SOTIF

Bedeutung der Sollfunktion für die Serienentwicklung

Dipl.-Ing (FH) Peter Krumbach, Dr.-Ing. René S. Hosse | ACI Mobility 2021 | 22. September 2021

Engineering und Software-Entwicklung

ESE Engineering und Software-Entwicklung GmbH

Part of DB E.C.O. Group

Engineering und Software-Entwicklung

364

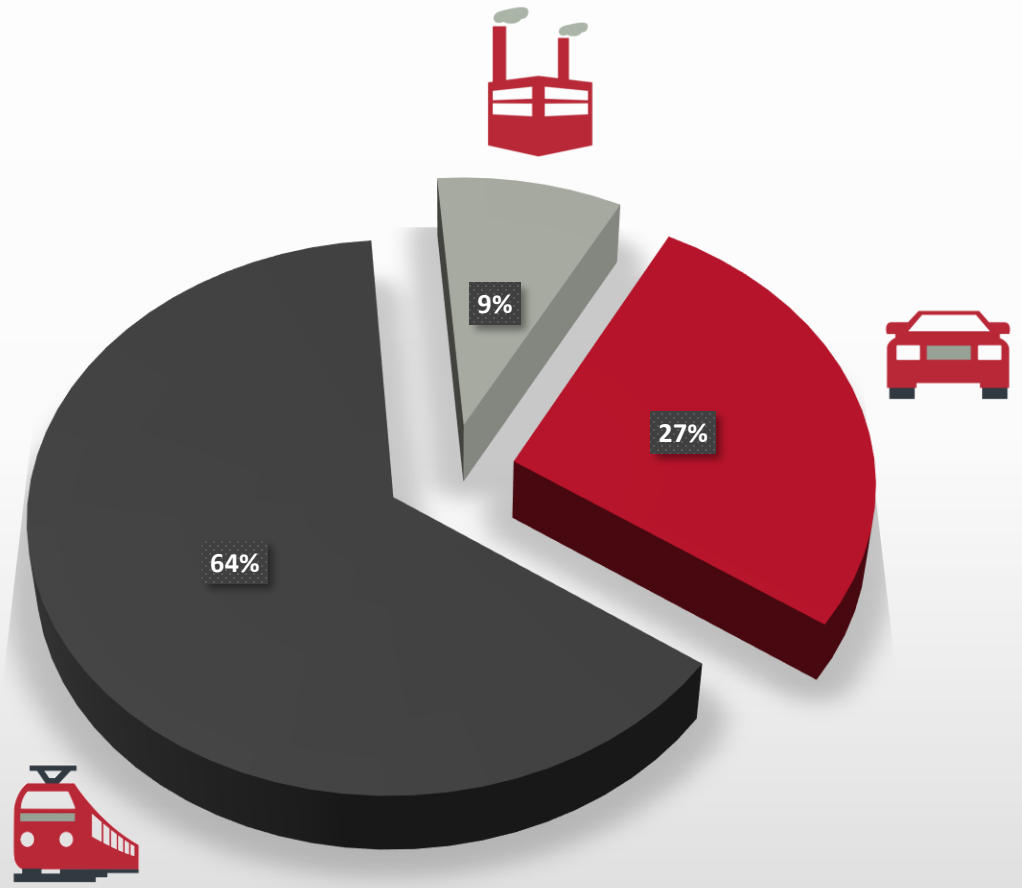
MITARBEITER

24 Jahre Erfahrung

7 Standorte

7 Geschäftsfelder

31,7 MIO. EURO UMSATZ



Agenda

Engineering und Software-Entwicklung

1. Motivation und Zielsetzung des Beitrags
2. Vorstellung des aktuellen Normvorhabens ISO 21448
3. Konzept zur strukturierten Erarbeitung der Sollfunktion

Agenda

Engineering und Software-Entwicklung

1. Motivation und Zielsetzung des Beitrags
   - **Differenzierung zwischen Funktionaler Sicherheit, SOTIF, Cybersecurity**
   - Missmatch zwischen Entwicklungsaufwendungen und Unfallzuordnung
   - Abgrenzung zwischen „Zu erwartender Fehlgebrauch“ und „Missbrauch“

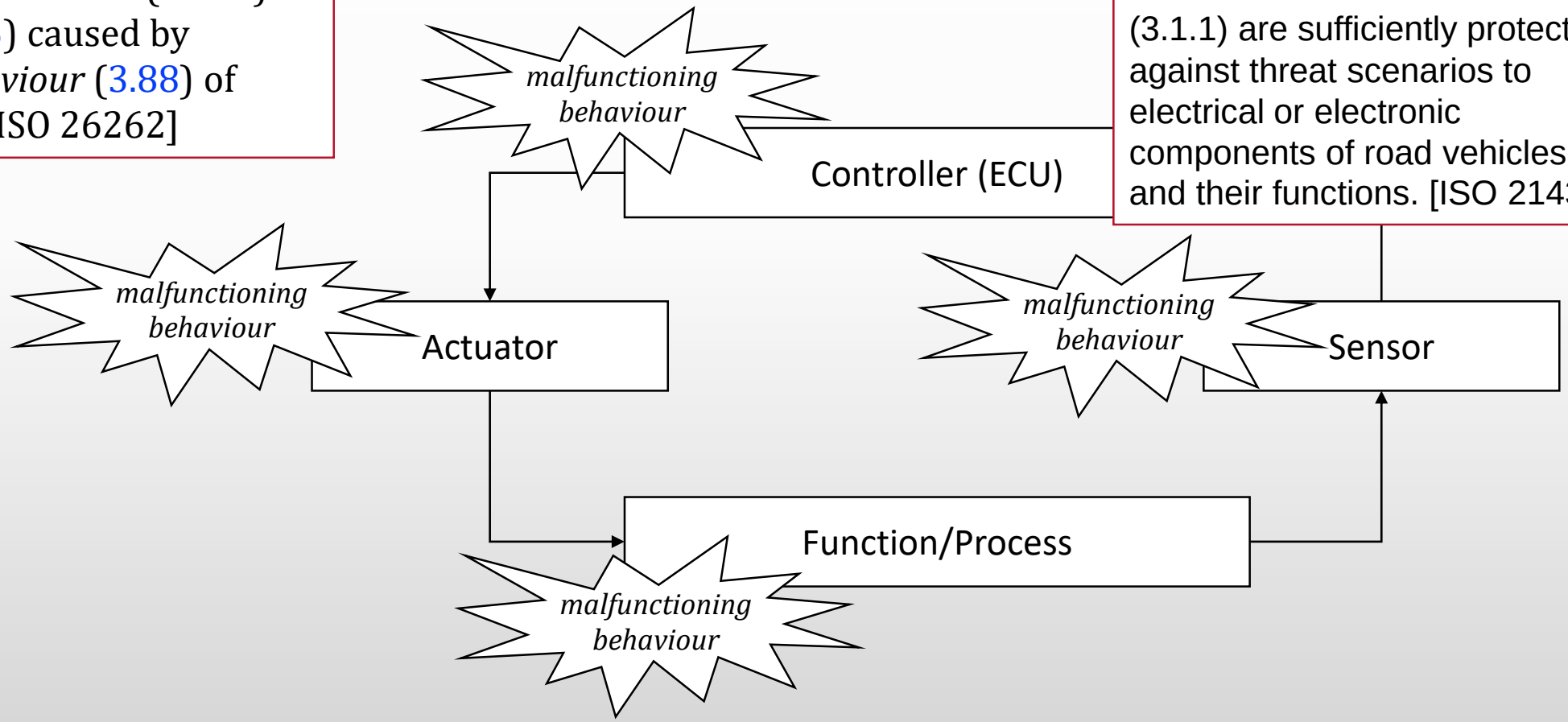
2. Vorstellung des aktuellen Normvorhabens ISO 21448

3. Konzept zur strukturierten Erarbeitung der Sollfunktion

Differenzierung zwischen Funktionaler Sicherheit, SOTIF, Cyber Security

Definition 3.67
functional safety
absence of *unreasonable risk* (3.176) due to *hazards* (3.75) caused by *malfunctioning behaviour* (3.88) of *E/E systems* (3.40) [ISO 26262]

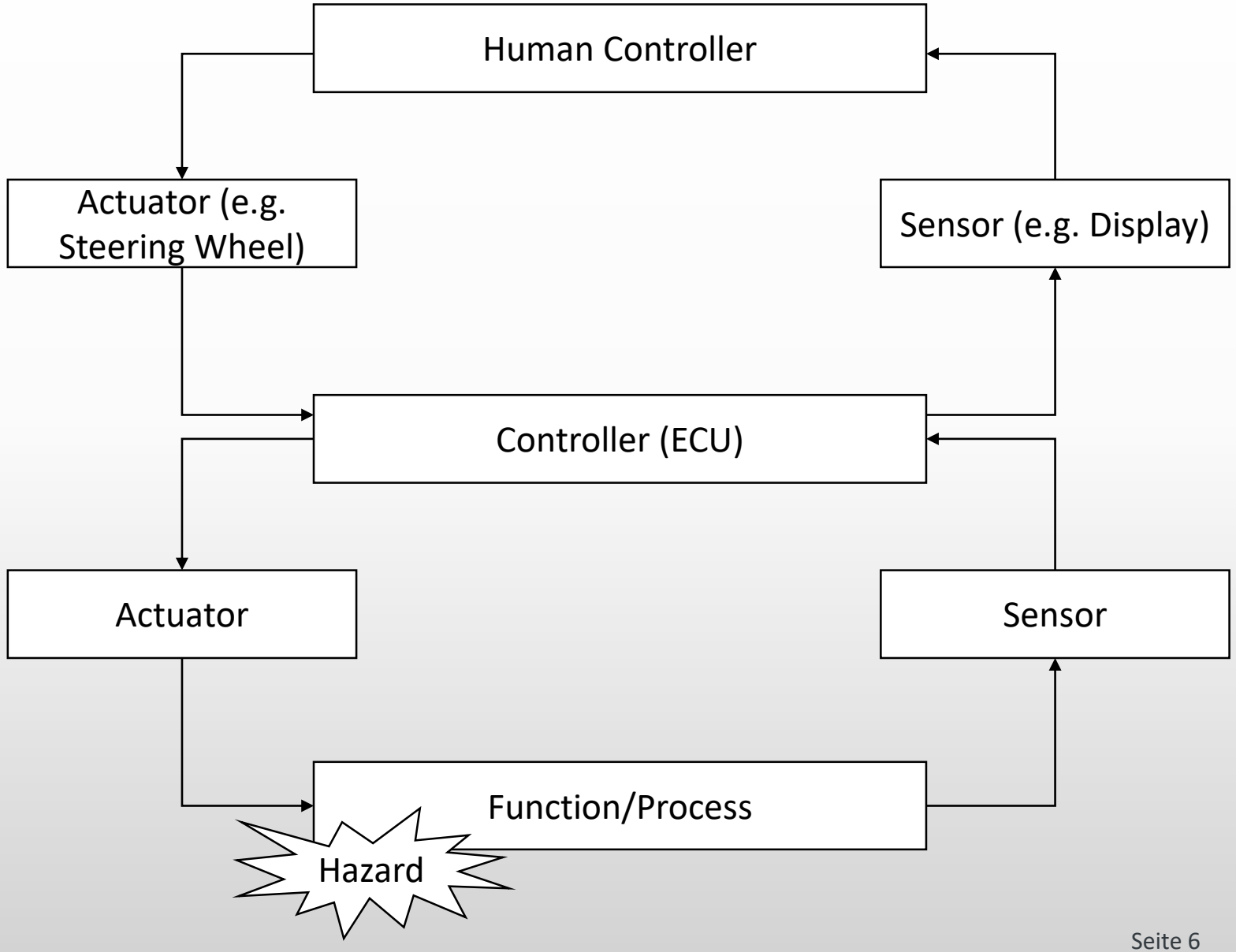
Definition 3.1.8
CYBERSECURITY
Road Vehicle Cybersecurity
Condition in which *assets* (3.1.1) are sufficiently protected against threat scenarios to electrical or electronic components of road vehicles and their functions. [ISO 21434]



Differenzierung zwischen Funktionaler Sicherheit, SOTIF, Cyber Security

Engineering und Software-Entwicklung

Definition: 3. 10 Safety Of The Intended Functionality SOTIF
absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by persons [ISO 21448]



Agenda

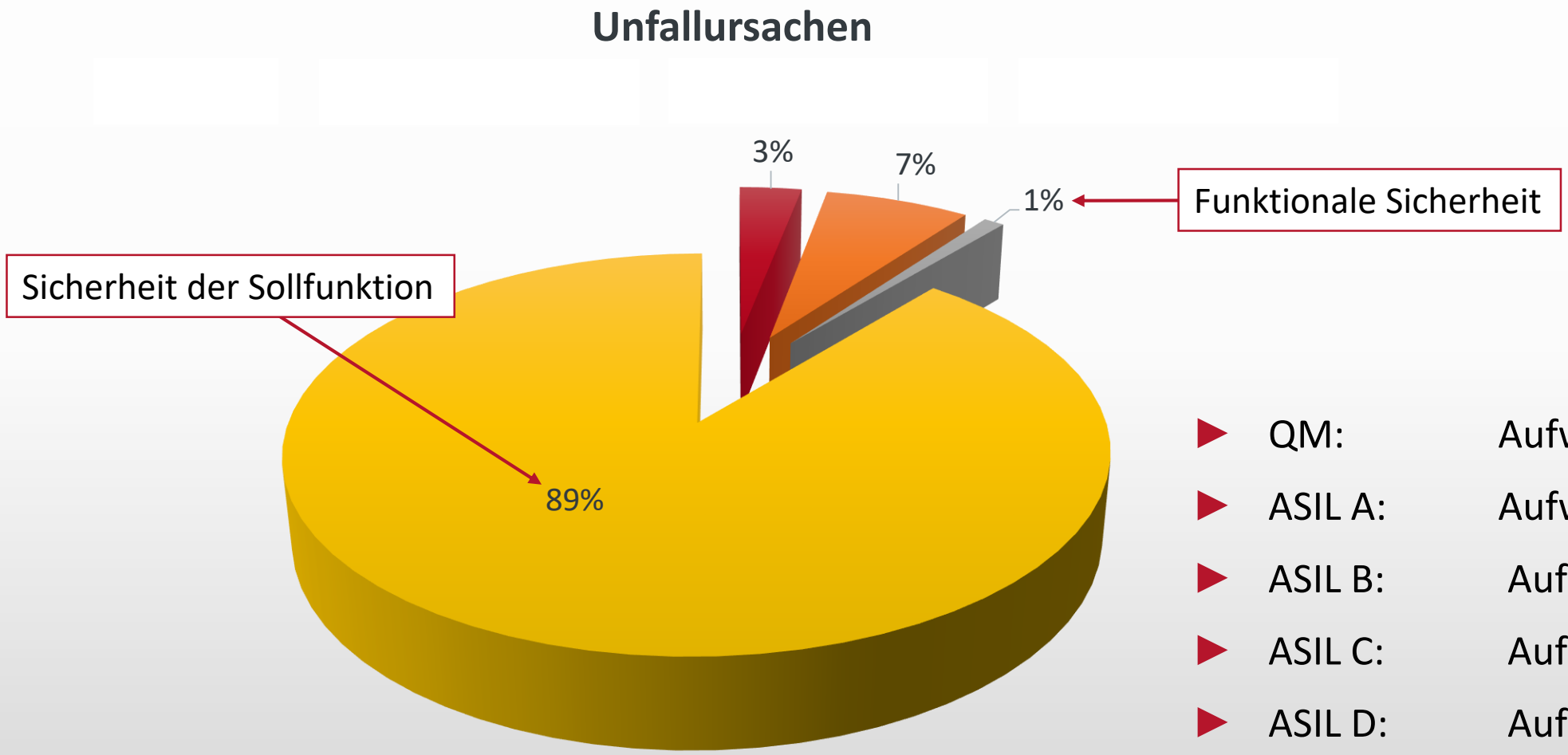
Engineering und Software-Entwicklung

1. Motivation und Zielsetzung des Beitrags
   - Differenzierung zwischen Funktionaler Sicherheit, SOTIF, Cybersecurity
   - **Missmatch zwischen Entwicklungsaufwendungen und Unfallzuordnung**
   - Abgrenzung zwischen „Zu erwartender Fehlgebrauch“ und „Missbrauch“

2. Vorstellung des aktuellen Normvorhabens ISO 21448

3. Konzept zur strukturierten Erarbeitung der Sollfunktion

Missmatch zwischen Entwicklungsaufwendungen und Unfallzuordnung



- QM: Aufwandsfaktor 1,0
- ASIL A: Aufwandsfaktor 1,5
- ASIL B: Aufwandsfaktor 2,0
- ASIL C: Aufwandsfaktor 3,5
- ASIL D: Aufwandsfaktor 5,0

[destatis 2018]

Agenda

Engineering und Software-Entwicklung

1. Motivation und Zielsetzung des Beitrags
   - Differenzierung zwischen Funktionaler Sicherheit, SOTIF, Cybersecurity
   - Missmatch zwischen Entwicklungsaufwendungen und Unfallzuordnung
   - **Abgrenzung zwischen „Zu erwartender Fehlgebrauch“ und „Missbrauch“**

2. Vorstellung des aktuellen Normvorhabens ISO 21448

3. Konzept zur strukturierten Erarbeitung der Sollfunktion

Definitionen gemäß Normen

Engineering und Software-Entwicklung

- **ISO PAS 21448** Misuse

  Usage of the System by a human in a way not intended by the manufacturer of the System

  Note 1:Misuse can result from overconfidence in the performance of the System.

  Note 2:Misuse includes human behavior that is not specified but does not include deliberate System alterations.

- **ISO 14971** (Vorhersehbarer Missbrauch)

  Verlangt von den Herstellern, den ‚vernünftigerweise vorhersehbaren Missbrauch zu dokumentieren'. Was die Norm darunter versteht, verrät sie nur in einer Anmerkung:

  „ANMERKUNG 1 In diesem Zusammenhang ist beabsichtigt, dass der Begriff Missbrauch eine fehlerhafte oder ungeeignete Anwendung des Medizinproduktes bedeutet."

  Diese Festlegung unterscheidet nicht, ob diese „Anwendung" absichtlich, unabsichtlich, in guter oder in schlechter Absicht erfolgt. Jede fehlerhafte oder ungeeignete Anwendung stellt einen Missbrauch

- **DIN EN 82079-1** (Vorhersehbarer Fehlgebrauch)

  Anwendung eines Produkts in einer Weise, die nicht von Produzent oder Lieferant beabsichtigt ist, die sich jedoch aus vorhersehbarem menschlichen Verhalten ergeben kann.

- **IEC 62366-1** (Anomaler Gebrauch) bewusste, vorsätzliche Handlung oder vorsätzliche Unterlassung einer Handlung, die dem BESTIMMUNGSGEMÄSSEN GEBRAUCH entgegensteht oder ihn verletzt und außerdem außerhalb jeglicher weiterer vernünftiger Mittel der USER INTERFACE-bezogenen RISIKOBEHERRSCHUNG durch den Hersteller liegt'

- **IEC 60601-1** (Vorhersehbarer Missbrauch)

  Die Hersteller müssen sicherstellen, dass die Medizinprodukte die anzuwendenden zutreffenden Anforderungen auch bei vorhersehbarem Missbrauch erfüllen.

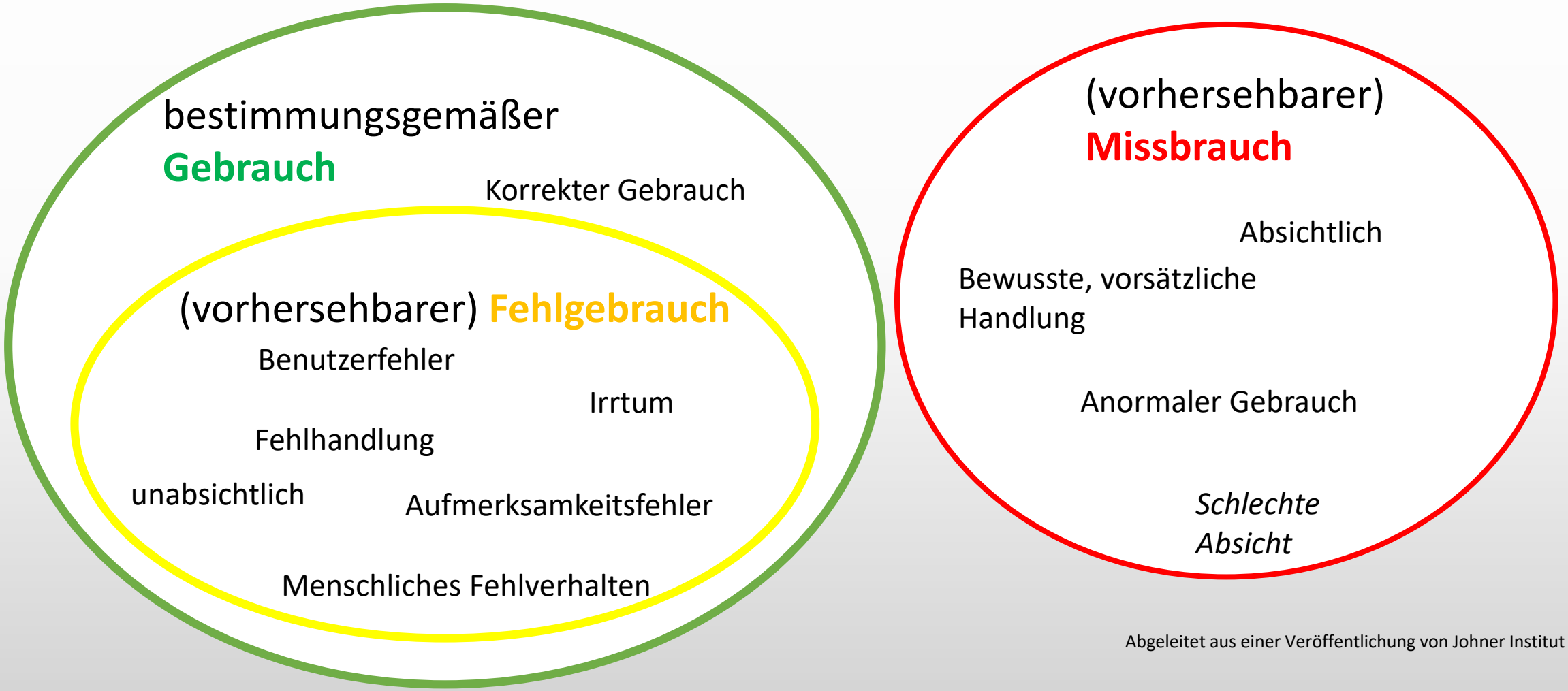
Abgeleitet aus einer Veröffentlichung von Johner Institut GmbH

Abgrenzung zwischen „Zu erwartender Fehlgebrauch“ und „Missbrauch“

Engineering und Software-Entwicklung

Innerhalb der Produkthaftung

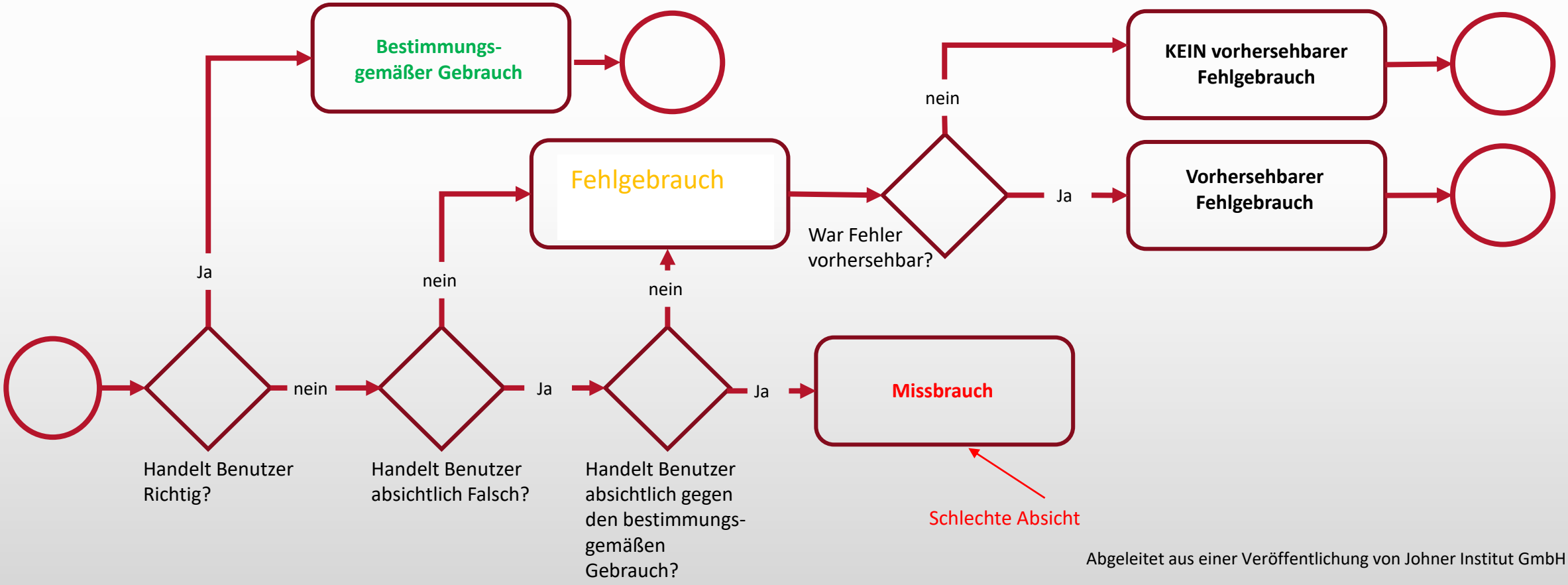
Außerhalb der Produkthaftung



Abgeleitet aus einer Veröffentlichung von Johner Institut GmbH

Abgrenzung zwischen „Zu erwartender Fehlgebrauch“ und „Missbrauch“

Engineering und Software-Entwicklung



Abgeleitet aus einer Veröffentlichung von Johner Institut GmbH

Agenda

Engineering und Software-Entwicklung

1. Motivation und Zielsetzung des Beitrags

2. Vorstellung des aktuellen Normvorhabens ISO 21448
   - Zielsetzung der Norm
   - Lebenszykluskonzept des Normentwurfs und Zusammenhang zur ISO 26262
   - SWOT Analyse

3. Konzept zur strukturierten Erarbeitung der Sollfunktion

Vorstellung des aktuellen Normvorhabens ISO 21448

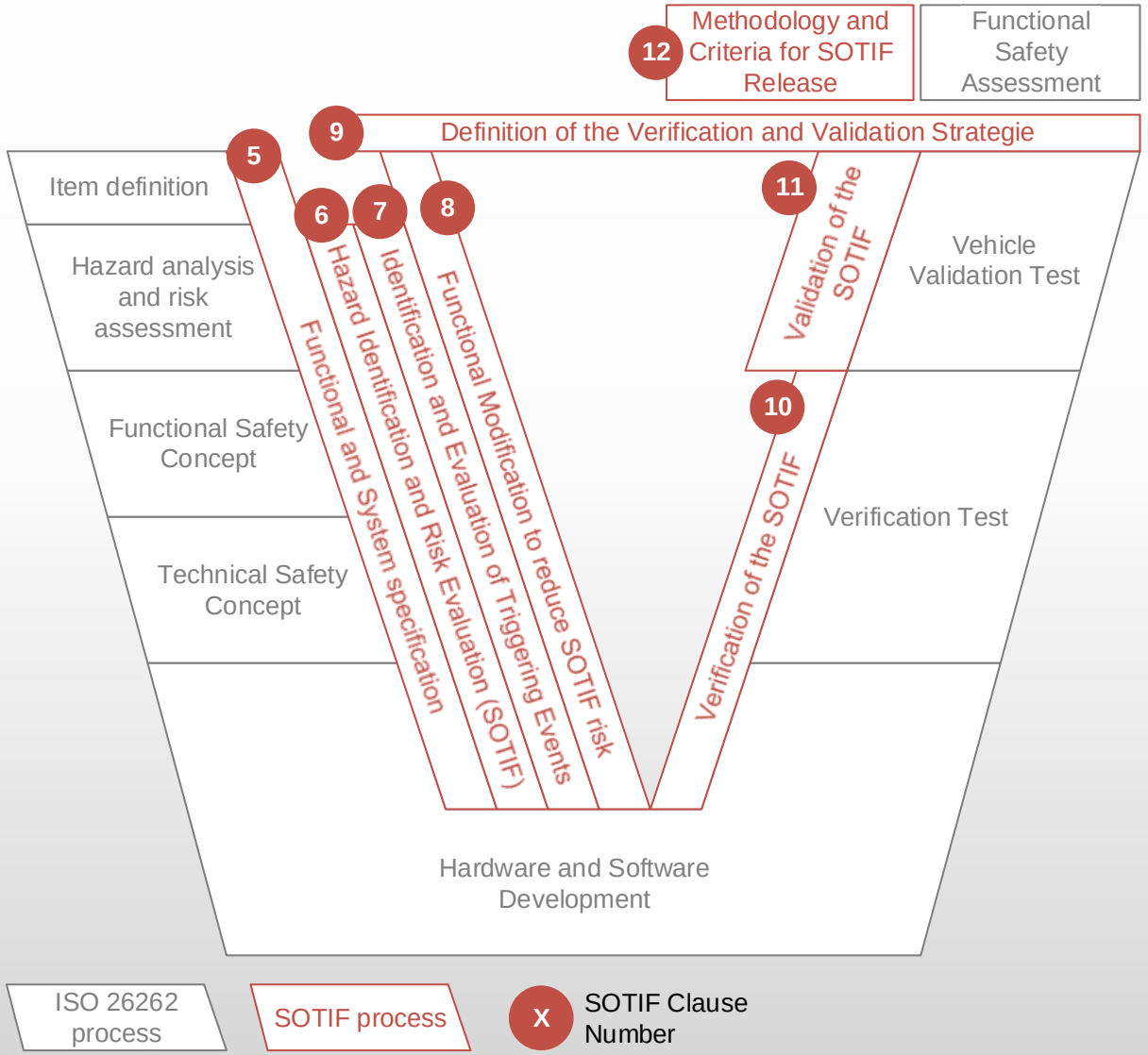
Zielsetzung der Norm

Engineering und Software-Entwicklung

"[ISO 21448] is intended to be applied **to intended functionality** where **proper situational awareness** is **critical to safety**, and where that situational awareness is **derived from complex sensors** and **processing algorithms**; especially emergency intervention systems (e.g. emergency braking systems) and **Advanced Driver Assistance Systems** (ADAS) with **levels 1** and **2** on the OICA/SAE standard J3016 automation scales." [ISO 21448]

Vorstellung des aktuellen Normvorhabens ISO 21448

Lebenszykluskonzept des Normentwurfs und Zusammenhang zur ISO 26262



Vorstellung des aktuellen Normvorhabens ISO 21448

SWOT Analyse

Engineering und Software-Entwicklung

		Analyse des SOTIF-Dokuments	
		Stärken (Strength) ▪ Abrundung des normativen Sicherheitsverständnisses ▪ Höhere Qualität der Sollfunktion möglich	**Schwächen (Weakness)** ▪ Fehlende Quantifizierung des SOTIF Risikos erschwert stringentes Management ▪ Fokus auf „Awareness“ Funktionen
Analyse des Marktumfelds	**Chancen (Opportunities)** ▪ Unfallursachen liegen primär im Fehlgebrauch ▪ Fokus in der Konzeptphase ▪ Gute Sollfunktion fördert Akzeptanz von ADAS und HAF		
	Risiken (Risks) ▪ Parallele Entwicklung verschiedener Normen ▪ Wenig praktische Erfahrung in der strukturierten Erarbeitung der Sollfunktion		

Konzept zur strukturierten Erarbeitung der Sollfunktion

Agenda

Engineering und Software-Entwicklung

1. Motivation und Zielsetzung des Beitrags

2. Vorstellung des aktuellen Normvorhabens ISO 21448

3. **Konzept zur strukturierten Erarbeitung der Sollfunktion**

Konzept zur strukturierten Erarbeitung der Sollfunktion

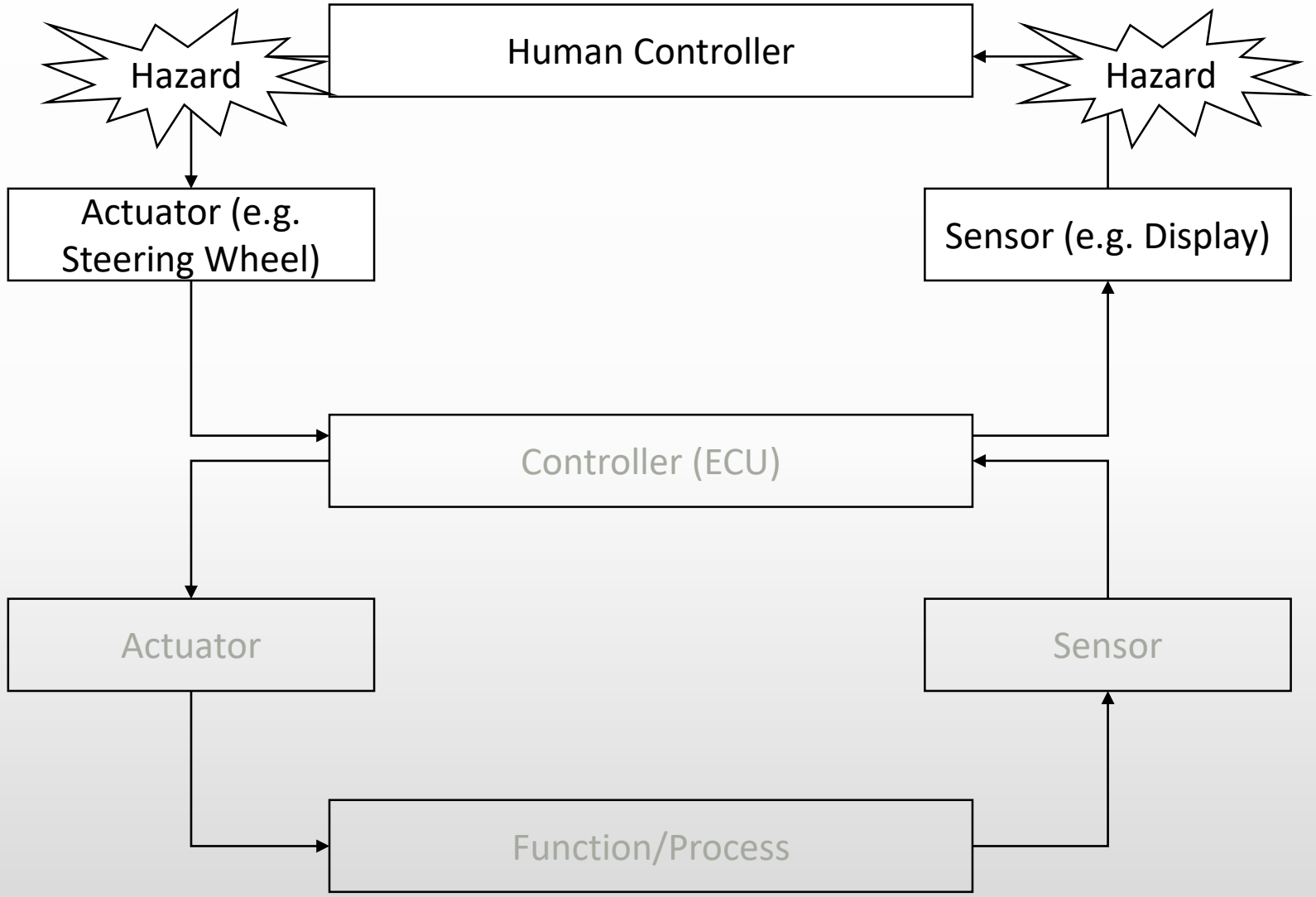
Engineering und Software-Entwicklung

		Analyse des SOTIF-Dokuments	
		Stärken (Strength) ▪ Abrundung des normativen Sicherheitsverständnisses ▪ Höhere Qualität der Sollfunktion möglich	**Schwächen (Weakness)** ▪ Fehlende Quantifizierung des SOTIF Risikos erschwert stringentes Management ▪ Fokus auf „Awareness“ Funktionen
Analyse des Marktumfelds	**Chancen (Opportunities)** ▪ Unfallursachen liegen primär im Fehlgebrauch ▪ Primärer Fokus in der Konzeptphase ▪ Gute Sollfunktion fördert Akzeptanz von ADAS und HAF	▪ Fokussierung der Sollfunktion auf die Konzeptphase ▪ **Integration des Menschen als Funktionsbestandteil in die SOTIF-Analyse**	▪ **Überdenken einer Quantifizierung für das Risiko der Sollfunktion in Anlehnung an ASIL (E, C, S)** ▪ **Erweiterung des Scopes auf alle Funktionen (Bestandsfunktionen) im Fahrzeug**
	Risiken (Risks) ▪ Parallele Entwicklung verschiedener Normen ▪ Wenig praktische Erfahrung in der strukturierten Erarbeitung der Sollfunktion	▪ Vervollständigen des SOTIF Lebenszyklus zu einem Engineering Lebenyzklus (Plan, Do, Act, Check) über alle Entwicklungsphasen	▪ Erarbeitung der Relevant der Sollfunktion für HW, SW und Mechanik-Komponenten

Konzept zur strukturierten Erarbeitung der Sollfunktion

Integration des Menschen als Funktionsbestandteil in die SOTIF-Analyse

- Ergänzung des Fahrers als (Ausfall-)Funktion im Rahmen der SOTIF-HARA
- Quantifizierung der menschlichen Zuverlässigkeit zur ASIL-Einstufung
- Erweiterung des Funktionalen Sicherheitskonzepts um den Fahrer, Definition von Sicherheitsfunktionen



Konzept zur strukturierten Erarbeitung der Sollfunktion

Engineering und Software-Entwicklung

Überdenken einer Quantifizierung für das Risiko der Sollfunktion in Anlehnung an ASIL (E, C, S)

- **E** (?)
- **C** (ab Automatisierungslevel L3 für hochautomatisiertes Fahren immer „3“)
- **S** (ggf. Sachschaden oder Funktionsverhalten im Sinne Nutzerakzeptanz)

- Der **Grad der Gefährdung** kann in **Anlehnung** dem methodischen Vorgehen einer **HARA** nach **ISO 26262** eingestuft werden, indem man die Kennzahlen der **Schadensschwere** „S“ sowie die **Kontrollierbarkeit** der Schadenabwehr „C“ bewertet.

- Eine **Häufigkeit** der Funktionsnutzung oder ein Quantifizierung über das Befinden in der gefährlichen Situation (Exposition) „E“ ist jedoch **schwer anzuwenden**.
  - Es ist hier eine **Fallunterscheidung** je nach **Szenario** zu bewerten, ob eine **Exposition einen Einfluss** auf die „Hazard Identification and Risk Evaluation“ hat und
  - welche **Eingrenzungen** dieses bei der **Auslegung der Funktion** und dem Prozess mit sich bringt.

Konzept zur strukturierten Erarbeitung der Sollfunktion

Engineering und Software-Entwicklung

Erweiterung des Scopes auf alle Funktionen (Bestandsfunktionen) im Fahrzeug

- Ein **Ungleichgewicht** zwischen **sollfunktionsresultierenden Unfällen** und den von **Systemfehlern** basierten Unfällen, **rechtfertigt** die **Bestandsfunktionen** in einem methodischen Vorgehen in Anlehnung an die SOTIF zu durchleuchten.

- Besonders auch innerhalb der Funktionalen Sicherheit sollte jede (Bestands) Funktion im **Kontext des hochautomatisiertes Fahren** in einer HARA bewertet werden.
  - Ziel sollte es sein, die Nutzung des hochautomatisierten Fahrens in den Situationskatalog mit aufzunehmen.
  - Beispiel: Lenkradheizung

Zusammenfassung

Engineering und Software-Entwicklung

1. Motivation und Zielsetzung des Beitrags
   - Differenzierung zwischen Funktionaler Sicherheit, SOTIF, Cybersecurity
   - Missmatch zwischen Entwicklungsaufwendungen und Unfallzuordnung
   - Abgrenzung zwischen „Zu erwartender Fehlgebrauch“ und „Missbrauch“
2. Vorstellung des aktuellen Normvorhabens ISO 21448
   - Zielsetzung der Norm
   - Lebenszykluskonzept des Normentwurfs und Zusammenhang zur ISO 26262
   - SWOT Analyse
3. Konzept zur strukturierten Erarbeitung der Sollfunktion