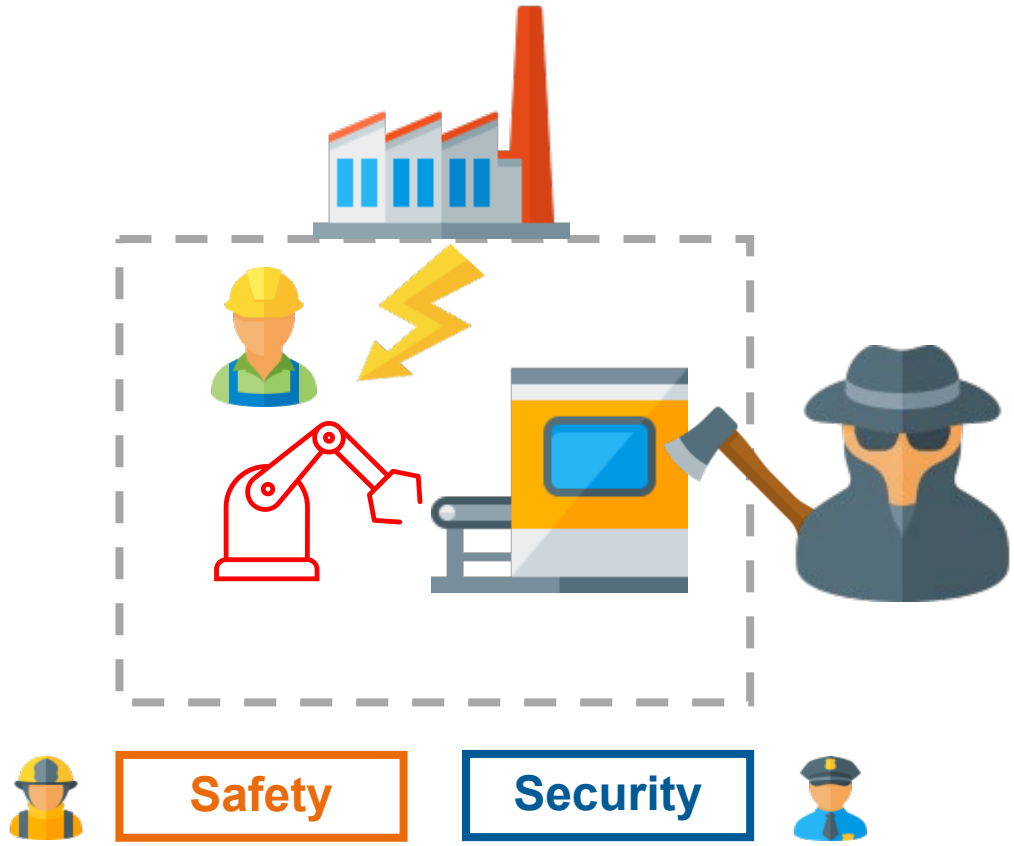


Probleme

- Differenzierte Betrachtung von Safety- und Security-Aspekten
- Hohe Kosten und lange Entwicklungszeiten
- Viele sicherheitstechnische Überschneidungen werden erst spät erkannt

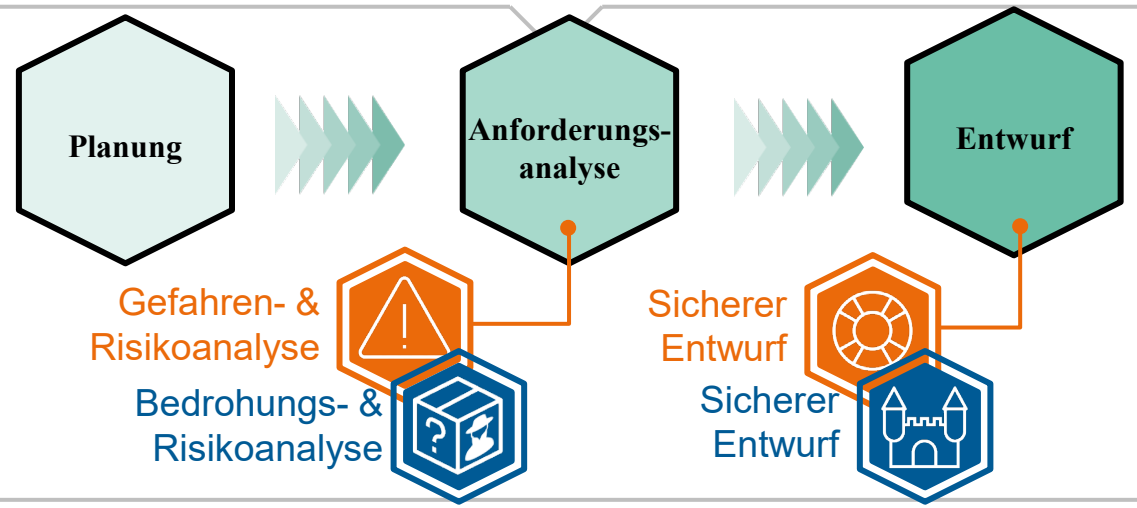
Safety- und Security-by-Design – Frühzeitige integrierte Safety- und Security-Risikoanalyse für (CPS)

Ausgangssituation und Projektziel



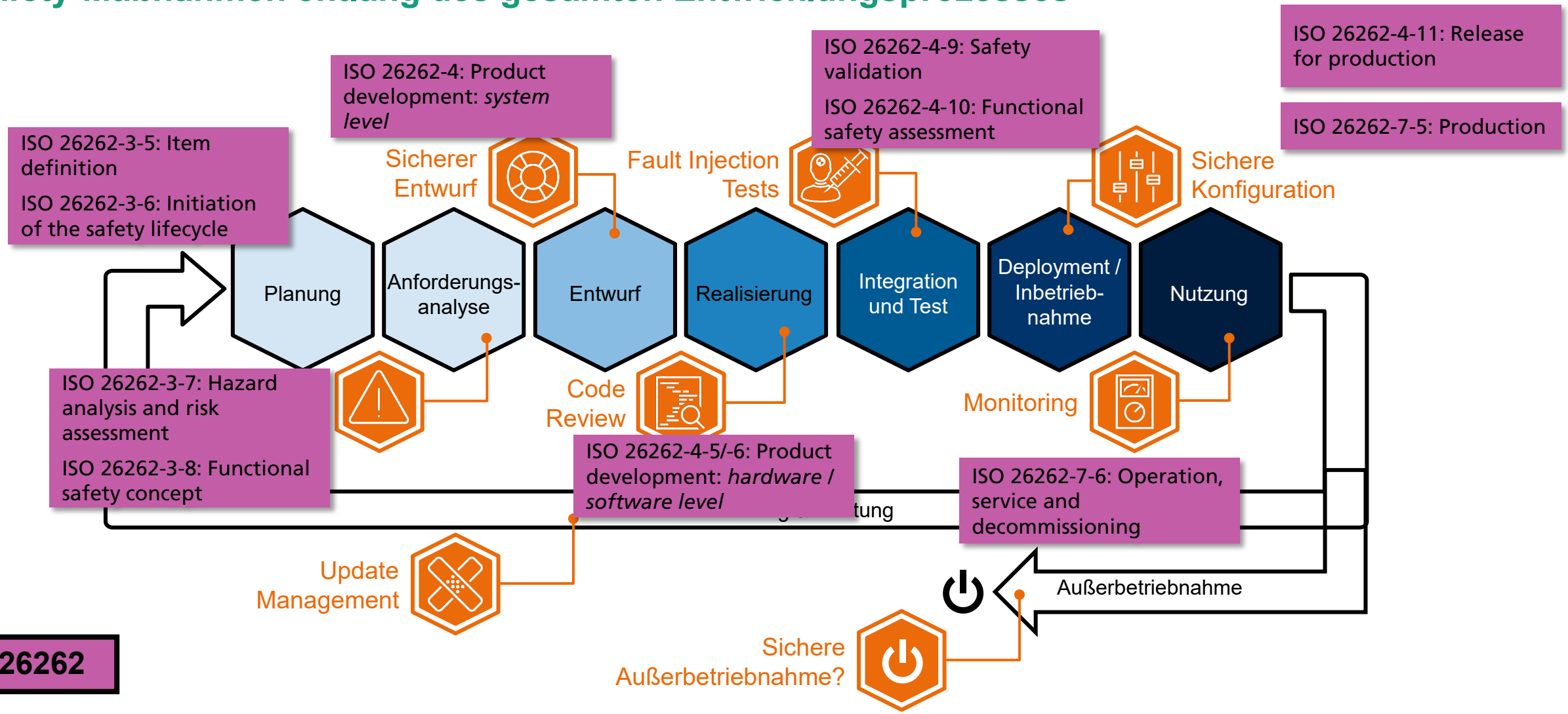
Projektziele

- Unterstützung der frühen Phase der Entwicklung von CPS durch eine integrierte Safety- & Security-Risikoanalyse
- Eine werkzeugunterstützte Methode soll Konflikte beider Welten aufdecken und Synergieeffekte nutzbar machen
- Orientierung an den Bedarfen der Industrie



Lebenszyklus betriebssicherer Hard-/Software (Safety by Design)

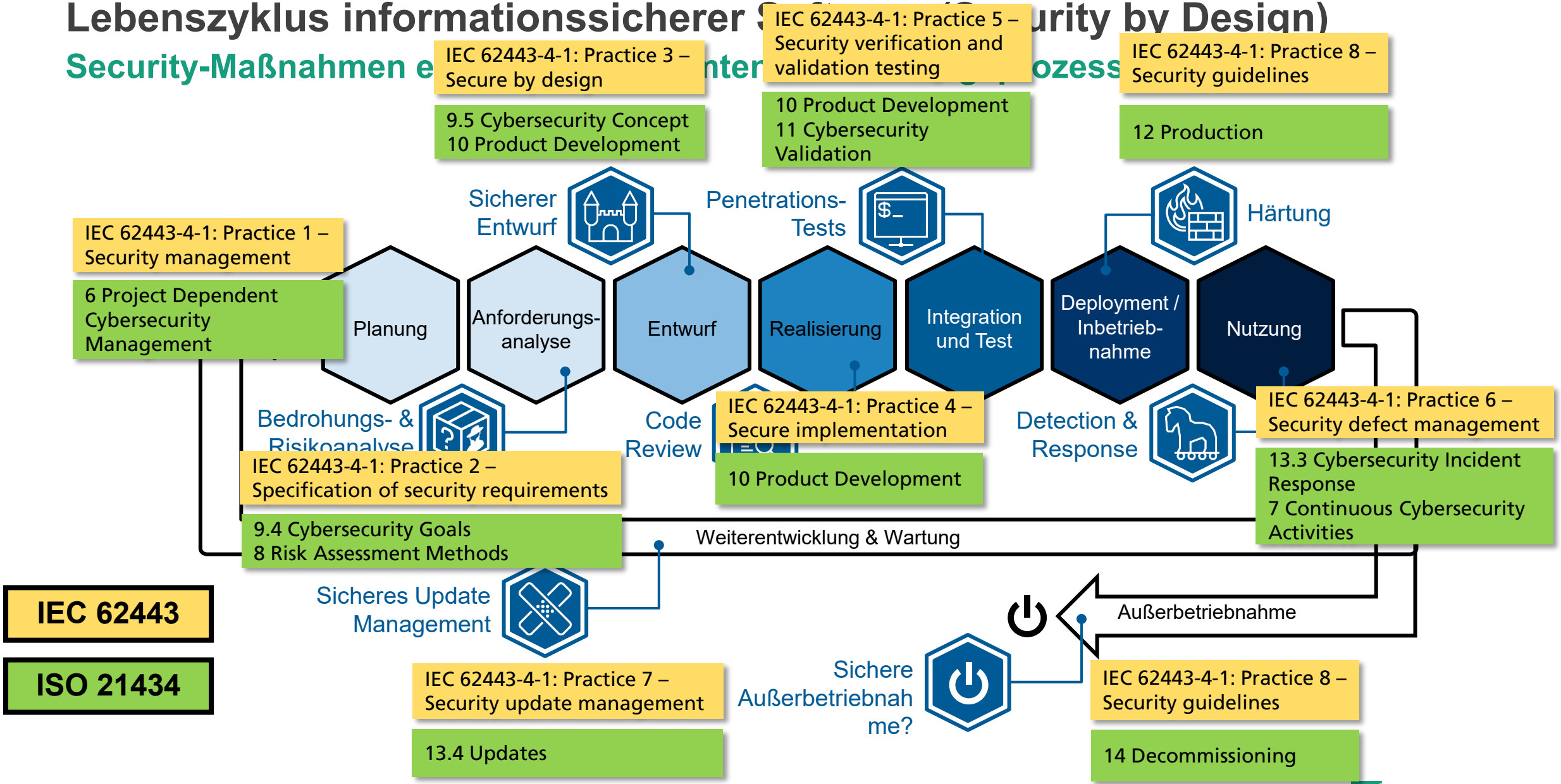
Safety-Maßnahmen entlang des gesamten Entwicklungsprozesses



ISO 26262

Lebenszyklus informationssicherer S urity by Design)

Security-Maßnahmen e nter ozess

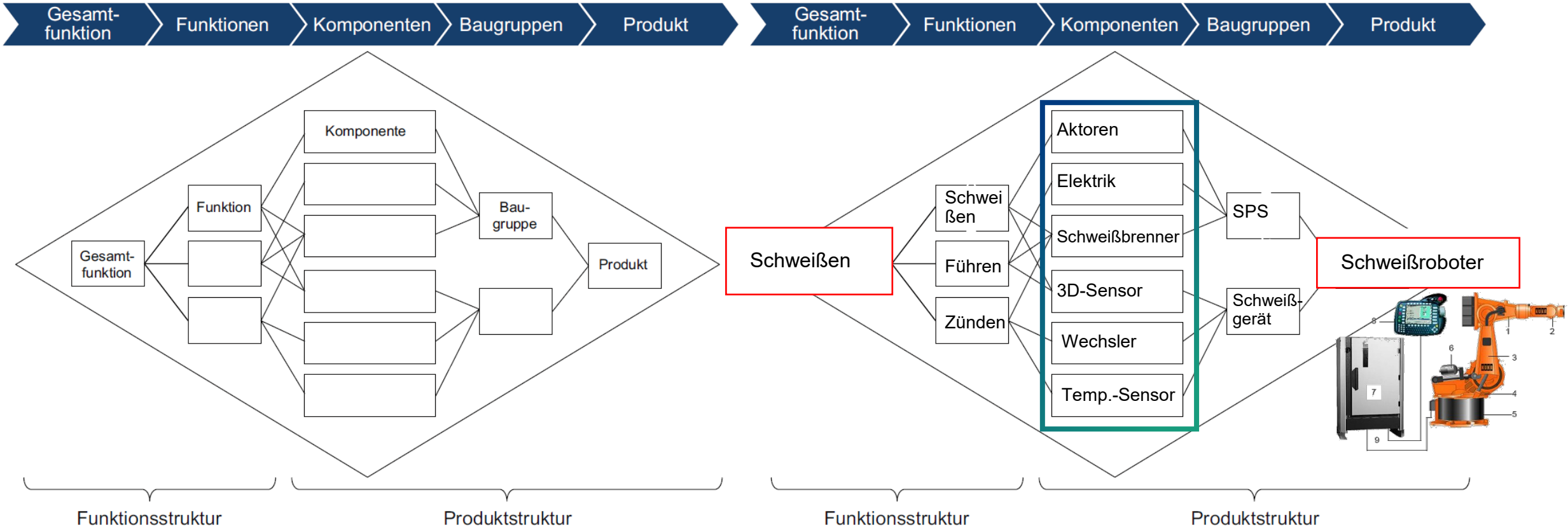


HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

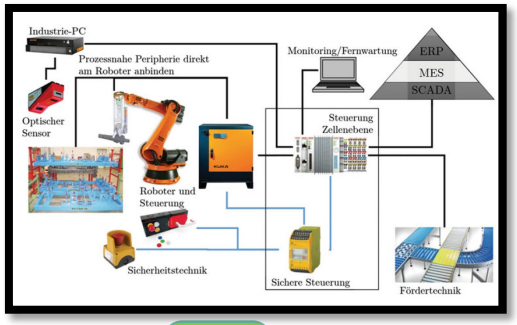
Kollaborierende Roboter

Funktions-/Wirkstruktur nach VDI2221



Kollaborierende Roboter

Strukturbaum



Service Rechner

WWW

WLAN-Modul

Zentraler Rechner

SPS Rechner

Tasten

Datenbank

Safety

Controller Roboter

Controller Portal

Controller Schweißgerät

Controller Messtechnik

Technischer Prozess

FMEA

Safety

Security

FTA

Trust Boundary

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Tool-gestützte Analyse

Programmablauf (Threat Dragon)

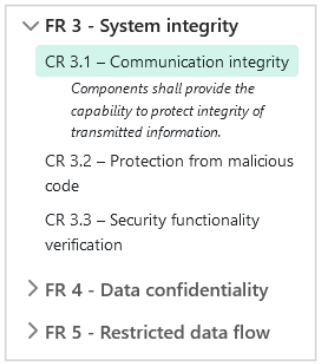
Threat Generation Expressions:

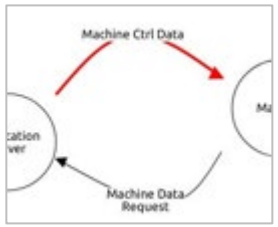
Generation expressions determine when an instance of a threat type gets created for a threat model. An example of generation expression is: flow.[Authenticates Destination] is 'Yes'.

Include: target is [Generic Physical Medical Component] and (flow crosses [Generic Trust Line Boundary] or flow crosses [Generic Trust Border Boundary])

Exclude: flow.[Provides Integrity] is 'Yes'

Alle CRs auflisten → CR auswählen, Modell highlighten → GSN Goal erstellen: „CR X umsetzen“ → Gegenmaß-nahmen (Properties) vorschlagen → Properties im DFD ändern → GSN Nodes hinzufügen → Threats generieren





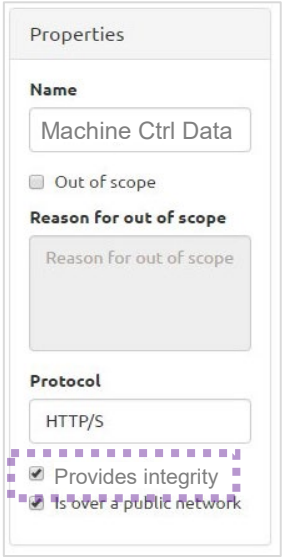
Prevent modification of data on *machine ctrl data*

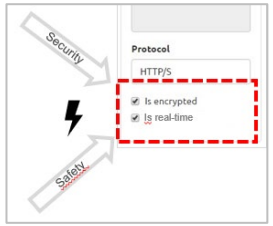
IEC 62443-4-2

CR 3.1 – Communi-cation integrity

Potential Architectural Enhancements:

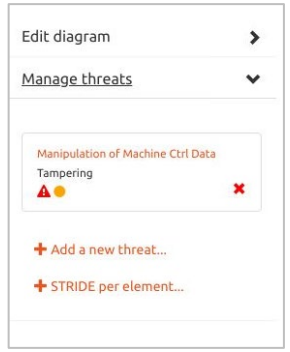
- Change property „*Provides integrity*“ to „*true*“





...

Data flow „*Machine Ctrl Data*“ provides integrity



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

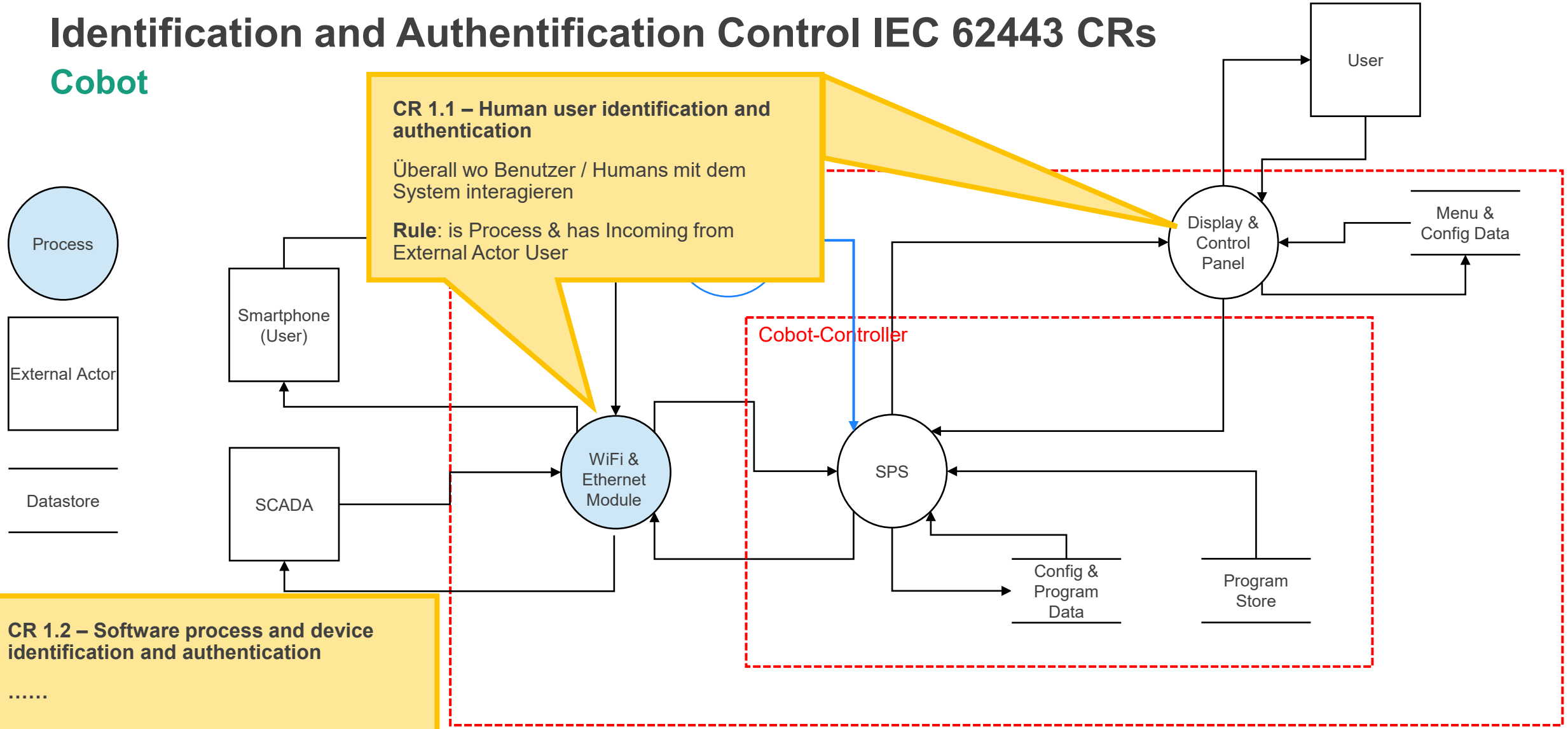
Identification and Authentification Control IEC 62443 CRs

Cobot

CR 1.1 – Human user identification and authentication

Überall wo Benutzer / Humans mit dem System interagieren

Rule: is Process & has Incoming from External Actor User



CR 1.2 – Software process and device identification and authentication

……

……

CR 1.13 – Access via untrusted networks

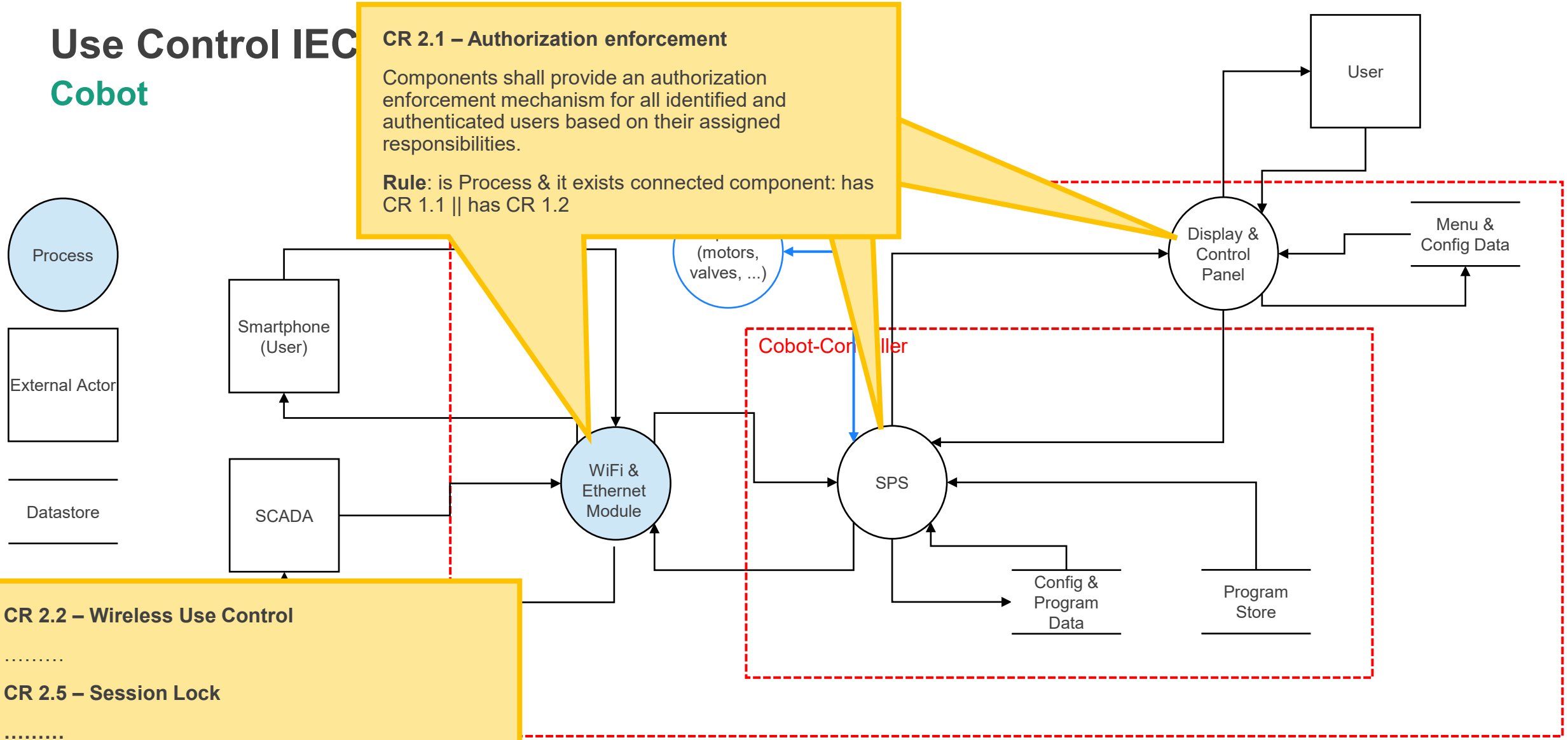
Use Control IEC

Cobot

CR 2.1 – Authorization enforcement

Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.

Rule: is Process & it exists connected component: has CR 1.1 || has CR 1.2



CR 2.2 – Wireless Use Control

……

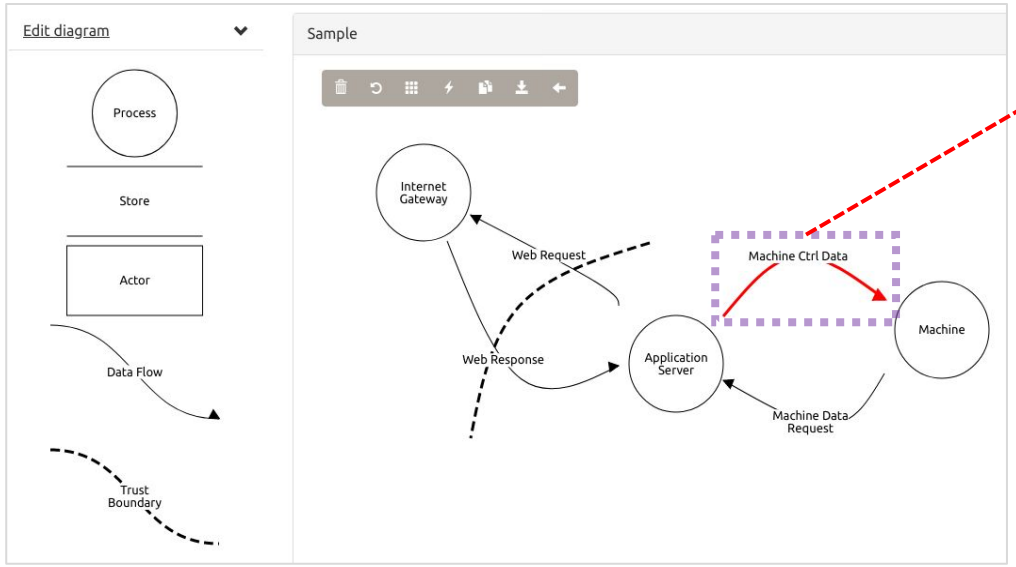
CR 2.5 – Session Lock

……

CR 2.11 – Timestamps

Threat Dragon und IEC 62443-4-2

Auflistung von vorgeschriebenen Anforderungen aus relevanten Normen



Goal Structuring Notation (GSN) [1]

Tampering Threat #42:
„Manipulation of machine control data"

Cyber Security Goal:
"Provide the capability to protect the integrity of machine control data"

Cyber Security Control:
"Encrypt data flow *machine ctrl data"*

Threat *„Manipulation of machine control data"* is prevented

The integrity of *machine ctrl data* is protected

IEC 62443-4-2

CR 3.1 – Communication integrity

Use an encrypted communication channel

Justification: Encryption provides integrity

The data flow *machine ctrl data* is encrypted

Sicherheitsnachweis:

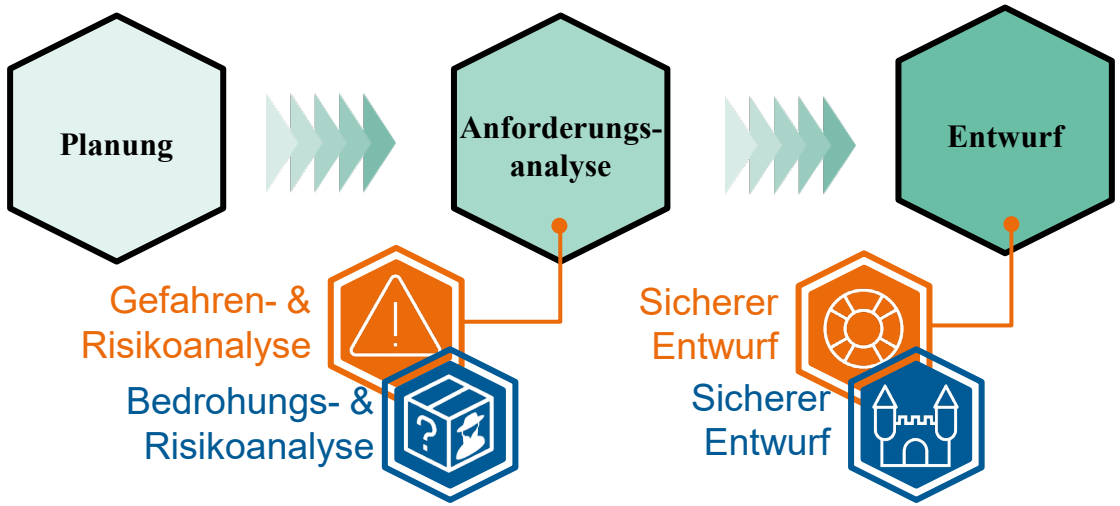
Maschinendaten können nicht auf dem Weg vom Application Server zur Maschine **manipuliert werden (Threat #42),** weil die **Integrität der Daten geschützt** wird, indem eine **verschlüsselte Verbindung** zur Übertragung genutzt wird (und Verschlüsselung Integrität sicherstellt).

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Zusammenfassung und Ausblick

- Safety- und Security-Risikoanalyse ist ein wichtiger Baustein für eine sichere Entwicklung von CPS
- Intelligente und intuitive Werkzeuge sind wichtig, um Zusammenhänge und Wechselwirkungen zwischen Gefahren und Bedrohungen, Gegenmaßnahmen sowie Safety- und Security-Anforderungen zu berücksichtigen und den Entwicklungsprozess systematisch zu assistieren.
- Viele Unternehmen müssen in ihrer Produktentwicklung größere Sorgfalt auf die IT-Sicherheit legen. Dies geht aus einer Umfrage des Fraunhofer IEM hervor. Das Forschungsinstitut entwickelt ein Werkzeug, um Betriebe dabei zu unterstützen.
- Validierung an Use-Cases (z.B. automatisiertes Schweißen mit Cobots)



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Kontakt

Dr.-Ing. Christian Henke

Fraunhofer IEM
Zukunftsmeile 1
33102 Paderborn
Tel +49 5251 5465 -126
christian.henke@iem.fraunhofer.de
www.iem.fraunhofer.de

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer
IEM

Vielen Dank für Ihre Aufmerksamkeit