

# Tag 1: Fachvorträge

Motto 2024



---

# SILusionen der funktionalen Sicherheit

---

SIL Sprechstunde 2024

18./19.09.2019, Mannheim

Andreas Hildebrandt, Ivo Hanspach

---



# SiLusionen

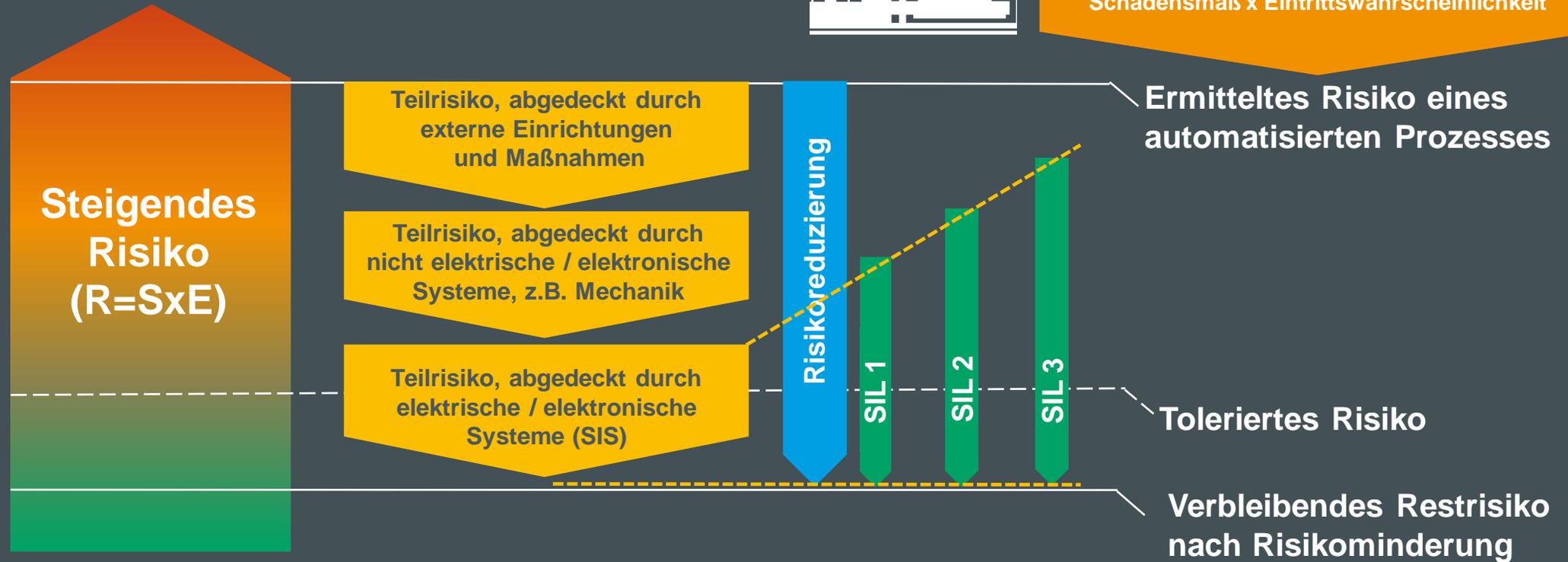


SMART  
SAFETY.

# SIL als Maßnahme zur Risikominderung



Gefahren- und Risikoanalyse  
Schadensmaß x Eintrittswahrscheinlichkeit



# Sicherheits-Integritätslevel

(Safety Integrity Level)



Anforderungsbetriebsart (Low Demand Mode)		
SIL Sicherheits-Integritätslevel (Safety Integrity Level)	PFD avg Mittlere Wahrscheinlichkeit eines gefahr- bringenden Ausfalls bei Anforderung der Sicherheitsfunktion (Probability of failure on demand)	RRF Zielwert für Risikominderung (Risk Reduction Factor)
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	100 to 10
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	1000 to 100
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	10000 to 1000
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	100000 to 10000

## SIL ist

- ..ein Maßstab für die Risikominderung die durch eine Sicherheitsfunktion erreicht werden soll
- ..ein Maßstab für Qualitäts- und Performance-Anforderungen an diese Sicherheitsfunktion

# SILusion #1: „SIL ist eine Geräteeigenschaft“



## 3.5.8

### Sicherheits-Integritätslevel

(en: safety integrity level)

#### SIL

eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

EN 61508 Teil 4

ANMERKUNG 1 Die Ausfallgrenzwerte (siehe 3.5.17) für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 der IEC 61508-1 festgelegt.

ANMERKUNG 2 Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen, die dem sicherheitsbezogenen E/E/PE-System zugeordnet werden, verwendet.

ANMERKUNG 3 Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung der Redensart „sicherheitsbezogenes System mit SIL  $n$ “ (wobei  $n$  1, 2, 3 oder 4 ist) ist, dass das System möglicherweise fähig ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu  $n$  zu unterstützen.

# SILusion #2: “Der SIL steht im Zertifikat”



**Funktionale  
Sicherheit?**

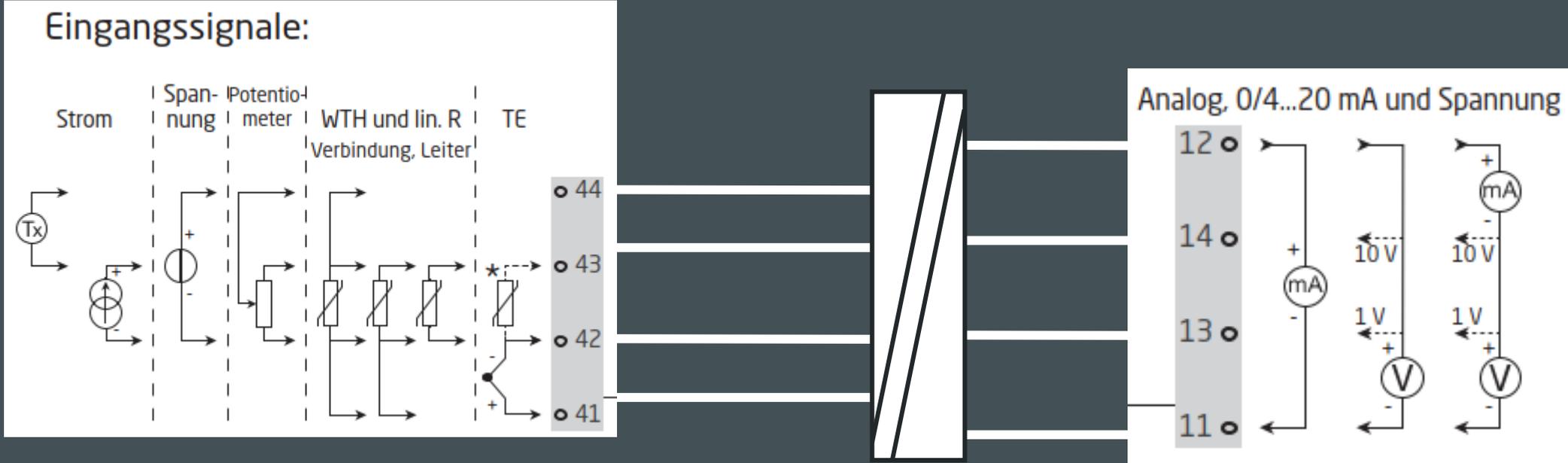
**Die richtigen und wichtigen mitgeltenden Unterlagen beachten!!!**

- TÜV Bericht, TÜV Revisionsliste
- Benutzerhandbuch, Sicherheitshandbuch, Wartungshandbuch, Functional-Safety Datasheet

# Zertifikat vs Benutzerhandbuch (1)



Signaltypen und technische Verschaltungsoptionen eines multifunktionalen Trennschaltverstärkers:



# Zertifikat vs Benutzerhandbuch (1)

## SIL DECLARATION OF CONFORMITY MANUFACTURER DECLARATION

instrumented system up to a Safety Integrity Level of SIL 2<sup>2</sup> if are observed.

The reliability data summarized in the following table are the according to IEC61508 carried out on the [redacted] Univ assessment consists of an FMEDA done by Exida.

[redacted] Universal Transmitters are considered to be a T fault tolerance (HFT) of 0.

	PFH <sup>3</sup> 1/h	PFD <sub>AVG</sub> T[Proof] = 1 year
[redacted]	8.22E-08	3.60E-04
with TC <sup>4</sup>	3.32E-07	1.45E-03
with 4W RTD <sup>4</sup>	1.02E-07	4.46E-04

<sup>1</sup> [redacted]  
<sup>2</sup> [redacted] with 4W RTD: For T[Proof] = 5 year  
TC: For T[Proof] = 1 year

<sup>3</sup> Maximum demand rate: 1.5 h  
<sup>4</sup> Sensor in low-stress environment

## Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the [redacted] Table 1 gives an overview of the different types that belong to the considered transmitter. The [redacted] are DIN rail mounted.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). An FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

**Table 1: Version overview**

[redacted]	Universal transmitter, rail mounted – (Standard Version)
[redacted]	Universal transmitter, [redacted]

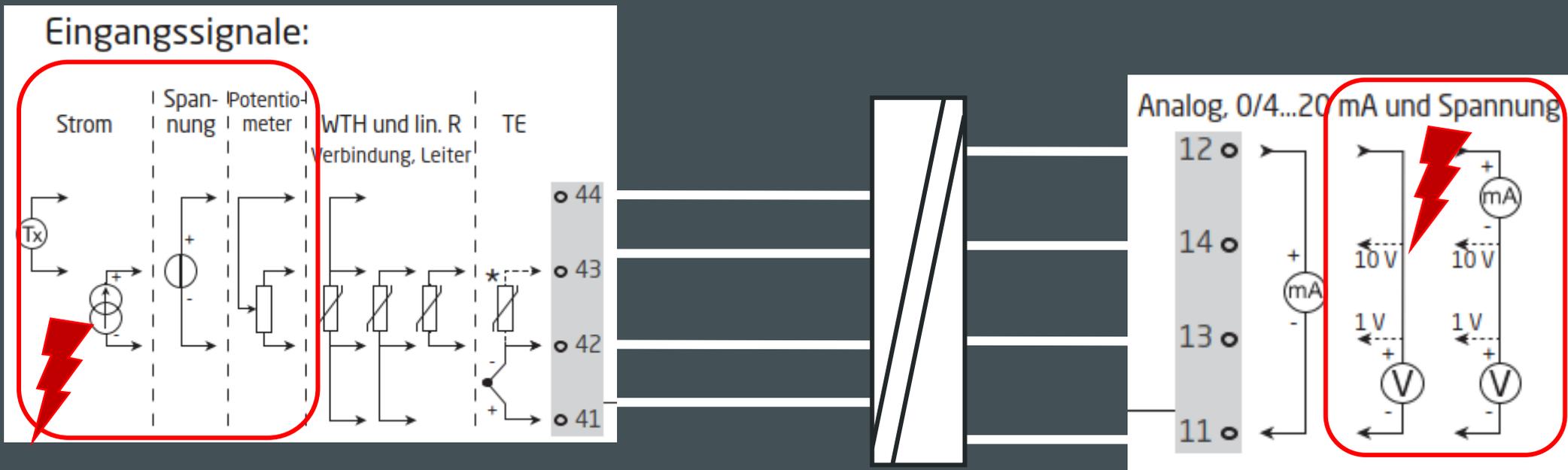
For safety applications only the 4..20 mA c [redacted] the 4..20 mA current of safety applications. All other possible out [redacted] unit.

## Wenn die rote LED in der Front leuchtet / Display zeigt AO.ER

[redacted] SIL-2-Gerät mit einem hohen Sicherheitsniveau entwickelt worden. Deshalb erfolgt eine kontinuierliche Messung des Ausgangs-Stromes bei dem 4...20 mA -Ausgangssignal. Wenn der Strom 0 mA ist, schaltet das Gerät in den Fehler-Modus und die LED-Anzeige leuchtet rot. Diese Funktion ist keine Standard-Option, sondern muss aktiv im Menü ausgewählt werden. Der Fehler-Modus kann nur zurückgesetzt werden durch Aus- und wieder Einschalten der Spannungsversorgung des Gerätes

# Zertifikat vs Benutzerhandbuch (1)

Technische Verschaltung und Signaltypen eines multifunktionalen Trennschaltverstärkers:



=> Die Überprüfung der zugelassenen und betrachteten Betriebsmodi ist für einen Einsatz in SIF unbedingt notwendig!!!

# Zertifikat vs Sicherheitshandbuch (2)

CERTIFICAT

**COMPLIA**  
with IEC EN 61508

<i>E/EE/EP safety-related system (final element)</i>	actuators Rack & Pinion produced by					
<i>System type</i>	Type A					
<i>Size</i>	Type	Type	Type	Type	Type	Type
<i>Safety Function Definition</i>	Complete switching on demand (open to closed & closed to open) with correct torque as for technical data sheets in low demand mode of operation					
<i>Max SIL</i>	SIL 2 with HFT = 0 (single actuator configuration)	SIL3 with HFT = 1 (redundant configuration)	SIL 2 with HFT = 0 (single actuator configuration)	SIL3 with HFT = 1 (redundant configuration)	SIL 2 with HFT = 0 (single actuator configuration)	SIL3 with HFT = 1 (redundant configuration)
<i>Additional requirements for the max SIL classification</i>	Execution of Partial Stroke Test with time interval not higher than 12 months AND Full Functional Proof Test with time interval not higher than 36 months		Execution of Partial Stroke Test with time interval not higher than 4 months AND Full Functional Proof Test with time interval not higher than 18 months		Execution of Partial Stroke Test with time interval not higher than 3 month AND Full Functional Proof Test with time interval not higher than 9 months	
$\lambda_{TOT}$	1,472E-08		4,854E-08		7,939E-07	
$\lambda_{SD}$	9,478E-09		3,126E-08		5,113E-07	
$\lambda_{SU}$	0,000E+00		0,000E+00		0,000E+00	
$\lambda_{DD}$	0,000E+00		0,000E+00		0,000E+00	
$\lambda_{DU}$	5,238E-09		1,728E-08		2,826E-07	
$\lambda_{DU,PST}$	4,346E-09		1,434E-08		2,345E-07	
$\lambda_{DU,FPT}$	8,916E-10		2,941E-09		4,810E-08	
<i>PPFD<sup>(1)</sup></i>	3,075E-05		4,025E-05		4,147E-04	
<i><math>\beta</math> and <math>\beta_D</math> factor</i>	10%		10%		10%	
<i>MTTR</i>	8 h		8 h		8 h	
<i>Hardware Safety Integrity</i>	Route 2 <sub>II</sub>		Route 2 <sub>II</sub>		Route 2 <sub>II</sub>	
<i>Systematic Safety Integrity</i>	Route 2 <sub>S</sub>		Route 2 <sub>S</sub>		Route 2 <sub>S</sub>	

„SIL2 Ventil“ – aber nur mit Partial Stroke Test und vollständigem Test <= 9Monate

# Zertifikat vs Sicherheitshandbuch (3)



## 4. Sicherheitshandbuch/ Safety Manual

Seite 8 von 52

### 4.1. Normengrundlage

- IEC61508 Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Systeme
- IEC61511 Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie
- EN ISO 13849-1 (in Anlehnung) Sicherheitsbezogene Teile von Steuerungen

Mit der Kennzeichnung des Gerätes mit dem CE-Zeichen bestätigt die [REDACTED] die Erfüllung der gesetzlichen Anforderungen der zutreffenden EG-Richtlinien.

Der Schallgeber [REDACTED] erfüllt die Anforderungen an die funktionale Sicherheit nach IEC 61508 bzw. IEC61511.

### 4.2. Besonderheit

Der beschriebene Schallgeber alleine übt keine Schutzfunktion aus (Teilsystem) sondern ist zum Einbau als Ausgabeeinheit mit Diagnose (Output) in den Loop einer Schutzfunktion (SIF) konzipiert. Das Gerät (siehe Abb. 1 und Abb. 2) stellt somit immer nur ein Teilsystem eines sicherheitstechnischen Systems (SIS) dar. Durch den Systemintegrator ist zu beachten, dass der gesamte Loop entsprechend der Anwendung den geforderten SIL-Level erreichen muss. Der Systemintegrator muss alle Maßnahmen festlegen, um im Fehlerfall in der SIS den sicheren Zustand zu erreichen oder aufrechtzuerhalten.

Das Diagnosesystem des Gerätes diagnostiziert bei Anforderung des akustischen Warnsignals dessen Nichtauslösung und Funktion und meldet dieses über ein Alarmrelais an ein übergeordnetes Leitsystem.

## Manufacturer Declaration



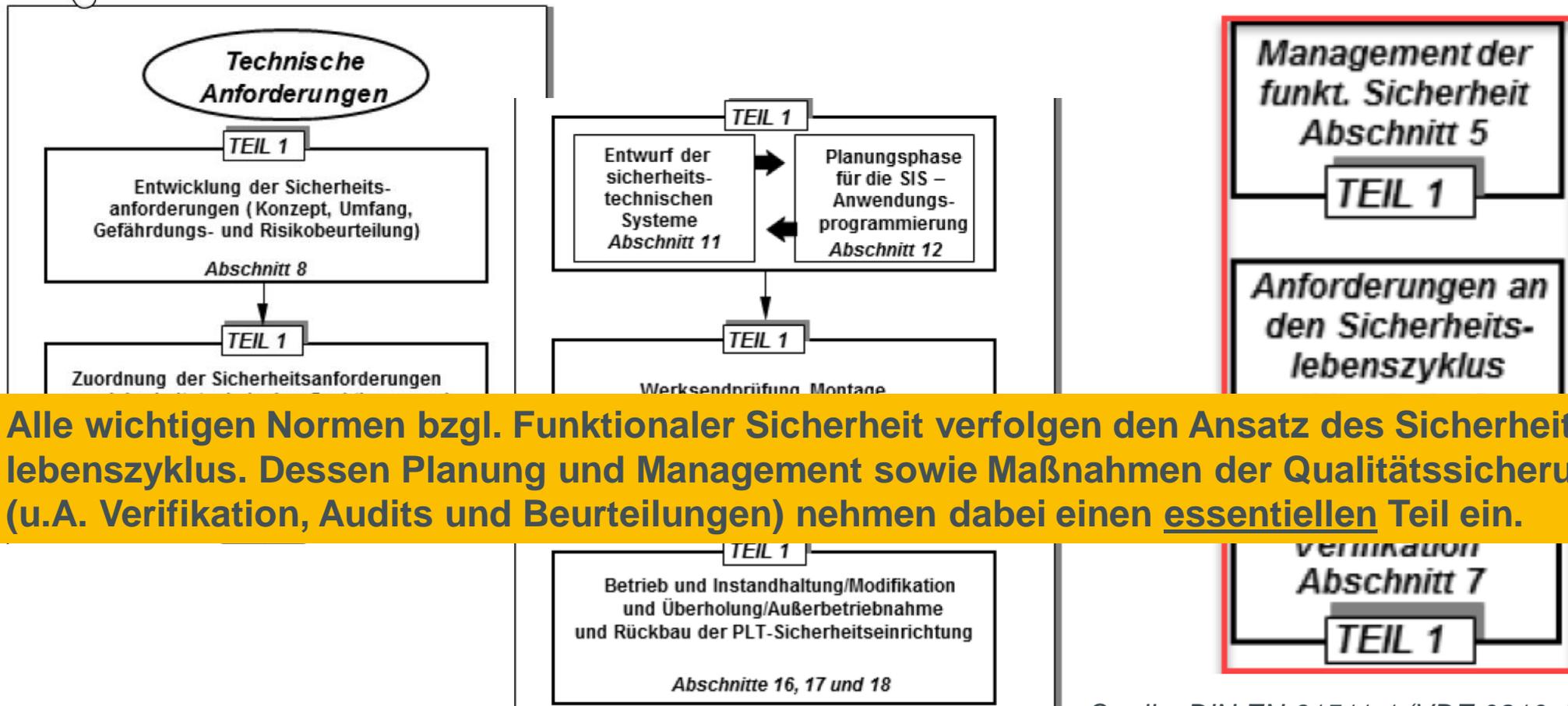
/ IEC 61511 u. IEC 62061 bis zu SIL 2

IEC 61511 a. IEC 62061 up to SIL 2.

Sicherheitshandbuch:  
Manual:

# SILusion #3:

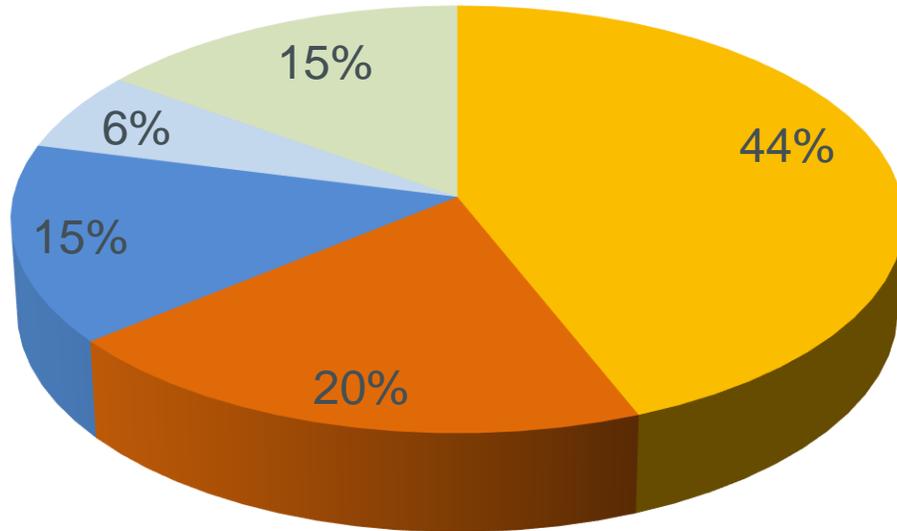
## “SIL Normen beschreiben nur technische Inhalte”



Alle wichtigen Normen bzgl. Funktionaler Sicherheit verfolgen den Ansatz des Sicherheitslebenszyklus. Dessen Planung und Management sowie Maßnahmen der Qualitätssicherung (u.A. Verifikation, Audits und Beurteilungen) nehmen dabei einen essentiellen Teil ein.

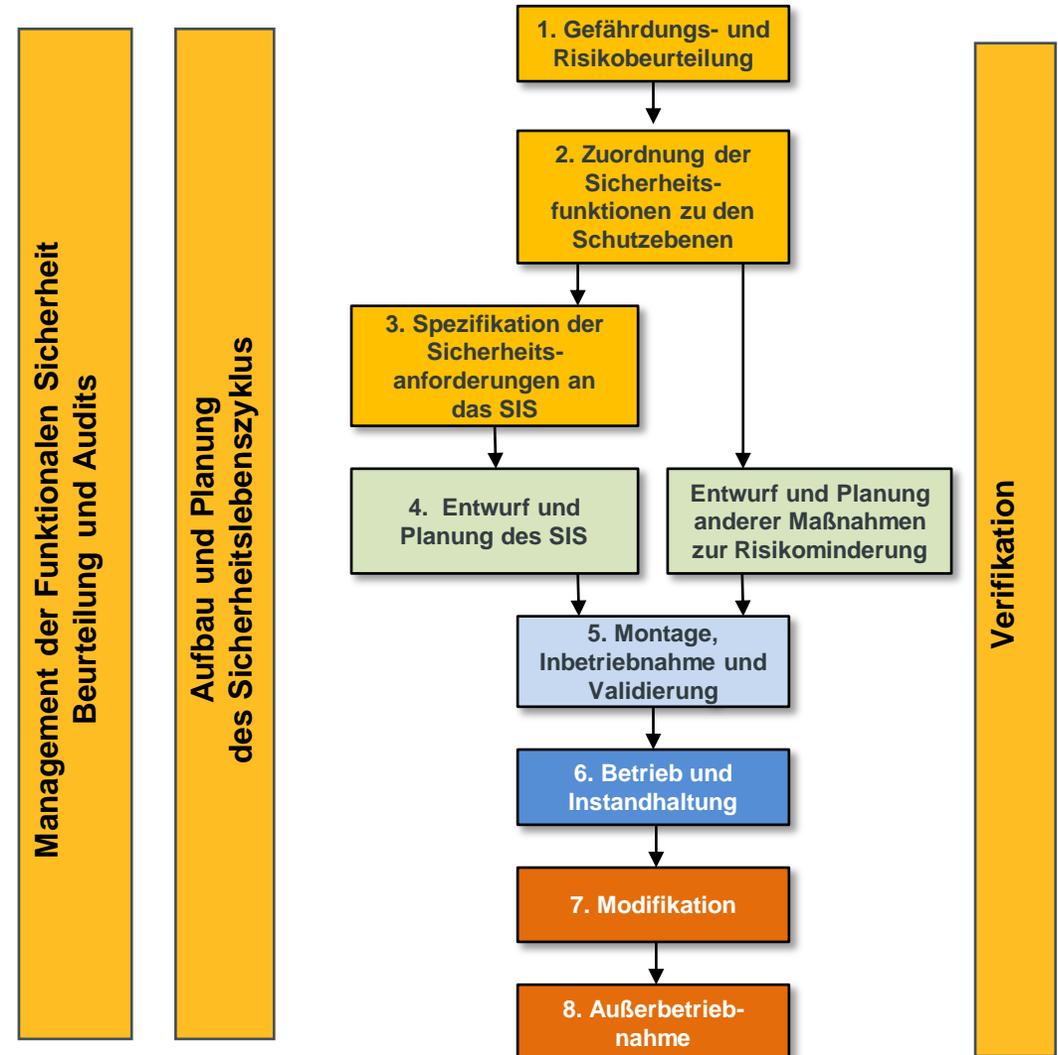
Quelle: DIN EN 61511-1 (VDE 0810-1):2019-02

# Lebenszyklus und Fehlerhäufigkeit

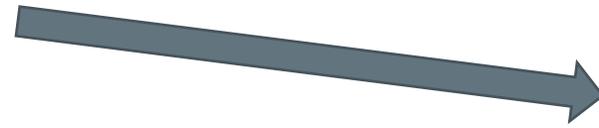
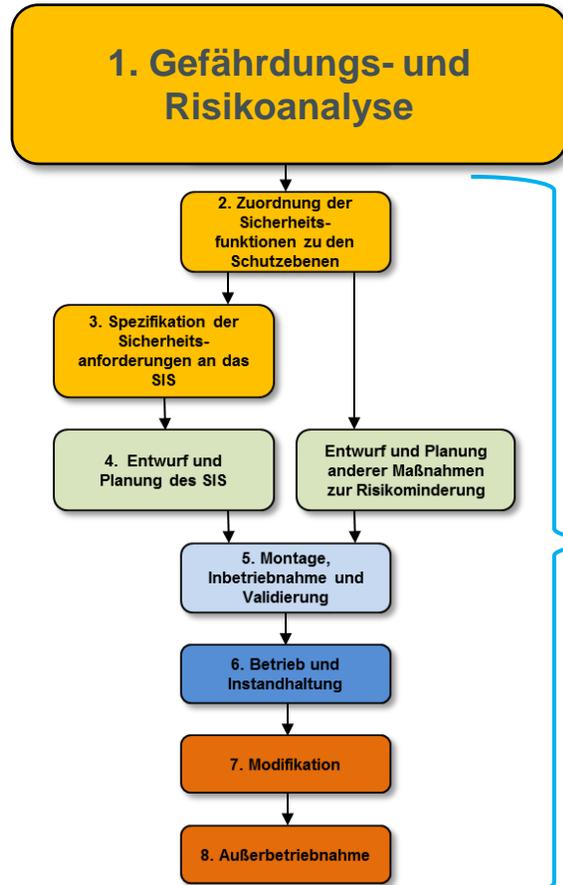


- Spezifikation
- Änderung nach Inbetriebnahme
- Betrieb und Wartung
- Installation und Inbetriebnahme
- Design und Implementierung

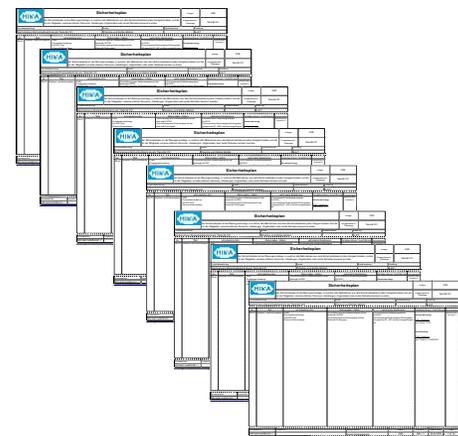
Quelle: Studie der britischen Gesundheits- und Sicherheitsbehörde Health & Safety Executive (HSE)



# Safety Plan



Beschreibung der Details pro Phase

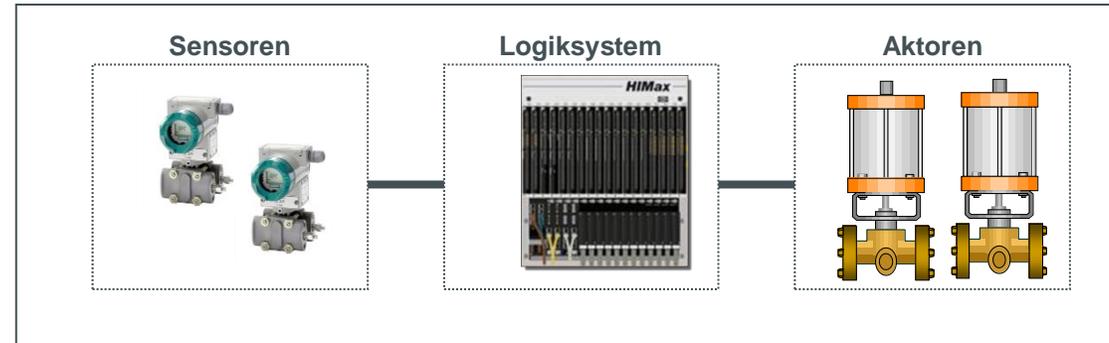


HIMA SMART SAFETY		Sicherheitsplan			A-Nr.	CLK
Der Sicherheitsplan ist die Planungsunterlage, in welcher alle Maßnahmen aus dem Sicherheitslebenszyklus festgeschrieben und die für die Tätigkeiten verantwortlichen Personen, Abteilungen, Organisation oder andere Einheiten benannt werden.						
Projektbeschreibung		Name		Kundennummer		Revision
Nachrüstung Sicherheitstechnik am Tank EL101		Chemie und Kohle GmbH				E-ILT
Nr.	Titel	erforderliche Info.	Zielvorgabe / Aktion	geforderte Ergebnisse	Verantwortung / Ausführung	Referenzen
SP.01	Gefahren- und Risikoanalyse	-PAD -Prüfprotokolle -HAZOP Plan -Plan zur Risikoanalyse	-Durchführung einer Gefahrenanalyse mit der Methode HAZOP -Durchführung einer Risikoanalyse mit der Methode Riskograph	- Dokumentierte Gefahrenanalyse (HAZOP) - Dokumentierte Risikoanalyse (Riskograph) - Eingetragene SP + SP's inklusive Angehörigen	Verantwortlich: CLK / Abteilung: Herr Strobel / E-ILT  Ausführung: CLK / Abteilung: Herr Theisen / LANGSAM	EN 61508-1 Abschnitt 8
Document No.	Project No.	Safety Plan No.	Owner	Revision	Date of Issue	Page
SPS160015/KP09/001-1		S160015/SPSCS/SP001	CLK	Rev.: 1	16.03.2016	1 of 19

- Titel der Phase
- Erforderliche Info (Eingangsdokumente)
- Zielvorgabe / Aktion
- Geforderte Ergebnisse
- Verantwortlichkeiten / Ausführung durch
- benötigte Kompetenzen
- Anforderungen aus ...

In der Praxis können unterschiedliche individuelle Lebenszyklen definiert werden für Betreiber, Errichter, Integratoren, Planer, Entwickler für Hardware / Software ...

# SILusion #4: “SIL-Nachweis = Rechnen”



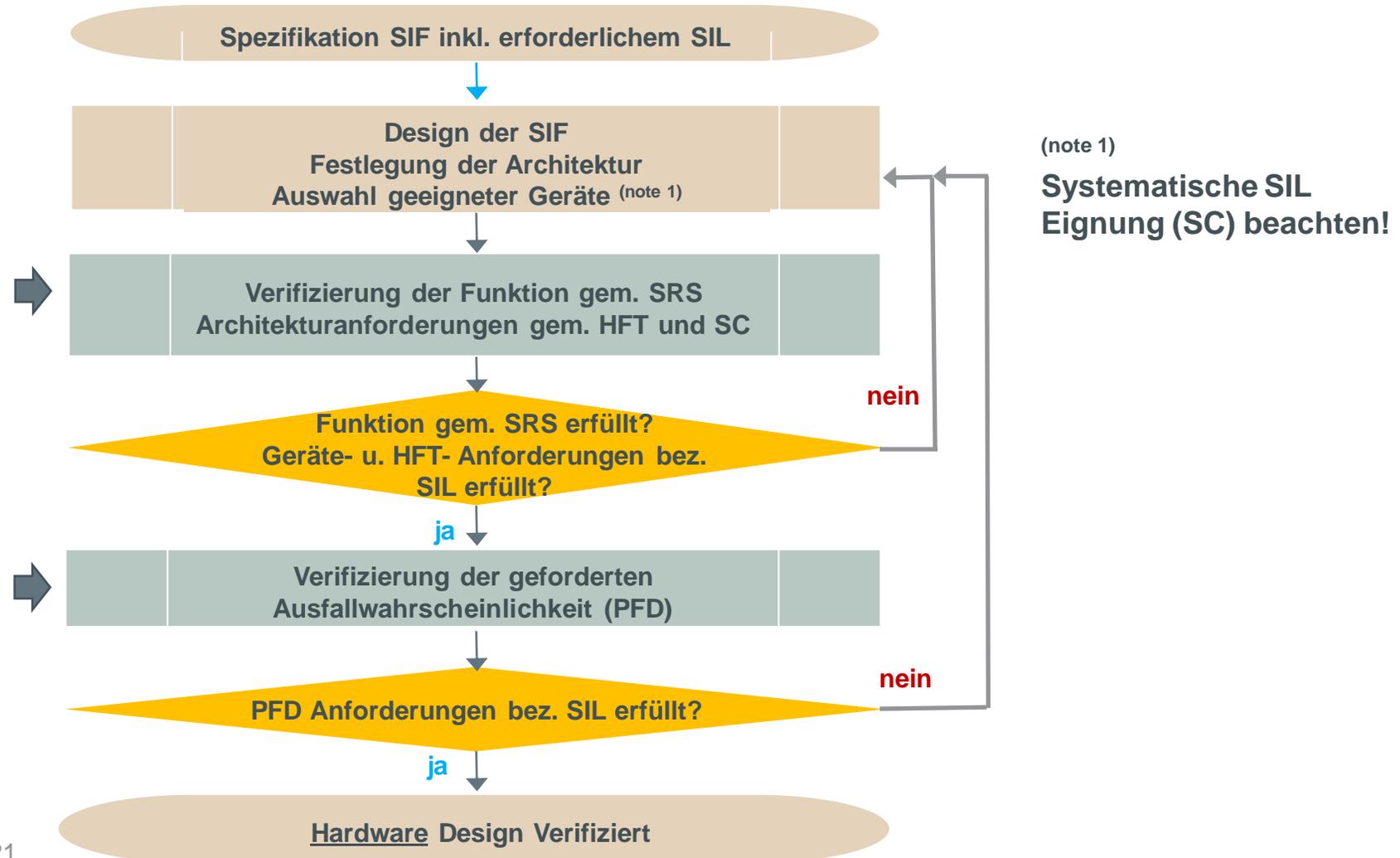
SIL Berechnung

Subsystem	Sensor	Logic Solver	Final Elements																
SIF Loop																			
Voting	1oo2	1oo1	1oo2																
PFDavg	1,60E-04	2,40E-04	9,17E-05																
SIL (PFD, HFT, SFF)	3	3	3																
Provo Test (Jahren)	1	10	1																
MTTR (h)	8	8	8																
Typical	S-00024 E+H Diversitäre 1oo2-Architektur: (Liquiphant MS FTL 50/ FTL 51/ FTL 51C / FTL 70/ FTL71 + FEL57 + FTL 325P) + (Vegapuls Serie 60) Füllstandsmessung LEVEL MAX	LS-0001 Siemens 6ES7F6H ind. VO (1oo1) und Kommunikation in SIL3 Konfiguration Safety PLC	FE-0002 NAMUR SAV mit Sicherheitsrelais 1. SAV (Kugelhahn oder Drehkegelventile) mit Antrieb u. Magnetventil 2. Sicherheitsrelais - DETAILIERTE AUSWAHL möglicher GERÄTE siehe AKTOR-Liste -																
Typical / ID	S-L-1oo2-SIL3-014	LS-0001	F-V-1oo2-SIL3-001																
	PFDavg Sensor: 1,60E-04	PFDavg Logic Solver: 2,40E-04	PFDavg Final Element: 9,17E-05																
SIL acc. PFD, HFT and SFF	3	<table border="1"> <tr> <td colspan="2">made by:</td> <td colspan="2">verified by</td> </tr> <tr> <td>Date</td> <td>29.04.2012</td> <td>Date</td> <td>02.05.2012</td> </tr> <tr> <td>Name</td> <td>FS</td> <td>Name</td> <td>GG</td> </tr> <tr> <td>Rev.</td> <td>0</td> <td>Rev.</td> <td>0</td> </tr> </table>		made by:		verified by		Date	29.04.2012	Date	02.05.2012	Name	FS	Name	GG	Rev.	0	Rev.	0
made by:				verified by															
Date	29.04.2012			Date	02.05.2012														
Name	FS	Name	GG																
Rev.	0	Rev.	0																
SIL acc. PFD	3	<table border="1"> <tr> <td>SIL total:</td> <td>3</td> <td>PFD total:</td> <td>4,92E-04</td> </tr> </table>		SIL total:	3	PFD total:	4,92E-04												
SIL total:	3	PFD total:	4,92E-04																
Proof test Intervall (Years)	1																		
		Behälteranlage XYZ 5110064	MASTER SIF x																

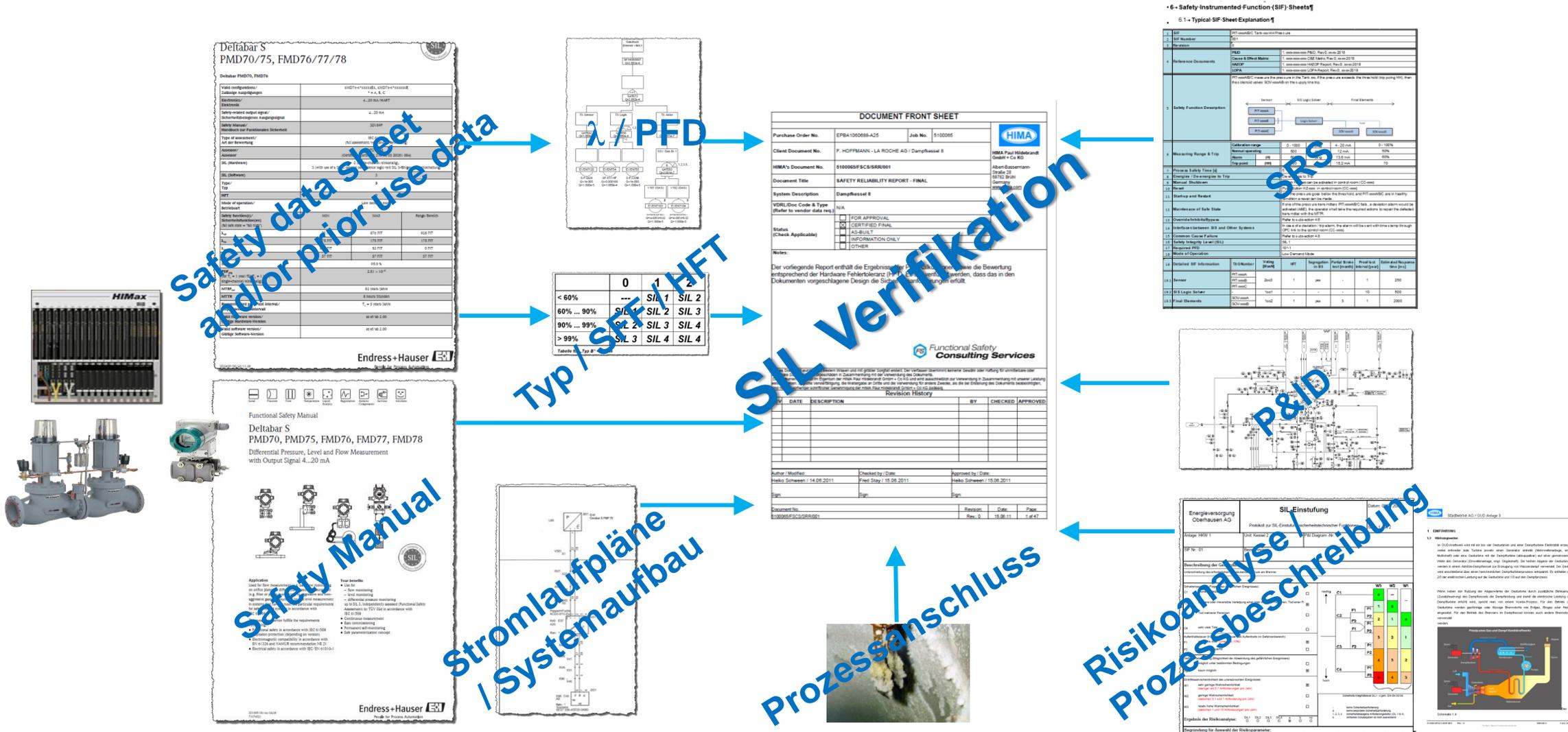
# Design und Verifizierung sicherheitstechnischer Funktionen (HW)



Verifizierung  
im Vier-Augen Prinzip!  
Unabhängigkeit der  
Personen entsprechend  
SIL und Komplexität  
notwendig.



# SIL Verifikation – mehr als nur Berechnungen



# Prüfen und Verifizieren des Anwenderprogramms / Systems



Geräte-/Systemtechnische Anforderungen & Funktionen

## Prozess-Funktionen

Table F.14 – Cause and effect diagram

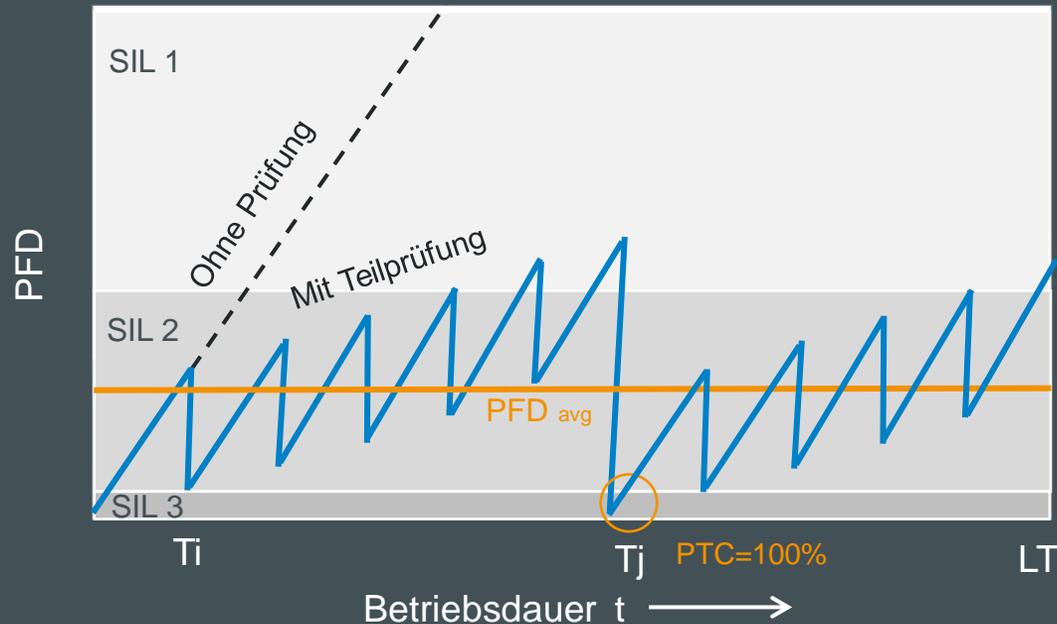
Reactor cause and effect diagram (table)

Cause				
Safety function No.	Sensor/ Input	Description	Trip Setting	F
S-1	100PT 100PT1	Reactor pressure <b>OR</b>	> 125 psig	10
	100TT	Reactor temperature	> 200 °F	10
S-2	100PT 100PT1	Reactor high pressure	> 125 psig	10
S-3	200PT	Reactor seal pressure	>10 psig	100PV 100PV1

HIMA		Check list design verification HIMax Application software / HW/SW integration		HIMA Auftragsnummer / Job no	
Projektleiter: Project manager:		Bearbeiter: Engineer:		Verifikation: Verification:	
Projektbenennung: Project description:		<p style="color: red; text-align: center;"><b>Verifizierung im Vier-Augen Prinzip/Unabhängigkeit der Personen entsprechend SIL und Komplexität notwendig.</b></p>			
Sicherheitshandbuch: Safety manual:					
		ja	nein no	N/A	Date & Sign
1	Parametrierung des PES / Configuration of the PES				
1.1	Sicherheit / Safety				
1.1.1	Erfolgte die Parametrierung der Ressource gemäß den Auflagen des Sicherheitshandbuchs und in Absprache mit dem Kunden? Have the parameters of the resource been set according to the regulations of the safety manual and to the agreement made with the client?				
1.1.1.1	Wurde die Einstellung der Watchdog- bzw. Sicherheitszeit mit der realen Zykluszeit verglichen und ist die reale Zykluszeit kleiner als die geforderte max. Zykluszeit? Do the settings of watchdog and safety time meet to the real cycle time and in the real cycle time?				
1.1.1.2	Ist die Zyklenzeit des Prozessmoduls mit der realen Zykluszeit verglichen und ist die reale Zykluszeit kleiner als die geforderte max. Zykluszeit? Is the cycle time of the process module compared to the real cycle time and is the real cycle time smaller than the required max. cycle time?				
1.1.2	Erfolgte die...				

**Wurden Architektur der SIF, Diagnose u. Fehlerauswertungen der Geräte sowie entsprechende Reaktionen entsprechend den Anforderungen der Spezifikation umgesetzt?**

# SILusion #5: “Einmal SIL ist immer SIL”

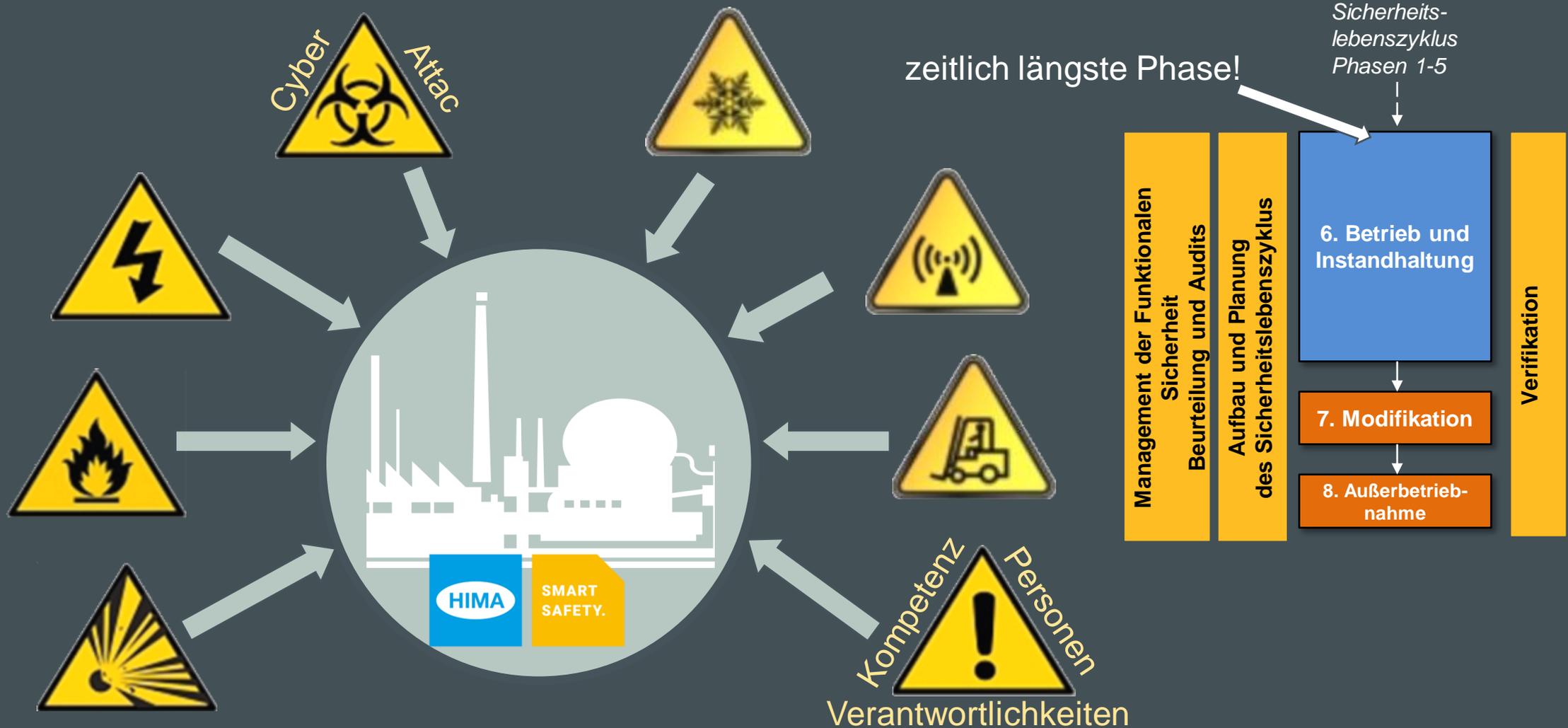


$$PFD_{avg} \approx \frac{1}{2} \lambda_{du} \times T_i \times PTC + \frac{1}{2} \lambda_{du} \times T_j \times (1 - PTC)$$

PTC – Prüftiefe,  $T_i$  – Testintervall (Teilprüfung),  $T_j$  – Testintervall (Vollprüfung)

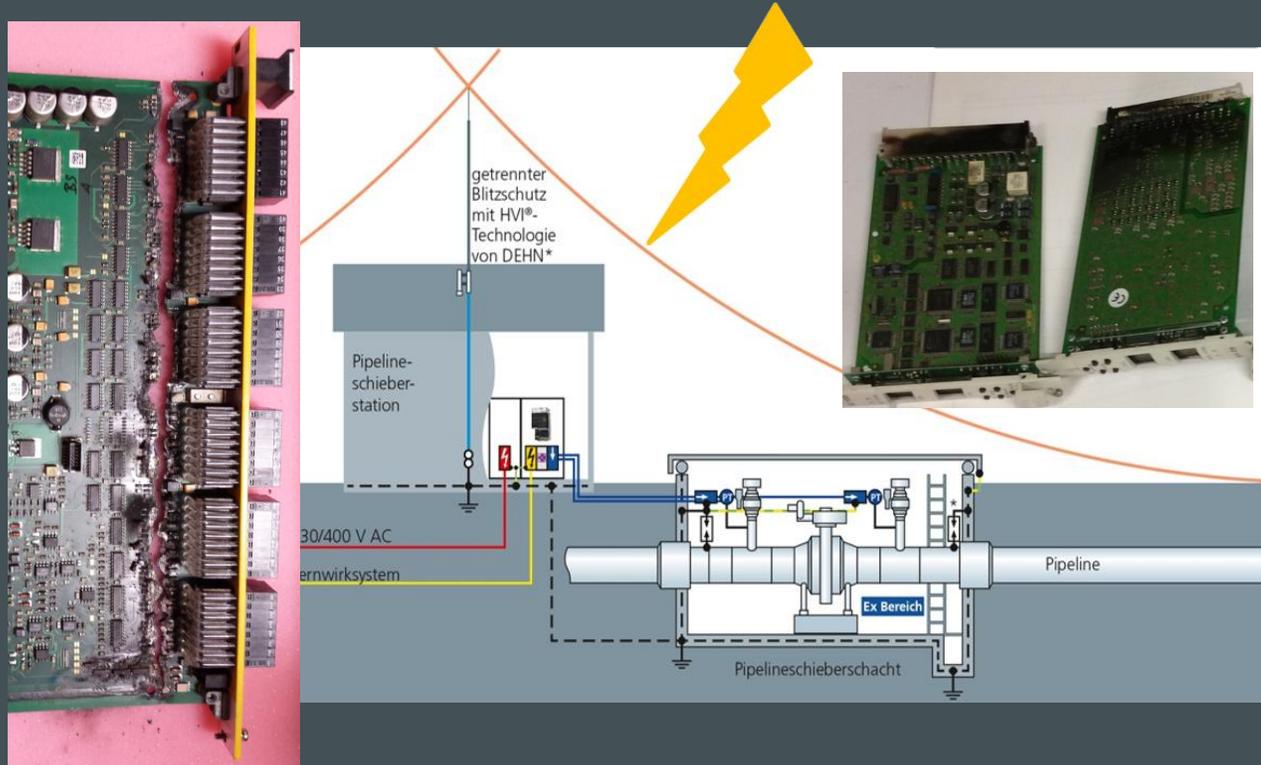
„Die Zuverlässigkeit der Sicherheitsfunktion lässt sich berechnen“...zu kurz gedacht!

# Integrität der SIF – Erhalt im Betrieb



# Funktionale Sicherheit – Integrität erhalten

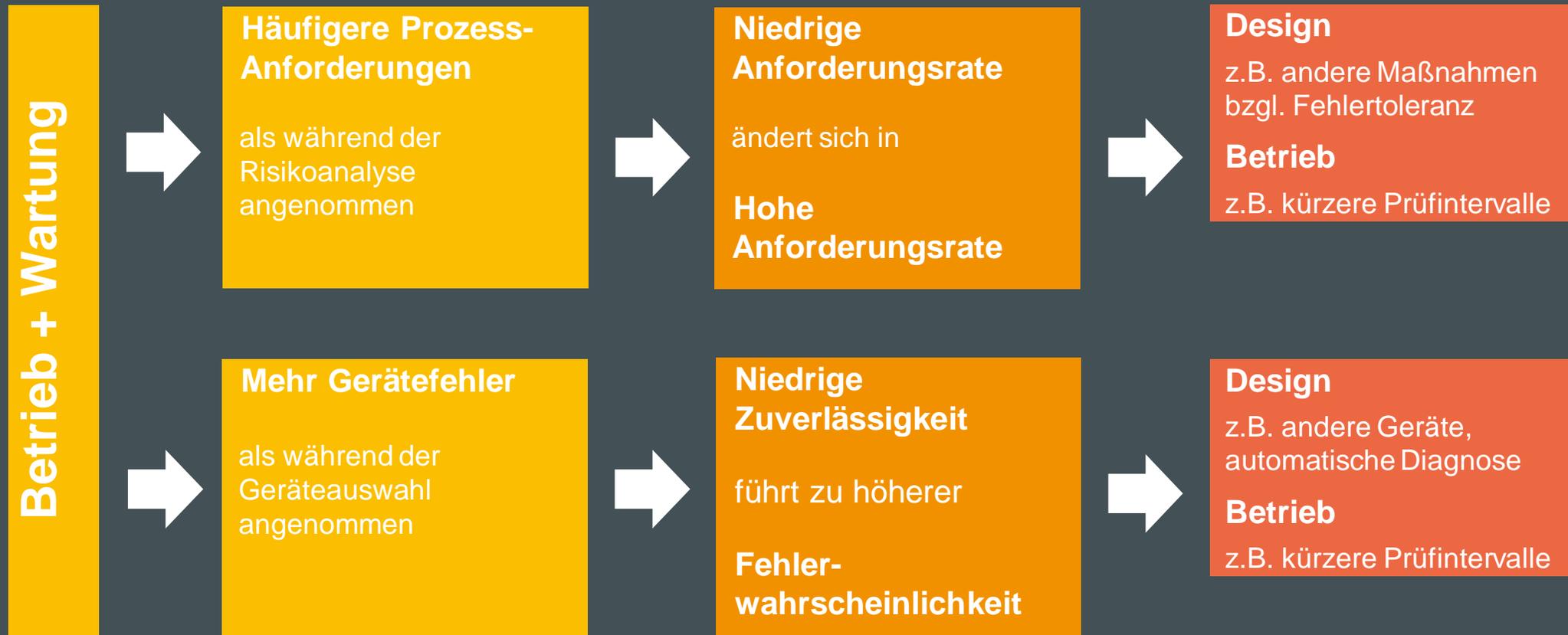
Umwelt und Prozesseinflüsse, Abnutzung und Alterung lassen sich nicht oder nur bedingt berechnen. Hier sind qualitative Maßnahmen (Funktionsprüfung, optische u. innere Prüfung, etc.) notwendig. Diese sind Teil eines gelebten FSM.



# Überwachung der Leistungsfähigkeit



Konsequenzen bei Abweichungen zu Planungsdaten



# Widerstandsfähigkeit gegen Security Risiken



Der Entwurf des SIS muss eine ausreichende Widerstandsfähigkeit gegen identifizierte Security Risiken aufweisen (siehe IEC61511/1 8.2.4). (IEC61511/1 11.2.12)

Diese Herausforderung ist, diese Widerstandsfähigkeit über die Betriebszeit zu erhalten - in einem Szenario von sich ständig ändernder Bedingungen



# Questions?



Even simple things can be very difficult!!!



HIMA Paul Hildebrandt GmbH  
Albert-Bassermann-Str. 28  
68782 Brühl, Germany

Phone: +49 (0) 6202 / 709-145  
Fax: +49 (0) 6202 / 709-107

Email: [i.hanspach@hima.com](mailto:i.hanspach@hima.com)  
Website: [www.hima.com](http://www.hima.com)

---

# SILusionen der funktionalen Sicherheit

---

SIL Sprechstunde 2024

18./19.09.2019, Mannheim

---

Ivo Hanspach

Director of Product Management / Obsolescence Management

---



Vielen Dank für Ihre Aufmerksamkeit!

# 25 Jahre EN 61508 - Titel, Thesen, Temperamente

Wie sieht die Norm für die funktionale Sicherheit in 25 Jahren aus?

-  
Wie haben wir 1999 25 Jahre in die Zukunft gesehen?

Vertical text in a futuristic font, possibly representing data or code, with a green glow.



# „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“ *Lernender? Anlernbarer?*

Mit einer Verspätung von zwei Monaten bringt [HMD Global](#) einen Klassiker aus dem Handy-Zeitalter zurück: Das Handy aus dem Film Matrix gibt es als Neuauflage wieder zu kaufen. Das neue Nokia 8110 4G hat die Bananenform - aber diesmal mit aktueller Mobilfunktechnik.



20. Juli 2018, 11:28 Uhr, Ingo Pakalski

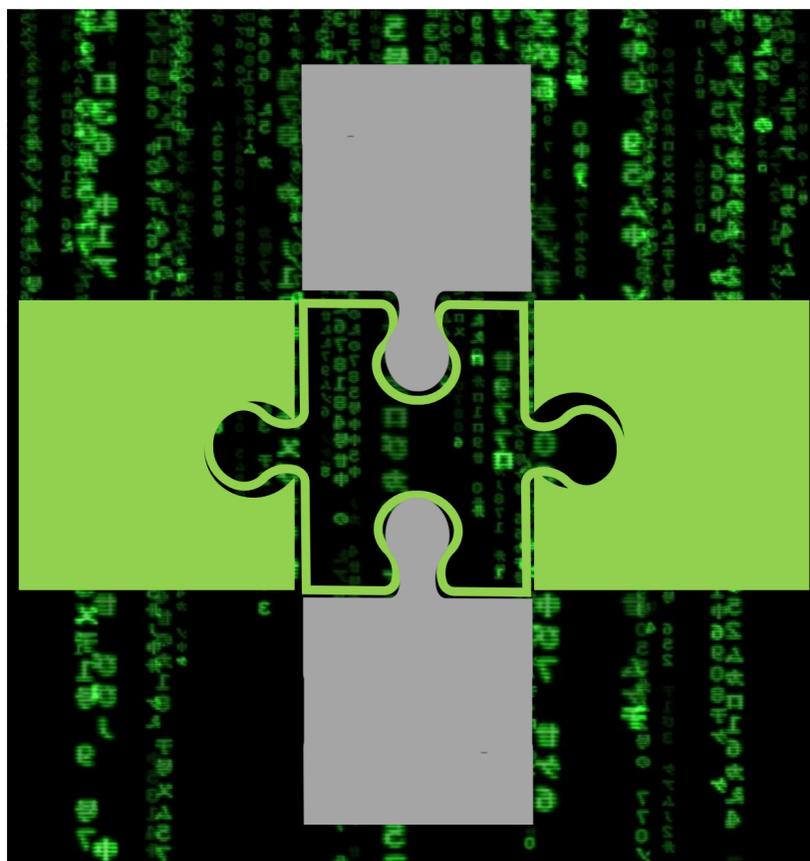


(Bild: Michael Wiczorek/Golem.de)



# Weitere 25 Jahre EN 61508 - Thesen

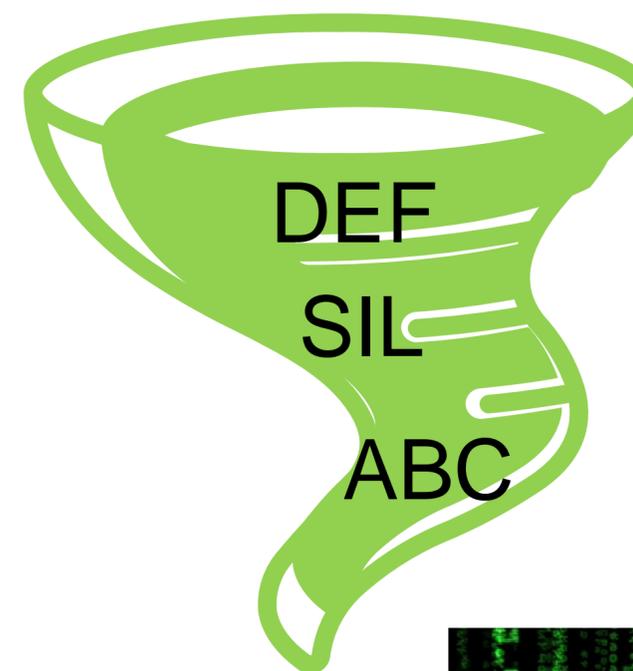
Wie zahlt die Norm zeitgemäß



auf die Sicherheit ein?

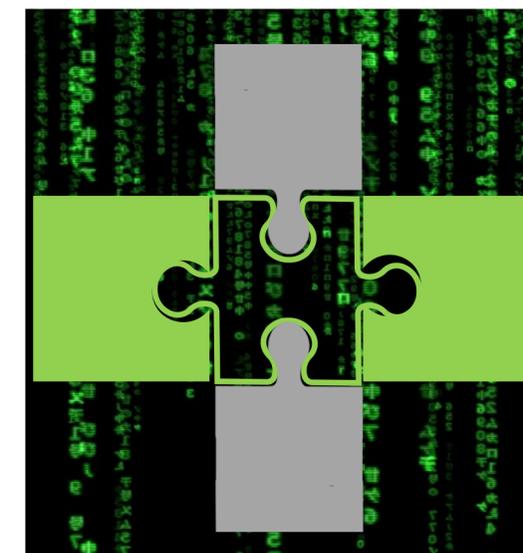
## weitere 25 Jahre EN 61508 – wer schreibt, der bleibt?

„Die IEC 61508 ist eine branchenübergreifende generische Richtlinie für funktionale Sicherheit in Systemen. Sie umfasst weit über 500 Seiten. Eine leichtverdauliche Einführung zu den wichtigsten Konzepten gibt Experte...“



-> oder ChatGPT...?

Für Menschen von Menschen geschrieben und von Menschen gelesen?

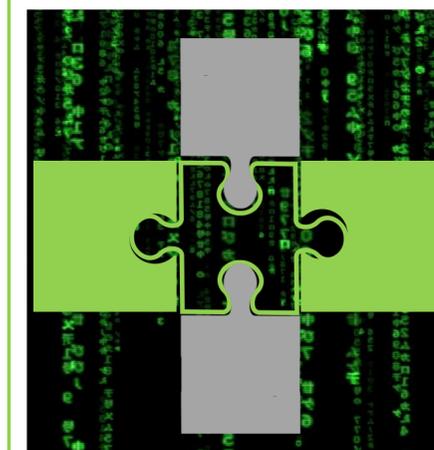
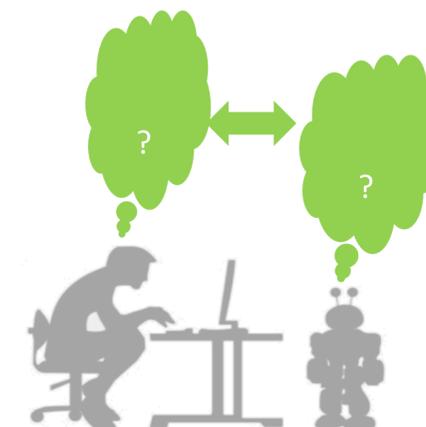


## „Die Zukunft der Standards... SMART Standards für die digitale Transformation“

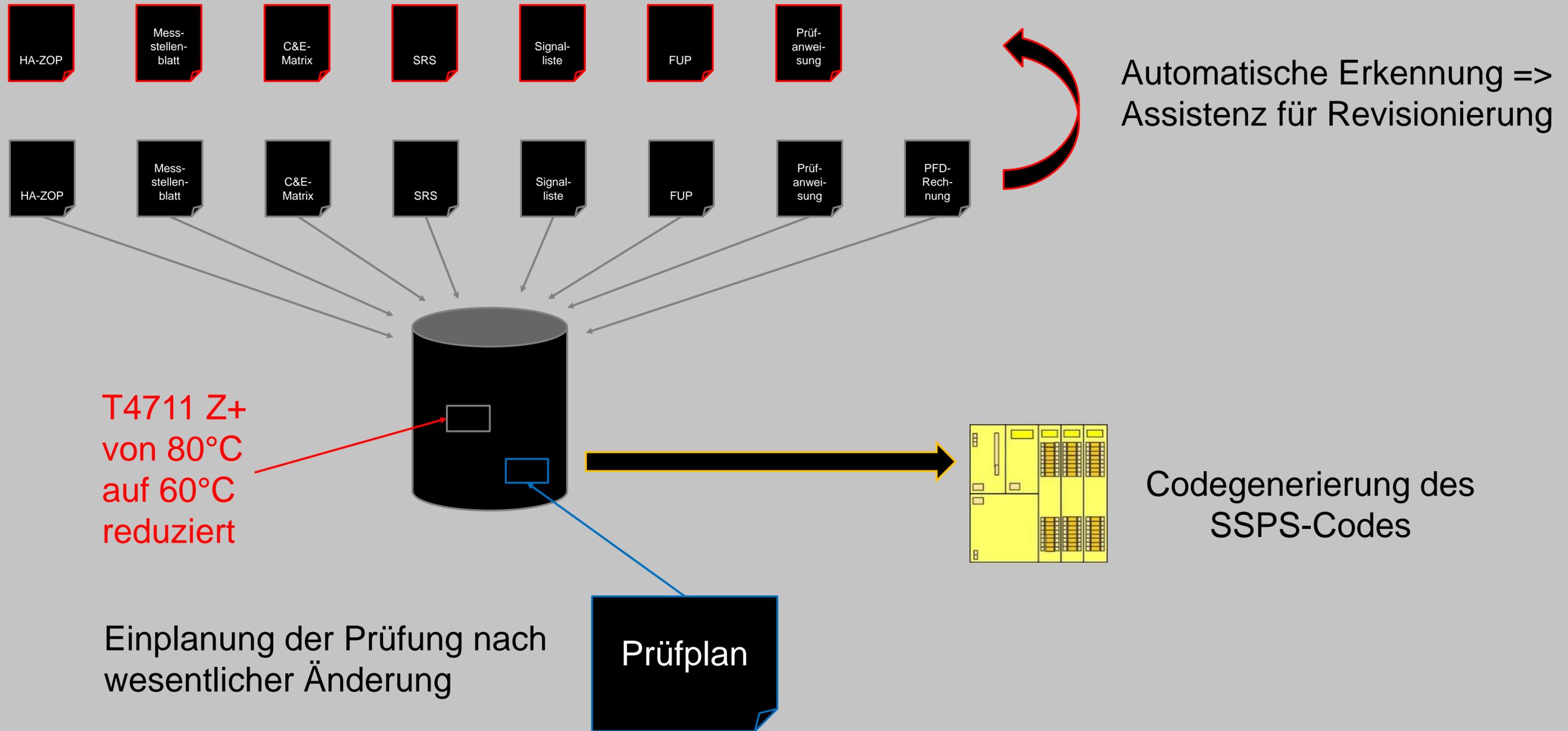
Für Maschinen & Menschen geschrieben

-> EN 61508 erreicht Level 4

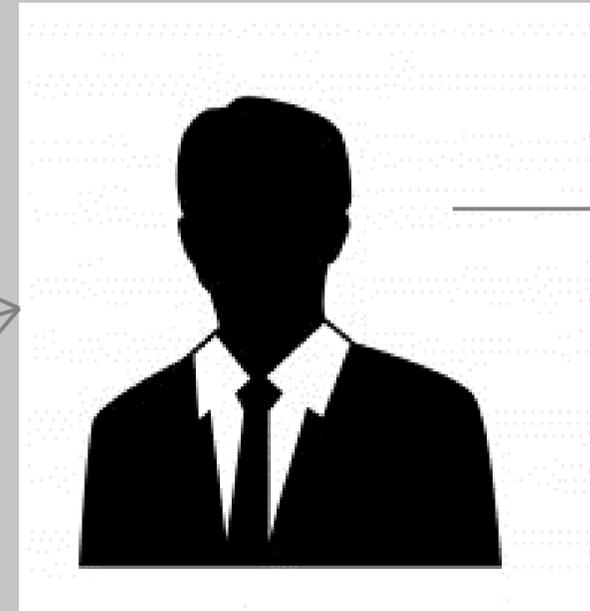
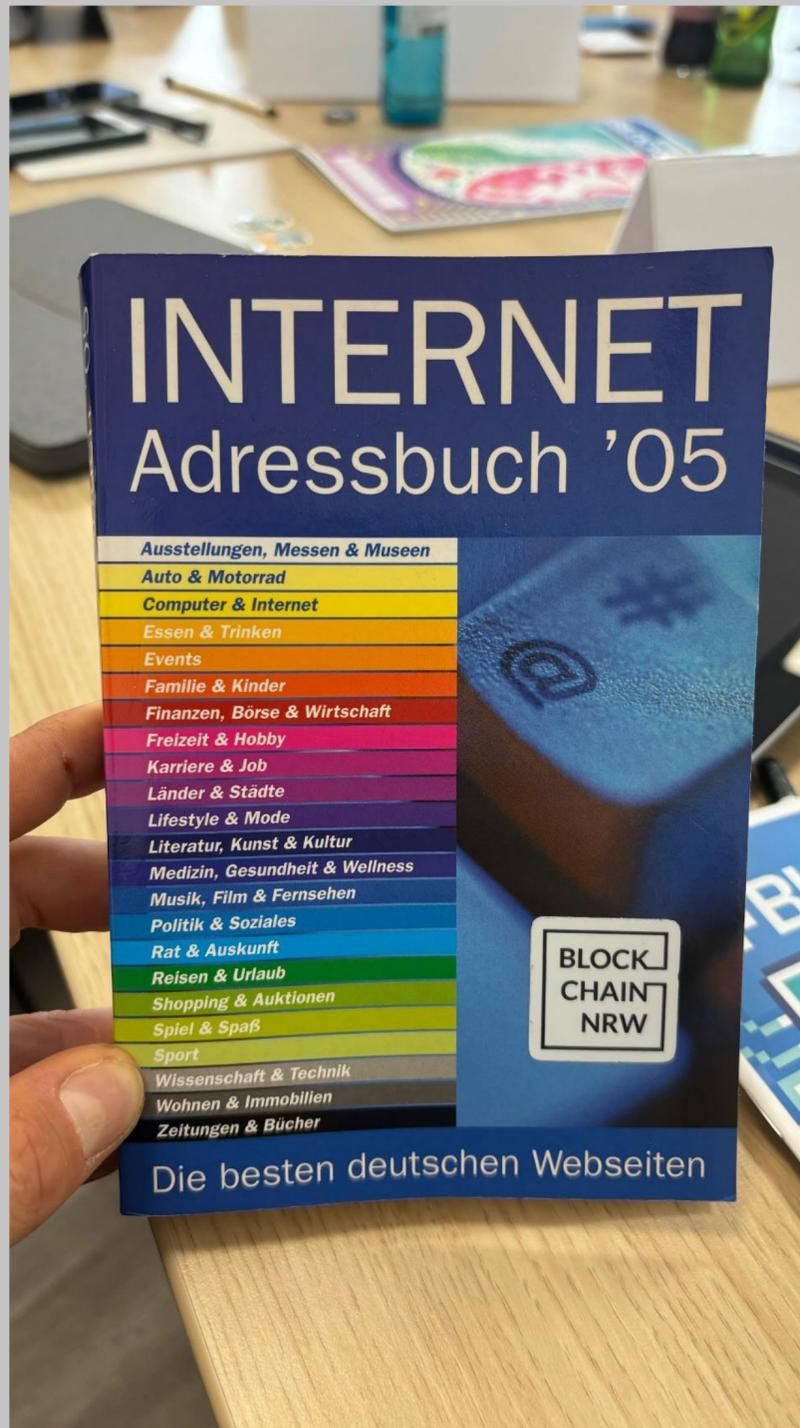
- Maschinenlesbare und interpretierbare Inhalte
- Informationsmodelle, die Inhalt und Beziehungen zwischen Informationen beschreiben und erklären
- Selbstlernende Analyse sowie automatische Validierung und Optimierung
- Mehrwertdienste möglich wie Konformitätsprüfung, Question Answering, Predictive Content Supply
- Unterbrechungsfreie digitale Wertschöpfungskette möglich



# WANTED: Daten in strukturierte Information



# Klassische Ermittlung der Informationen



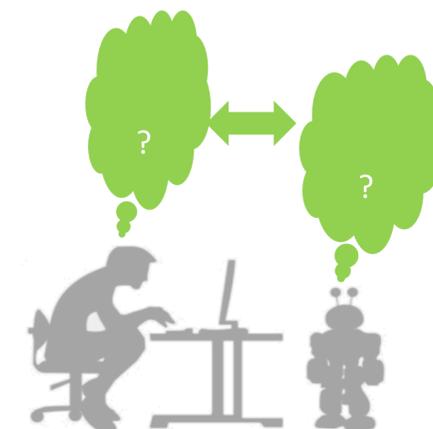
"Bild: Freepik.com". Diese Folie wurde mit Ressourcen von Freepik.com erstellt.

## weitere 25 Jahre EN 61508 - These 2

**„Vertrauen ist gut. Kontrolle ist besser...“**

EN 61508 adressiert das Zusammenwirken  
Mensch-Maschine + Maschine-Maschine

- inhärente Vertrauensmechanismen
- rekonfigurierbare dynamische Systeme
- System of systems



# Komplexität managen im „System of Systems“ (SoS), bspw. MTP

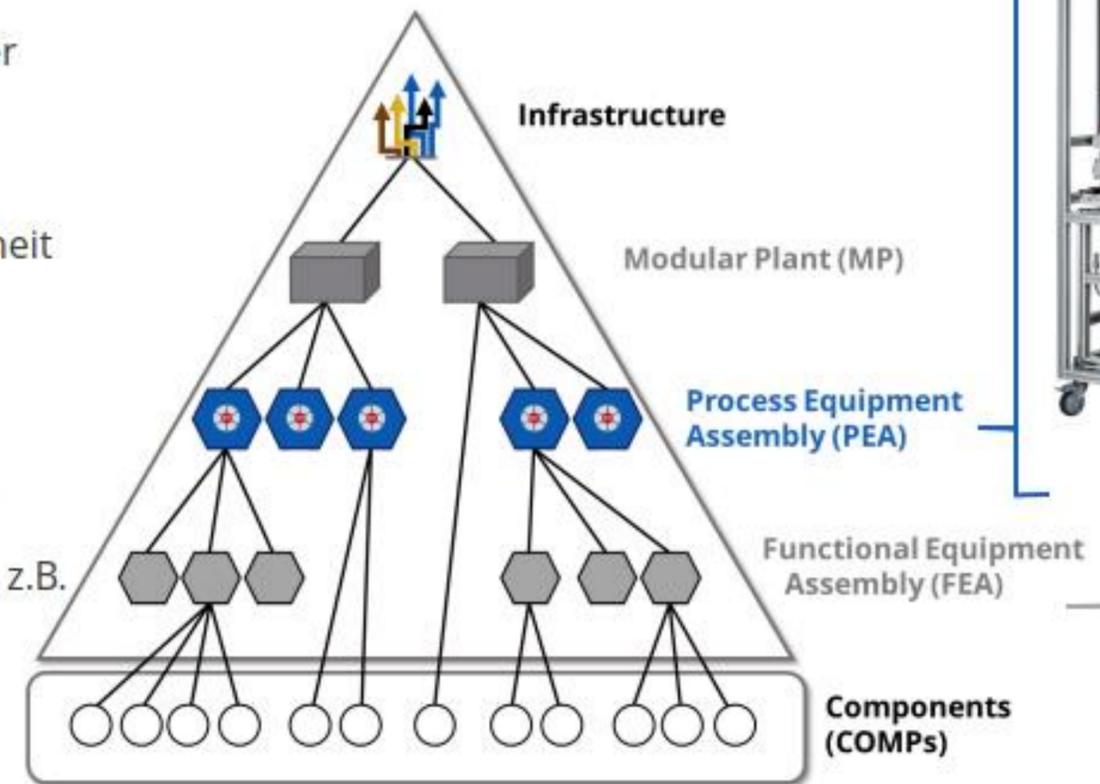
„Assuring **interconnectedness** –  
How to **modularize safety**?”

Considering safety **challenges** associated with interconnectedness, [...] assuring the safety of **applications/functions** that are rendered through a **collaboration of different (maybe even dynamically) interconnected systems of different manufacturers** [...] adequate means for safety modularization are required...”

Standardisierte und nicht proprietäre Informationsmodelle benötigt!

## Struktur modularer Anlagen nach VDI 2776 (2020)

- **MP:** Zusammenschluss mehrerer PEAs (komplexe Prozesse)
- **PEA:** Austauschbare Prozesseinheit (verfahrenstechnischen Prozessschritt, z.B. dosieren)
- **FEA:** Einfach auszutauschendes Modul innerhalb einer PEA (verfahrenstechnische Funktion, z.B. Fördern)
- **COMP:** Kleinste, nicht weiter zerlegbare Einheit



(Pelzer, et al. 2021)

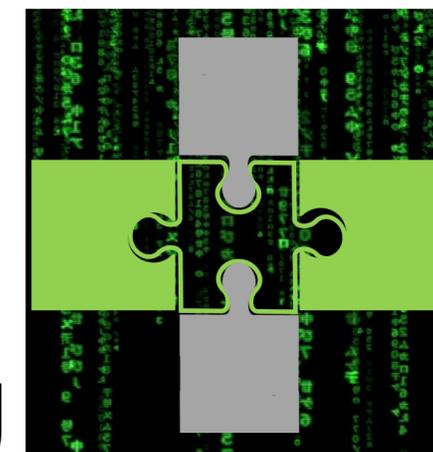
## weitere 25 Jahre EN 61508 - These 3

„Prognosen sind schwierig, insbesondere wenn sie die Zukunft betreffen.“

EN 61508 betrachtet die Zuverlässigkeit im erweiterten Kontext

$$PFD_{x,t} = PTC_x f(\lambda)_x \frac{T_x}{2}$$

- Rekonfigurierbarkeit & Modularität x Interconnectedness
- Zuverlässigkeit/ Probabilistik x Uncertainty quantification
- Dynamik der Betrachtung? Überwachung zur Laufzeit\*?
- Datenqualität & -Kontextualisierung für die FuSi-Eignung



\*Runtime uncertainty estimation & handling

# Quantifizierbare Zuverlässigkeit von KI?

[...] the UCI is to be understood more like a systematic capability as in IEC 61508 (all parts) for software elements, but it still has other characteristics.

In the future it might be possible to calculate a fault rate for AI elements, consequently called Lambda AI. This fault rate needs to be compatible to the fault rate Lambda of hardware elements.

The benefit would be to calculate an overall fault rate of a system including all contributors like hardware faults, AI uncertainties etc. In any case these values are heavily depending on the assumptions on the environment. This holds true for hardware (e.g. increased operating temperature) and for AI elements.

VDE-AR-E 2842-61-1:2021-07

The presented approach can be summarized by combining the three kinds of technology (HW = hardware/electronics, SW = software; AI = artificial intelligence) with the three types of failures as presented in Figure 11.

- To avoid systematic failures in all kinds of technology (HW = hardware, SW = software; AI = artificial intelligence) mature processes, proven methods and trained persons are the appropriate measures.
- Random failures occur in HW elements. They are handled through proves by certain metrics (e.g.  $\lambda$  and safe failure fraction).
- Failures due to uncertainty are primarily associated with AI elements. There are discussions in research and in the standardization community to apply this to complex software as well. However currently there is no suitable overall metric that covers this uncertainty. Nevertheless there are metrics (e.g. for neural networks) that are able to generate confidence about the absence of failures due to uncertainty. We use  $\lambda_{AI}$  to denote this phenomenon.

type of failure	measures	Requirements on platform (HW and classical SW)		
		measures for HW	measures for SW	measures for AI
systematic	<u>Qualitative Requirements:</u> Culture, Experts, QS Process, Design, Methods & Measures	systematic capability	systematic capability	systematic capability
random	<u>Quantitative Requirements:</u> Metrics and Thresholds	$\lambda$ , SFF, DC, SIL-related target	-- / --	-- / --
uncertainty-related	<u>Structured Approach:</u> Metrics, References, Measures and Argumentation	-- / --	-- / --	Uncertainty confidence indicator (UCI)

evidences within the argumentation (e.g. GSN) of the trustworthiness assurance case

Figure 11 – Types of failures and technology specific Measures

Combining these thoughts of this section there is – of course – no non-determinism in AI elements (as long as they are executed on classical platforms). But there are forms of uncertainty that are handled in a similar way

$$PFD_{1001,AI} = PTC_0 \lambda_{AI} \frac{T_0}{2} + (PTC_1 - PTC_0) \lambda_{AI} \frac{T_1}{2} + (1 - PTC_1) \lambda_{AI} \frac{T_2}{2} !?$$

# KI-Unsicherheit quantifizieren?

## \*Runtime uncertainty estimation & handling

[https://www.researchgate.net/profile/loannis-Sorokos/publication/351659571\\_Handling\\_Uncertainties\\_of\\_DataDriven\\_Models\\_in\\_Compliance\\_with\\_Safety\\_Constraints\\_for\\_Autonomous\\_Behaviour/links/60a39746299bf1d21d6ee26f/Handling-Uncertainties-of-Data-Driven-Models-in-Compliance-with-Safety-Constraints-for-Autonomous-Behaviour.pdf](https://www.researchgate.net/profile/loannis-Sorokos/publication/351659571_Handling_Uncertainties_of_DataDriven_Models_in_Compliance_with_Safety_Constraints_for_Autonomous_Behaviour/links/60a39746299bf1d21d6ee26f/Handling-Uncertainties-of-Data-Driven-Models-in-Compliance-with-Safety-Constraints-for-Autonomous-Behaviour.pdf)

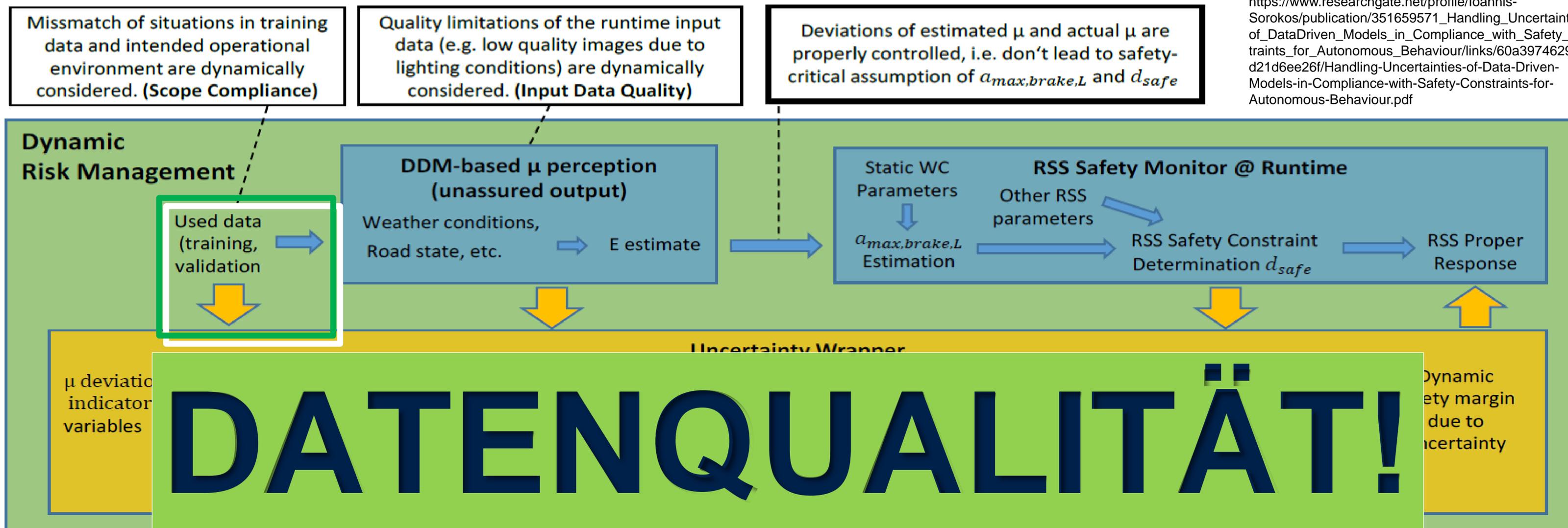
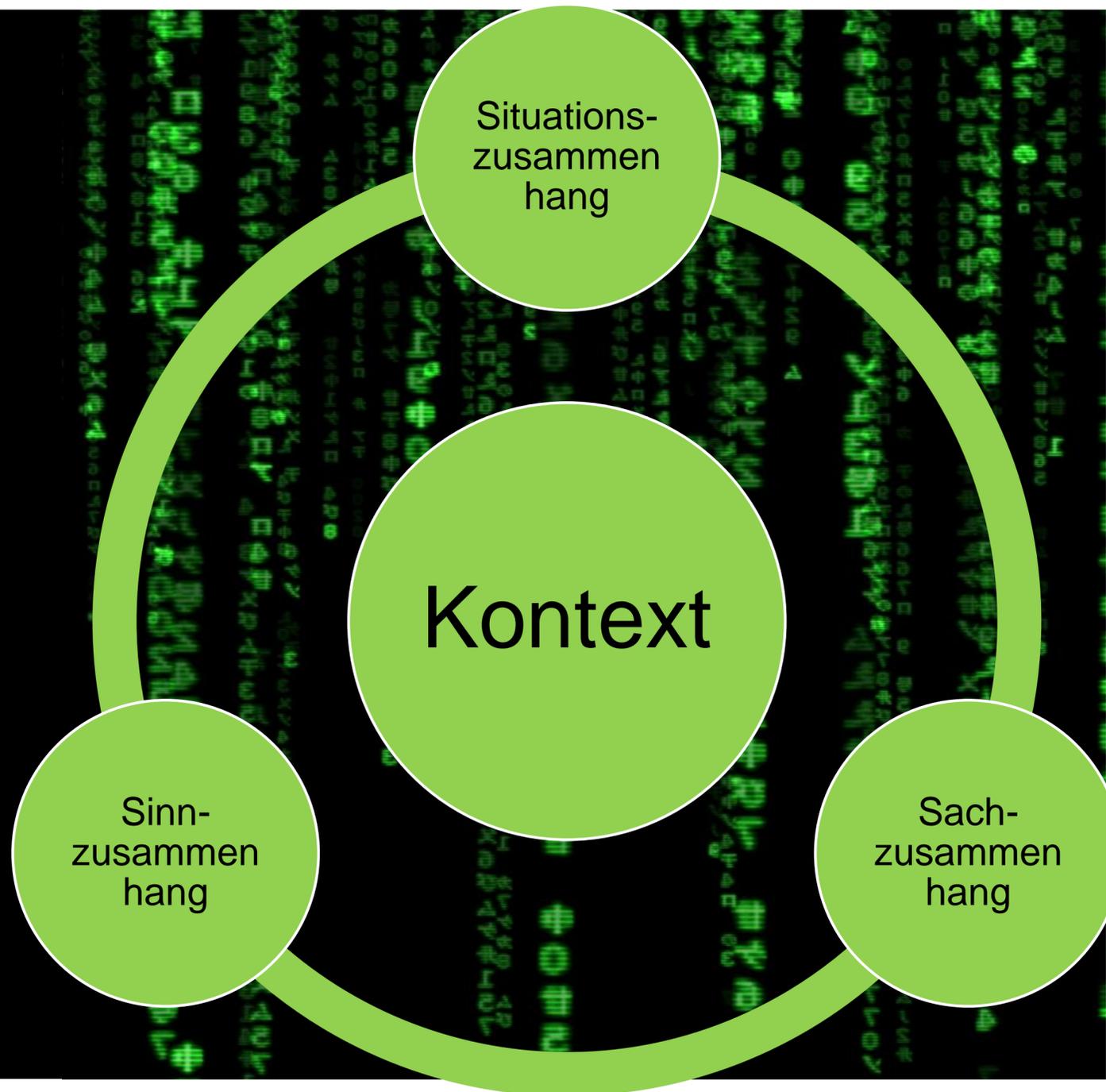


Fig. 3. Uncertainty Wrappers enable using data-driven models for assured dynamic RSS Monitoring (Responsibility-Sensitive Safety)

Vgl. DIN SPEC 92005 „Künstliche Intelligenz – Quantifizierung von Unsicherheiten im Maschinellen Lernen/ Artificial Intelligence – Uncertainty quantification in machine learning -> ISO/IEC JTC 1/SC 42 and IEC TC 65/SC 65A have approved ISO/IEC NP TS 25223, titled "Information Technology — Artificial Intelligence — Guidance and Requirements for Uncertainty Quantification in AI Systems".



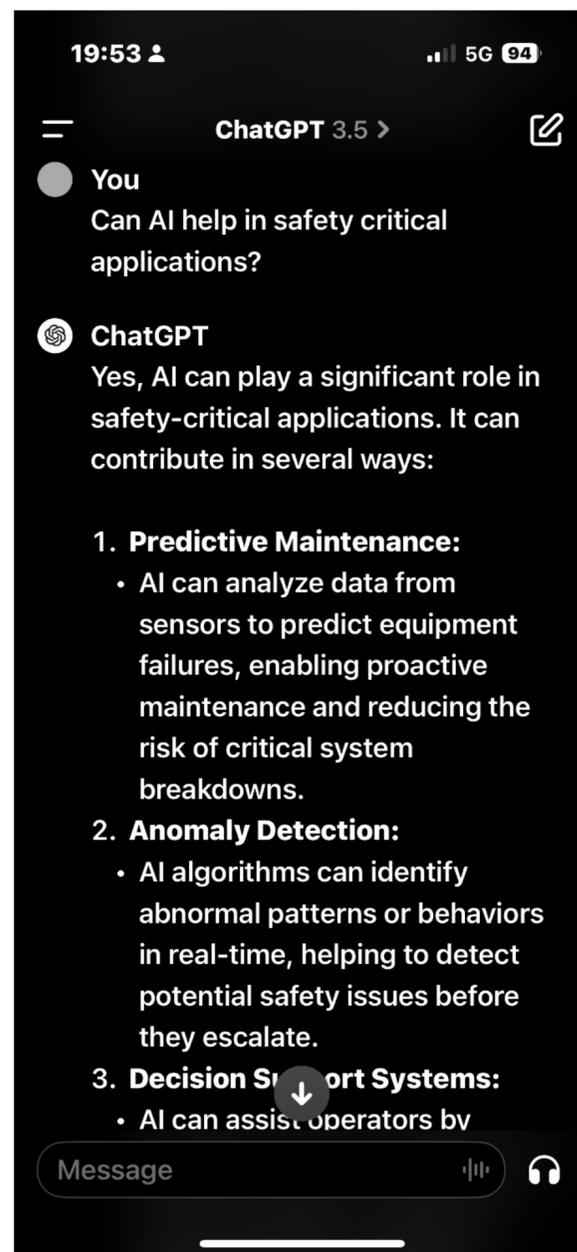
Vgl. NE 198, Kontextualisierung von Produktionsdaten in der Prozessindustrie  
„ **Derzeit** halten produktionsnahe Systeme **aufgezeichnete Messstellen und Meldungen als einzelne Datenpunkte** vor. Diese sind in den Systemen oftmals hierarchisch[...] abgelegt [...]. Weitere Strukturinformationen, z.B. Zusammenhänge von Rohstoff- und Produktchargen, Quelle und Ziel eines gemessenen Durchflusses oder Informationen über die Medien, die gemessen werden, fehlen. **Durch** die Ausnutzung der Kenntnis über den **Bezug von Daten** untereinander **kann -> MUSS** ein **wesentlicher Informationsgewinn zur Analyse und Bewertung von Prozess- und Anlagenzuständen [...]** abgeleitet werden. “



Was ChatGPT dazu sagt...

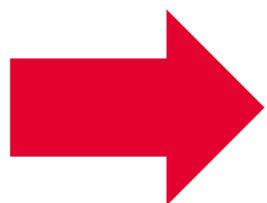
Entspricht Use Cases wie im Zuge eines Aufrufes im Rahmen der Arbeit an **ISO-TS 22440** eingereicht

Nicht zwingend SIL -> „proactive safety“ durch umfassende Informations- und Entscheidungsgrundlage zur sicheren und optimierten Betriebsführung – Akzeptanzkriterien in EN 61508, um davon Kredit zu nehmen



Yes, **AI can play a significant role in safety-critical applications**. It can contribute in several ways:

1. **Predictive Maintenance:**
  - AI can analyze data from sensors to predict equipment failures, enabling proactive maintenance and reducing the risk of critical system breakdowns.
2. **Anomaly Detection:**
  - AI algorithms can identify abnormal patterns or behaviors in real-time, helping to detect potential safety issues before they escalate.
3. **Decision Support Systems:**
  - AI can assist operators by providing real-time insights and decision support, enhancing human decision-making in critical situations.
4. **Autonomous Systems:**
  - In some cases, autonomous systems driven by AI can be employed to perform tasks in hazardous environments, reducing human exposure to risks.
5. **Machine Learning for Risk Assessment:**
  - ML models can analyze historical data to identify patterns and assess risks, aiding in the development of more effective safety protocols.
6. **Human-Machine Collaboration:**
  - AI can enhance human capabilities through collaboration, improving the overall efficiency and safety of complex systems.

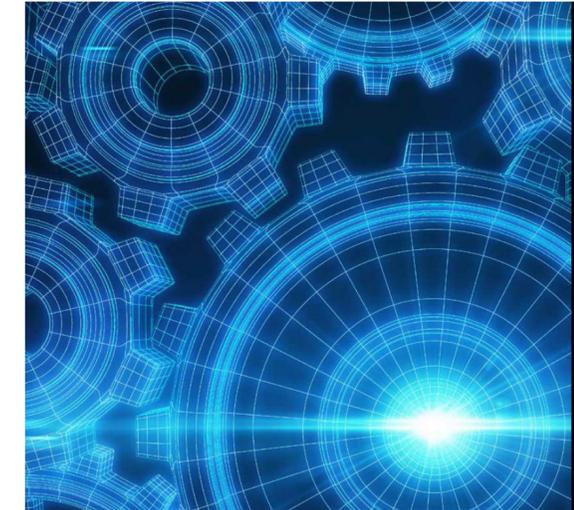


“While AI offers valuable contributions, it's crucial to integrate it responsibly, ensuring that the technology aligns with safety standards and regulations. **Additionally, maintaining a balance between human oversight and automated systems is essential in safety-critical applications.**”

## -> weitere 25 Jahre EN 61508 – These 4

EN 61508 folgt dem **IEC WP Safety in the future:2020-10(en)**

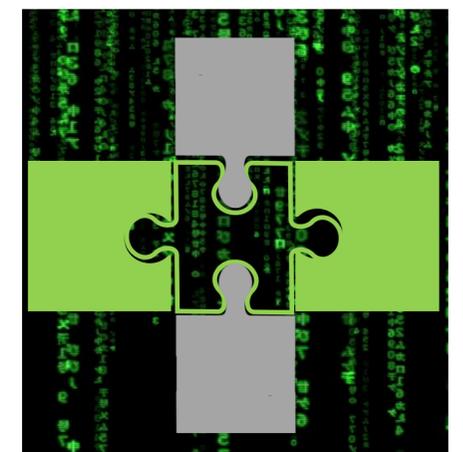
“As humans continue to play a major role in causing workplace accidents, whether at the design and planning stages or during execution of the work, any efforts to improve safety in human-machine collaboration must focus specifically on human/worker behaviour. And while the future can hardly be predicted with precision, technological, societal and legislative megatrends will clearly impact the future of work and safety.[...]”



Safety in the future

White Paper

“In other words, it is recommended that in the development of future safety standards, clear attention be paid to non-technical factors”



# weitere 25 Jahre EN 61508 Temperamente...

IN73LLIG3NC3

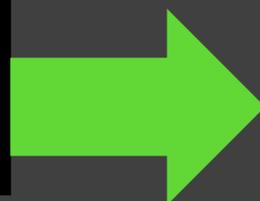
0141587H3158

43481L17Y480

7004D4P7870

183CH4NG314

573PH3N  
H4WK1NG



Nicht mehr, sondern smarter

# Danke für eure Aufmerksamkeit!

## *Marco Knödler*

- – NAMUR AK 4.5 – VDI/VDE-GMA FA 2.18
- – DIN NA 003-01-01 AA - CEN/TC 69/WG 1 -
- – DKE AK 914.0.11 & STD\_1941.0.8 - SCI 4.0
- Expertenrat KI in industriellen Anwendungen

## *Teamleiter EMSR-Technik*

## **Automatisierungstechnik**

## **Engineering**

**YNCORIS GmbH & Co. KG** | Industriestraße 300 |  
50354 Hürth  
**FON** +49(2233)48 6537 | **MOBIL** +49(172) 2661517  
[Marco.Knoedler@yncoris.com](mailto:Marco.Knoedler@yncoris.com) | [www.yncoris.com](http://www.yncoris.com)

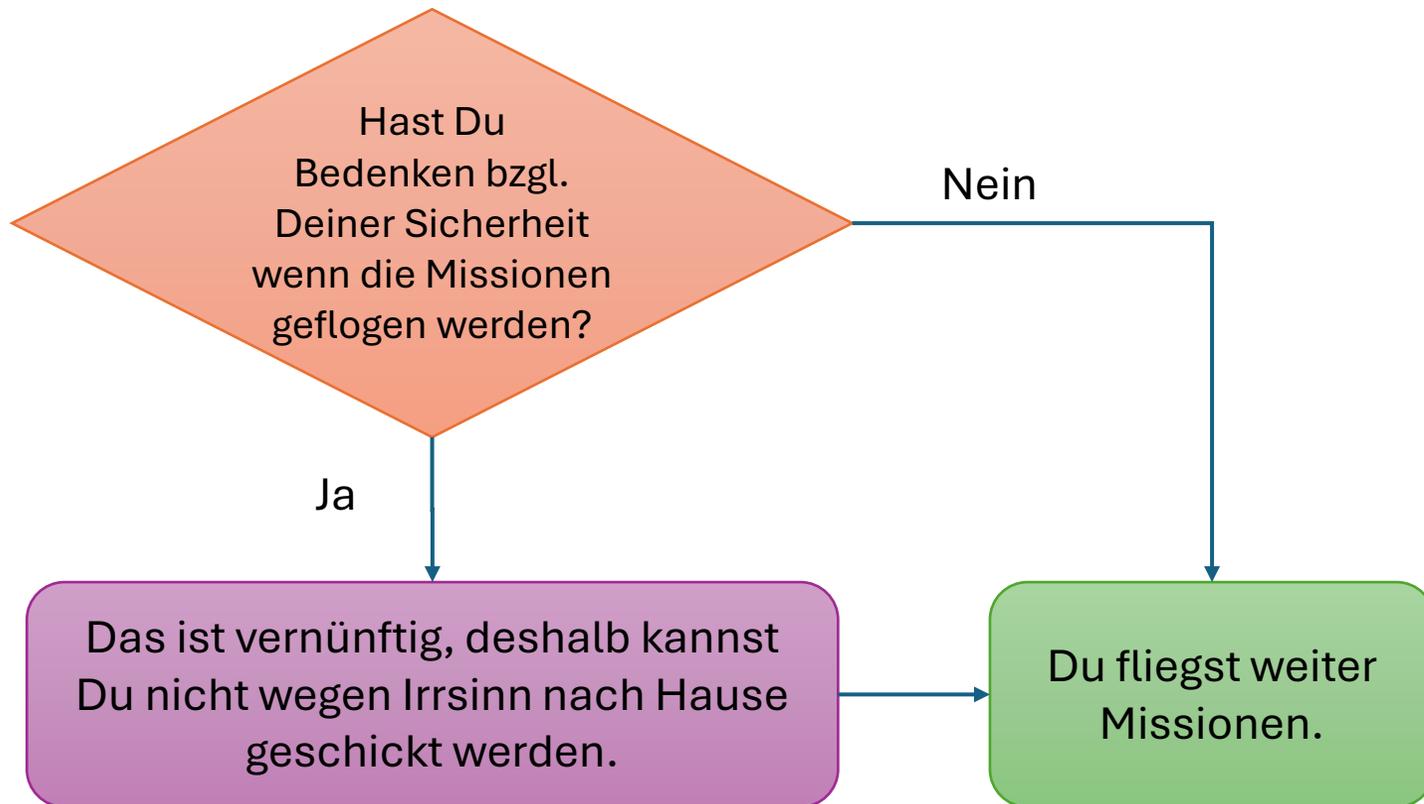


<https://www.linkedin.com/in/marco-knoedler-50653467/>



# Catch 22s in KI und MVO<sup>1</sup> oder warum Philosophie nicht nur für Safety wichtig ist.

„Dilemma or difficult circumstance from which there is no escape because of mutually conflicting or dependent conditions.“

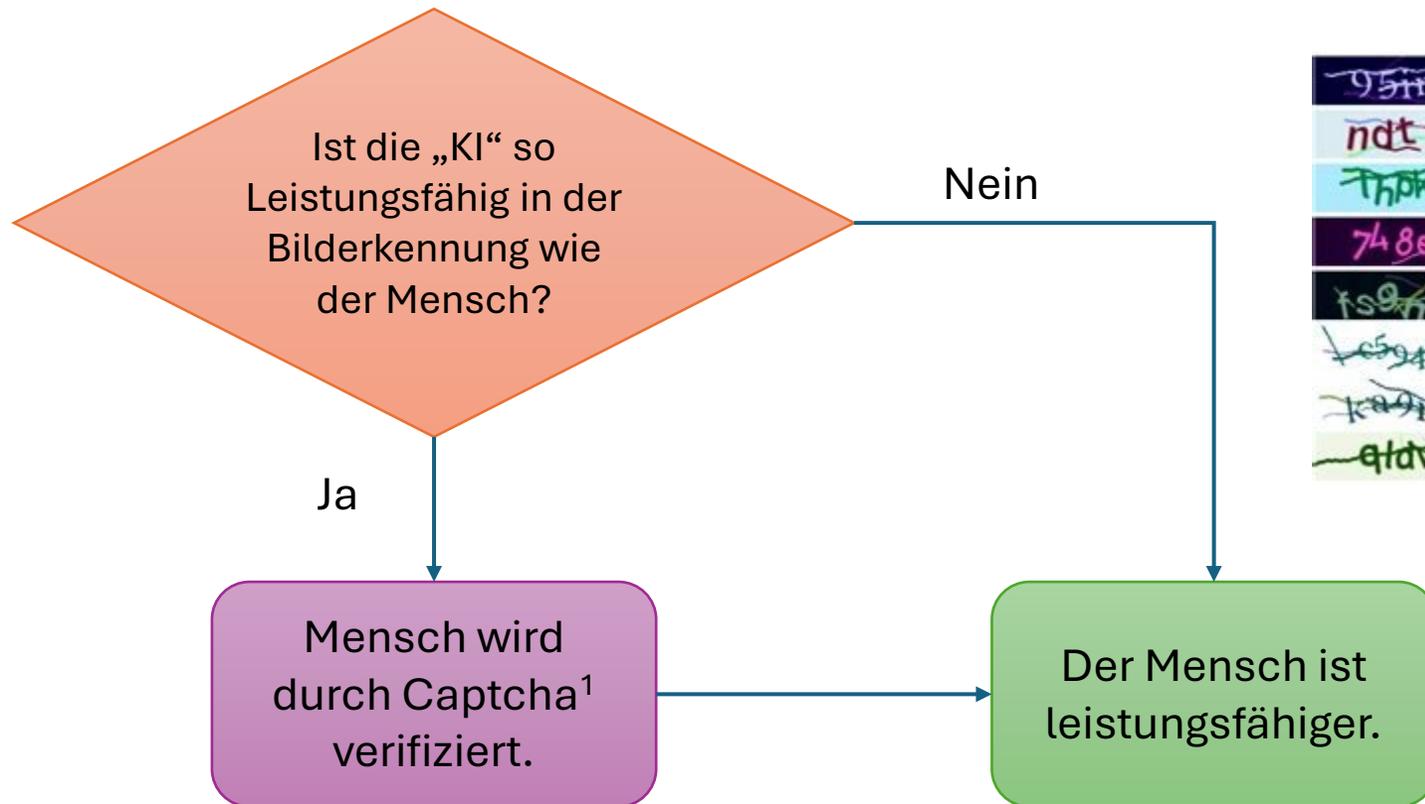


<sup>1</sup> Maschinenverordnung



# Fähigkeiten der KI?

Oder: Wenn man immer noch das Captcha ausfüllen muss...

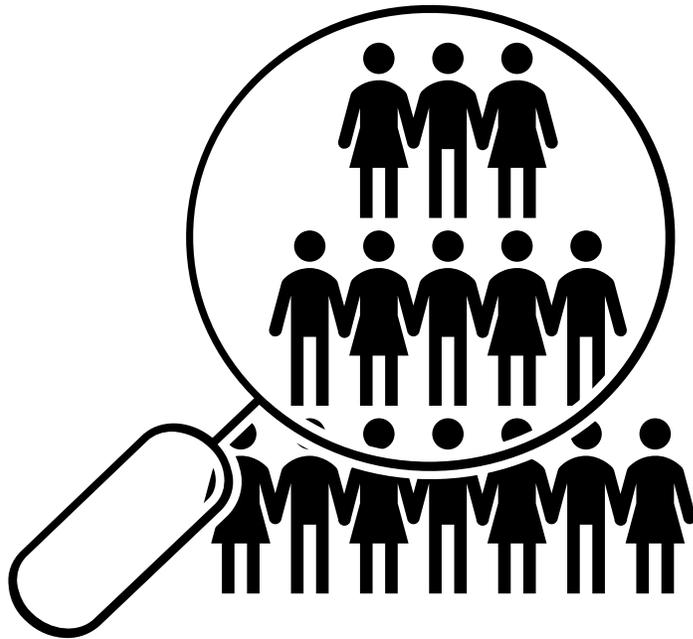


<sup>1</sup>completely automated public Turing test to tell computers and humans apart

# Problem der Repräsentativität vs. Minderheiten oder seltenen Ereignissen

Repräsentativität nach P. von der Lippe und A. Kladroba:

**„Die Auswahl einer Teilgesamtheit ist so vorzunehmen, dass „aus dem Ergebnis der Teilerhebung möglichst exakt und sicher auf die Verhältnisse der Gesamtmasse geschlossen werden kann.“**



Bei Querschnittsstudien ist die Repräsentativität wichtig.

Bei Längsstudien sind weitere Einflussfaktoren (z.B. demographische Entwicklung) einzubeziehen.

*Vorsicht bei Angaben von absoluten Zahlen, oder aus dem Kontext gerissenen Aussagen!*

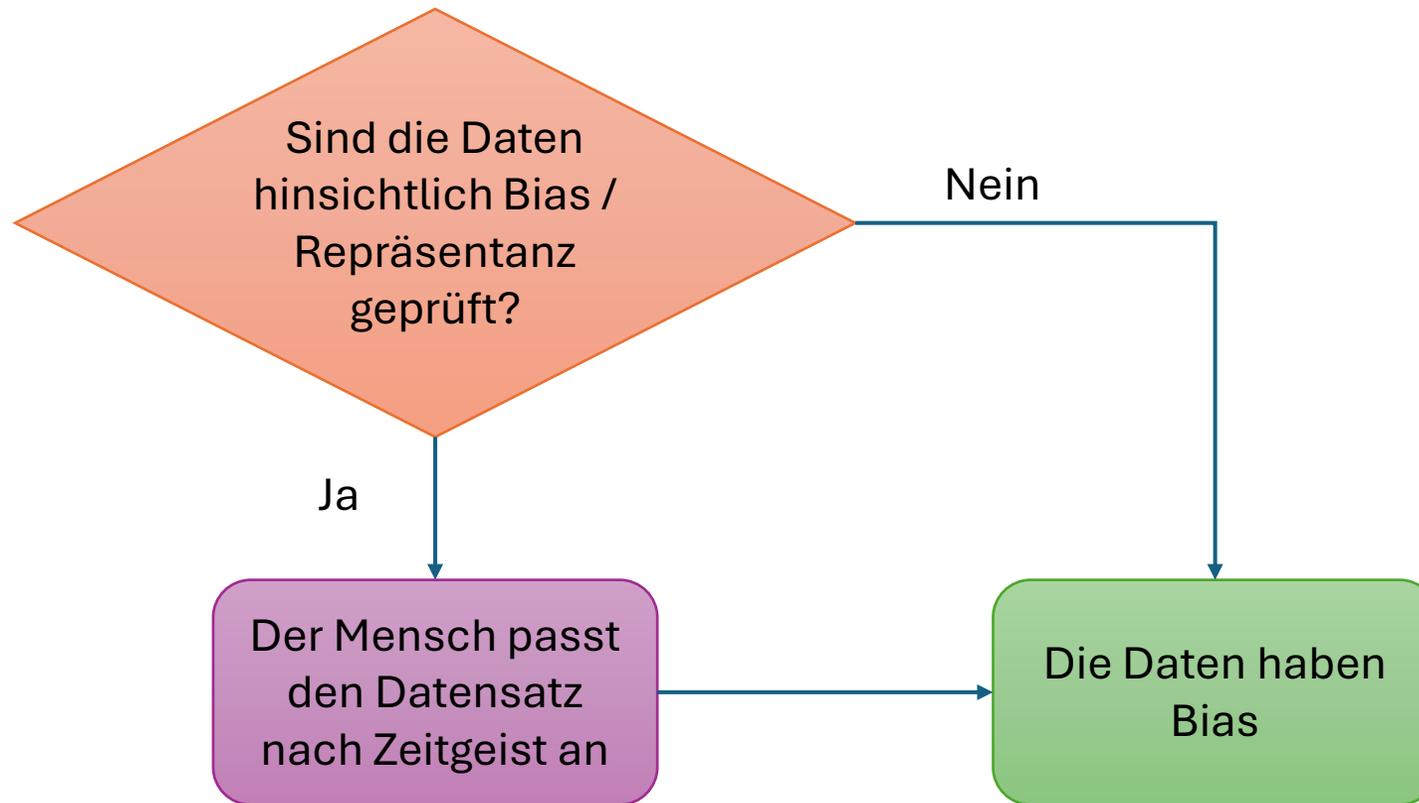
*Beispiel: „Es sterben immer mehr Menschen an Krebs.“*

*Mögliche Rückfragen dazu:*

- *Sterben prozentual mehr Menschen in einer repräsentativen demographiebereinigten Gruppe?*
- *Sterben insgesamt anteilig mehr Menschen?*
- *Hat sich die Definition von Krebs geändert?*

# Daten ohne Bias – gibt es das?

## Beispiel: Geschlecht vs. Repräsentativität



# Problem der Repräsentativität vs. Minderheiten oder seltenen Ereignissen

## **Beispiel:**

Ein ML Algorithmus wird nun auf die Erkennung des Geschlechtes trainiert (was eigentlich schon Persönlichkeitsrechte verletzen könnte). Entgegen der bestehenden Wahrnehmung wird die Gruppe „Divers“ nur mit 0,0012 % in die Repräsentanz eingehen<sup>1</sup>.

Aufgrund des akt. Zeitgeistes könnte nun dieser Anteil höher gewichtet werden, was aber zu einem Bias in den Daten führt, welcher die Gruppe der „Männer“ und „Frauen“ entsprechend benachteiligt. Umgekehrt wird bei Verwendung von repräsentativen Daten die „Divers“ Gruppe durch ihre statistische Seltenheit übergangen.

Oder man ist der Meinung, dass die Geschlechter in jeder Situation gleich verteilt vorkommen, obwohl in der Realität nur 20 % der Frauen<sup>2</sup> z.B. "Informations- und Kommunikationstechnologien,, studieren.

## **Fazit:**

Wird von der statistischen Repräsentativität abgewichen kommt es Ungleichbehandlung im Algorithmus. Deshalb ist es bei Studien wichtig zu fragen, ob diese repräsentativ sind.

# Datenzuordnung (menschlich) vs. Korrektheit des Algorithmus

Korrelation zwischen dem Rückgang der Storchpopulation und der Abnahme der Geburtenzahl in Baden-Württemberg

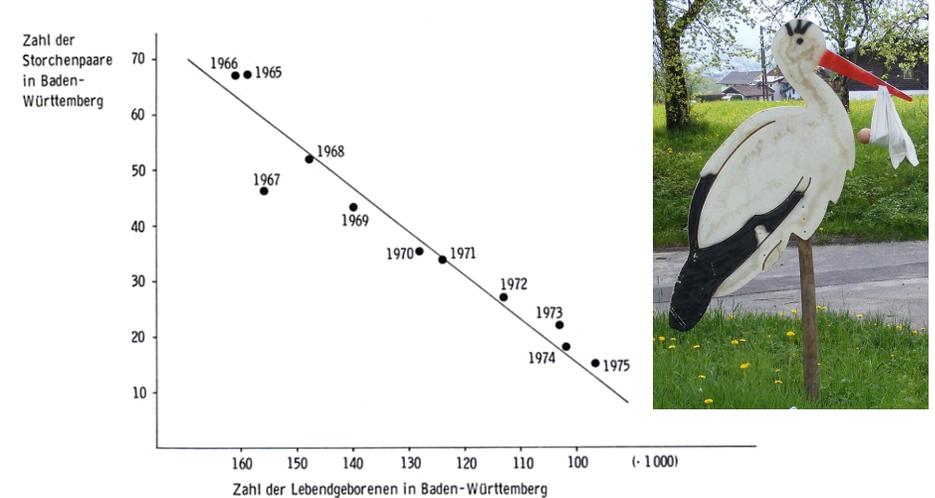
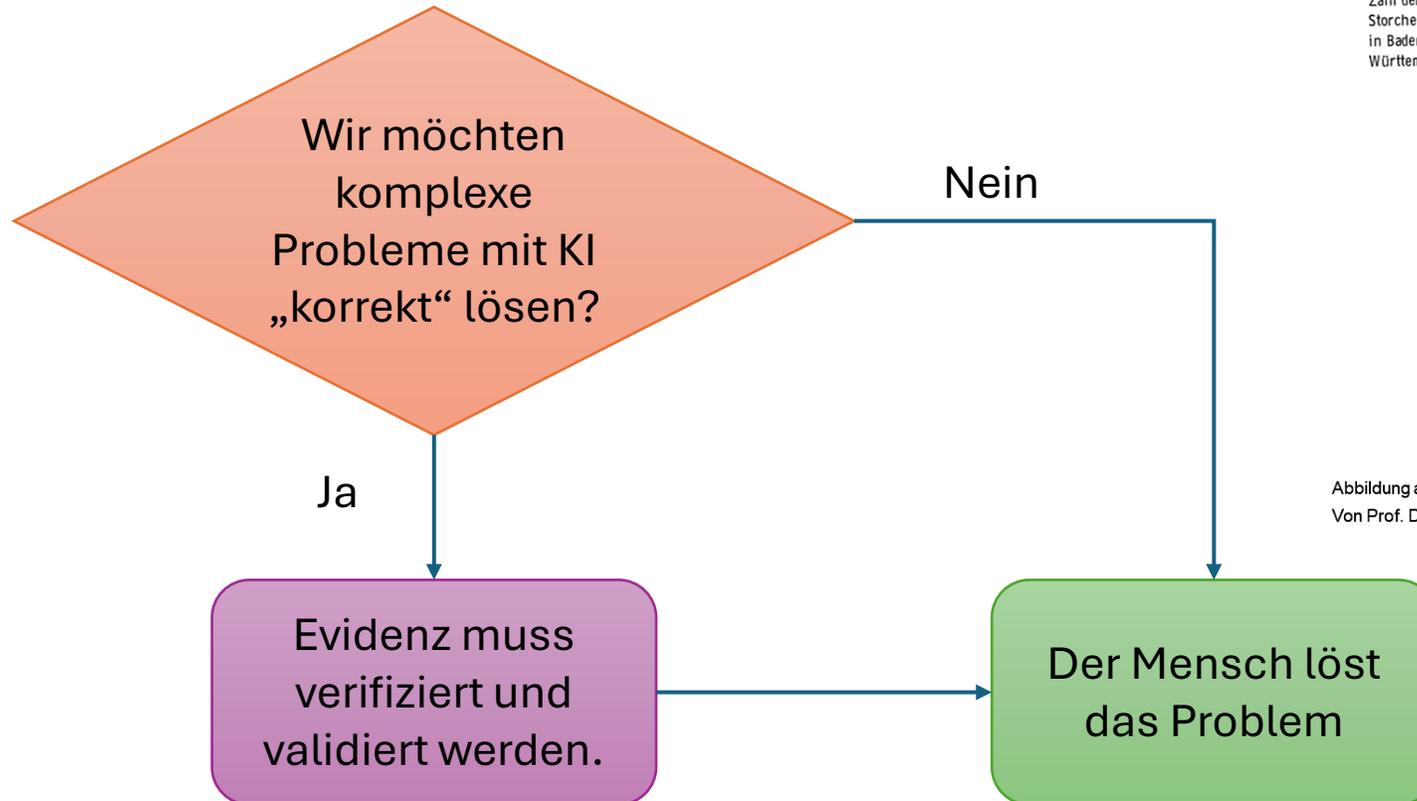


Abbildung aus der Monographie „Kontrazeption mit Hormonen“  
Von Prof. Dr. Hans-Dieter Taubert und Prof. Dr. Herbert Kuhl (Georg Thieme Verlag, Stuttgart 1981)

Scheinkorrelation (Quelle: Wikipedia)



# Kausalität vs. Korrelation

- Dazu benötigt man aufwändige Verfahren welche die relevanten Variablen (den kausalen Zusammenhang) mit:
  - **randomisierten und repräsentativen Daten / Gruppen;**
  - **durch Blind- oder Doppel-Blind-Studien;**
  - **durch Isolation oder Eliminierung von Einflußparametern;**nachweisen.
- Studien scheitern häufig an diesem Kriterium (auch aufgrund von Manipulationen in der Studie, z.B. durch wirtschaftliche Interessen)!
- Bei im Alltag erhobenen Daten wird dies noch schwieriger, weil diese auch unter Datenschutzkriterien und repräsentativ erhoben werden müssten.
- Rückschlüsse auf die Grundgesamtheit liefern i.d.R. nur Wahrscheinlichkeiten und keine Evidenzen!

# Analogie in der Funktionalen Sicherheit

Risiko = Schadensausmaß x Eintrittswahrscheinlichkeit

- Komponenten der Funktionalen Sicherheit (also mit SIL oder PL) liefern dem Kunden ein Versprechen über die Ausfallwahrscheinlichkeit und damit über die Fähigkeit Funktionen zu implementieren, welche garantiert zur Minimierung des Risikos beitragen.
- Die Entwicklungsarbeit, insbesondere Verifizierungs- und Validierungsarbeit (=> **Kausalität**), die für SIL / PL fähige Systeme geleistet wurde, sind die Grundlage für dieses Versprechen.
- Kann ein Verfahren mit „KI-Algorithmus“ insgesamt keinen garantierten „Arbeitsvorteil“ erzeugen entsteht kein sicherheitstechnischer oder wirtschaftlicher Nutzen.

# Vollständigkeit vs. Systematische Abstraktion

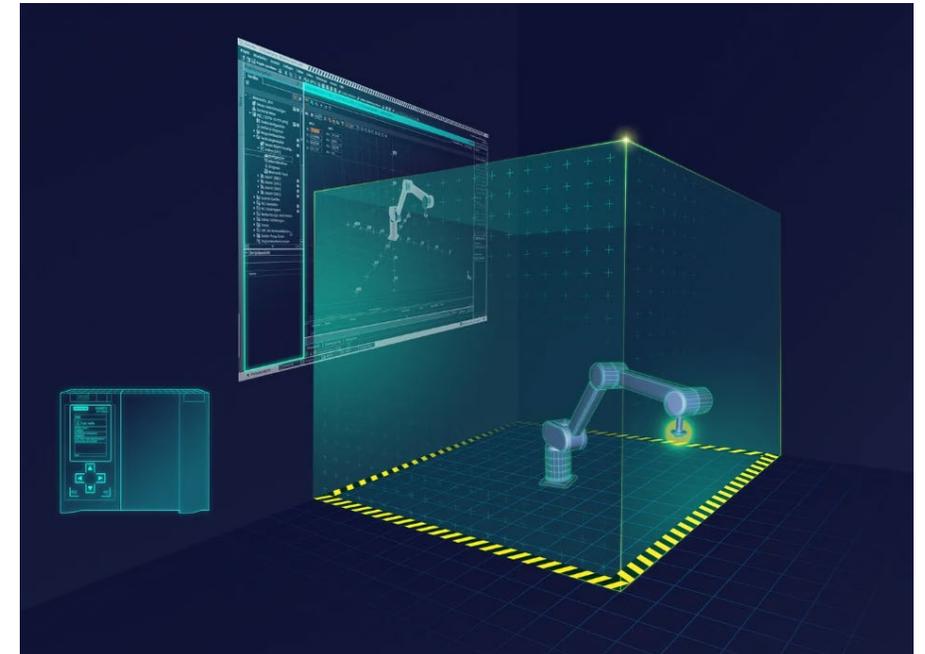
Funktionale Sicherheit verlangt systematische Entscheidungen, um die Komplexität zu adressieren.

## **Beispiel:**

Die Entscheidung eine Maschine mit Schutzzaun auszurüsten, vereinfacht das Safety-Problem zu: **Geöffnete Schutztür und Maschine in Betrieb ist zu verhindern.**

Soll nun die Maschine ohne Schutzzaun gebaut werden folgen daraus komplexe Fragestellungen:

- Wie kann der gefährliche Zustand für den Menschen definiert werden?
- Wie wird erkannt, dass es sich um ein Objekt oder einen Menschen handelt?
- Welche Arbeitsmodi – Kooperativ oder koexistierend können stattfinden?
- Welche Situationen und Zustände sind im Maschinenarbeitsbereich akzeptabel oder inakzeptabel?



**Diese Entscheidungen bleiben immer Entscheidungen des Menschen. Wäre dem nicht so, wäre der Mensch zu seiner Unversehrtheit nicht mehr in der souveränen Entscheidung!**

# Anforderungen in der Machinenverordnung (EU) 2023/1230

## Annex III Part B – General principles

The risk assessment and risk reduction shall include hazards that might arise during the lifecycle of the machinery or related product that are foreseeable at the time of placing the machinery or related product on the market as an intended evolution of its fully or partially self-evolving behaviour or logic as a result of the machinery or related product designed to operate with varying levels of autonomy.

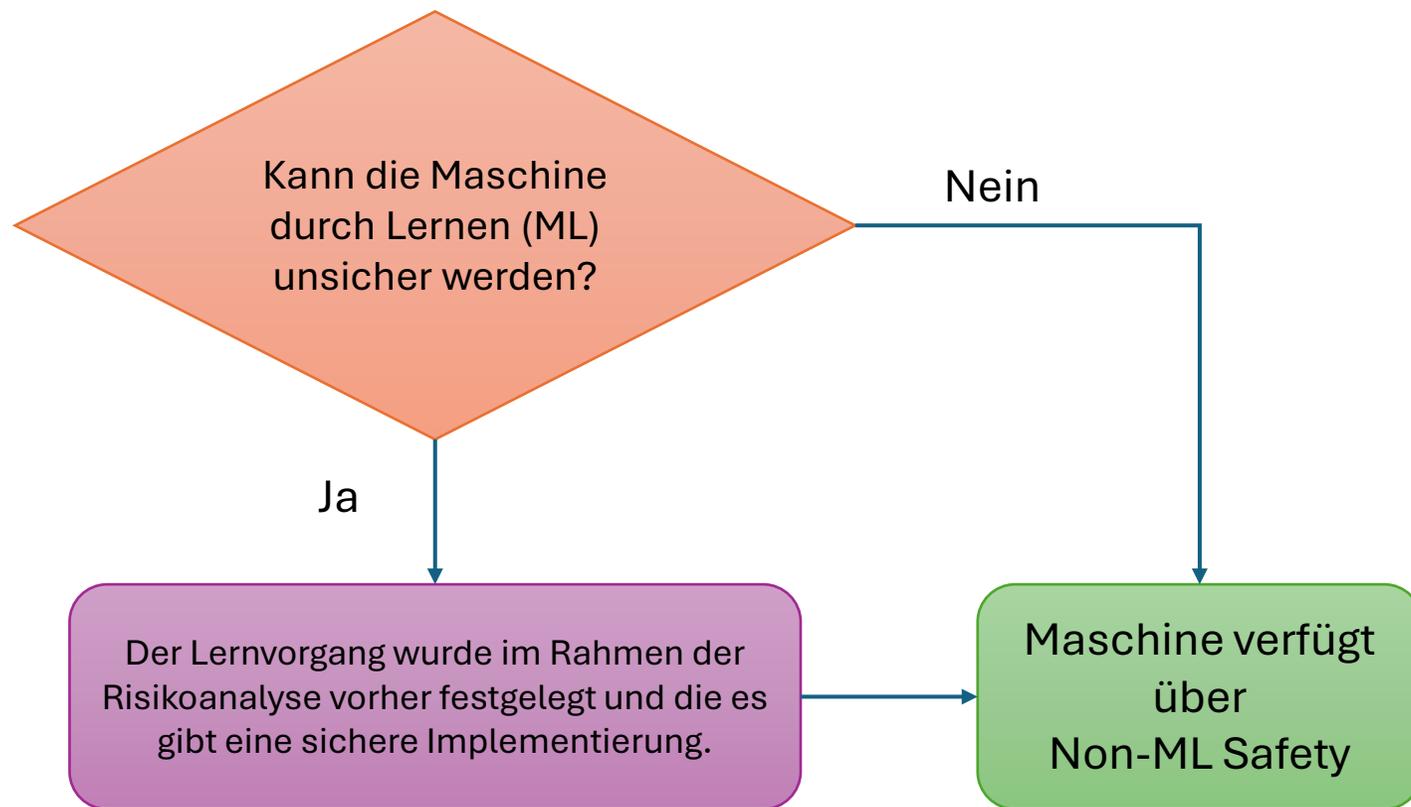
### 1.2.1. Safety and reliability of control systems

(d) the limits of the safety functions are to be established as part of the risk assessment performed by the manufacturer and no modifications are allowed to the settings or rules generated by the machinery or related product or by operators, including during the machinery or related product learning phase, where such modifications could lead to hazardous situations;

### Fazit:

Die Maschine darf sich selbst weiterentwickeln, solange dies nicht zu einem gefährlichen Zustand führt!

# Safety-Paradoxon der selbstlernenden Maschine



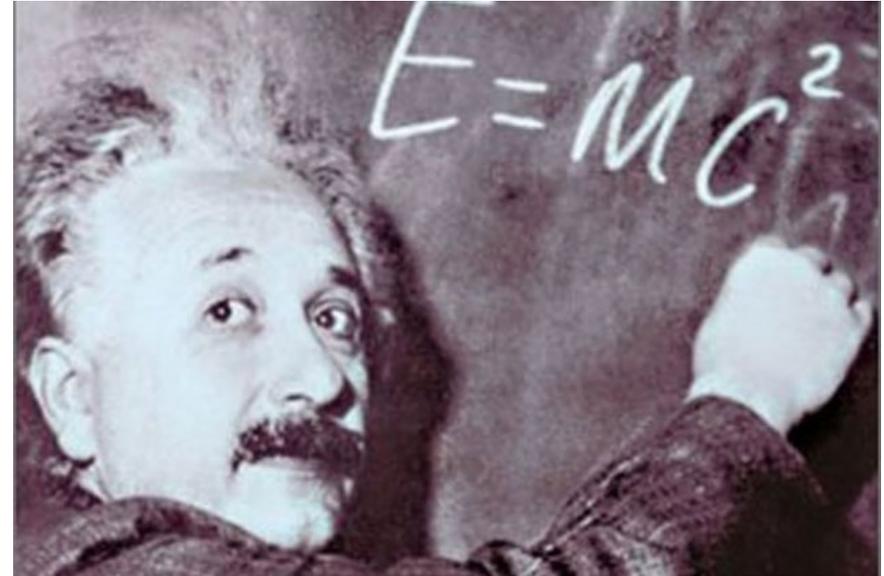
# Exkurs: Parsimonie

Das **Prinzip der Sparsamkeit**, die einfachste Lösung ist die Beste, dies vertrat auch Leibniz.

Es war lange das Prinzip in der Wissenschaft, z.B. Formeln durch umformen zu vereinfachen.

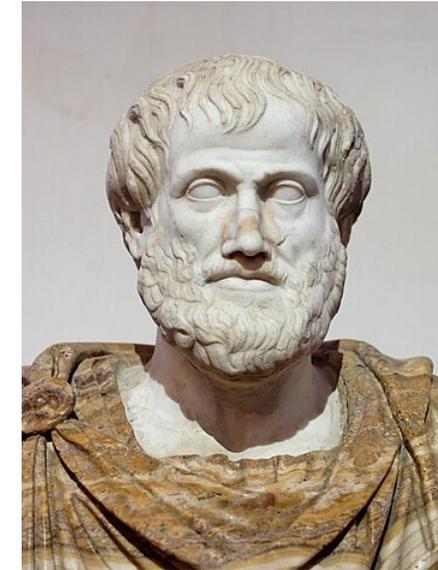
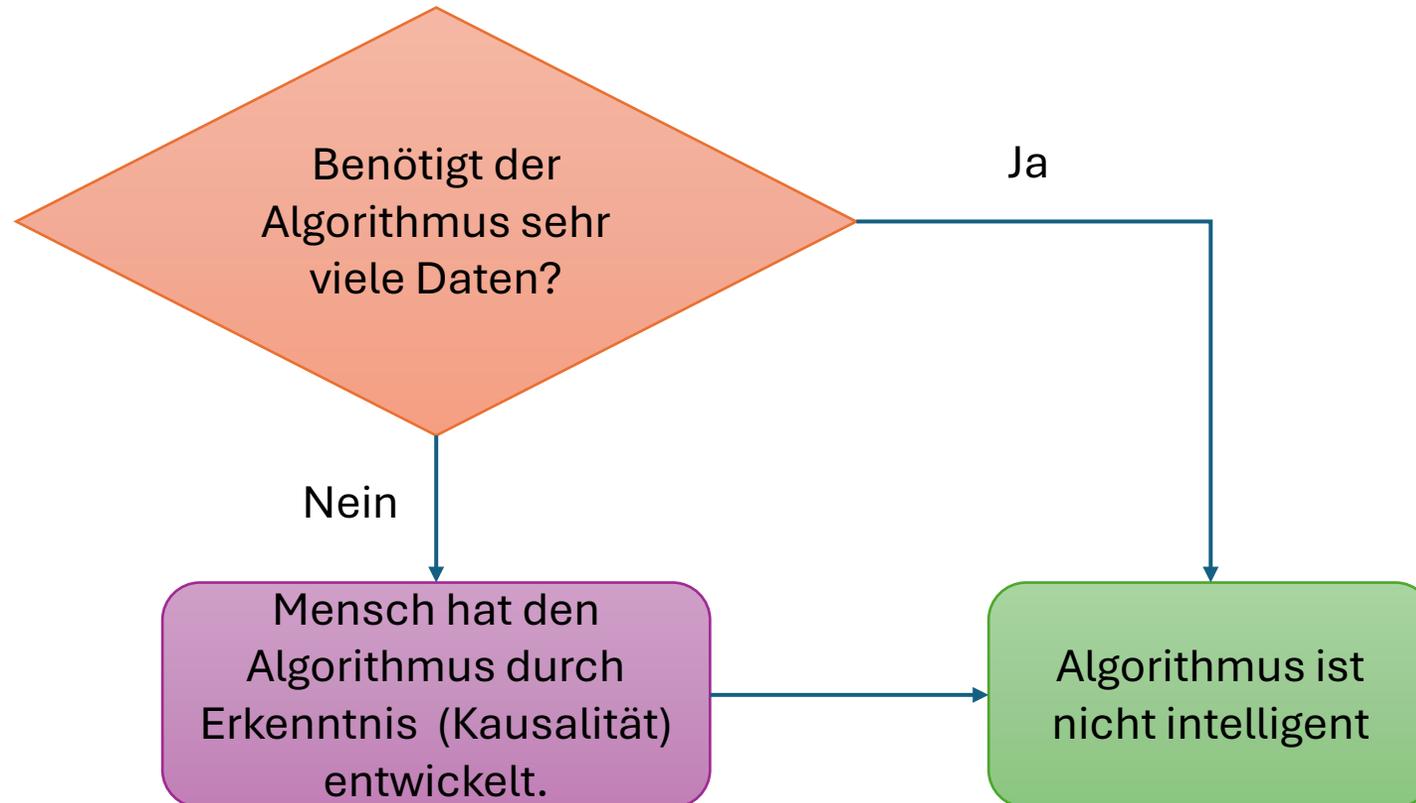
Vereinfachung kann aber dazu führen, dass man z.B. fälschlicherweise Einflussgrößen vernachlässigt.

Das „KI“ Narrativ ist allerdings, dass der Algorithmus immer besser wird, je mehr Daten er analysiert hat. **Warum eigentlich?**



Einstein faszinierte mit einer sehr „einfachen“ Formel.

# Datenmenge vs. Qualität des Algorithmus



Aristoteles behauptete, dass die Natur den einfachsten Weg wählt.

Intuitiv ist das auch einleuchtend aufgrund des Energieaufwandes.

# Parsimonie bei der Gesichtserkennung

Beispiel:

Mit 205 Nervenzellen im Gehirn von Affen kann ein Gesicht rekonstruiert werden<sup>1</sup>.

Beobachtung:

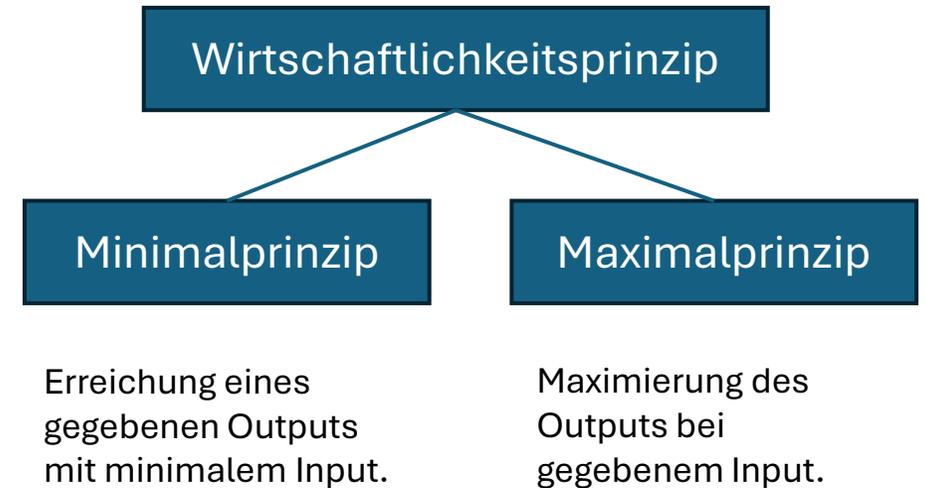
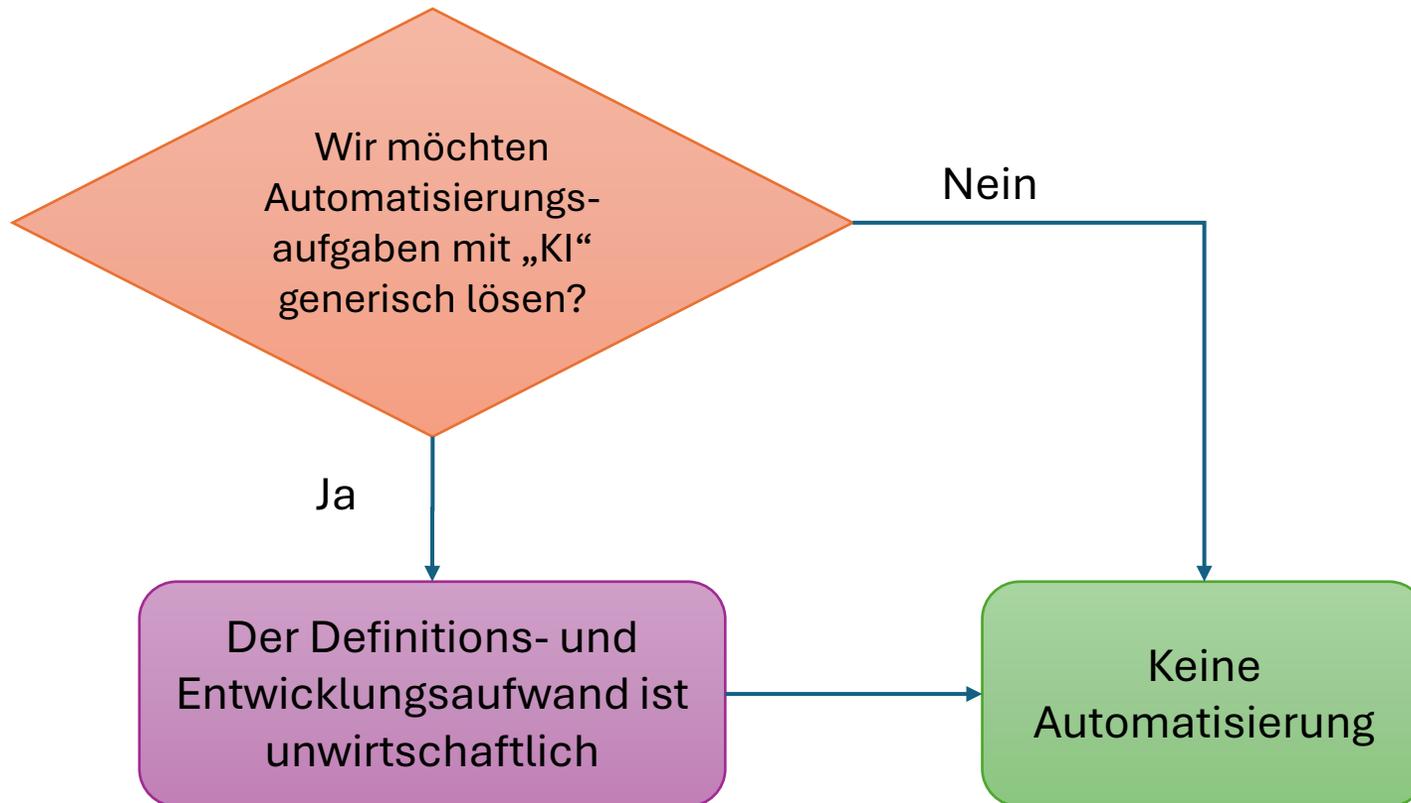
Bei Big-Data ML wird mit großem Aufwand kompensiert, dass grundsätzliche Wirkprinzipien **nicht verstanden** sind.

Durch die Vergabe von hohen Forschungsgeldern wird die KI-Forschung weiter bevorzugt.



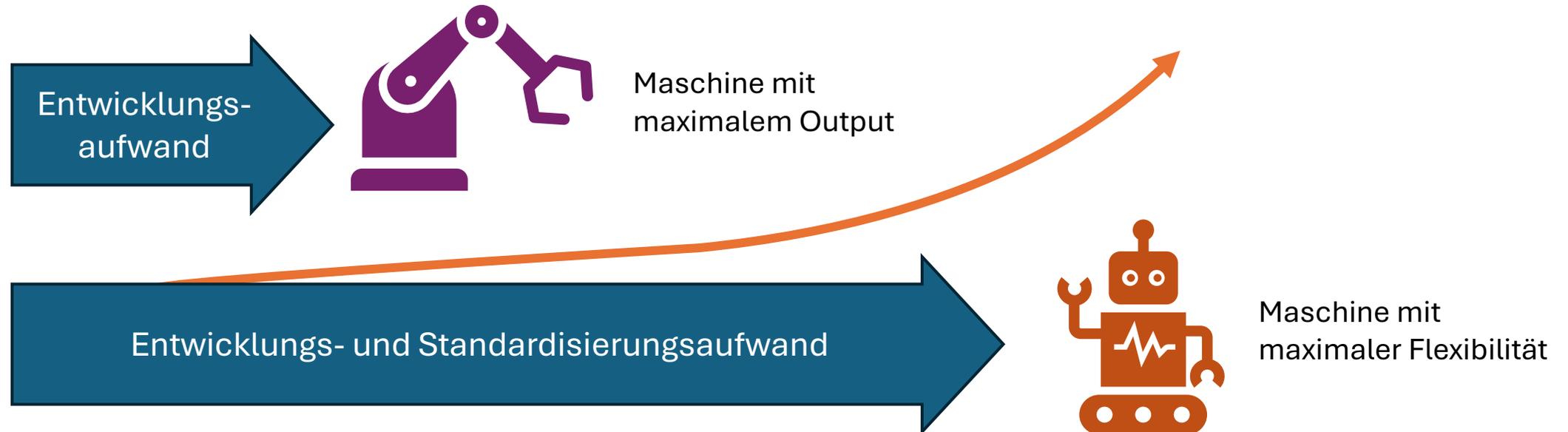
Links das Originalbild und rechts die Rekonstruktion.

# „KI“ Automatisierung vs. Wirtschaftlichkeitsprinzip



# Engineering und Standardisierungsaufwand

- Geschwindigkeit vs. Präzision, Universalität, Qualität
- Automatische Verarbeitung vs. Standardisierung, Vollständigkeit
- Ressourcen vs. Wirtschaftlichkeit



# Rechenleistung (Energieeinsatz) vs. Nutzen

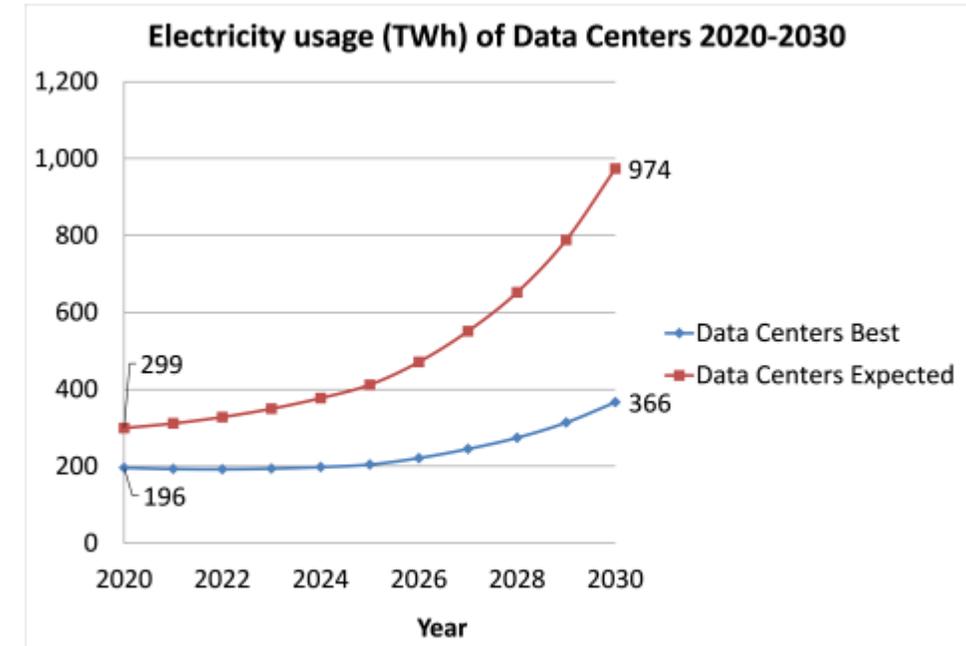
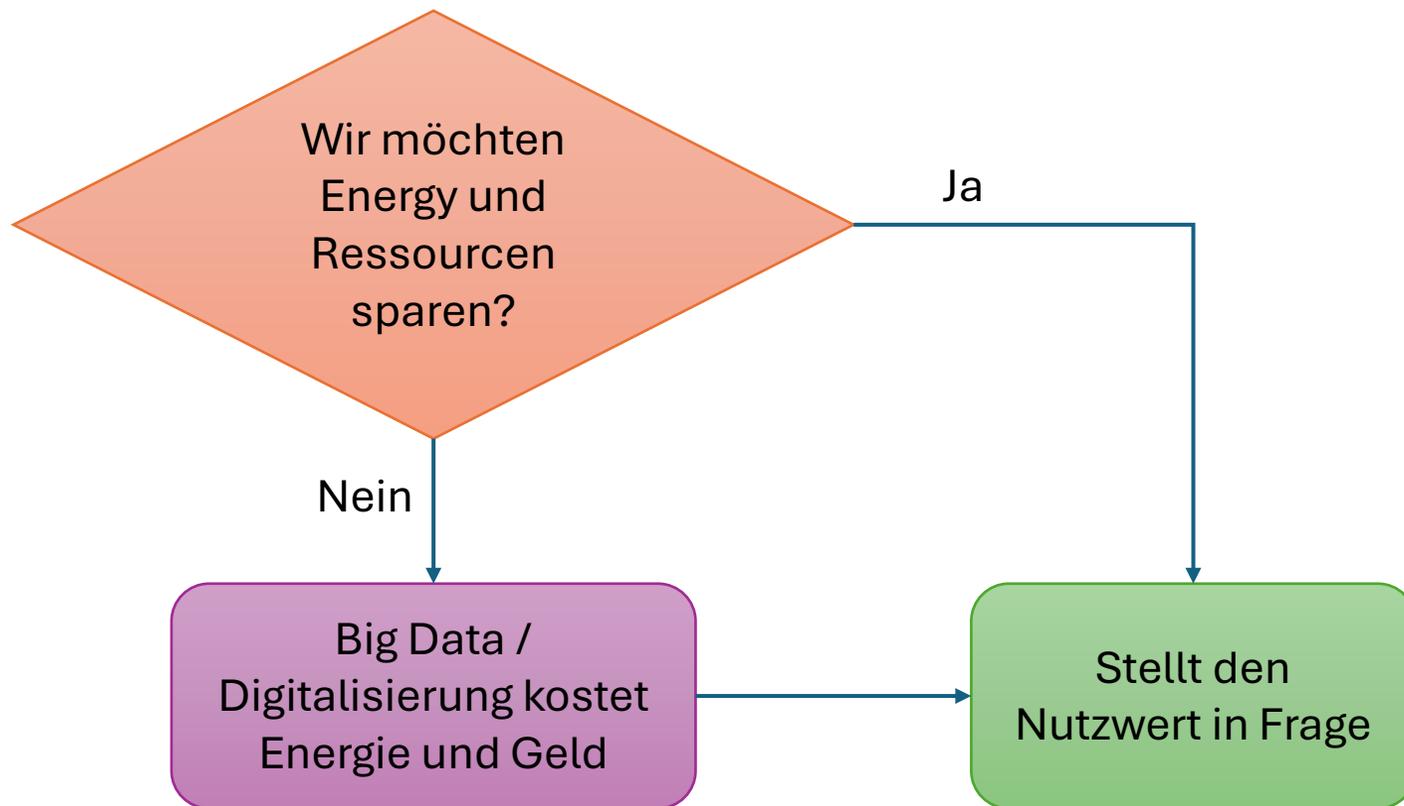
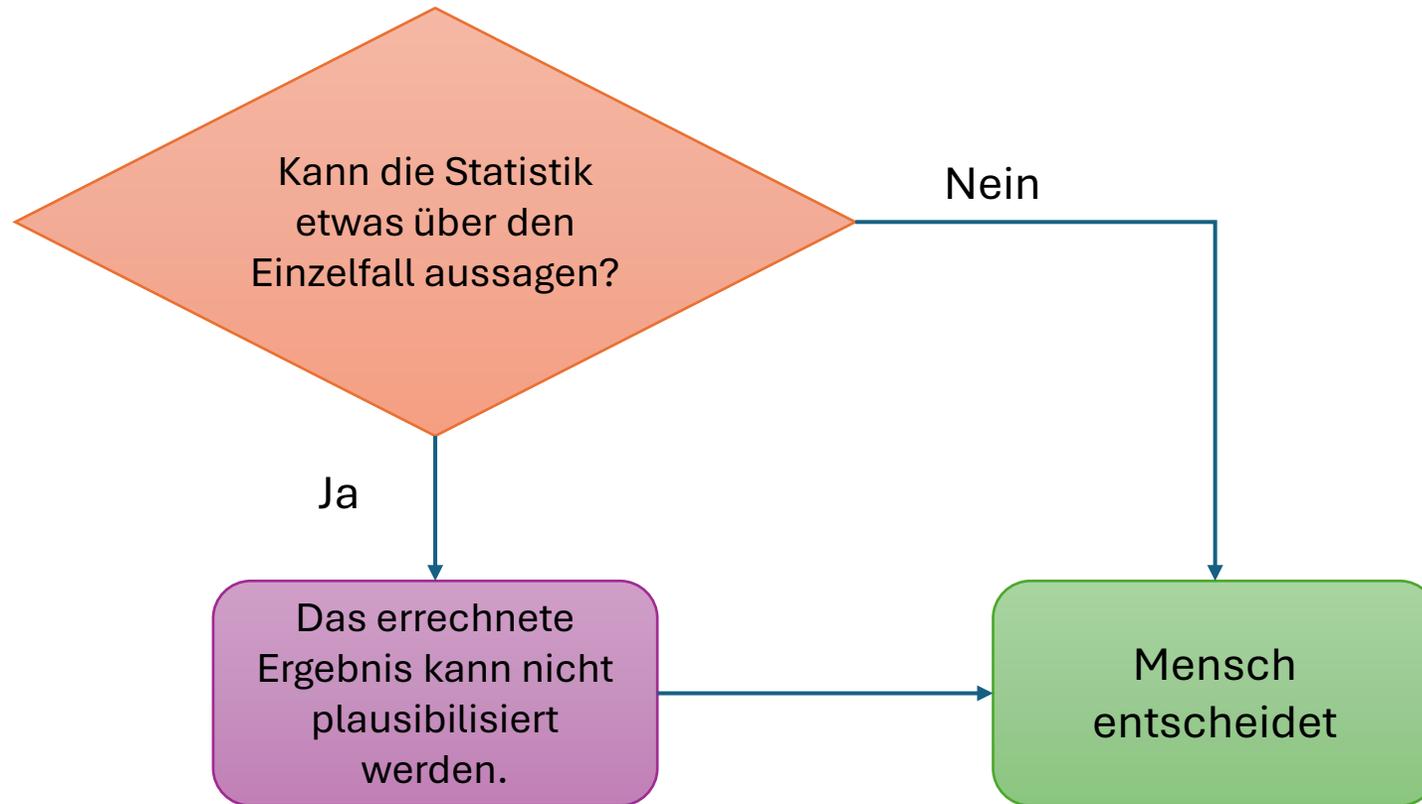


Figure 1. Trends for data centers 2020 to 2030.

Energieverbrauch (Quelle: researchgate)

# Statistik vs. spezifische Korrektheit

## Beispiel: „KI“ für individualisierte Medizin



Dieser Punkt überschneidet sich auch mit dem Punkt „Kausalität vs. Korrelation“

In der Medizin ist es besonders schwierig Kausalität zu erkennen.

# Beispiel: Krebsfrüherkennung - PSA Wert

Mit dem PSA Wert glaubt man einen Indikator für Prostata-Krebs zu haben.

Datenlage<sup>1</sup>: 12 000 Tote / Jahr (3.-häufigste Krebserkrankung) => 3 % der Männer  
Krebs wächst meist langsam und  
im Alter zwischen 55 – 60 Jahren ist das die Todesursache nur an Platz 22.

1980 wurden 17 000 Neuerkrankungen / Jahr diagnostiziert;  
im Jahr 2000 - 48 000 und in 2015 - 70 000.

Lebenserwartung der Männer im Jahr 1980 war 76,5 Jahre,  
aber 2010 schon 81,2 Jahre.

Die 5 Jahre mehr Lebenserwartung kann den Anstieg nicht erklären,  
aber ein großer Teil der „Neuerkrankungen“ geht auf die Früherkennung zurück.

Studie von 1995 an toten Männern (durch Autounfälle) - **asymptomatisch** bzgl. Prostata:  
Männer zwischen 20 - 29 Jahren haben schon zu 10 % Prostatakrebs,  
zwischen 50 – 59 Jahren schon 45 %, und  
zwischen 70 – 80 Jahren über 80 %.

1) Buch: „Krank durch Früherkennung“

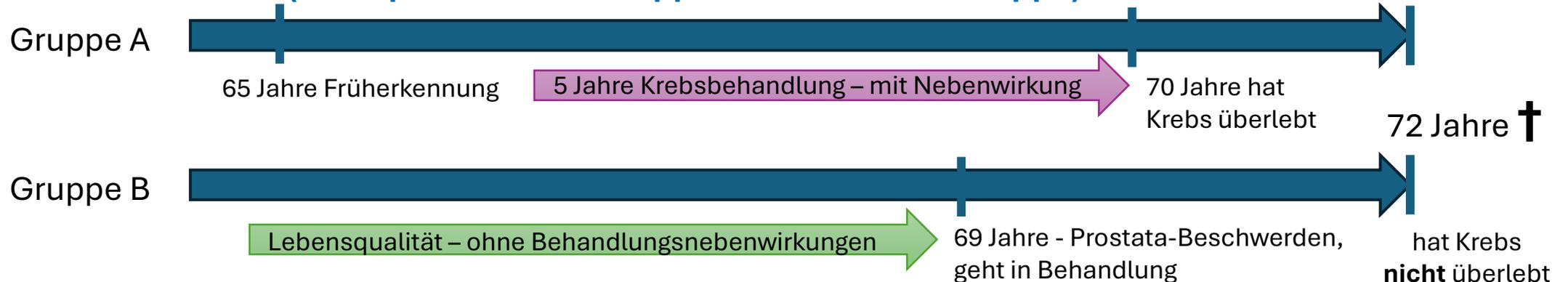
# Beispiel: Krebsfrüherkennung - PSA Wert

Erkenntnis: Wo ist der Nutzen, wenn nur jeder 16. Mann ein Problem bekommt, aber man 15. Männer ggf. sinnlos früherkennt und behandelt?

Solche Messgrößen und Annahmen werden aber in der **Big-Data Medizin** der Regelfall sein.

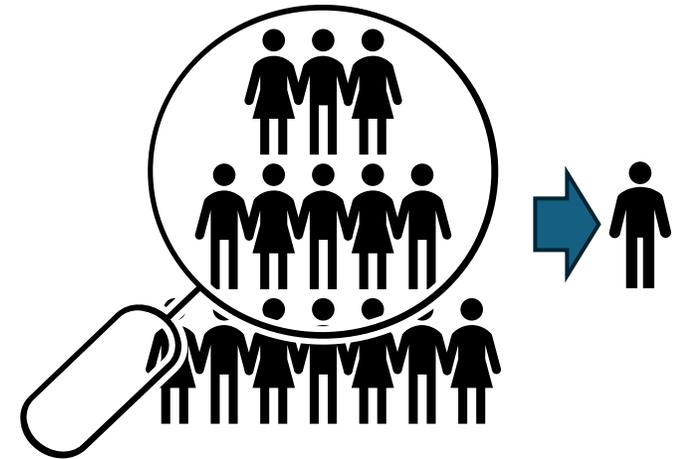
Gruppe A ist durch Früherkennung „erfolgreich“ (5 Jahre Überlebensrate) behandelt worden. Wirklich? Der PSA Grenzwert wird z.B. von Interessensvertretern festgelegt!

**Entscheidend ist aber die Mortalität (der repräsentativen doppelt-verblindeten Gruppe) und nicht ein Zielwert wie PSA!**



# Offene Fragen bei Früherkennung durch „KI“

- Patient wird analysiert und bekommt aufgrund von Diagnosen und Datenanalysen eine Prognose, dass er in 5 Jahren Krebs bekommen würde (55 % Wahrscheinlichkeit).
- Der Patienten wird präventiv mit einem individuellen Medikament behandelt.
- **Folgende Fragen drängen sich auf:**
  - Kann Statistik etwas über den Einzelfall sagen?
  - Wer ist die Vergleichsgruppe bei einem individuellen Medikament?
  - Wie kann der Erfolg der Behandlung bewertet werden?
  - Werden Patienten mit einer präventiven Behandlung eine gesundheitliche Verbesserung bzw. Lebensverlängerung haben?



Die bisherigen Daten (mit repräsentativen doppelt-verblindeten Gruppen) zur Früherkennung bestätigen **keinen** Nutzen (auch bei Brustkrebs, Cholesterin, Blutdruck).

# Betrachtung zu 25 Jahren IEC 61508

Die Quote tödlicher Arbeitsunfälle hält sich auf dem historischen Tiefstand von 0,01 je 1.000 (2022) Vollarbeiter seit 2009 (1987 waren es 0,04).

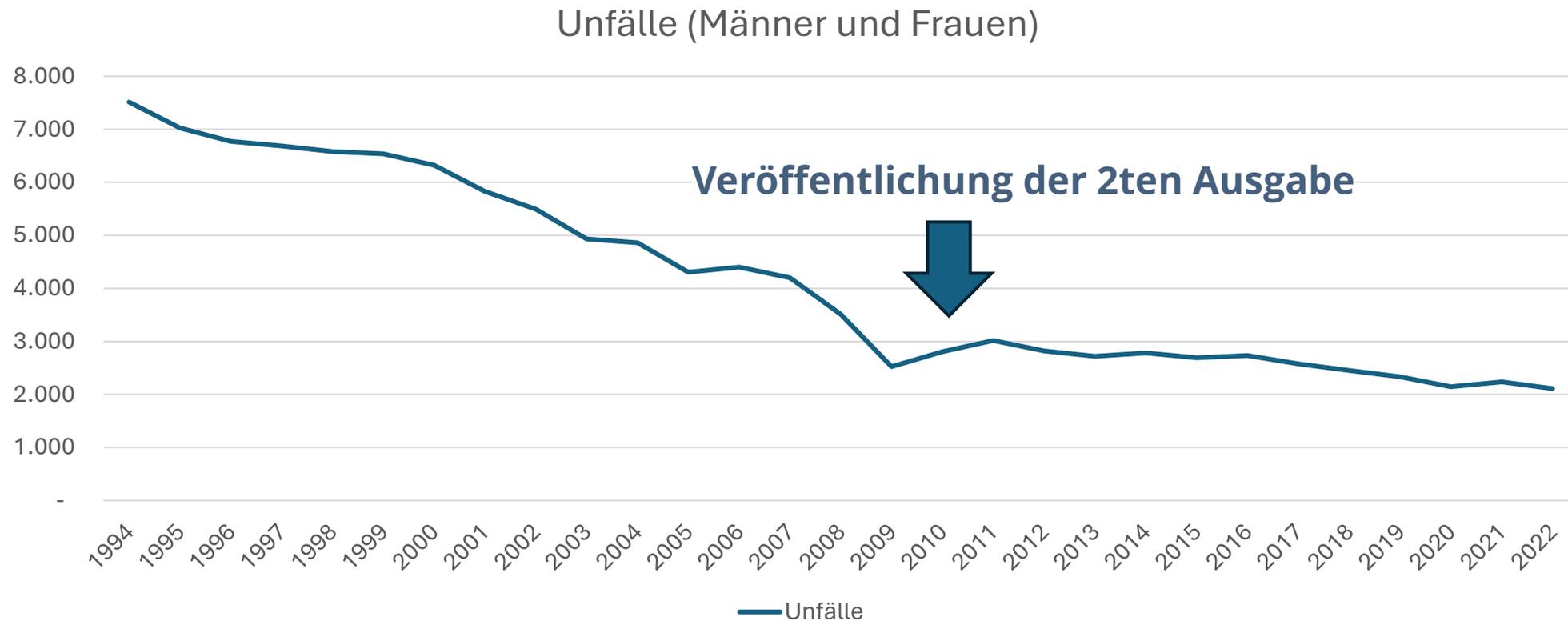
**D.h. die Veröffentlichung der 2ten Ausgabe im Jahre 2010 hatte hinsichtlich der Todesfälle am Arbeitsplatz keine Auswirkung!**

Die 7 häufigsten Arbeitsunfälle

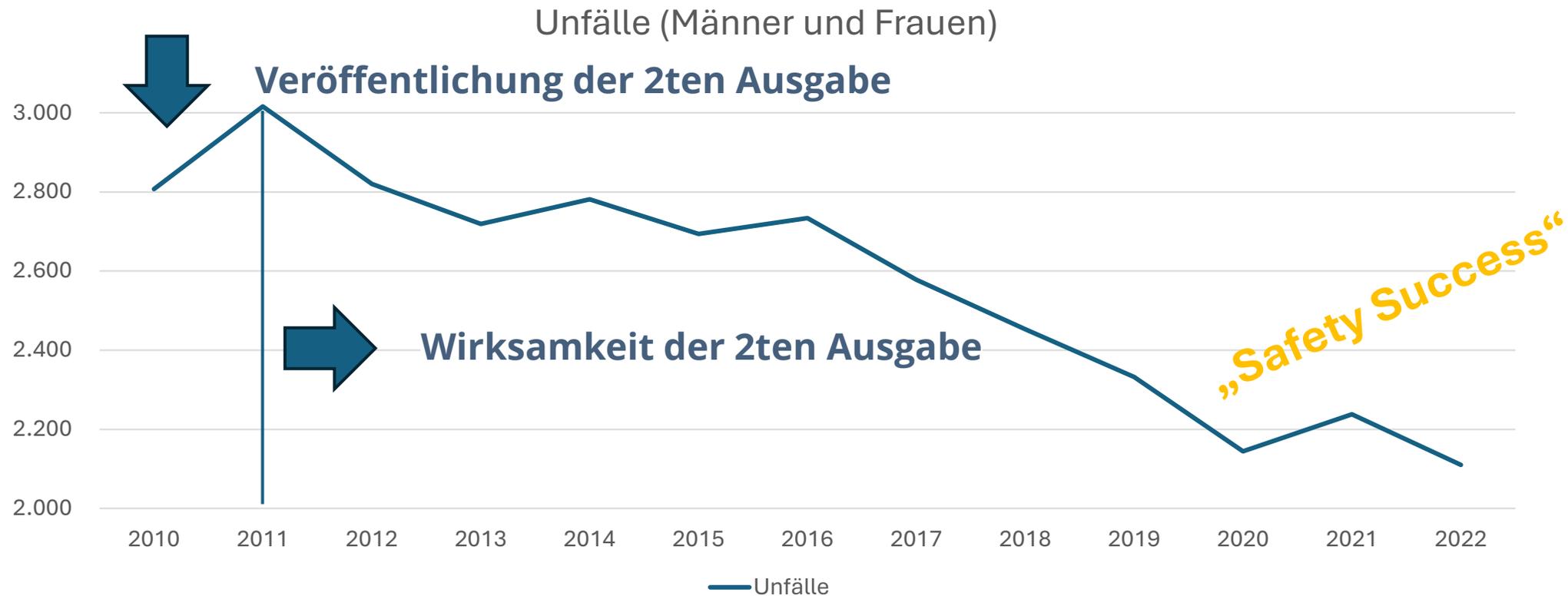
1. Stolpern, Rutschen, Stürzen
2. Falsches Bedienen von Werkzeug und Maschinen => Könnte indirekt relevant sein für FuSi.
3. Falsches Heben, Tragen und Lagern
4. Missachten von Sicherheitsvorschriften => Könnte indirekt relevant sein für FuSi.
5. Mangelnde Erfahrung => Könnte indirekt relevant sein für FuSi (es geht um Erfahrung des Bedieners).

**Die gute Nachricht ist, dass die bestehenden Normen (nicht nur 61508) eine gute Basis für Safety sind, solange diese beachtet werden (daher im Folgenden nochmals deutsche Zahlen).**

# Nicht-tödliche Arbeitsunfälle mit mehr als 3 Tagen Abwesenheit je 100 000 Erwerbstätige



# Nicht-tödliche Arbeitsunfälle (anders dargestellt)



# Impact der 3ten Ausgabe

Die Unfallzahlen rechtfertigen keine inhaltlichen Verschärfungen der Anforderungen (was auch im deutschen Spiegel anfangs so beschlossen wurde).

Bekannt gewordene Vorfälle beziehen sich in der Regel auf systematische Themen.

Real wurden aber in folgenden Bereichen erhöhte Anforderungen entwickelt:

- 1) Tool Qualifikation
- 2) Diagnosefunktionen

Praktisch führt dies nur zu mehr Entwicklungs-, Beratungs- und Zulassungskosten.

**... aber es gibt auch Neuerungen mit aktueller Relevanz....**

# Neue Definitionen zu „KI“- Safety

## **Software Technology Class I (SWTC I)**

implemented software being developed by human programming or coding, which can be completely followed-up, understood and reviewed over all lifecycle phases, including the software off-line support tools used (e.g. code compilers), where all data sources / parameters are predetermined and limited by humans and no functional self-evolvment of the software itself during operation is possible

## **Software Technology Class II (SWTC II)**

implemented software at least initially being developed by human programming but partly developed or coded by software algorithms (e.g. machine learning), which cannot be completely followed-up, understood and reviewed by humans over all lifecycle phases, including the software off-line support tools used (e.g. code compilers), where all data sources / parameters are predetermined and limited by humans and no functional self-evolvment of the software itself during operation is possible

## **Software Technology Class III (SWTC III)**

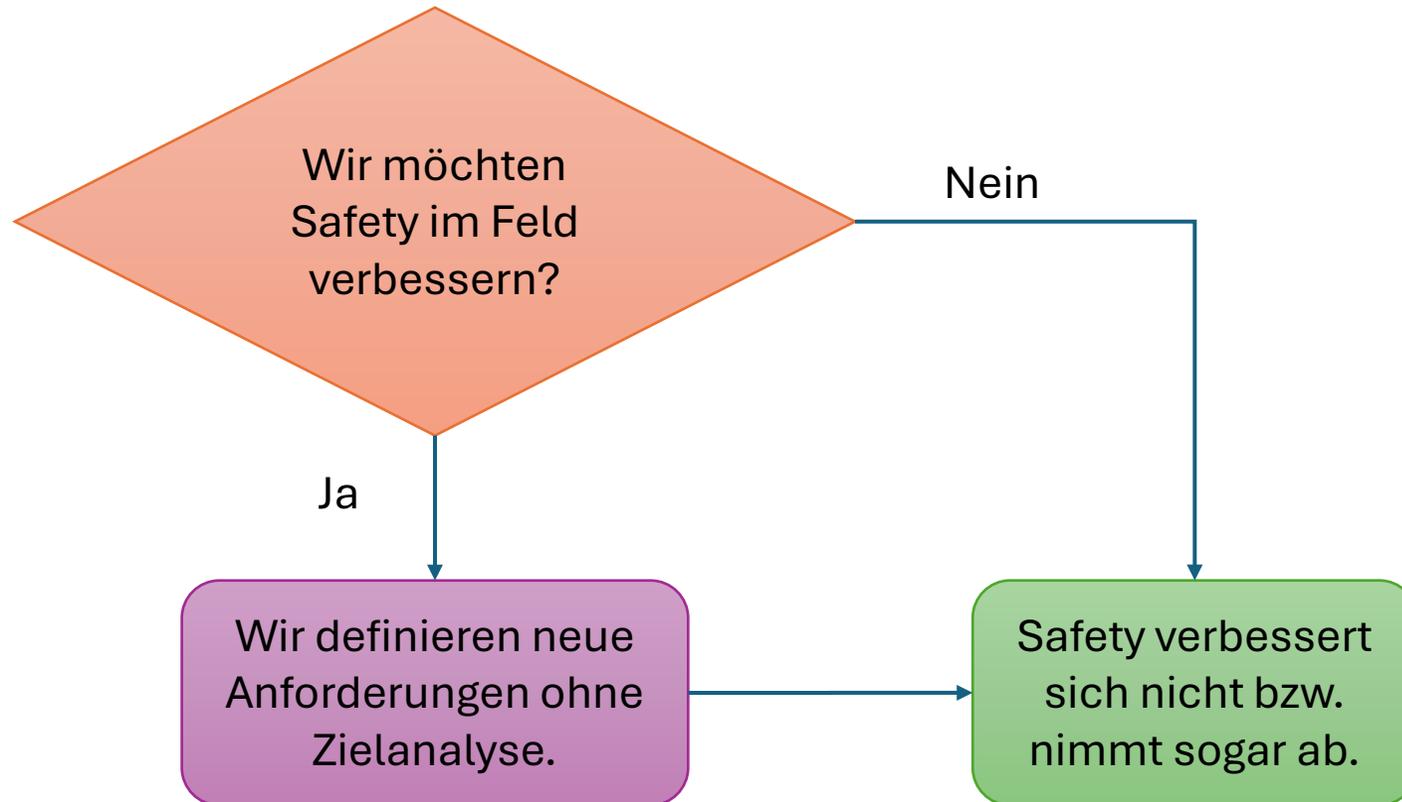
Software not meeting the criteria of software technology class I (SWTC I) or software technology class II (SWTC II).

# „KI“ Anwendungs-Klassifizierung

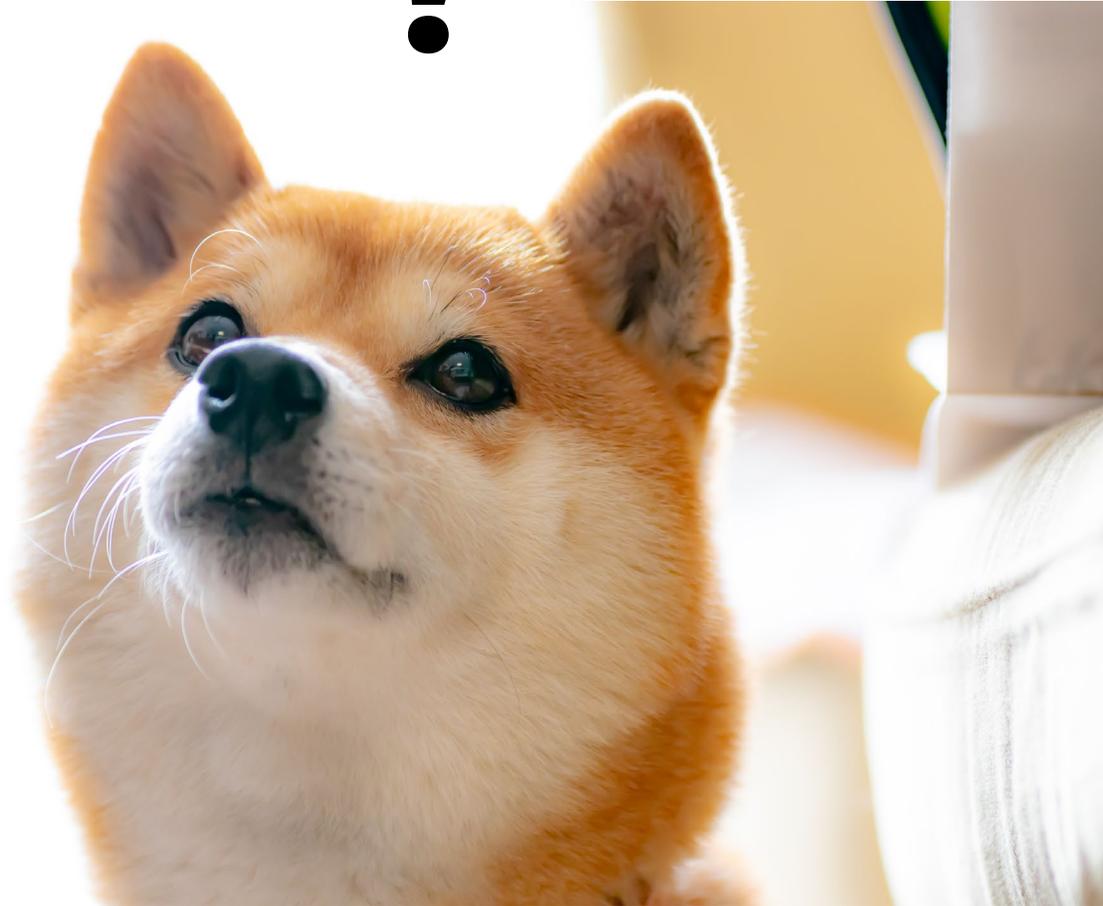
**Table 1 —AI technology classification table**

AI Technology Class = >	SWTC I	SWCT II	SWCT III
<b>AUL-A1</b> <sup>a</sup>	Application of risk reduction concepts of existing functional safety International Standards possible	Appropriate set of requirements <sup>c</sup>	At the time of publication of this document no appropriate set of properties with related methods and techniques is known to achieve sufficiently reduction of risk
<b>AUL-A2</b> <sup>a</sup>		Appropriate set of requirements <sup>c</sup>	
<b>AUL-B1</b> <sup>a</sup>		Appropriate set of requirements <sup>c</sup>	
<b>AUL-B2</b> <sup>a</sup>		Appropriate set of requirements <sup>c</sup>	
<b>AUL-C</b> <sup>a</sup>		Appropriate set of requirements <sup>c</sup>	
<b>AUL-D</b> <sup>b</sup>	Application of risk reduction concepts of existing functional safety International Standards		
<p><sup>a</sup> Static (offline) teaching or learning during development only, (see also 6.6).</p> <p><sup>b</sup> Dynamic (online) teaching or learning possible.</p> <p><sup>c</sup> The appropriate set of requirements for each usage level is established by application of risk reduction concepts of existing functional safety International Standards and additional considerations based on the literature review performed in <a href="#">Clauses 8, 9, 10</a> and <a href="#">11</a>. Examples are provided in <a href="#">Annex B</a>.</p>			

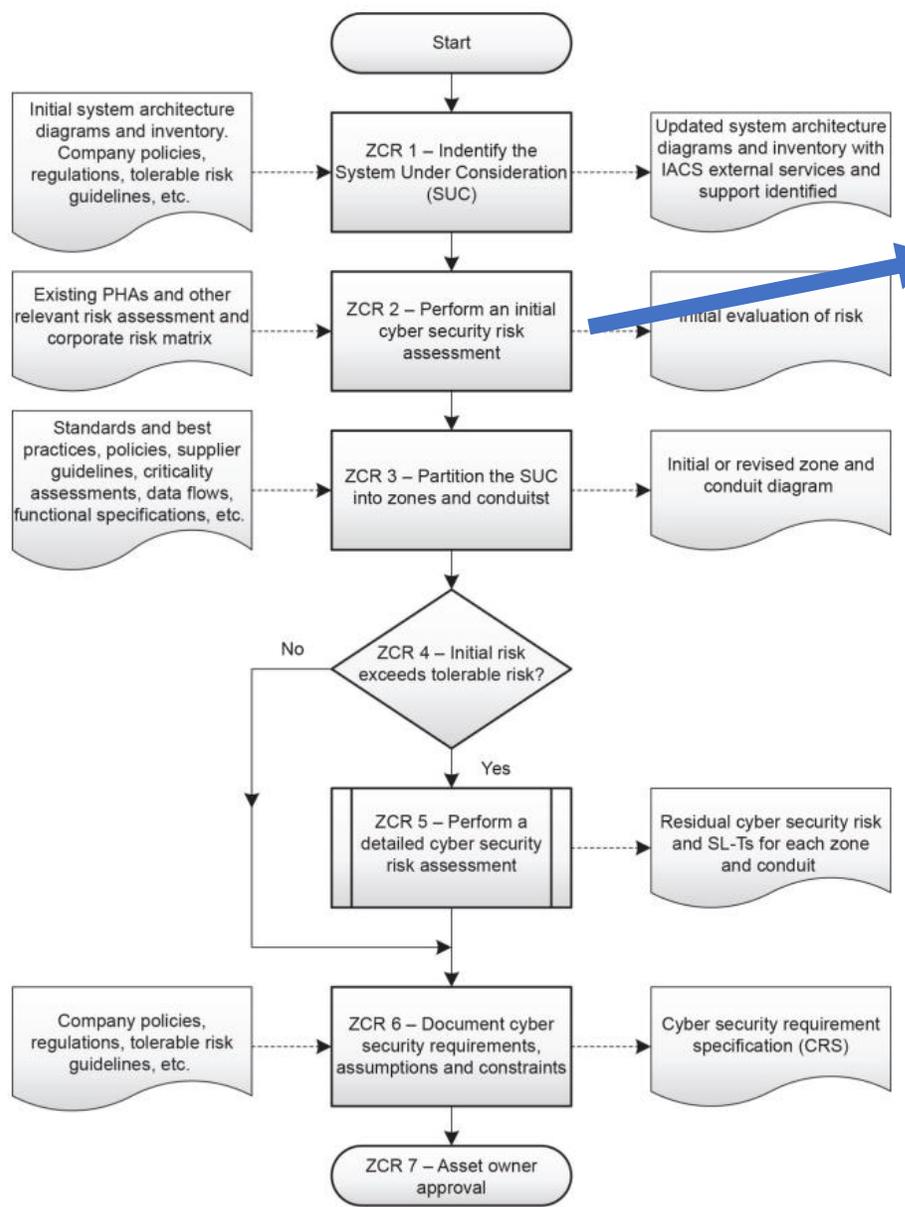
# Safety Catch 22 in Standardization



?



# Safety & Security Analysis – Was sollen wir nach IEC 62443-3-2 tun?



## 4.3 ZCR 2: Initial cyber security risk assessment

### 4.3.1 ZCR 2.1: Perform initial cyber security risk assessment

#### 4.3.1.1 Requirement

The organization shall perform a cyber security risk assessment of the SUC or confirm a previous initial cyber security risk assessment is still applicable in order to identify the worst case unmitigated cyber security risk that could result from the interference with, breach or disruption of, or disablement of mission critical IACS operations.

sieht aus wie die Risikoanalyse für fuSi



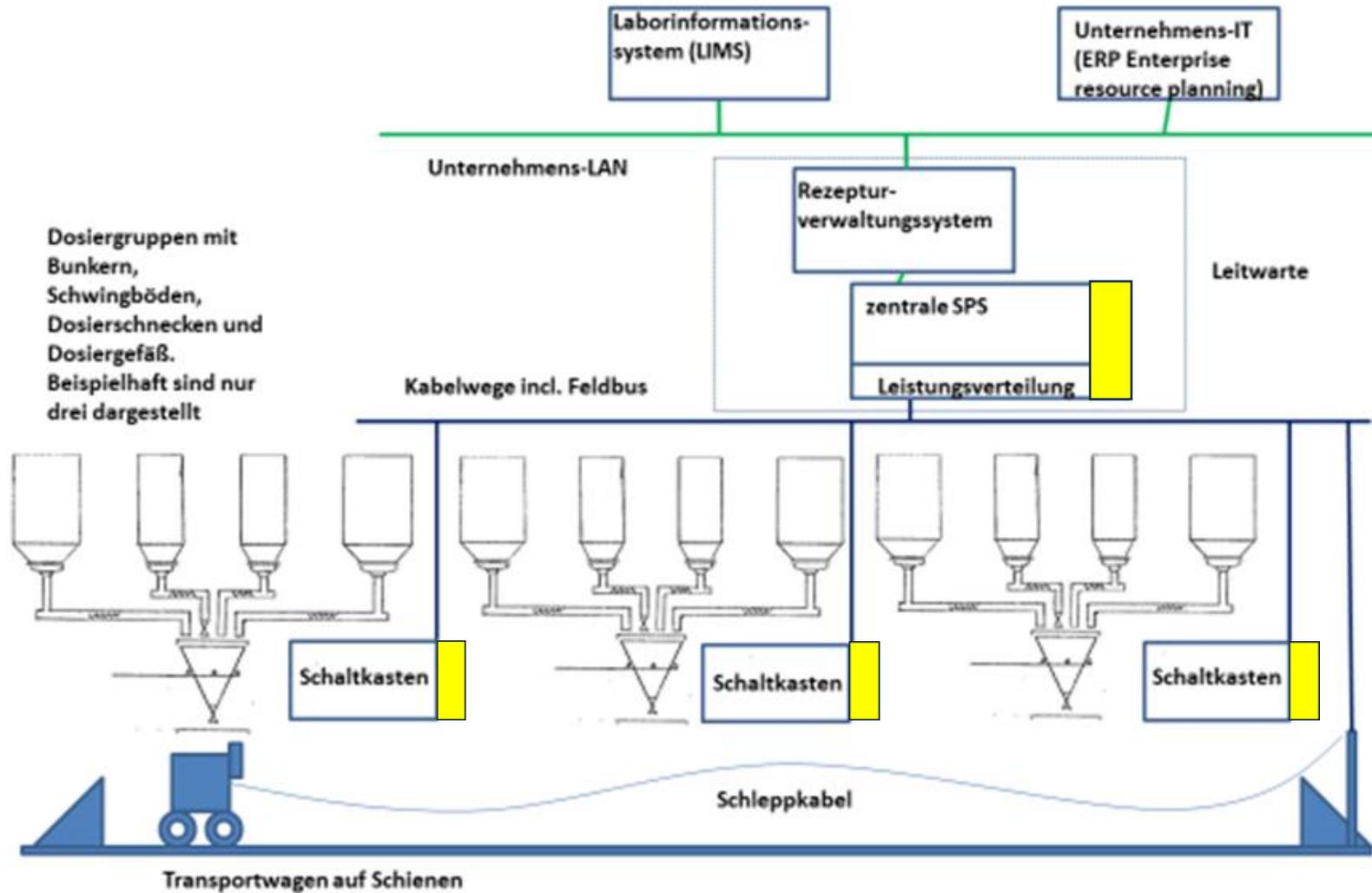
# **Safety & Security Analysis – Nehmen wir ein Beispiel: Gemengeanlage einer Glasfabrik (1)**

**In einer Glasfabrik werden Schüttgüter aus Silos automatisch nach Rezept in Dosiergefäße dosiert. In einer Produktionscharge werden so verschiedene Stoffe zusammengebracht und der Weiterverarbeitung zugeführt, die hier nicht mit dargestellt ist. Die Anlage stellt das Gemenge für eine Anzahl unterschiedlicher Öfen her, die jeweils unterschiedliche Glassorten erschmelzen.**

**Die Rezepte für die Chargen, deren Inhaltsstoffe in der betrachteten Anlage dosiert werden, sind auf die unterschiedlichen Öfen abgestellt. Die Inhaltsstoffe sind verschiedene Mineralien, wie Quarzsand, Pottasche, Feldspat oder auch Scherben. Einige davon sind sehr giftig.**

**Die Anlage ist so aufgebaut, dass jeweils zwei oder vier Bunker zu einer Gruppe zusammengefasst sind. Zu jeder Gruppe gehört ein Dosiergefäß, also eine elektronische Waage und Fördereinrichtungen, die aus einem Bunker in das Dosiergefäß fördern. Unter den Dosiergefäßen läuft ein Wagen auf Eisenbahnschienen und holt die eingewogenen Mengen ab.**

# Safety & Security Analysis – Gemengeanlage (2)



Dies möge die IT- und OT-Umgebung sein.  
Geräte zur Ausführung von Sicherheitsfunktionen

# Safety & Security Analysis – Ein Auszug aus der Liste der aufgefundenen Gefährdungen (EUC-Risiken)

Gefährdung (EUC-Risiko)	gefährliches Ereignis	Ursache	Nr.	Bereits getroffene Maßnahmen zur Risikoreduzierung	Einschätzung, dass die Gefährdung trotzdem auftritt	Schwere	Weitere Risikominderung notwendig?	wie?	Bemerkung
Freisetzung giftiges Schüttgut in beträchtlicher Menge mit Fluidisierung	Überfüllung des Dosiergefäßes und Reißen des Tuchs zwischen Dosiergefäß und Scheibe	Waage wiegt falsch (zu geringes Gewicht)	1	regelmäßiges Freimachen der Fesselungselemente und Überprüfung der Waage	möglich	mittel	ja	Zeitüberwachung, Instandhaltungsprozedur nach festgelegten Intervallen	Keine betriebsbewährte, sicherheitsgerichtete Wägetechnik verfügbar
Freisetzung giftiges Schüttgut in beträchtlicher Menge mit Fluidisierung	Entleerung Dosiergefäß, ohne dass Wagen darunter steht	Wagen wurde für den Entleervorgang falsch positioniert. Mögliche Kausalkette: Die Kette für den Encoder ist gerissen und die Kettenglieder haben sich im Boden verschoben.	2	Gelegentliche Sichtprüfung der Kette per Betriebsanweisung	möglich	hoch (da viel Material aus großer Höhe herunterfällt)	ja	SF3: richtige Positionierung prüfen mit ind. Näherungsgeber.	

# Safety & Security Analysis – Beginn der Bedrohungsanalyse: Mögliche Ziele des Angreifers

Art des Ziels	Beispiele
1.1 Sicherheit für Menschen und Umwelt	Eine Sicherheitsfunktion kompromittieren und auf eine Anforderung warten Eine Sicherheitsfunktion kompromittieren und eine Anforderung über das betriebliche System herbeiführen.
1.2 Sicherheit per Seitenkanal – diejenigen Abläufe herbeiführen, die nicht durch eine Sicherheitsfunktion abgedeckt sind	Durch Angriff auf das betriebliche System – insbesondere auf die Messtechnik – ein verringertes Gewichtssignal der Verwiegung zuführen und die Waage dadurch überfüllen.
1.3 Sicherheit per Seitenkanal – Überbrückung provozieren	Lauter Störungen im BCPS erzeugen und sie wie Fehlalarme des sicherheitsgerichteten Systems darstellen. Auf Überbrückung durch das Personal warten.
2.1 Produktsicherheit - Produktfehler	Das Rezept so verändern, dass das Glas nach 3 Jahren springt oder undurchsichtig wird. (Nahrungsmittelindustrie: Herbeiführen von vorzeitiger Verderbnis)
2.2 Produktsicherheit - Dokumentation	Dokumentation fälschen, so dass Reklamationen nicht sinnvoll bearbeitet werden können. (Nahrungsmittelindustrie: die Dokumentation über durchgeführte Hygiene-Maßnahmen angreifen)

# Safety & Security Analysis – Beginn der Bedrohungsanalyse: Mögliche Ziele des Angreifers

Art des Ziels	Beispiel
<b>3.1 Anlagenverfügbarkeit - Leitrechner</b>	<b>Den Rechner für die Rezepturverwaltung außer Betrieb setzen (z.B. Ransom-Angriff). In diesem Beispiel der Gemengeanlage für eine Glasfabrik kann eine Unverfügbarkeit erhebliche Konsequenzen haben, im Hinblick auf den Betrieb der kontinuierlichen Durchlauföfen (Energieverbrauch und Produktionsqualität).</b>
<b>3.2 Anlagenverfügbarkeit – Apparate beschädigen</b>	<b>Diejenige Funktion des betrieblichen Systems angreifen, die die Abreinigung der Enstaubungsfilter steuert. Zu oft und zu lange abreinigen lassen und dadurch vorzeitigen Verschleiß herbeiführen.</b>
<b>4.1 Guter Ruf – aktiver Angriff</b>	<b>Die Produktions- und Verbrauchsberichte stören und in den sozialen Medien behaupten, das Unternehmen fälscht seine Bilanzen</b>
<b>4.2 Guter Ruf – passive Angriff durch belauschen</b>	<b>Abwarten, bis ein Produktionsproblem auftritt und das Unternehmen einen Rückruf starten muss. Bevor dieser veröffentlicht wird, das Problem in den sozialen Medien platzieren</b>
<b>5.1 Finanziell – aktiver Angriff auf Messgeräte und Systeme zum Handeln</b>	<b>Beispiel aus einem anderen Betriebsbereich: Die Fahrzeugwaage der Fabrik oder das Warenwirtschaftssystem so beeinflussen, dass für einen bestimmten Spediteur, der Rohware anliefert, zu viel abgerechnet wird.</b>
<b>5.2 Finanziell – passiver Angriff durch Belauschen</b>	<b>Beispiel aus einem anderen Betriebsbereich: Erfahren, was die wichtigsten Kunden sind und zu welchen Preisen und mit welchen Mengen sie beliefert werden. Diesen Kunden dann zur gleichen Zeit Super-Billig-Angebote unterbreiten.</b>

# Safety & Security Analysis – Aussichten?

Die Risikoanalyse im Rahmen der funktionalen Sicherheit für die Gemengeanlage (eine vergleichsweise einfache Anlage) war bereits 3,5 Seiten lang. (Hier wurde nur ein Auszug gezeigt)

Das Herbeiführen der dort genannten gefährlichen Abläufe durch einen Angriff auf das sicherheitsgerichtete System war eine von insgesamt 5 Klassen.

Das bedeutet, dass die IT-Bedrohungsanalyse mindestens den fünffachen Aufwand der Risikoanalyse für die funktionale Sicherheit erfordert?



Mein Chef sagt,  
dass die IT-  
Bedrohungs-  
analyse kein  
Problem ist,  
sondern nur eine  
Herausforderung

# SIL Sprechstunde 2024

Zufällige Fehler in Mechanik  
Mythos oder Wirklichkeit?

Dipl.-Ing. Univ. Christoph Theilen



**Mehr Wert.  
Mehr Vertrauen.**



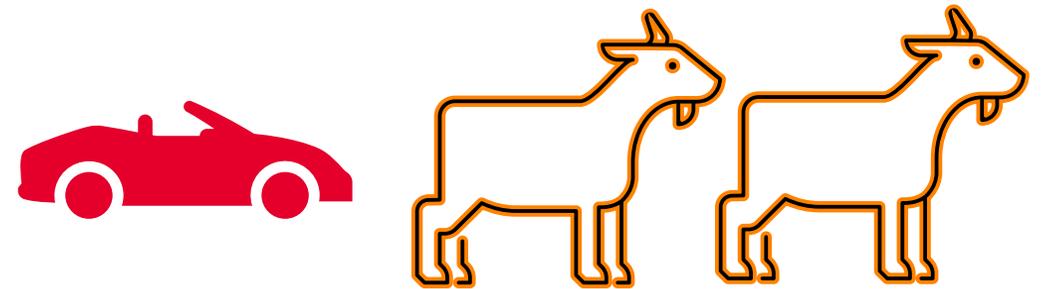


## Dipl.-Ing. Univ. Christoph Theilen

Vertrieb, Bereichsentwicklung, Strategic Account Manager

TÜV SÜD Industrie Service GmbH  
Region Bayern  
Westendstr. 199  
80686 München  
Germany

Tel. 0941/9910 416  
Fax 089 5791-2425  
Mobil 0160 704 3804  
mail to: christoph.theilen@tuev-sued.de



Zufällige Fehler in Mechanik.  
Mythos oder Wirklichkeit?

# Der Fehler - Es gibt zwei Typen – eine theoretische physikalische Betrachtung

## Exkurs in die physikalische Messtechnik

### Zufällige Fehler $x_{zuf}$

Bei vielen Wiederholungen der Messung ist nicht vorhersagbar, wie stark und in welche Richtung eine Abweichung des Bestwertes vom wahren Wert erfolgt. Der Zufall kann bei der Planung und Ausführung der Messung nicht ausgeschlossen werden.

- Die zufälligen Abweichungen vom wahren Wert haben gleichhäufig beiderlei Vorzeichen,
- vorausgesetzt man führt die Messung sehr oft durch.
- Es gibt also Messwerte, die größer, und solche, die kleiner als der wahre Wert sind.
- Die bei wiederholter Messung bestimmten Werte streuen um den Mittelwert  $\bar{x}$  herum.

### Systematische Fehler $x_{sys}$

- Bei vielen Wiederholungen der Messungen wirken sich systematische Fehler stets gleich auf die Abweichung des Bestwertes vom wahren Wert aus.
- Die systematischen Abweichungen haben stets das gleich Vorzeichen. Bei wiederholter Messung
- sind die Werte sämtlich größer oder sämtlich kleiner als der wahre Wert.

# Der Fehler in Sicherheitsfunktionen

Fehler bzw. fehlerhafte Schaltprozesse elektronischen Bauteilen treten zufällig auf, das bedeutet:

- Sie sind nicht vorhersehbar.
- Sie sind nicht reproduzierbar.
- Sie sind den EIE / PE-Systemen immanent.

Diese zufälligen Fehler sind prinzipiell unvermeidbar, müssen also antizipiert und das Versagen der Bauteile somit einkalkuliert werden.

Dem gegenüber stehen die systematischen Fehler, die durch kausale Zusammenhänge gekennzeichnet sind:

- Sie treten immer dann auf, wenn bestimmte Rahmenbedingungen erfüllt sind.
- Sie haben eine nachvollziehbare und fest stellbare Ursache.
- Sie führen zu einer vorhersehbaren Wirkung und sind stets auf menschliches (Fehl-) Verhalten zurückzuführen.
- Ursache und Wirkung hängen kausal zusammen.

# Der Fehler in Sicherheitsfunktionen



Woher kommt dann die Aussage vom Zufall in der Mechanik?



# Klassifizierung von Fehlern

- Der Betreiber einer Prozessanlage hat von seinem Ventillieferanten 100 Ventile unterschiedlicher Bauart eingesetzt.
- Bei der jährlichen Funktionsprüfung wird ein gefährlicher Fehler eines Ventils festgestellt.
  - Ursache: Federbruch
- Der Betreiber führt eine Fehleranalyse durch um den Fehler zu klassifizieren (zufällig oder systematisch).
- Zur Analyse des Fehlers werden alle Ventile der gleichen Bauart ebenfalls geprüft.
  - Resultat: Bei keinem weiteren Ventil ist die Feder gebrochen, trotz gleicher Umgebungsbedingungen.
- Ergebnis: Der Betreiber erfasst den Fehler als zufällig in seiner Stördatenstatistik und meldet dies an den Hersteller zur Berechnung des PFD-Werts.

# Beispiel

Lieferant  
(Federn)

Der Hersteller der Federn gießt seinen Stahl bei zu hoher Temperatur. Dadurch kommt es zu Lufteinschlüssen, welche Federbruch zur Folge haben können.

Ventilhersteller

Der Ventilhersteller kauft 1000 Federn bei seinem Lieferanten.

Betreiber

Der Betreiber hat 100 Ventile des Herstellers im Einsatz.

# Ursachen von systematischen Fehlern

- Fehler bei der Materialauswahl (z. B. Dichtungen oder Körper)
  - *Fehler in der Spezifikation*
- Fehler bei der Auslegung/Auswahl von Komponenten, z. B. zu schwache Auslegung von Stellantrieben
  - *Fehler in der Spezifikation*
- falsche Kalibrierung oder Justierung
  - *Fehler in der Installation*
- mangelhafte Montage oder Instandhaltung
  - *Fehler in der Installation oder dem Betrieb*
- Fehler im Fertigungsprozess aufgrund eines mangelhaften Qualitätsüberwachungssystems
  - *Gerade diese Fehler sind durch den Betreiber schwer zu klassifizieren*

# Klassifizierung von Fehlern

## **Problem**

Der Betreiber einer Anlage soll den Ausfall eines Ventils klassifizieren, ohne Einfluss oder detaillierte Kenntnis über den Herstellungsprozess des Ventils zu haben.

## **Folge**

Aussagen über die Art eines Fehler im Feld unterliegen Unsicherheiten.

Es ist meist schlechthin nicht möglich eine eindeutige Einteilung zu machen, da das Wissen über den Fehler unvollständig ist.

Dadurch werden Fehler, die mit statistischen Verfahren ermittelt werden auch falsch einsortiert (Systematischer Fehler durch den Menschen aufgrund von Unkenntnis).

Bei einer theoretischen Betrachtung der physikalischen Eigenschaften der Mechanik, kommt man zu dem Schluss, dass Mechanik keine zufälligen Fehler enthalten kann, auch wenn es uns manchmal so erscheint.



We create chemistry

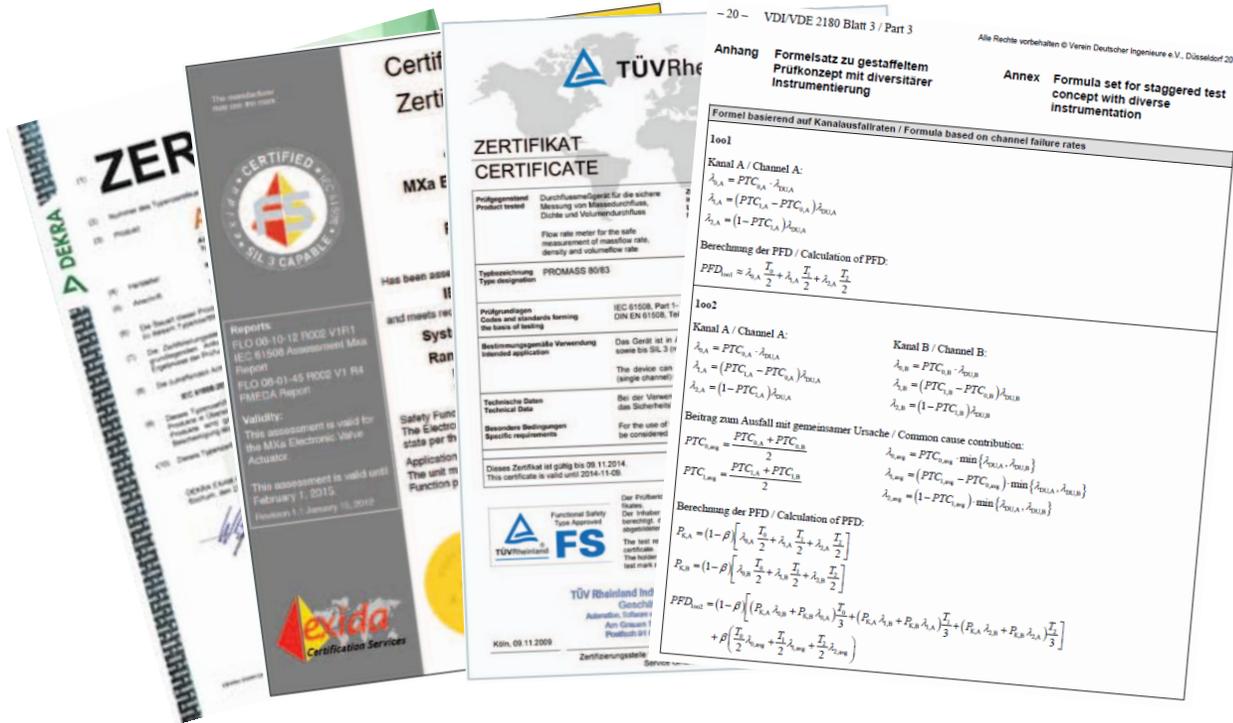
# Jede PFD ist falsch!

Eine Diskussion über verschiedene  
Sichtweisen ...

SIL-Sprechstunde, Mannheim, 18.09.2024

Dirk Hablawetz (BASF), Gregor Schmitt-Paukszkat (Bayer),  
Andreas Hildebrandt (P+F), Norbert Matalla

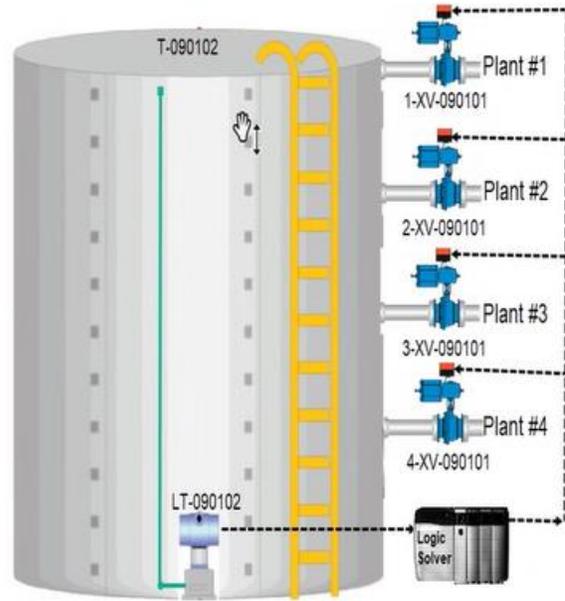
# Wie wird die Zuverlässigkeit von PLT-SE häufig wahrgenommen?



# Das Dilemma ...

## SPRING23+19<sup>TH</sup> GCPS A Joint AIChE and CCPS Meeting

- High level trips supply valves on 4 lines (4oo4)
- Device Proof Test Interval – 4 years
- Sensor + LS =  $\lambda_{DU} = 133$  FITS



Using FE $\lambda_{DU}$ from	Final Element FITS	SIS PFDavg	SIS RRF	SIS SIL
Certificate (not by exida)	102	0.0095	106	SIL 1
SilSafeData Lower Bound	674	0.0496		
SilSafeData Avg(min.max)	1336	0.097		
SIL-Solver (Ball FTC – Clean)	1353	0.098		
SIL-Solver (Ball FTC-Dirty)	1776	0.131		
FARADIP Lower Bound	510	0.037		
FARADIP Geometric Mean	3160	0.233		
OREDA Lower Bound	1459	0.108		
OREDA Mean	8248	0.611		



NAMUR - Interessengemeinschaft  
Automatisierungstechnik der Prozessindustrie e.V.

AK PRAXIS

Application of VDI/VDE 2180-4

Status: 2021-07-28

AK PRAXIS

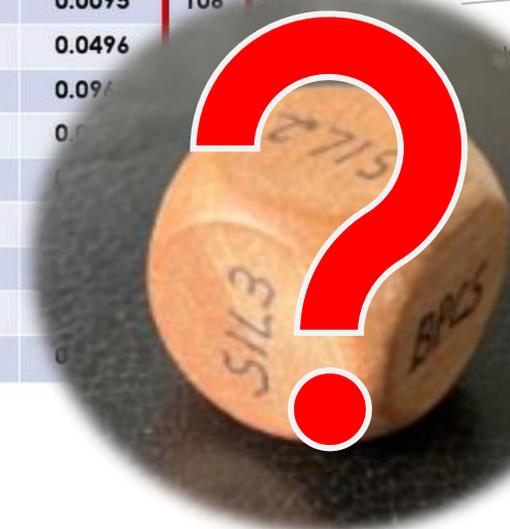
Application of VDI/VDE 2180-4

2021-07-28

Table 2: Failure rates "NAMUR.smart"

Year	2017	2018	2019	total
Mean time to failure	425 · 10 <sup>6</sup> h	477 · 10 <sup>6</sup> h	569 · 10 <sup>6</sup> h	1.471 · 10 <sup>6</sup> h
ALL				
the fi-	374	446	572	1.392
sub-				
	24	26	22	72
	2	6	6	14
	947 FIT	1.002 FIT	1.072 FIT	~1.000 FIT
	75 FIT	72 FIT	52 FIT	< 100 FIT
	13 FIT	22 FIT	19 FIT	< 25 FIT

Quelle: 2023 AIChE Spring Meeting and 19th Global Congress on Process Safety



# Zufälliger oder systematischer Fehler?

## Beispiel 1

Bei einer Wiederholungsprüfung wurde festgestellt, dass eine Schwimmer-Füllstandsmessung "hängen geblieben" war. Ein leichtes Antippen führte jedoch dazu, dass der Messwert jedoch wieder korrekt angezeigt wurde.



## Beispiel 2

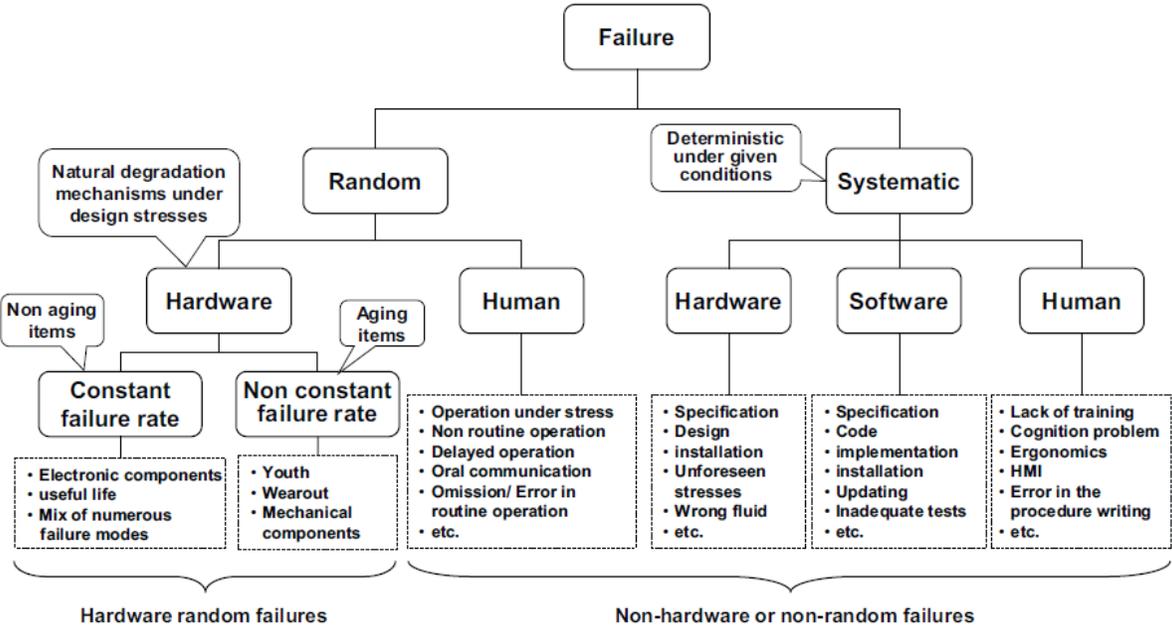
Ein SSPS-Ausgangsmodul fiel aus und lieferte keinen Ausgangsstrom mehr an ein Magnetventil. Ein Widerstand in der Ausgangsschaltung wies einen korrodierten Draht auf, der keinen Strom mehr leitete. Dies war überraschend, da die gesamte Leiterplatte zum Schutz vor Korrosion beschichtet ist. Bei näherer Betrachtung zeigte sich, dass die Beschichtung bei der Herstellung der Leiterplatte nicht korrekt aufgetragen wurde. Es gab kleine Lunker in der Beschichtung, weil die Beschichtungsmaschine falsch gereinigt wurde, obwohl das Reinigungsverfahren korrekt beschrieben war.

## Beispiel 3

Ein Magnetventil konnte einen Stellantrieb während einer Wiederholungsprüfung einer PLT-SE nicht entlüften. Eine Analyse des Magnetventils deutete darauf hin, dass innere Korrosion dazu führte, dass sich die Spule verhakte und die Feder nicht genügend Kraft hatte, um die "Korrosionsbindung" zu überwinden. Die Korrosion wurde verursacht weil der Deckel des Klemmenfachs nicht vollständig schloss. Der Deckel schloss nicht vollständig, weil die Magnetspule nicht richtig saß, als eine Presse versehentlich falsch eingestellt wurde.

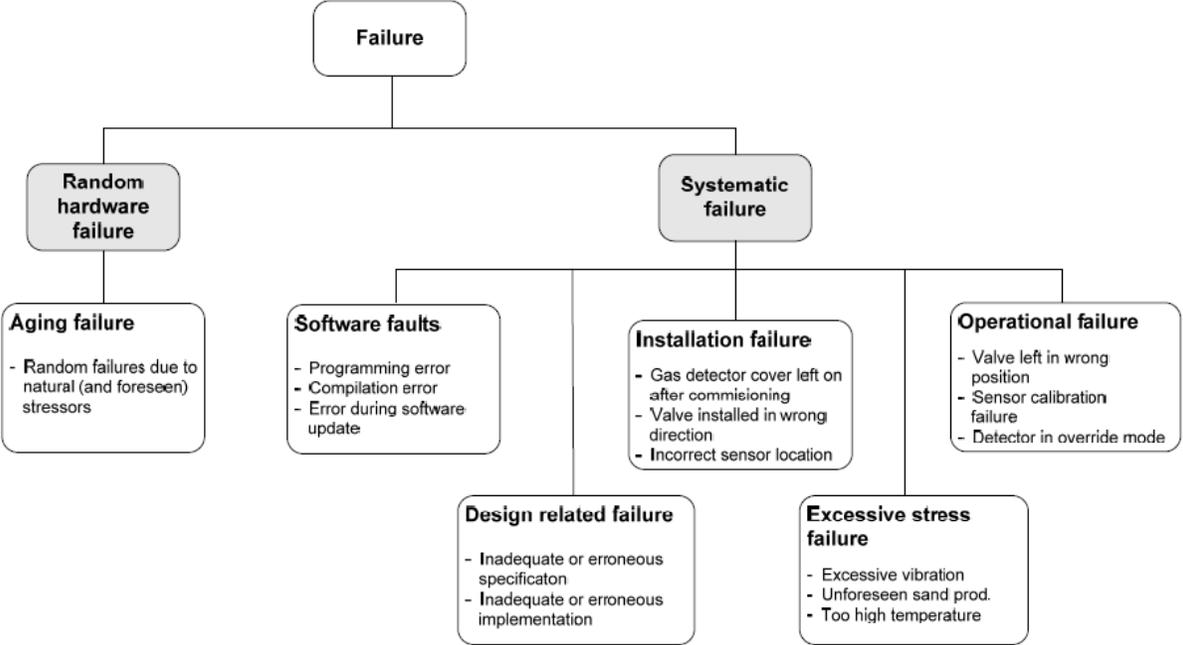
# Fehlerkategorisierung in verschiedenen Dokumenten

## ISO TR 12849



Quelle und ©: ISO TR 12489

## SINTEF / PDS-Methode



Quelle und ©: SINTEF PDS Method Handbook



# Fehlerkategorisierung in verschiedenen Dokumenten (DIN EN 61511)

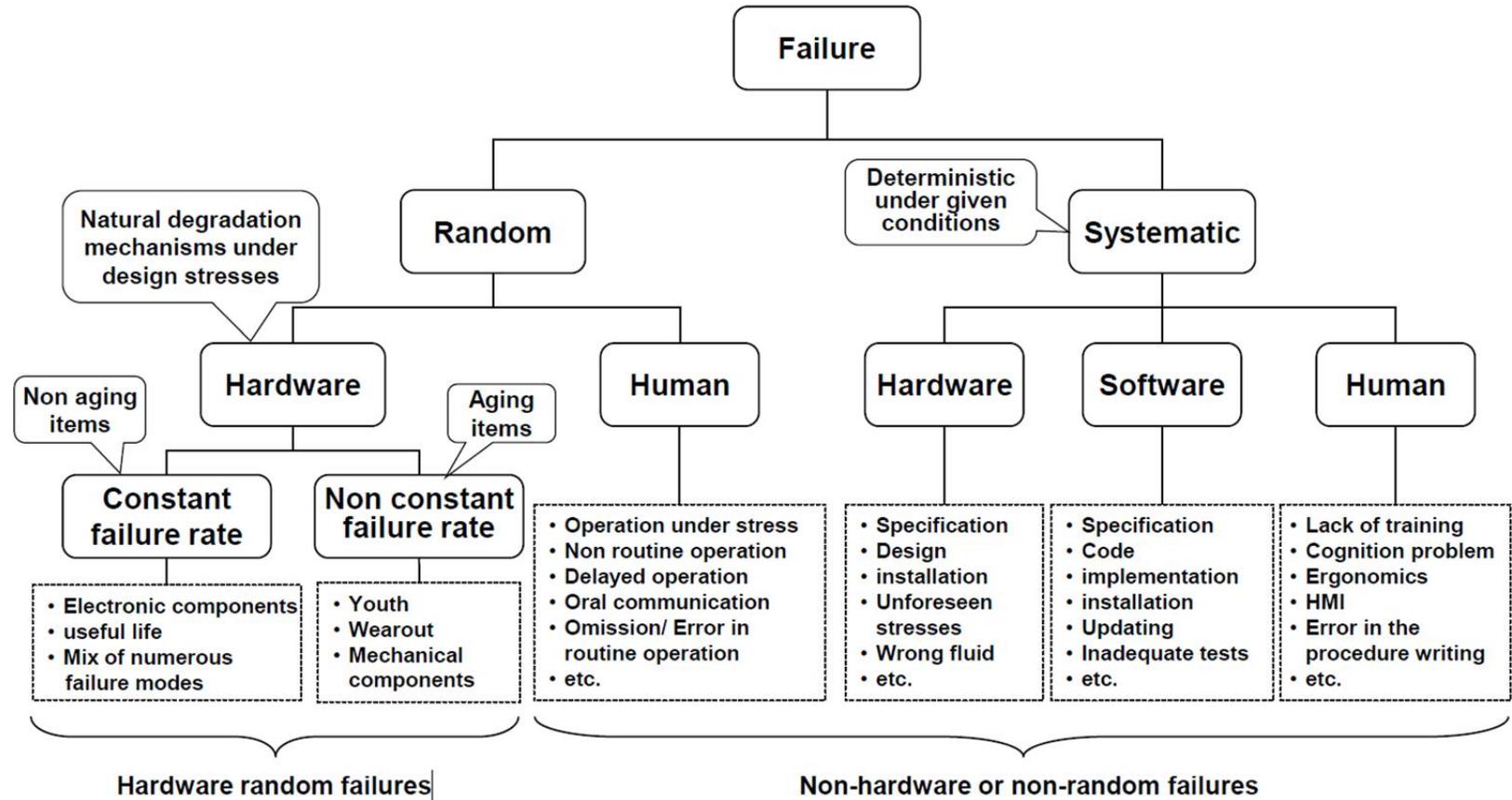
## Zufälliger Hardwareausfall $\rightarrow \lambda$

- Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Mechanismen in der Hardware resultiert, die zu einer Verschlechterung der Eigenschaften der Bauteile führen
- Anmerkung 2: Zwei wichtige Unterschiede bestehen zwischen zufälligen Hardwareausfällen und systematischen Ausfällen:
  - Ein zufälliger Hardwareausfall ist nur mit dem System selbst verknüpft, ein systematischer Ausfall dagegen sowohl mit dem System (einem Fehler) als auch mit einer bestimmten Bedingung (siehe 3.2.81). Ferner wird ein zufälliger Hardwareausfall durch einen einzigen Zuverlässigkeitsparameter (z. B. die Ausfallrate) beschrieben, ein systematischer Ausfall dagegen durch zwei (z. B. die Wahrscheinlichkeit eines bereits vorhandenen Fehlers und die Häufigkeit der Gefährdung durch eine bestimmte Bedingung). Ein systematischer Fehler kann nach seiner Entdeckung beseitigt werden, während zufällige Hardwarefehler dies nicht können.
  - Ein systematischer Ausfall kann nach seiner Entdeckung beseitigt werden, während dieses bei einem zufälligen Hardwareausfall nicht möglich ist.

## Systematischer Ausfall

- Ausfall, der auf einen bereits vorhandenen Fehler zurückgeführt werden kann, unter bestimmten Bedingungen immer wieder auftritt und nur durch Entfernen des Fehlers mit Hilfe einer Änderung des Entwurfs, des Fertigungsverfahrens, der betrieblichen Vorgehensweisen, der Dokumentation oder anderer Faktoren behoben werden kann
  - Anmerkung 2: Instandsetzung ohne Änderung wird gewöhnlich nicht die Ursache des unter bestimmten Bedingungen auftretenden Ausfalls beheben.
  - Anmerkung 3: Ein systematischer Ausfall kann durch absichtliche Herbeiführung der gleichen Bedingungen reproduziert werden, obwohl nicht alle reproduzierbaren Ausfälle systematischer Art sind.
  - Anmerkung 4: Beispiele für Fehler, die zu systematischen Ausfällen führen, sind auch menschliche Irrtümer, die ihren Ursprung haben in
    - Der Spezifikation, Konstruktion, Herstellung, dem Betrieb oder der Instandhaltung der Hardware, Entwurf oder Implementierung der Software

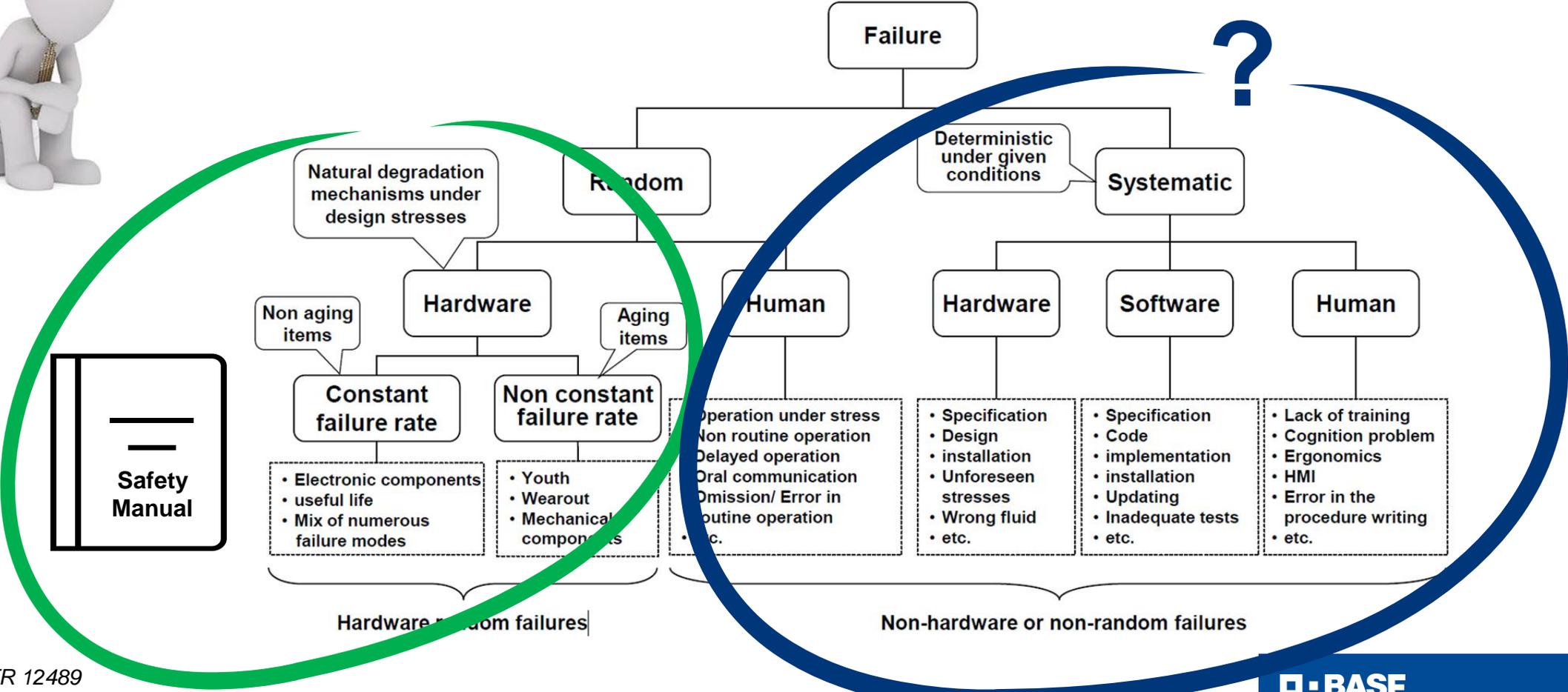
# Keine Ausfälle, sichere PLT-Sicherheitseinrichtung. Dauerhaft!



Quelle und ©: ISO TR 12489

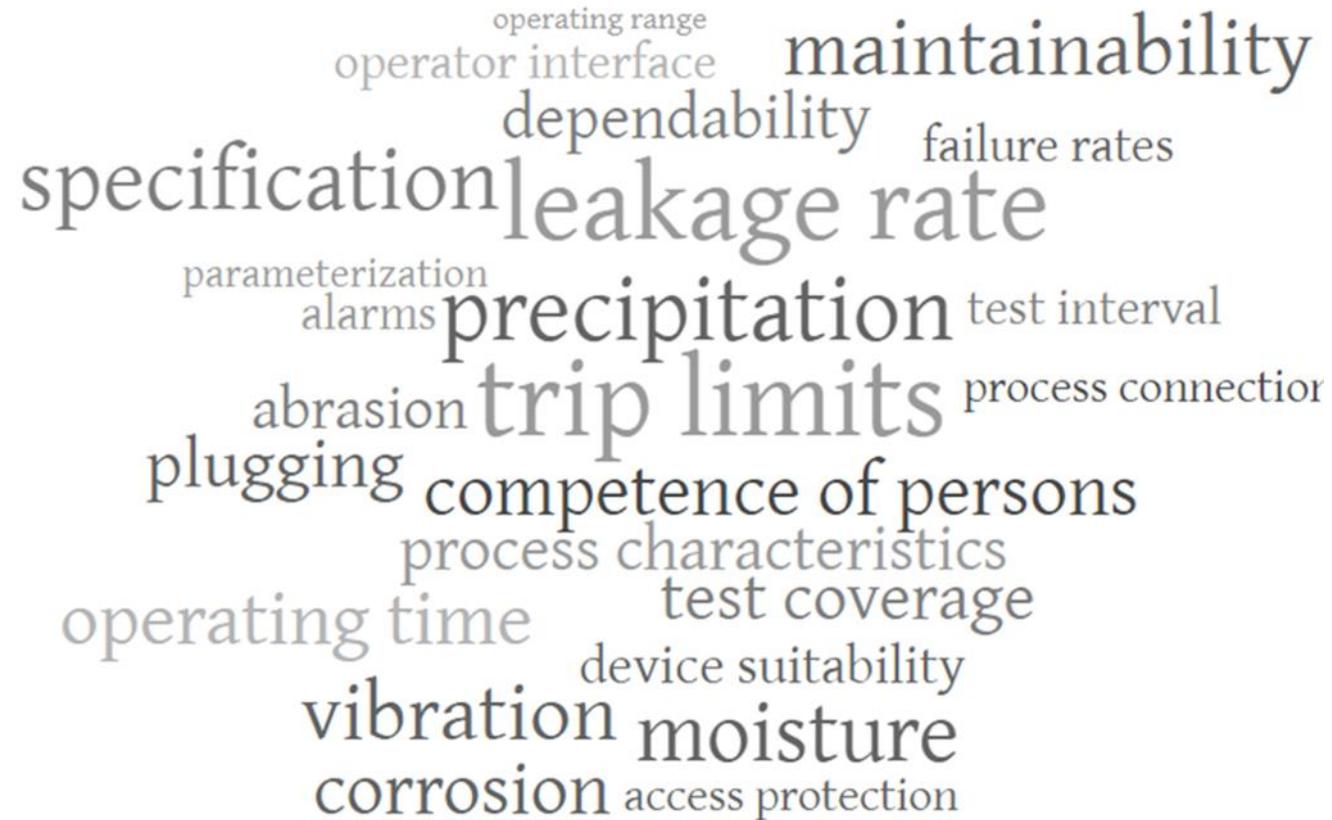


# Sicherheitsdaten des Herstellers - Was beinhalten sie (oft)?



Quelle und ©: ISO TR 12489

# Andere Faktoren, die die Sicherheit stark beeinflussen



# Fehlerkategorisierung in verschiedenen Dokumenten

(DIN EN 61511)

## Zufälliger Hardwareausfall → λ

- Ausfall, der zu einem... aus einem oder mehrere Hardware resultiert, die Eigenschaften der Bauelemente...
- Anmerkung 2: Zwei... zufälligen Hardwareausfällen...
  - Ein zufälliger Hardwareausfall... systematischer Ausfall... einer bestimmten Bedingung... Hardwareausfall durch ein... Ausfallrate) beschrieben, ... Wahrscheinlichkeit eines... Gefährdung durch eine be... seiner Entdeckung beseiti... können.
  - Ein systematischer Ausfall... dieses bei einem zufällige...

## Systematischer Ausfall

- Ausfall, der auf einen bereits vorhandenen Fehler... bestimmten Bedingungen... Entfernen des Fehlers... des Fertigungs... ensweisen, der Doku... hoben werden kann... derung wird gewöhnlich... n Bedingungen... all kann durch absichtliche... en reproduziert werden, ... fälle systematischer Art... zu systematischen... e Irrtümer, die ihren

**11.9.3** Die Zuverlässigkeitsdaten, die zur Quantifizierung zufälliger Ausfälle benutzt werden, müssen belastbar, nachvollziehbar, dokumentiert und begründet sein und müssen auf Felddaten für ähnliche Geräte in einer ähnlichen Betriebsumgebung beruhen.

**ANMERKUNG 1** Dieses beinhaltet vom Anwender gesammelte Daten, Hersteller/Lieferant/Anwender-Daten, die von Datensammlungen zu bestimmten Geräten herrühren, allgemeine Felddaten aus Zuverlässigkeits-Datenbanken, usw. In einigen Fällen kann ingenieurmäßiger Sachverstand verwendet werden, um Abschätzungen von fehlenden Zuverlässigkeitsdaten vorzunehmen oder den Einfluss von in einer unterschiedlichen Betriebsumgebung gesammelten Zuverlässigkeitsdaten zu bewerten.

**ANMERKUNG 2** Das Fehlen von Zuverlässigkeitsparameter, die die betrieblichen Randbedingungen widerspiegeln, ist ein häufiger Mangel bei Wahrscheinlichkeits-Berechnungen. Endanwender sollten entsprechende Datensammlungen in Übereinstimmung mit IEC 60300-3-2:2004 oder ISO 14224:2006 durchführen, um die Anwendung der IEC 61511-Reihe zu verbessern.

**ANMERKUNG 3** Herstellerdaten, die auf dem Rücklauf fehlerhafter Geräte beruhen, sollten auf Populationen begrenzt werden, bei der die Einsatz-/Betriebsbedingungen vollständig bekannt und entsprechend IEC 60300-3-2:2004 oder ISO 14224:2006 vollständig aufgezeichnet sind. Der Anwender kann ebenfalls die Betriebsbedingungen für eine PLT-Sicherheitsfunktion aufzeichnen und damit eine Übereinstimmung mit den Daten des Herstellers aufzeigen.

Ursprung haben in

- Der Spezifikation, Konstruktion, Herstellung, dem Betrieb oder der Instandhaltung der Hardware, Entwurf oder Implementierung der Software



# Unterschiedliche etablierte Vorgehensweisen zur Bestimmung PFD

## Diskussion NAMUR / ISA

### Two ways of appropriately reflecting the operating environment in the PFDavg:

#### Approach #1:

The theoretical failure rate appearing at the bottom of the curve from a certificate *might still be used justifiably* in the design PFDavg calculation **IF**

- A. **The effective service life for the affected components will be kept short enough through *preventive fixed schedule maintenance* (referred to in ISO14224 as “predetermined maintenance”)**
- AND
- B. **The specified interval for that maintenance is known/proven to be short enough for that operating environment.**

*Determining the interval and how much of the total failure rate will be addressed by the predetermined maintenance (vs. how much remains to be addressed by testing) requires understanding the expected impact of the operating environment on that type of installation.*

#### Approach #2:

**Use reliability parameters in the PFDavg calculation that reflect the expected actual performance in operating environment over the planned service life**

- Most commercial SIL calculation tools already provide modified failure rates to use in designs for “severe” or “dirty” operating environments.

#### Ideale Ausfallraten für Blick in die Zukunft

- Nutze Herstellerangaben / idealisierte Vergangenheit für Zukunftsaussagen
- UND kompensiere systematische Einflüsse wie Umwelt etc.

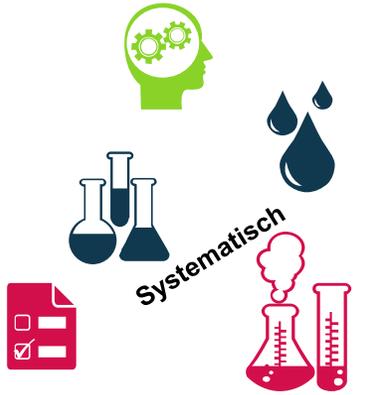


#### Reale Ausfallraten / Blick in die Vergangenheit

- Gehe davon aus, dass
  - Fehler nicht beseitigt werden, Wartungen nicht korrekt laufen und Geräte auf Verschleiß gefahren werden
  - System. Einflüsse, Temp etc. nicht kompensiert werden können

# Unterschiedliche etablierte Vorgehensweisen zur Bestimmung PFD

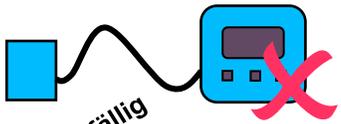
## Diskussion NAMUR / ISA



Systematisch



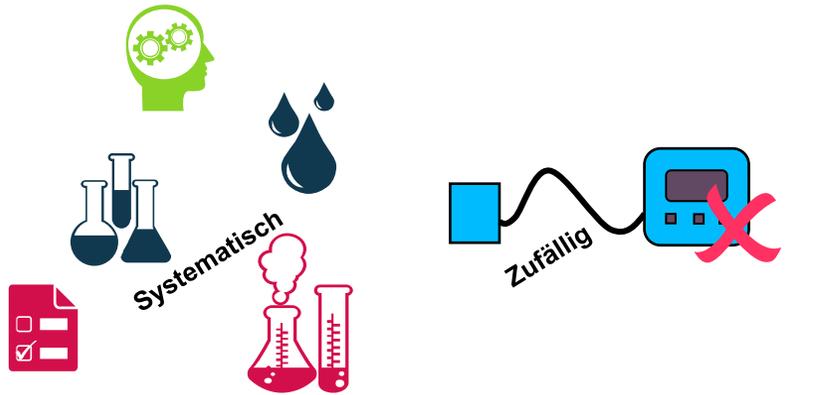
Bekommen wir in den Griff durch Prozeduren, Training, Erfahrung



Zufällig



Bekommen wir NICHT in den Griff  
⇒ PFD-Berechnung



Systematisch

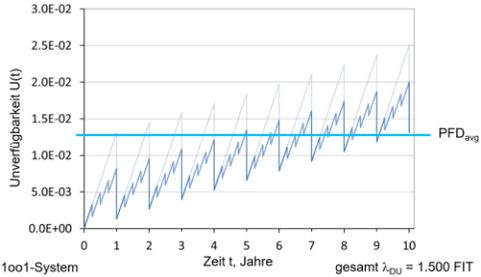
Zufällig



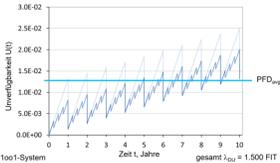
Bekommen wir NICHT in den Griff  
⇒ PFD-Berechnung

# Umwelteinflüsse

Was passiert, wenn wir die Umwelteinflüsse in die Ausfallraten und PFD einbeziehen?



Die Einbeziehung von Umwelteinflüssen spiegelt nicht die individuelle PFD eines SIFs wider, wenn man in die Zukunft blickt. Sie können nur angeben, wie viele Ausfälle wir z. B. aufgrund von Korrosion hatten, aber sie können nicht als Vorhersage für die Zukunft verwendet werden.

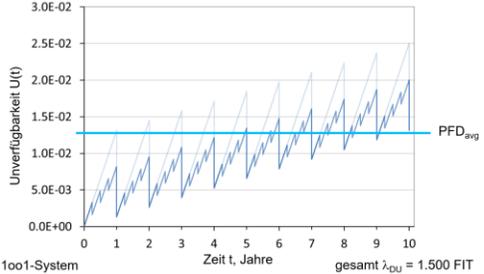


Führt zu mehr redundanten Geräten, die auf die gleiche Weise korrodieren. Keine Vermeidung der eigentlichen Störung!

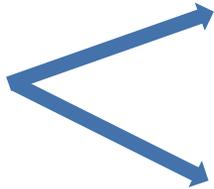
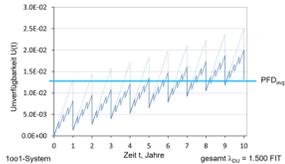
**Solche Auswirkungen können nur durch vorbeugende Wartung beherrscht werden, nicht durch PFD-Berechnung**

# Planungs- oder Konstruktionsfehler

Was passiert, wenn wir Planungs- oder Konstruktionsfehler in die in die PFD-Berechnung einbeziehen?



Das Versagen tritt binär für ein einzelnes SIF auf - nicht gleichmäßig über die Zeit verteilt. Es tritt dann und nur dann auf, wenn der einzelne ungeschulte Planer seine Hände im Spiel hat.



Keine Hilfe für zukünftiges Design → wird weiterhin fehlerhaft sein / nicht vermieden



Bestrafung von gut ausgebildeten / erfahrenen Planern  
 ⇒ Hohe Ausfallraten trotz korrekter Planung / Konstruktion  
 ⇒ Höhere Kosten (z. B. erhöhte HFT)

**Ausfallraten, die auch Planungs- und Konstruktionsfehler berücksichtigen, spiegeln nicht die individuelle PFD einer einzelnen PLT-Sicherheitseinrichtung wider.**

# Herausforderung - Analyse von Fehlern und Ausfällen

- Ziemlich komplex aufgrund der Unterscheidung zwischen zufälliger und systematischer Ursache
- Manchmal fehlende Kompetenz auf Betriebsebene
- Nur wenige Veranstaltungen pro Anlage und Jahr
- Teilnehmer aus aller Welt bei der Erfassung

**Zu viele fragwürdige Ergebnisse**

## Entwicklung von NAMUR.smart Entscheidungstabelle

Eingabe auf der Grundlage klarer und für den Benutzer verständlicher Fehlermuster

#	fault pattern	systematic fault caused by engineering	systematic fault caused by operation	random cause (if not systematic engineering or operation)
1	EMC	x		
2	Design fault	x		
3	Installation fault	x		
4	Influence of product	x		
5	Influence of environment	x		
6	Application programming fault/Parametrisation fault	x		
7	Constructional fault	x		
8	Corrosion	x	-	
9	Other systematic fault engineering	x		
10	Operating fault (human error)		x	
11	Unauthorized access / sabotage		x	
12	Unremoved bypass		x	
13	Incorrect test procedure		x	
14	Bad accuracy of measurement, signal drift (environmental influences)		x	
15	Internal leakage		x	
16	External leakage		x	
17	Mechanical blockage		x	
18	Other systematic fault maintenance		x	
19	Mechanical damage		x	
20	Internal device fault (not caused by product)			x
21	Wear out			x
22	Open circuit/ short circuit			x
23	Frozen signal, stuck-at (electronic fault)			x
24	Bad accuracy of measurement, signal drift (electronic fault)			x
25	Contact does not switch			x
26	Other random fault			x

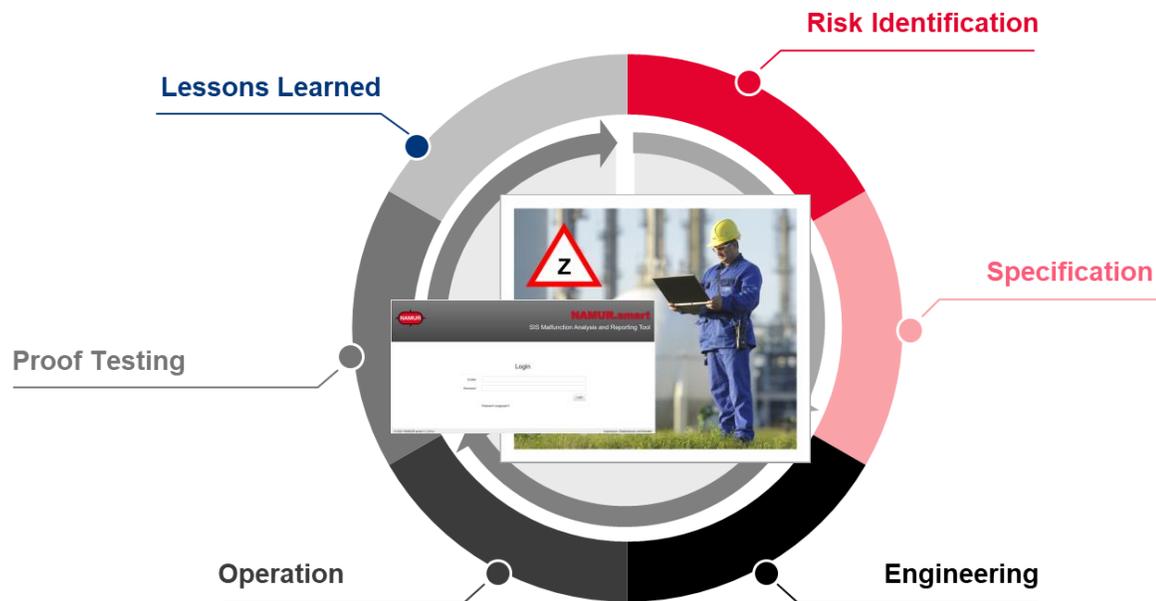
Zuverlässige und vergleichbare Ergebnisse





**NAMUR.smart**

# NAMUR.smart - Informationen zum Sicherheitslebenszyklus



## Leistungsindikator

- Reale Leistung - Management der technischen und funktionalen Sicherheit (anwendungsabhängig)
- Hardware / Faktor Mensch
- Fehlermuster zeigen Schwachstellen auf



## Technik

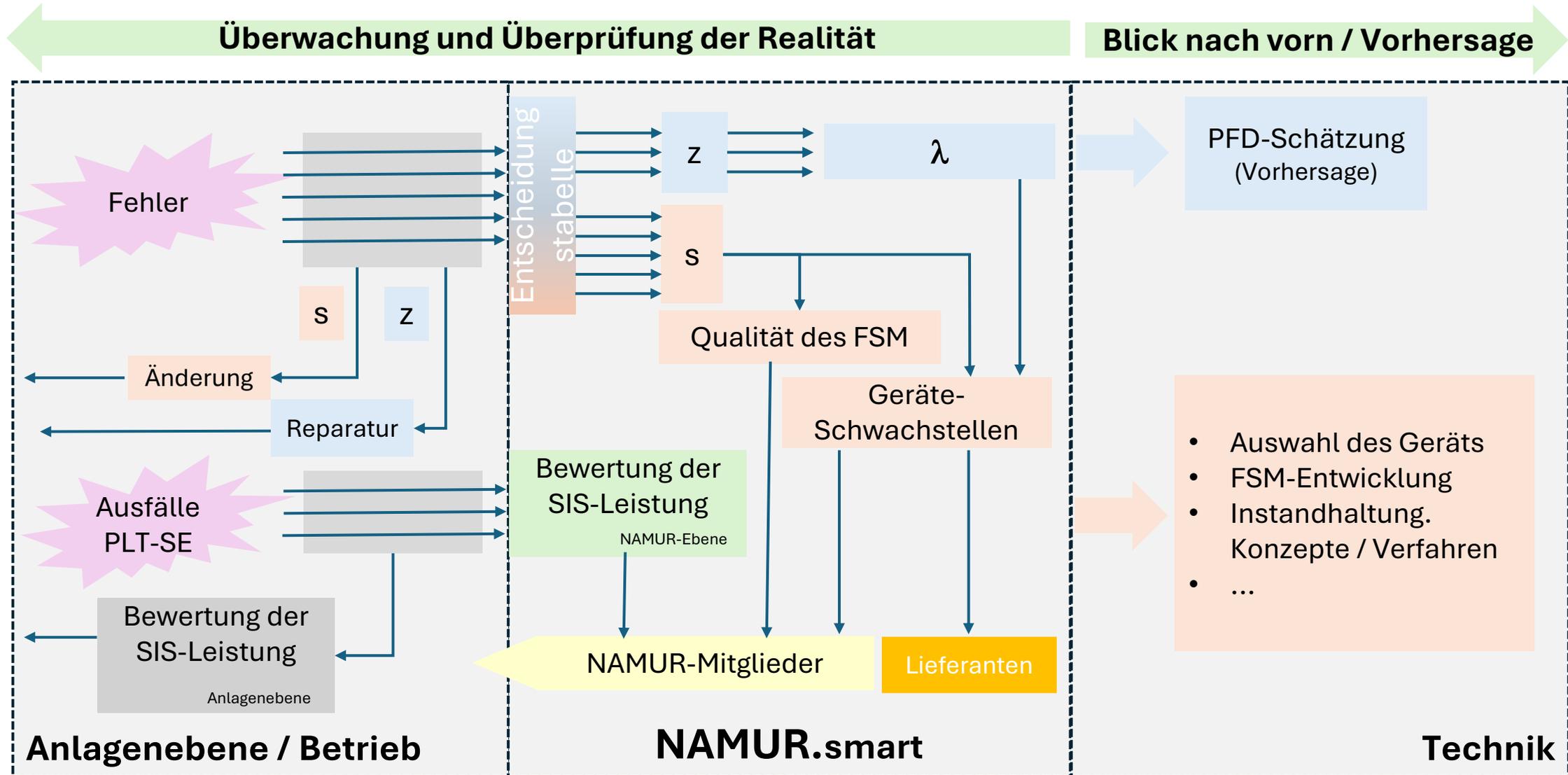
- Ausfallraten (anwendungsunabhängig)
- Vorherige Verwendung
- Versagensursache (zufällig oder systematisch)
- Schwachstellen bei der Umsetzung



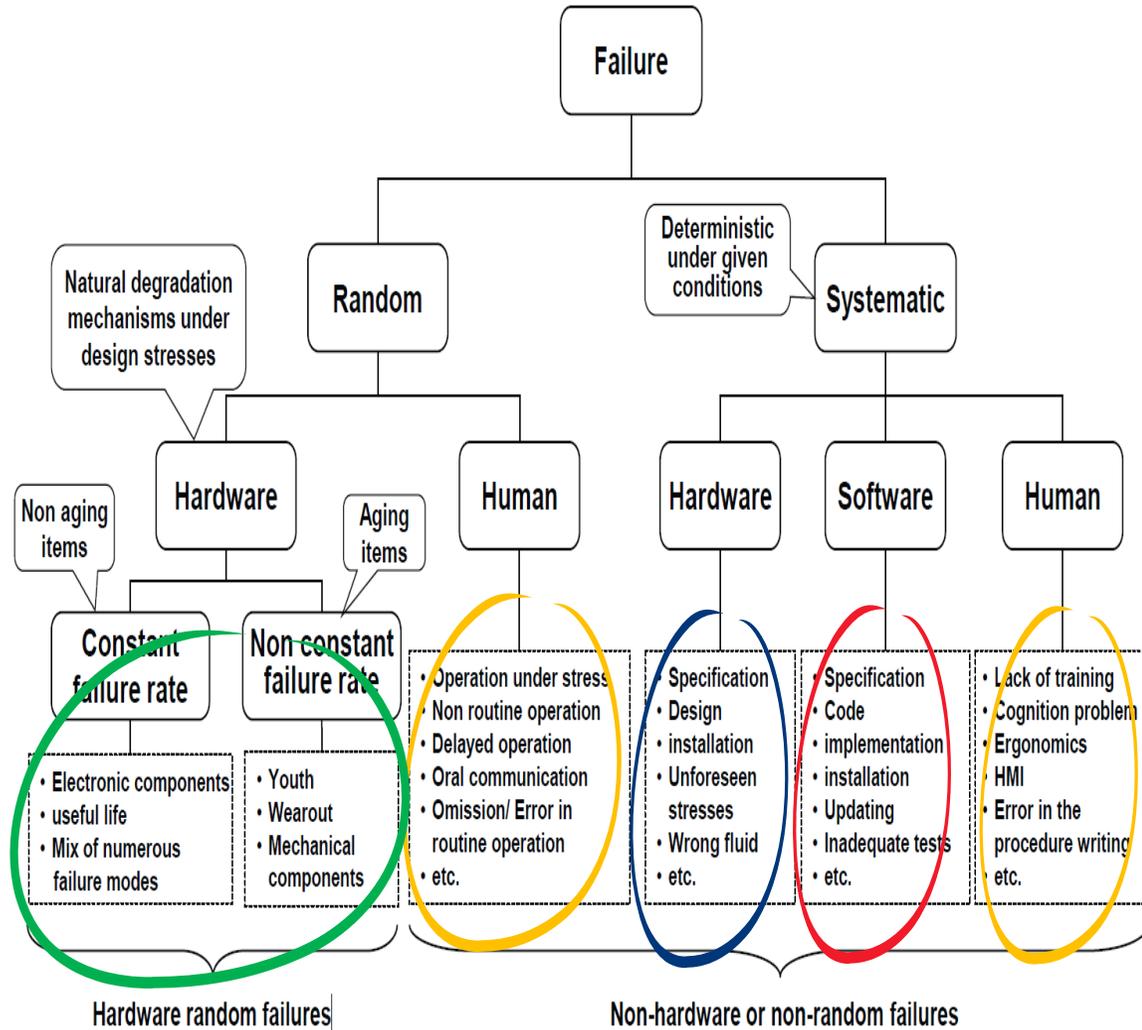
## Betrieb und Wartung

- Fehlererkennung und Ursachenanalyse
- Test-Ansatz
- Optimierte Prüfintervalle
- Nutzungsdauer

# NAMUR.smart Konzept



# NAMUR-Entscheidungstabelle und ISO 12489 - aktueller Ansatz



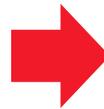
Fault Pattern	Cause of fault		
	Random*	Systematic Engineering	Systematic Operation
Internal device fault (not caused by product)	X		
Wear out	X		
Open circuit/ short circuit	X		
Frozen signal, stuck-at	X		
Other random fault	X		
Bad accuracy of measurement, signal drift (electronic fault)	X		
Contact does not switch	X		
EMC		X	
Design error		X	
Installation fault		X	
Influence of product		X	
Influence of environment		X	
Application program error / Parametrization error		X	
Constructional fault		X	
Other systematic fault engineering		X	
Corrosion		X	
Operating error (Human Error)			X
Unauthorized access / sabotage			X
Unremoved bypass			X
Incorrect test procedure			X
Bad accuracy of measurement, signal drift (environmental influences)			X
Internal leakage			X
External leakage			X
Mechanical blockage			X
Other systematic fault maintenance			X
Mechanical damage			X

\* Convention: Random is everything that has no clear systematic cau:

# Überarbeitung der Entscheidungstabelle für vollständige Übereinstimmung mit ISO 12489



#	Fehlerbild	Systematischer Fehler (Engineering)	Systematischer Fehler (Betrieb der Anlage)	Zufälliger Fehler Ursache (wenn nicht systematisch (Engineering/Betrieb))
1	EMC	x		
2	Konstruktionsfehler	x		
3	Fehler bei der Installation	x		
4	Einfluss des Produkts	x		
5	Einfluss der Umwelt	x		
6	Fehler in der Anwendungsprogrammierung/ Parametrisierungsfehler	x		
7	Konstruktionsfehler	x		
8	Korrosion	x		
9	Andere systematische Fehlersuche	x		
10	<b>Bedienungsfehler (Human Error)</b>		x	
11	Unbefugter Zugang / Sabotage		x	
12	Unentfernter Bypass		x	
13	<b>Falsches Prüfverfahren</b>		x	
14	Schlechte Messgenauigkeit, Signaldrift (Umwelteinflüsse)		x	
15	Interne Leckage		x	
16	Externe Leckage		x	
17	Mechanische Verstopfung		x	
18	Sonstige systematische Fehlerbehebung		x	
19	Mechanische Schäden		x	
20	Interner Gerätefehler (nicht durch das Produkt verursacht)			x
21	Abnutzung			x
22	Offener Stromkreis/ Kurzschluss			x
23	Eingefrorenes Signal			x
24	Schlechte Messgenauigkeit, Signaldrift (elektronischer Fehler)			x
25	Kontakt schaltet nicht			x
26	Andere zufällige Fehler			x



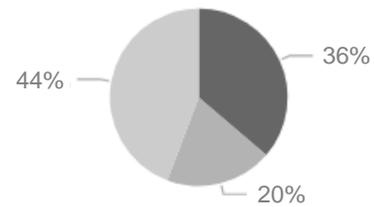
#	Fehlerbild	Systematischer Fehler (Engineering)	Systematischer Fehler (Betrieb der Anlage)	Zufälliger Fehler Ursache (wenn nicht systematisch (Engineering/Betrieb))
1	EMC	x		
2	Konstruktionsfehler	x		
3	Fehler bei der Installation	x		
4	Einfluss des Produkts	x		
5	Einfluss der Umwelt	x		
6	Fehler in der Anwendungsprogrammierung / Parametrisierungsfehler	x		
7	Konstruktionsfehler	x		
8	Korrosion	x		
9	Andere systematische Fehlersuche	x		
10	<b>Menschliches Versagen</b>			x
11	Unbefugter Zugang / Sabotage		x	
12	Unentfernter Bypass		x	
13	<b>Falsches Verfahren oder fehlende Ausbildung</b>		x	
14	Schlechte Messgenauigkeit, Signaldrift (Umwelteinflüsse)		x	
15	Interne Leckage		x	
16	Externe Leckage		x	
17	Mechanische Verstopfung		x	
18	Sonstige systematische Fehlerbehebung		x	
19	Mechanische Schäden		x	
20	Interner Gerätefehler (nicht durch das Produkt verursacht)			x
21	Abnutzung			x
22	Offener Stromkreis/ Kurzschluss			x
23	Eingefrorenes Signal			x
24	Schlechte Messgenauigkeit, Signaldrift (elektronischer Fehler)			x
25	Kontakt schaltet nicht			x
26	Andere zufällige Fehler			x

# Fehlerverteilung - Teilsysteme

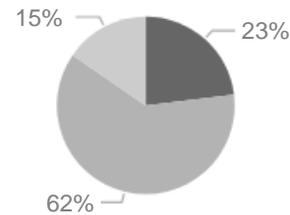


Zufällig  
Systematisch Engineering  
Systematisch Betrieb

**Teilsystem Sensoren**



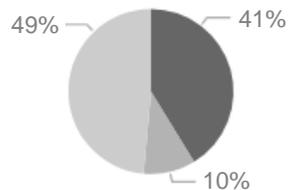
**Logiksystem**



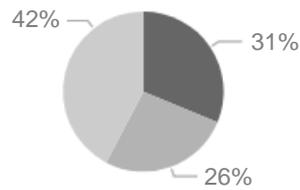
**Teilsystem Aktoren**



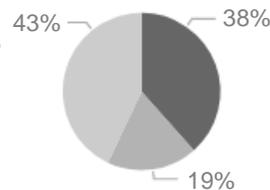
**Druck**



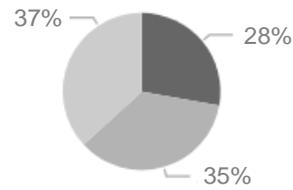
**Durchfluss**



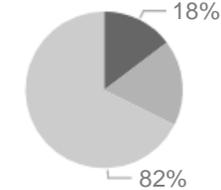
**Temperatur**



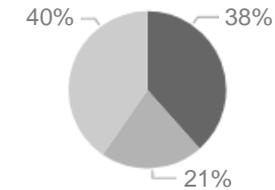
**Stand**



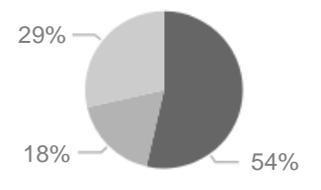
**Ventil**



**Magnetventil + Anbauten**

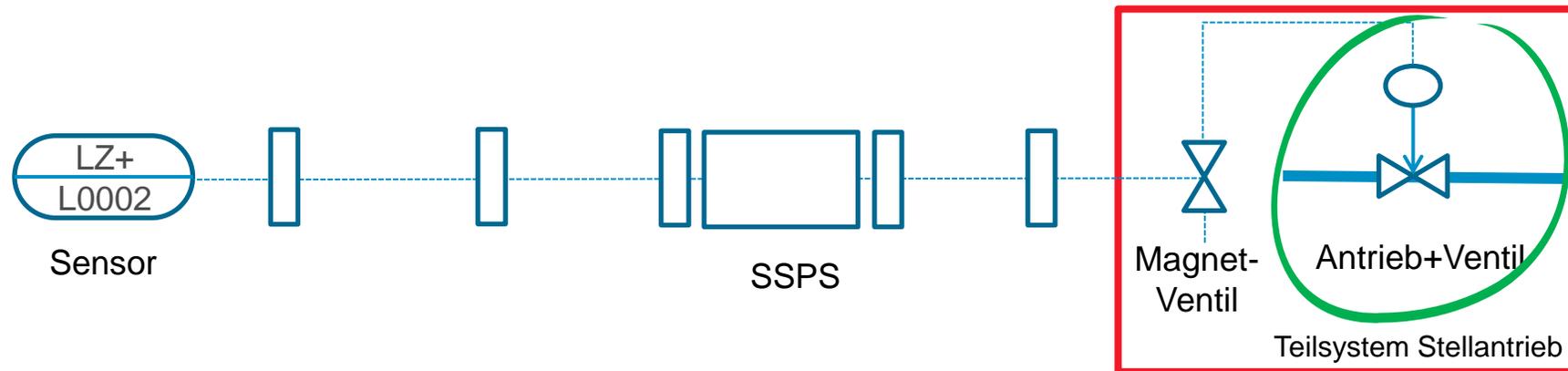


**andere Aktoren**



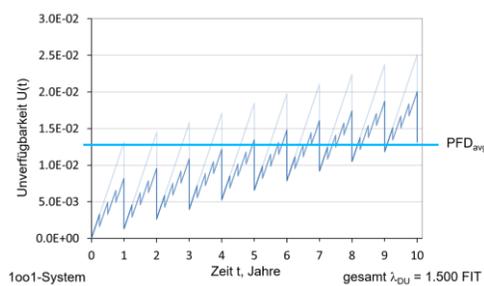
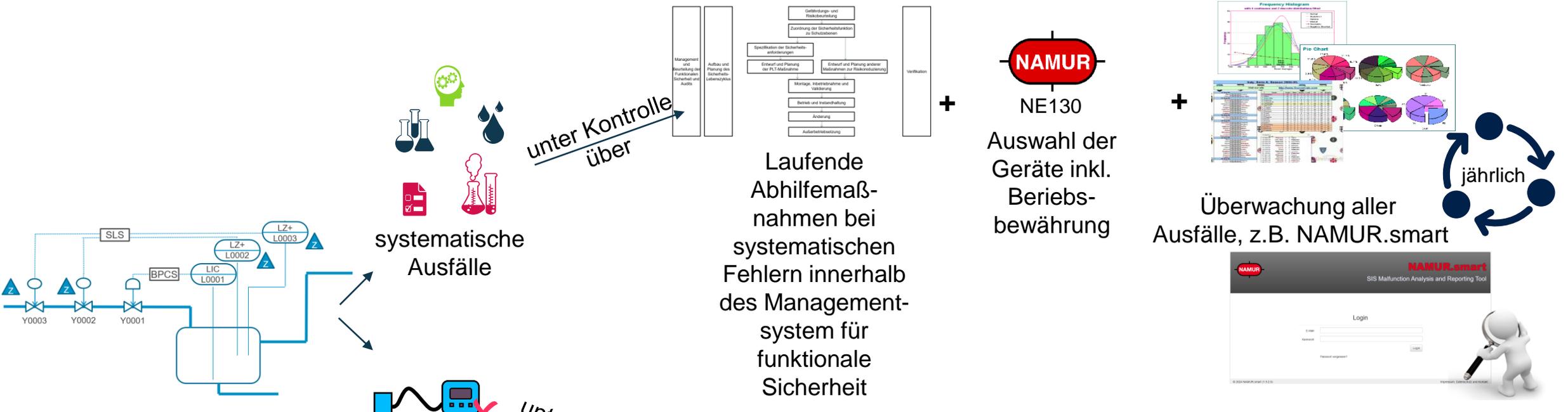
Kumulierte gefährliche Fehler 2017-2020

# Fehlerraten bei Stellantrieben 2017-2019



Jahr	2017	2018	2019	insgesamt
Betriebszeit	425·10 <sup>6</sup> h	477·10 <sup>6</sup> h	569·10 <sup>6</sup> h	1,471·10 <sup>6</sup> h
$\lambda_{total}$	947 FIT	1.002 FIT	1.072 FIT	~1.000 FIT
$\lambda_{DU}$ Teilsystem Stellantrieb	75 FIT	72 FIT	52 FIT	< 100 FIT
$\lambda_{DU, mech}$	13 FIT	22 FIT	19 FIT	< 25 FIT

# NAMUR-Ansatz zur Beherrschung von Fehlern bei PLT-SE



PFD-Berechnung in der Entwurfsphase

SIL	HFT
3	1
2	0
1	0

Hardware-Fehlertoleranz in der Entwurfsphase

# Ausfallraten in funktionaler Sicherheit - nützlich, schädlich oder was?

- Verantwortungsvoller Umgang mit Ausfallraten, keine blinde Nutzung von Datenbanken, Herstellerinformationen oder anderen Quellen
- Prüfen Sie immer kritisch und hinterfragen Sie die Herkunft der Daten
- Identifikation und Bewertung von systematischen Anteilen an den Ausfallraten
- Definieren von Randbedingungen, unter denen die gewählten Ausfallraten zum Anwendungsfall "passen"
- Definition und Durchführung von vorbeugender Wartung zur "Beherrschung" systematischer Einflüsse

**Konservative Ausfallraten (mit systematischen Anteilen) ersetzen keine (vorbeugende) Wartung!**

# Das kennen sie!



Quelle und ©: Andreas Hildebrandt

# Das gilt auch für den Umgang mit Fehlerraten!



Quelle und ©: Andreas Hildebrandt



We create chemistry

# Process Safety Time... Prozessfehlertoleranzzeit...

Brauchen wir das oder kann das weg.

# Agenda

- Teil 1: Process Safety Time
  - Definition der Process Safety Time
  - Motivation der Process Safety Time
  - Grafische Darstellung und Beispiel
  - Brauchen wir die Process Safety Time wirklich?
- Teil 2: Process Safety Time und Diagnose
  - Wo wird diese Zeit benutzt?
  - Zusammenhang mit Diagnostic
  - Was macht Diagnostic eigentlich aus
  - Beispiele

# Was ist die Definition der Process Safety Time?

DIN EN 61508 Teil 4 (2011)

## 3.6.20

### Prozess-Sicherheitszeit

(en: process safety time)

Zeitspanne zwischen dem Auftreten eines Ausfalls der EUC oder des EUC-Leit- oder Steuerungssystems mit dem Potential, einen gefährlichen Vorfall zu verursachen, und dem Zeitpunkt, bei dem die Reaktion in der EUC abgeschlossen sein muss, um das Auftreten des gefährlichen Vorfalls zu verhindern

IEC 61508 Teil 4

## 3.6.20

### process safety time

period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring

# Was ist die Definition der Process Safety Time?

DIN EN 61511 Teil 1 (2019)

## 3.2.53.1

### Prozessfehlertoleranzzeit

(en: process safety time)

Zeitraum zwischen einem Ausfall im Prozess oder der PLT-Betriebseinrichtung (mit dem Potential, einen gefährlicher Vorfall auszulösen) und, sofern die PLT-Sicherheitsfunktion nicht ausgeführt wird, dem Auftreten des gefährlichen Vorfalls,.

Anmerkung 1 zum Begriff: Diese ist nur eine Eigenschaft des Prozesses. Die PLT-Sicherheitsfunktion muss den Ausfall erkennen und ihre Aktion unter Berücksichtigung etwaiger Verzögerungen im Prozess (z. B. Kühlung eines Behälters) schnell genug ausführen, um den gefährlichen Vorfall zu verhindern.

IEC 61511 Teil 1 (ed. 2 2016)

## 3.2.52.1

### process safety time

time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed

Note 1 to entry: This is a property of the process only. The SIF has to detect the failure and complete its action soon enough to prevent the hazardous event taking into account any process lag (e.g. cooling of a vessel).

# Was ist die Motivation der Process Safety Time?

DIN EN 61511 Teil 1 (2019) & IEC 61511 Teil 1 (2016)

## 10.3 Sicherheitsanforderungen an die PLT-Sicherheitseinrichtung

**10.3.1** Ziel von 10.3 sind Fragestellungen, die bei der Erstellung der Sicherheitsanforderungen an die PLT-Sicherheitseinrichtung Berücksichtigung finden müssen.

**10.3.2** Diese Anforderungen müssen ausreichend für den Entwurf der PLT-Sicherheitseinrichtung sein und müssen eine Beschreibung der Absicht und Vorgehensweise während der Erstellung der Sicherheitsanforderungen an die PLT-Sicherheitseinrichtung beinhalten, die geeignet sind für:

(...)

Anforderungen an die Reaktionszeit für jede PLT-Sicherheitsfunktion, um den Prozess innerhalb der Prozessfehlertoleranzzeit in einen sicheren Zustand zu bringen

**ANMERKUNG** Für weitere Erläuterungen zur Prozessfehlertoleranzzeit siehe IEC 61511-2:2016.

## 10.3 SIS safety requirements

**10.3.1** Addresses issues that shall be considered when developing the SIS safety requirements.

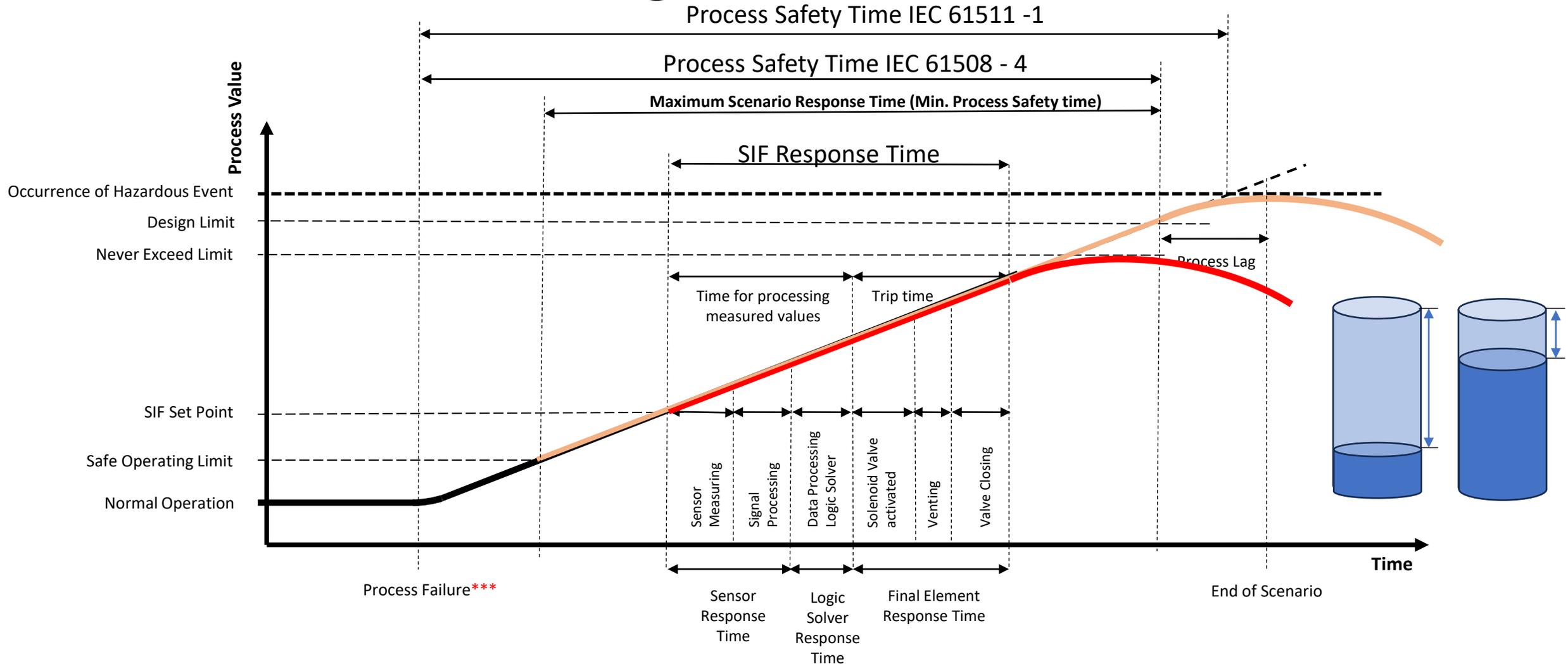
**10.3.2** These requirements shall be sufficient to design the SIS and shall include a description of the intent and approach applied during the development of the SIS safety requirements as applicable:

- response time requirements for each SIF to bring the process to a safe state within the process safety time;

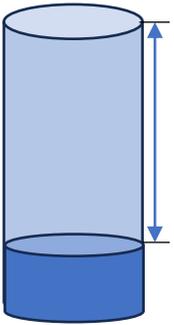
NOTE See IEC 61511-2:2016 for further discussion of process safety time.

Hier kann es dazu kommen, je nachdem wie der Startpunkt der Prozessfehlertoleranzzeit gewählt wurde, dass die Reaktionszeit der SIF nicht den worst Case abbildet.

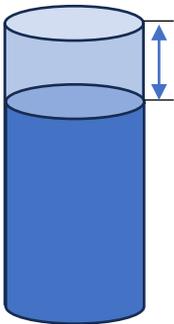
# Grafische Darstellung



# Oder mal am Beispiel

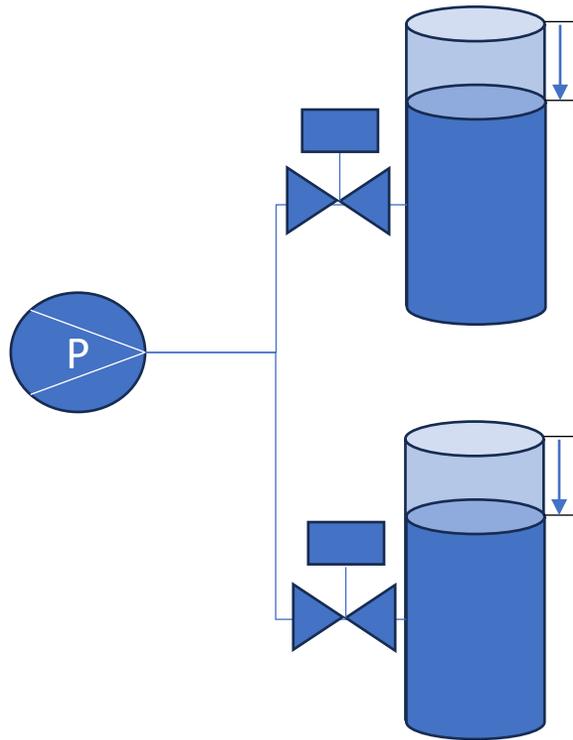


- Szenario 1:
  - Lagertank wird mit einer Füllrate von  $40\text{m}^3/\text{h}$  befüllt.
  - Tank hat ein Volumen von  $4.000\text{ m}^3$
  - Wenn dies bei einem leeren Tank die Füllstandsregelung gefährlich ausfällt hätte man eine Process Safety Time von 100h



- Szenario 2:
  - Wenn bei einem Tank mit einem freien Restvolumen von  $300\text{m}^3$  die Füllstandsregelung versagt, dann wäre die Process Safety Time 7,5h

# Berechnung an der ZGÜS



- Szenario 1:

- Wenn bei einem Tank mit einem freien Restvolumen von  $200\text{m}^3$  (95%) die Füllstandsregelung versagt, dann wäre die Minimale Process Safety Time 5h.
- Die Berechnung bzw. die Regeln kommen aus der ZGÜS (Zulassungsgrundsätze für Überfüllsicherungen)
- Wenn aber angenommen wird, dass das Ventil nicht dicht ist, und unter der Annahme das die Pumpe mehrere Tanks bedient, diese also nicht sofort abgestellt wird, dann kann bei einer zugelassenen Undichtigkeit (über eine Zeit von 24h) die minimale Process Safety Time plötzlich nur bei 3 Stunden liegen.

# Brauchen wir die Prozessfehlertoleranzzeit wirklich?

- Eigentlich nicht, aufgrund der folgenden Fakten:
  - Der Startpunkt dieser Zeit ist unbestimmt. Daher kann die Aussagekraft dieser Zeit entsprechend nicht hoch sein.
  - Der Endpunkt ist zwischen IEC 61508 und der IEC 61511 unterschiedlich definiert.
- Einige Unternehmen haben diese Zeit auf die SIF bezogen, ... also nicht im Sinne der IEC verwendet...
  - Einige Betreiber haben für sich die Prozessfehlertoleranzzeit neu definiert. Dabei beschreibt diese die maximale Zeit, die für die Reaktion der SIF verwendet werden kann.

# Und was nun..... Wie wird die Zeit denn verwendet?

IEC 61511 Teil 1 (2016)

## 3.2.39.1

### **demand mode SIF**

SIF operating in low demand mode (3.2.39 a)) or high demand mode (3.2.39 b))

Note 1 to entry: In the event of a dangerous failure of the SIF, a hazardous event can only occur

- if the failure is undetected and a demand occurs before the next proof test;
- if the failure is detected by the diagnostic tests but the related process and its associated equipment has not been moved to a safe state before a demand occurs.

Note 2 to entry: The safety integrity levels for SIF operating in demand mode are defined in Tables 4 and 5.

# Zusammenhang mit Diagnostic

**A.11.9.2** Schätzwerte der Ausfallraten können mittels einer quantitativen Analyse der Ausfallarten des Entwurfs unter Verwendung von Ausfalldaten einer anerkannten industriellen Quelle oder von Erfahrungen aus einer früheren Verwendung in der gleichen Umgebung wie bei der vorgesehenen Anwendung ermittelt werden. Der Konservativität halber kann bei Berechnungen die obere Grenze des 70-%-Konfidenzintervalls der Eingabedaten eingesetzt werden.

Es ist zu beachten, dass die gesamte unerkannte Ausfallrate von fehlertoleranten Gegenständen zeitabhängig ist und während der Intervalle der Wiederholungsprüfung zunimmt. Fehlertolerante Gegenstände können zeitabhängige Ausfallraten aufweisen.

**BEISPIEL** Ein Gegenstand aus zwei ähnlichen Komponenten A und B mit der gleichen unerkannten Ausfallrate  $\lambda$  hat eine insgesamt unerkannte Ausfallrate  $A$ , die von 0 nach  $\lambda$  zunimmt, wenn die Zeit zunimmt.

Bei der Quantifizierung zufälliger Hardware-Ausfälle einer PLT-Sicherheitseinrichtung (oder ihres PLT-Sicherheitseinrichtungs-Teilsystems) mit einer Hardware-Fehlertoleranz von Null und mit einer PLT-Sicherheitsfunktion in Betriebsart mit hoher oder kontinuierlicher Anforderungsrate sollten Diagnosen nur berücksichtigt werden, wenn:

- die Summe aus dem Diagnose-Testintervall und der Zeit zur Durchführung der festgelegten Maßnahme zum Erreichen oder Beibehalten eines sicheren Zustands geringer ist als die Prozess-Sicherheitszeit oder
- in Betriebsart mit hoher Anforderung das Verhältnis zwischen den Häufigkeiten der Diagnoseprüfung und der Anforderungshäufigkeit größer gleich 100 ist.

# Zusammenhang mit Diagnostic

IEC 61511 Teil 1 (2016)

## 3.2.39.2

### continuous mode SIF

SIF operating in continuous mode (3.2.39 c))

Note 1 to entry: In the event of a dangerous failure of the SIF a hazardous event will occur without further failure unless action is taken to prevent it within the **process safety time**.

Note 2 to entry: Continuous mode covers those SIF which implement continuous control to maintain functional safety.

Note 3 to entry: The safety integrity levels for SIF operating in continuous mode are defined in Table 5.

A dangerous failure can only be accounted for as detected in case the diagnostic is within the process safety time.

Without further failure → HFT 0.

# Zusammenhang mit Diagnostic

DIN EN 61511 Teil 1 (2019)

## 3.2.15

### Diagnose

(en: diagnostics)

Häufiger (im Vergleich zur Prozessfehlertoleranzzeit) automatischer Test zur Aufdeckung von Fehlern.

DIN EN 61508 Teil 4 (2011)

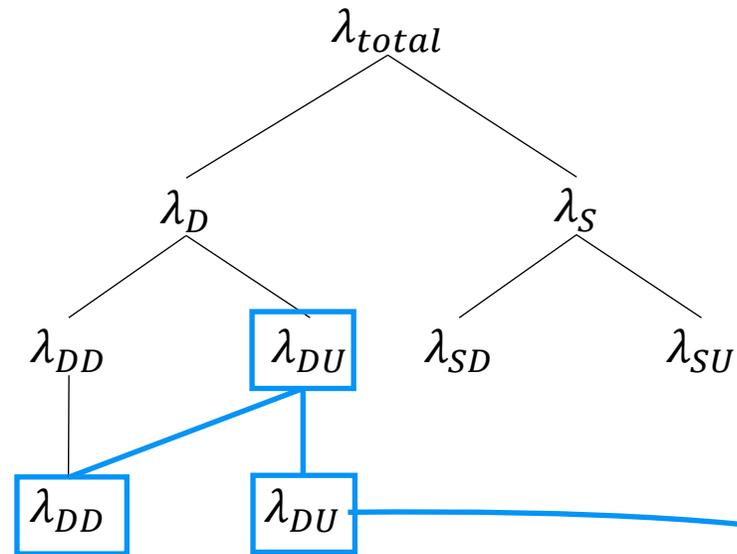
## 3.8.7

### Diagnose-Testintervall

(en: diagnostic test interval)

Zeitraum zwischen Online-Prüfungen, um Fehler in einem sicherheitsbezogenen System mit spezifiziertem Diagnosedeckungsgrad zu entdecken

# Was macht eine Diagnostic eigentlich aus



Zwei verschiedene Methoden:

- Teiltests
- Diagnostik (intern oder extern)

Die an unterschiedlichen Stellen in der Formel angreifen:

$$PFD_{avg} = \frac{T_{PT_1}}{2} \cdot PTC_1 \cdot \lambda_{DU} + \frac{T_{PT_2}}{2} \cdot (PTC_2 - PTC_1) \cdot \lambda_{DU} + \frac{T_{E\&R}}{2} \cdot (1 - PTC_2) \cdot \lambda_{DU}$$

**3.8.8 erkannt**  
(en: detected, overt, revealed)  
**offenkundig**  
in Verbindung mit Hardware erkannt durch diagnostische Prüfungen, Wiederholungsprüfungen, Bedienereingriff (zum Beispiel durch Inspektion und manuelle Prüfungen) oder durch üblichen Betrieb

BEISPIEL Diese Adjektive werden bei erkanntem Fehler und erkanntem Ausfall verwendet.

ANMERKUNG Ein durch Diagnoseprüfungen erkannter gefährbringender Ausfall ist ein erkannter Ausfall und kann nur als ein ungefährlicher Ausfall betrachtet werden, wenn wirksame automatische oder manuelle Maßnahmen ergriffen werden.

IEC 61508 – Teil 4 (2016)

# Zertifikate

- Prozesssicherheitszeit im Continuous Mode limitiert das Diagnosetestintervall. (Sonst darf ich die Vorteile der Diagnostic nicht verwenden. DD wird wieder zu DU)
- Prozesssicherheitszeit im Demand mode stellt theoretisch die gleiche Limitierung (siehe Def.). Dort ist aber der Demand-Fall selten, und für das Event müsste das sicherheitsgerichtete Gerät im Demand-Fall zeitgleich ausfallen. Da dies hinreichend unwahrscheinlich ist, wird in der Regel auf die Betrachtung verzichtet.

FMEDA	Kopftransmitter	Hutschienentransmitter
Sicherheitsfunktion(en)	Min., Max., Bereich	Min., Max., Bereich
$\lambda_{DU}^{2) 3)}$	40 FIT	41 FIT
$\lambda_{DD}^{2) 3)}$	258 FIT	258 FIT
$\lambda_{SU}^{2) 3)}$	127 FIT	123 FIT
$\lambda_{SD}^{2) 3)}$	3 FIT	3 FIT
SFF - Safe Failure Fraction	91%	90%
PFD <sub>avg</sub> für T1 = 1 Jahr <sup>3)</sup> (einkanalige Architektur)	$1,75 \cdot 10^{-4}$	$1,79 \cdot 10^{-4}$
PFD <sub>avg</sub> für T1 = 5 Jahre <sup>3)</sup> (einkanalige Architektur)	$8,76 \cdot 10^{-4}$	$8,98 \cdot 10^{-4}$
PFH	$4,0 \cdot 10^{-8} \cdot 1/h$	$4,1 \cdot 10^{-8} \cdot 1/h$
PTC <sup>4)</sup>	96%	96%
MTBF <sup>5)</sup>	156 Jahre	156 Jahre
Diagnose-Testintervall <sup>6)</sup>	4,3 min	4,3 min
Fehlerreaktionszeit <sup>7)</sup>	< 10,7 s	< 10,7 s
Prozesssicherheitszeit <sup>8)</sup>	7,2 h	7,2 h

*Hier wurde aus der Diagnosezeit die maximale zugehörige Prozesssicherheitszeit abgeleitet.*

*Dies macht natürlich NUR im Continuous Mode Sinn.*

<sup>8)</sup> Die Prozesssicherheitszeit beträgt: Diagnose-Testintervall x 100 (Berechnung nach IEC 61508)

# Beispiel: VCI Leitfaden zur TRGS 725

## 5.2.3 Kreiselpumpe mit Vermeiden des explosionsfähigen Gemisches durch das Betriebskonzept

durch Verlustleistung). Anhand der Verlustleistung, der verbleibenden Flüssigkeitsmenge und der Wärmekapazität von Flüssigkeit und Pumpe kann die Zeit abgeschätzt werden, die bleibt, bis die Flüssigkeit soweit erhitzt wird, dass Sieden der Flüssigkeit nicht mehr verhindert werden kann. In der Anlage ist ständig Personal in ausreichender Anzahl vorhanden, so dass angenommen werden kann, dass die Störung zeitnah erkannt und behoben oder die Pumpe vom Betriebspersonal abgeschaltet wird. Ein unbemerktes Verdampfen der verbleibenden Rest-

**Oder in anderen Worten: innerhalb der Prozessfehlertoleranzzeit wird der Fehler erkannt.**

# Beispiel Flammenwächter bei Brennern

- Ein Fehler in der Brennerausrüstung, der zu einem Abriss der Flamme führt
- Die Prozessfehlertoleranzzeit kann (?) sehr kurz sein
- Die Reaktion der PLT-Sicherheitseinrichtung muss sehr schnell erfolgen
- Es handelt sich dabei um eine zeitkritische Fragestellung
- Die Anforderungen an die DC des Flammenwächters sind sehr hoch
- $\lambda_{DD}$  muss gegen  $\lambda_{DU}$  sehr groß sein
- → und die Diagnose muss in sehr kurzer Zeit abgeschlossen sein

Viele Dank für die Aufmerksamkeit

Über eine rege Diskussion würden wir uns freuen.



Mehr Wert.  
Mehr Vertrauen.

## Wiederkehrenden Prüfung von PLT- Sicherheitseinrichtungen - Sinn und Unsinn

15. SIL-Sprechstunde 2024  
18. bis 19. September 2024

TÜV SÜD Industrie Service GmbH  
Inspektionsstelle für Funktionale Sicherheit /  
Prüfbereich Feuerungsanlagen und  
Thermoprozesstechnik Außenstelle Regensburg

Stefan Krause

# Inhalt

1 Was ist eine PLT-Sicherheitsfunktion

2 Rechtlicher Rahmen

3 Fehlerarten

4 Sinn und Unsinn

5 Zusammenfassung

6 Kontakt

# Inhalt

1

Was ist eine PLT-Sicherheitsfunktion

2

Rechtlicher Rahmen

3

Fehlerarten

4

Sinn und Unsinn

5

Zusammenfassung

6

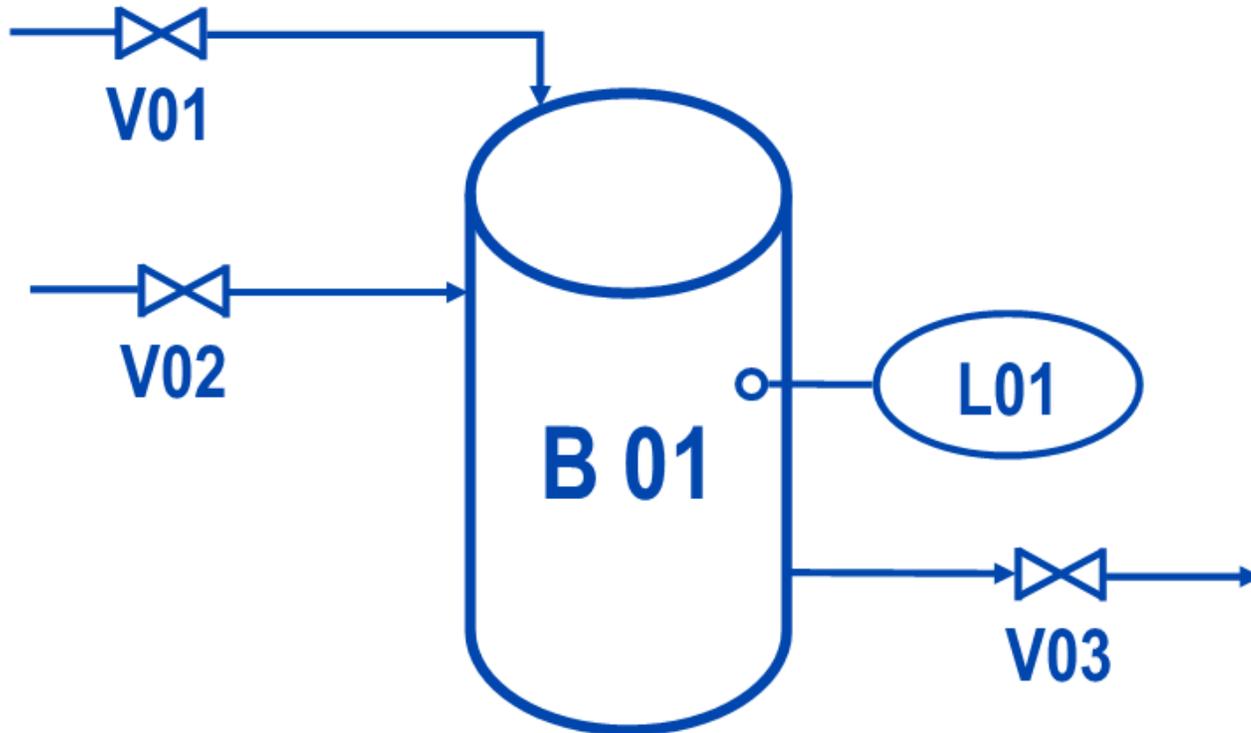
Kontakt

# Bestandteile einer funktionsfähigen Anlage

- Verfahrenstechnische Einrichtungen
    - Apparate
    - Rohrleitungen
    - Behälter
    - Ausrüstungsteile mit Sicherheitsfunktion (z.B. Sicherheitsventil)
  - **Automatisierungstechnik**
    - PLT- Betriebseinrichtungen
    - **PLT-Sicherheitseinrichtungen**
  - Aufstellfläche/raum
    - Gebäudeautomation
    - Verkehrsflächen
- ... und vieles mehr!**



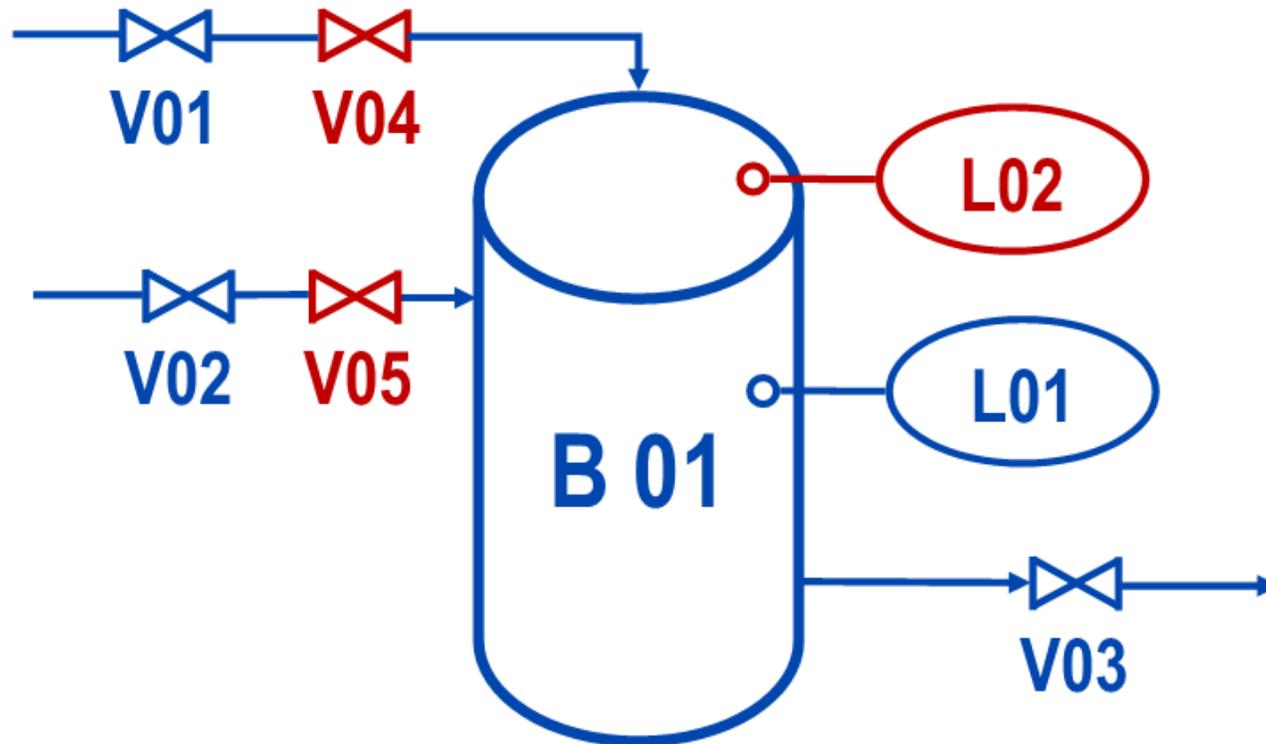
# Was ist eine PLT-Sicherheitsfunktion



## Funktionsbeschreibung

- Betriebsfunktion (blau)

# Was ist eine PLT-Sicherheitsfunktion



## Funktionsbeschreibung

- Zusätzlich zu den Betriebsfunktionen (blau) wird die Sicherheitsfunktion SIF 01 durch die roten Komponenten umgesetzt
- Über die Messung L02 wird erkannt, wenn der Füllstand über einen definierten Grenzwert steigt
- Durch das Schließen der beiden Ventile V04 und V05 wird verhindert, dass weitere Flüssigkeit in den Behälter gelangt

# Inhalt

1

Was ist eine PLT-Sicherheitsfunktion

2

Rechtlicher Rahmen

3

Fehlerarten

4

Sinn und Unsinn

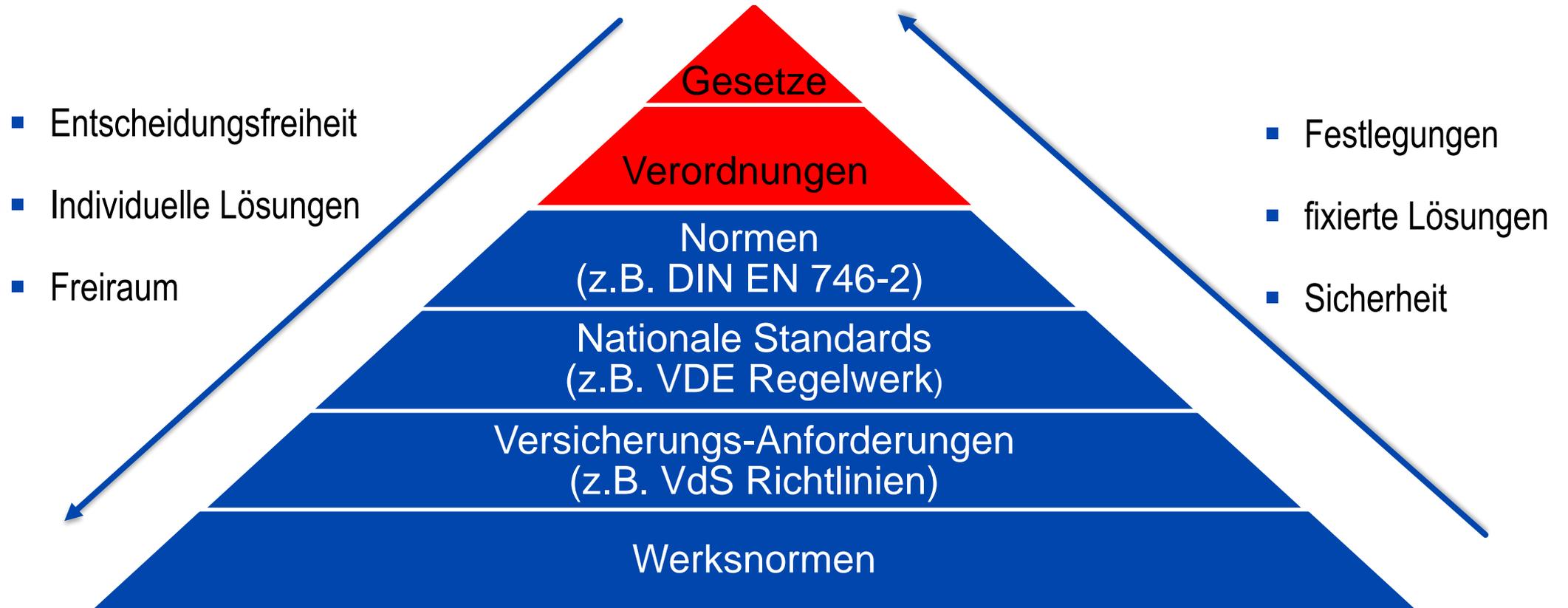
5

Zusammenfassung

6

Kontakt

# Rechtlicher Rahmen



# Rechtlicher Rahmen - Abgekürzt

- **Arbeitsschutzgesetz - ArbSchG**

- **§ 4 Allgemeine Grundsätze**

Der Arbeitgeber hat bei Maßnahmen des Arbeitsschutzes von folgenden allgemeinen Grundsätzen auszugehen:

1. Die Arbeit ist so zu gestalten, daß **eine Gefährdung** für das Leben sowie die physische und die psychische Gesundheit **möglichst vermieden** und die verbleibende **Gefährdung möglichst gering gehalten wird**;
2. Gefahren sind an ihrer Quelle zu bekämpfen;

...



# Rechtlicher Rahmen - Abgekürzt

## ■ Grundpflichten des Arbeitgebers

### ■ Absatz 5 § 4 BetrSichV

(5) Der Arbeitgeber hat die Wirksamkeit der Schutzmaßnahmen vor der erstmaligen Verwendung der Arbeitsmittel zu überprüfen. Satz 1 gilt nicht, soweit entsprechende Prüfungen nach § 14 oder § 15 durchgeführt wurden. Der Arbeitgeber hat weiterhin dafür zu sorgen, dass Arbeitsmittel vor ihrer jeweiligen Verwendung auf offensichtliche Mängel, die die sichere Verwendung beeinträchtigen können, kontrolliert werden und dass Schutz und **Sicherheitseinrichtungen einer regelmäßigen Kontrolle ihrer Funktionsfähigkeit unterzogen werden.** Satz 3 gilt auch bei Arbeitsmitteln, für die wiederkehrende Prüfungen nach § 14 oder § 16 vorgeschrieben sind.



# Inhalt

1 Was ist eine PLT-Sicherheitsfunktion

2 Rechtlicher Rahmen

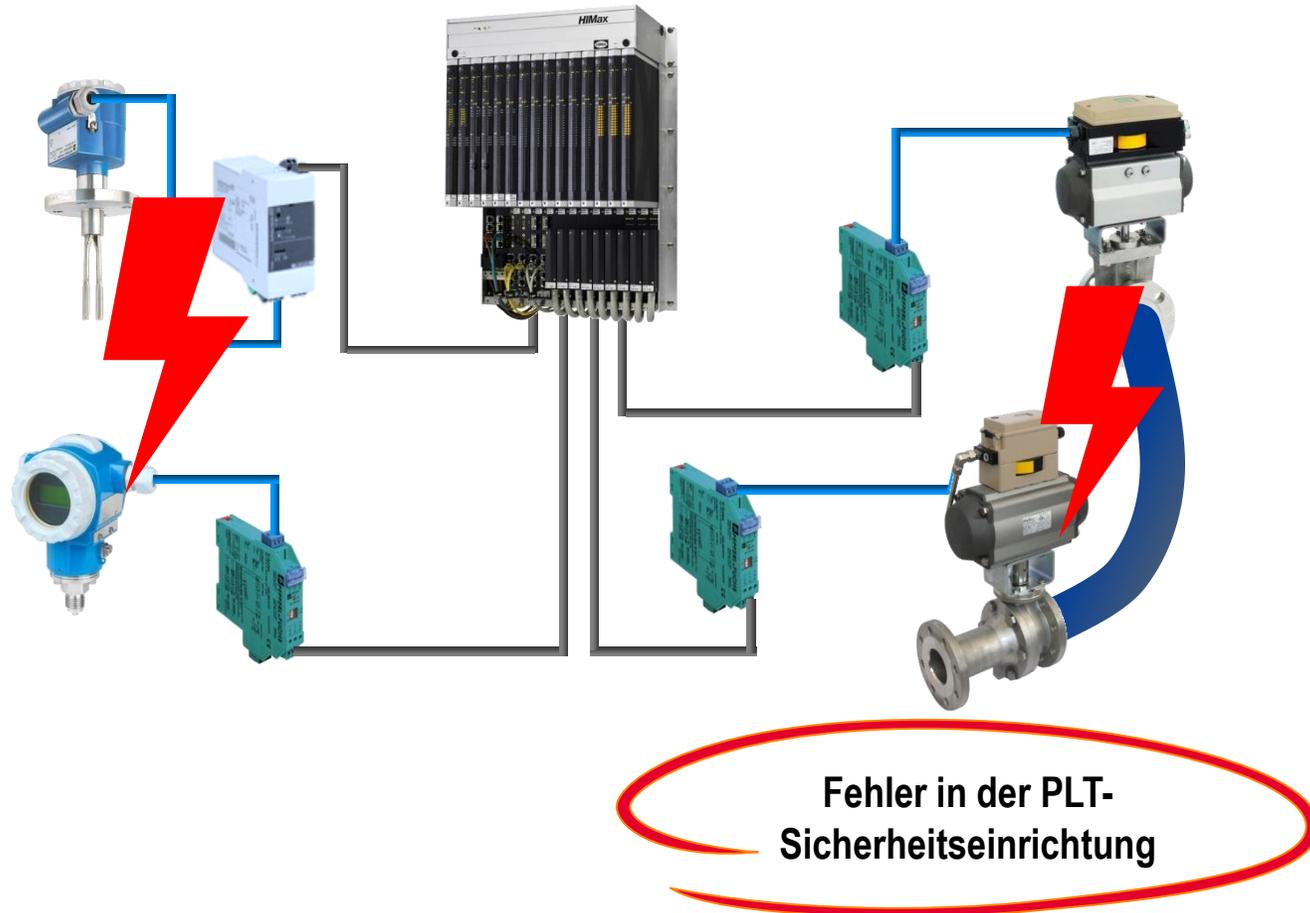
3 Fehlerarten

4 Sinn und Unsinn

5 Zusammenfassung

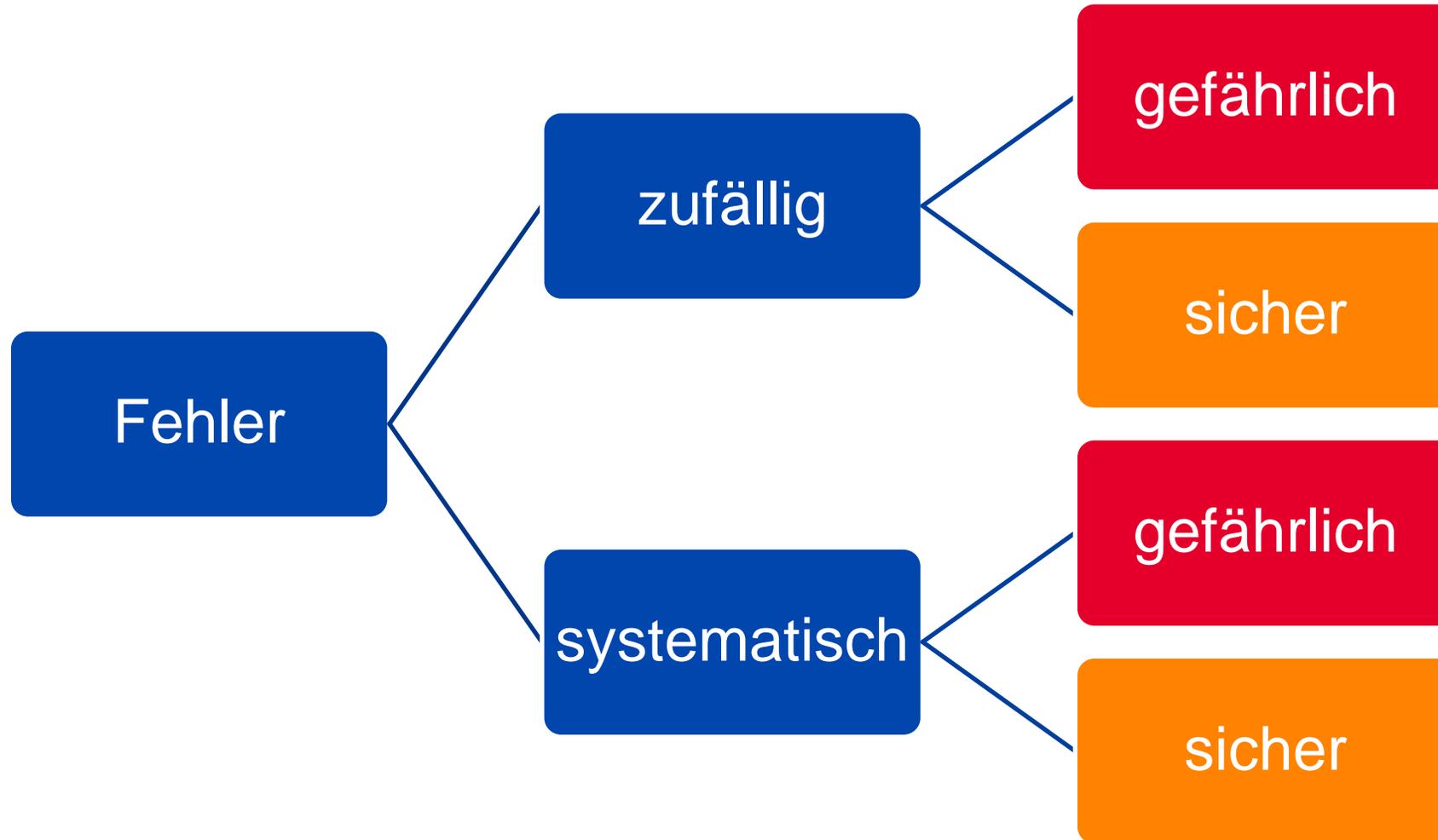
6 Kontakt

# Fehler und Fehlerarten

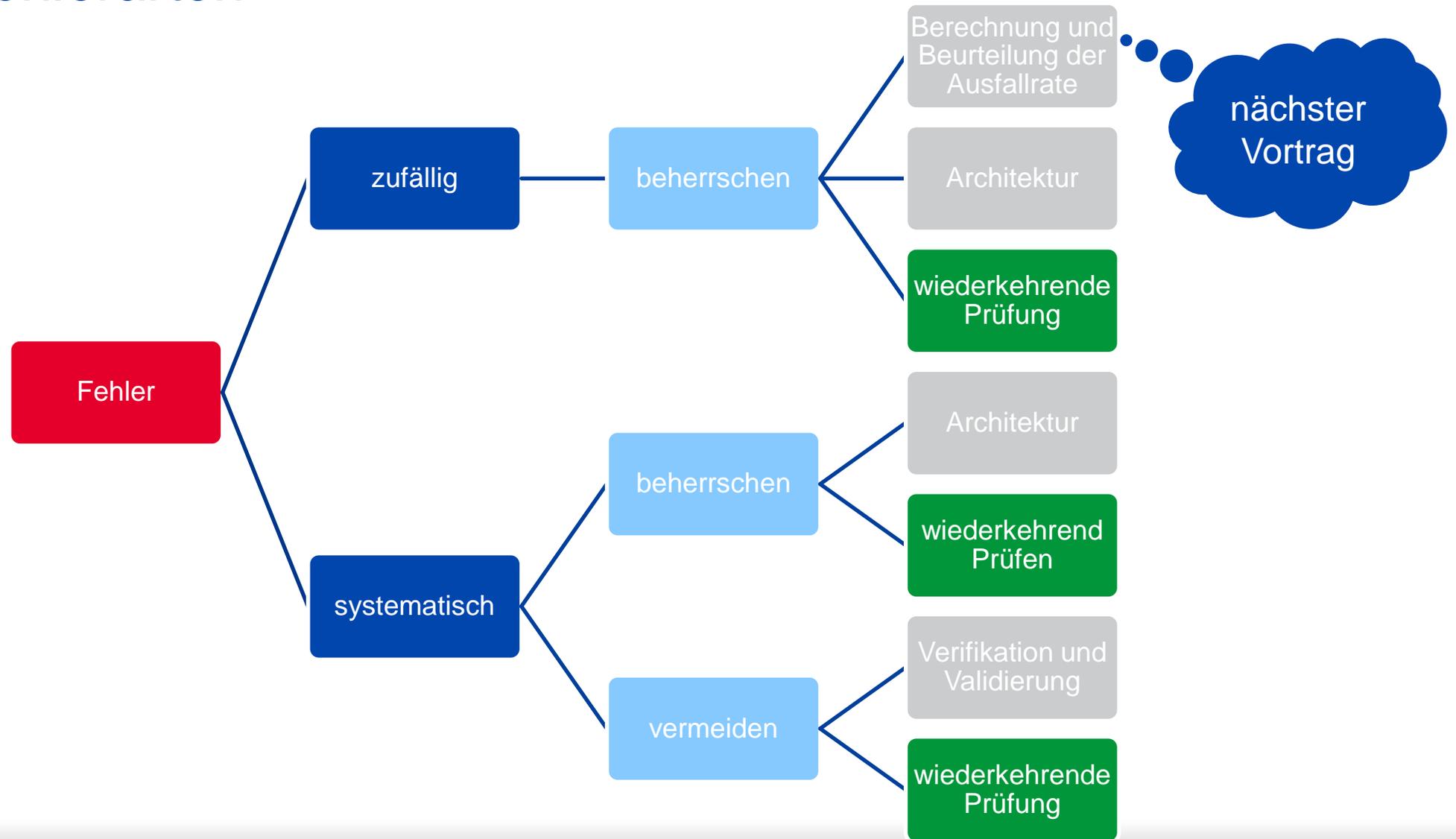


- Ein Fehler führt zum Ausfall der PLT-Sicherheitsfunktion

# Fehler und Fehlerarten



# Fehler und Fehlerarten



# Inhalt

1 Was ist eine PLT-Sicherheitsfunktion

2 Rechtlicher Rahmen

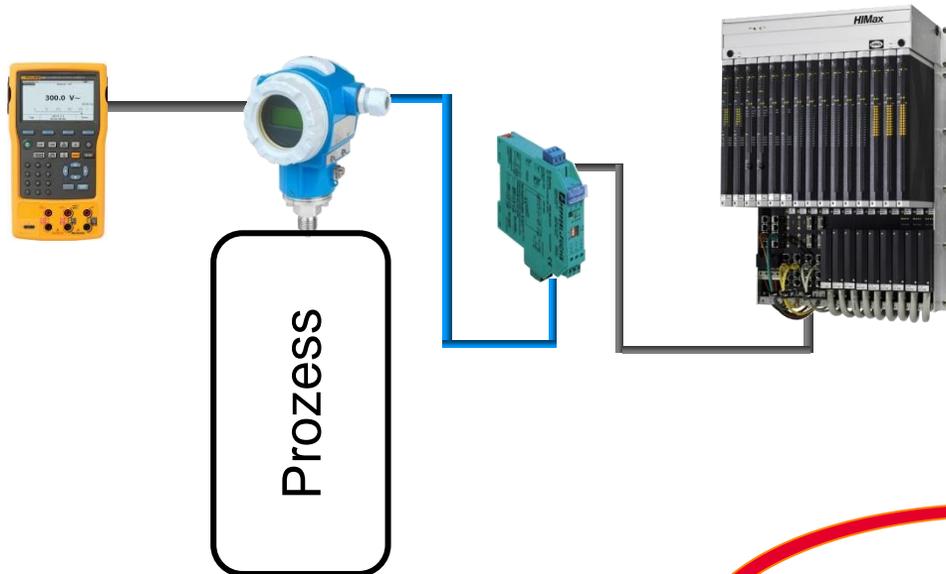
3 Fehlerarten

4 Sinn und Unsinn

5 Zusammenfassung

6 Kontakt

# Sinn und Unsinn: Beispiel 1



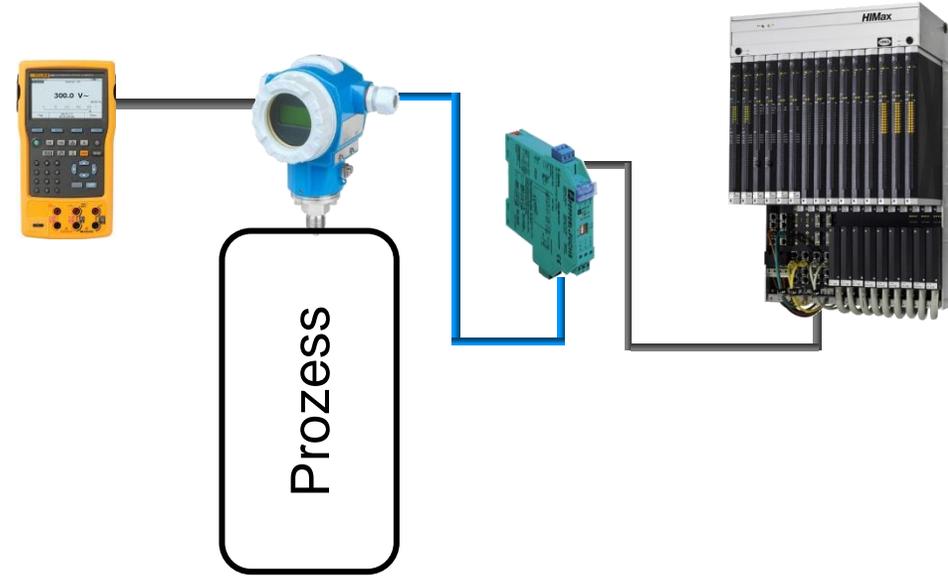
- Eine analoge Druckmessung soll geprüft werden

Vorgehen bei der Prüfung

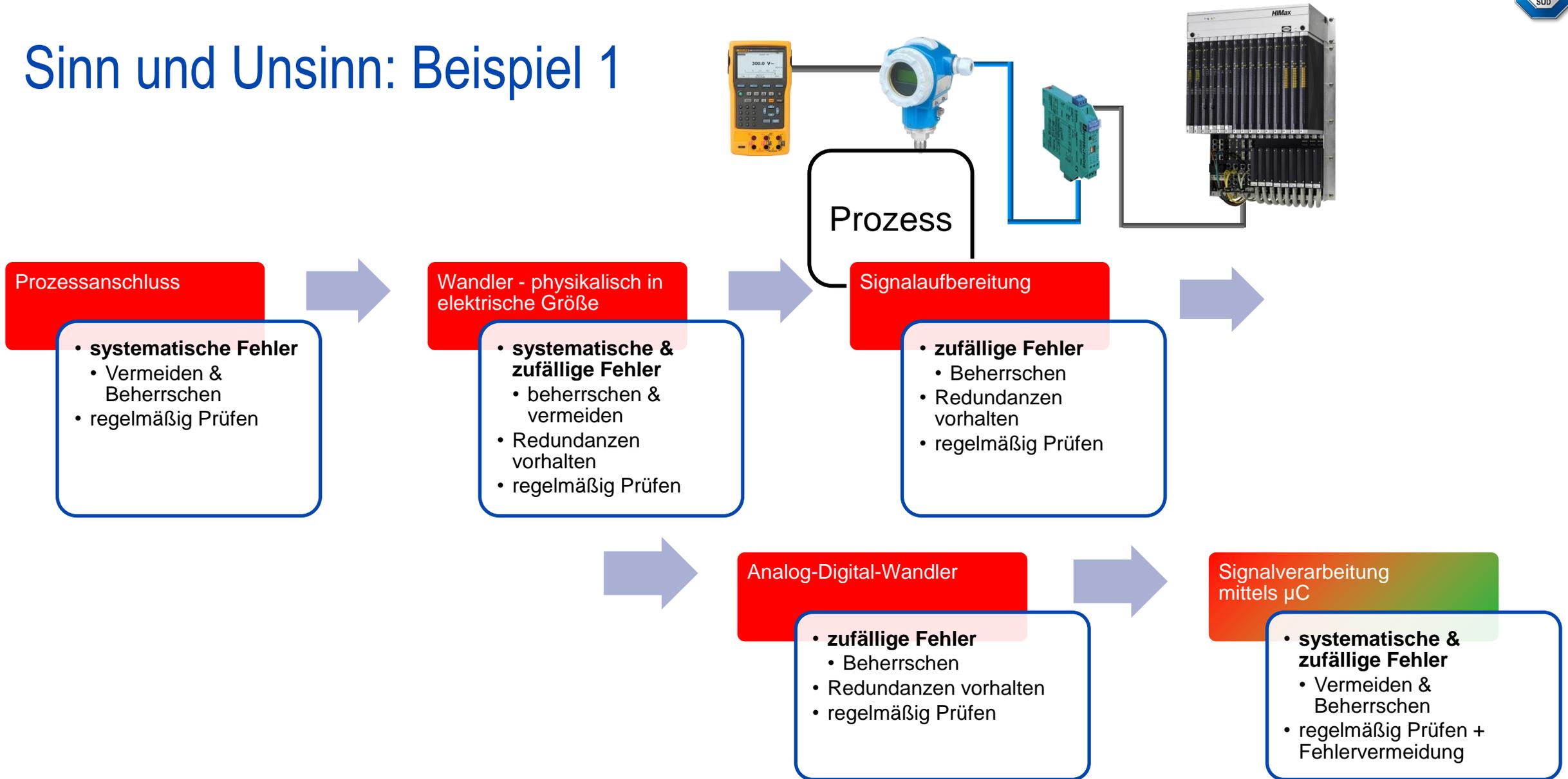
- Ausgangstreiber des Messumformers über Hart Kommunikator durchgeführt und im Anwenderprogramm verifiziert

Wie gut ist das Prüfergebnis?

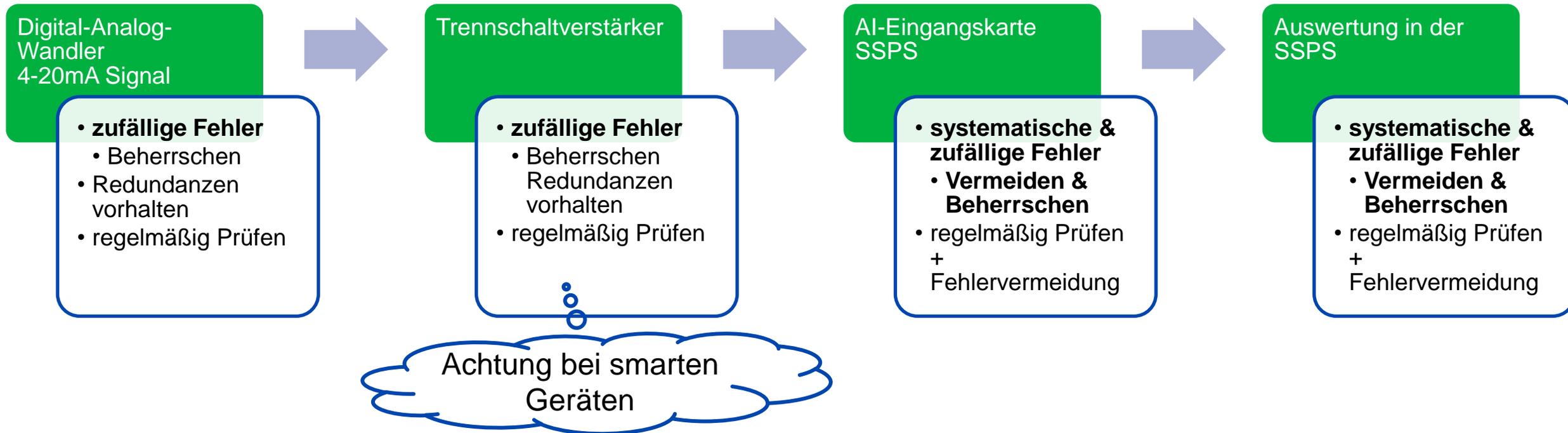
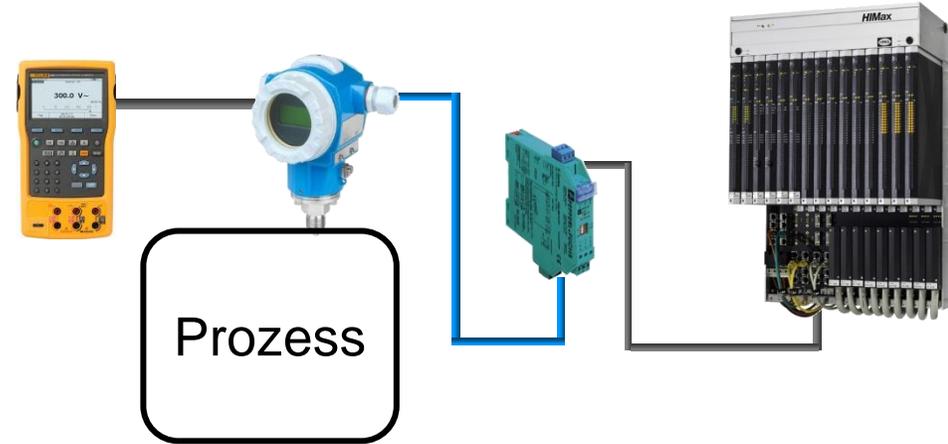
# Sinn und Unsinn: Beispiel 1



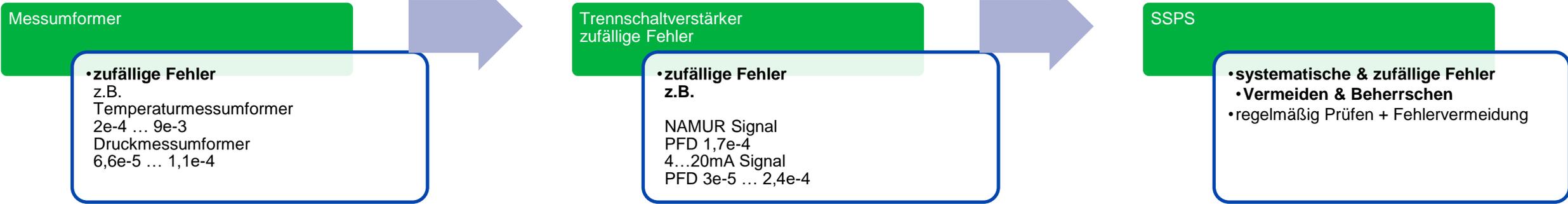
# Sinn und Unsinn: Beispiel 1



# Sinn und Unsinn: Beispiel 1



# Sinn und Unsinn: Beispiel 1

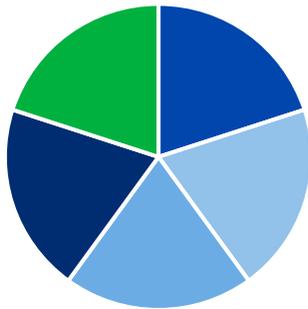


**• zufällige Fehler**  
 z.B.  
 Temperaturmessumformer  
 2e-4 ... 9e-3  
 Druckmessumformer  
 6,6e-5 ... 1,1e-4

**• zufällige Fehler**  
 z.B.  
 NAMUR Signal  
 PFD 1,7e-4  
 4...20mA Signal  
 PFD 3e-5 ... 2,4e-4

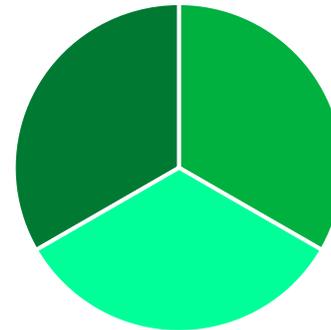
**• systematische & zufällige Fehler**  
 • Vermeiden & Beherrschen  
 • regelmäßig Prüfen + Fehlervermeidung

Zufällige Fehler des Messumformers



- Wandler
- Signalverarbeitung
- Analog-Digital-Wandler
- Signalverarbeitung
- Digital-Analog-Wandler

Zufällige Fehler des Trennschaltverstärkers



- Wandler Eingang
- Signalverarbeitung
- Wandler Ausgang

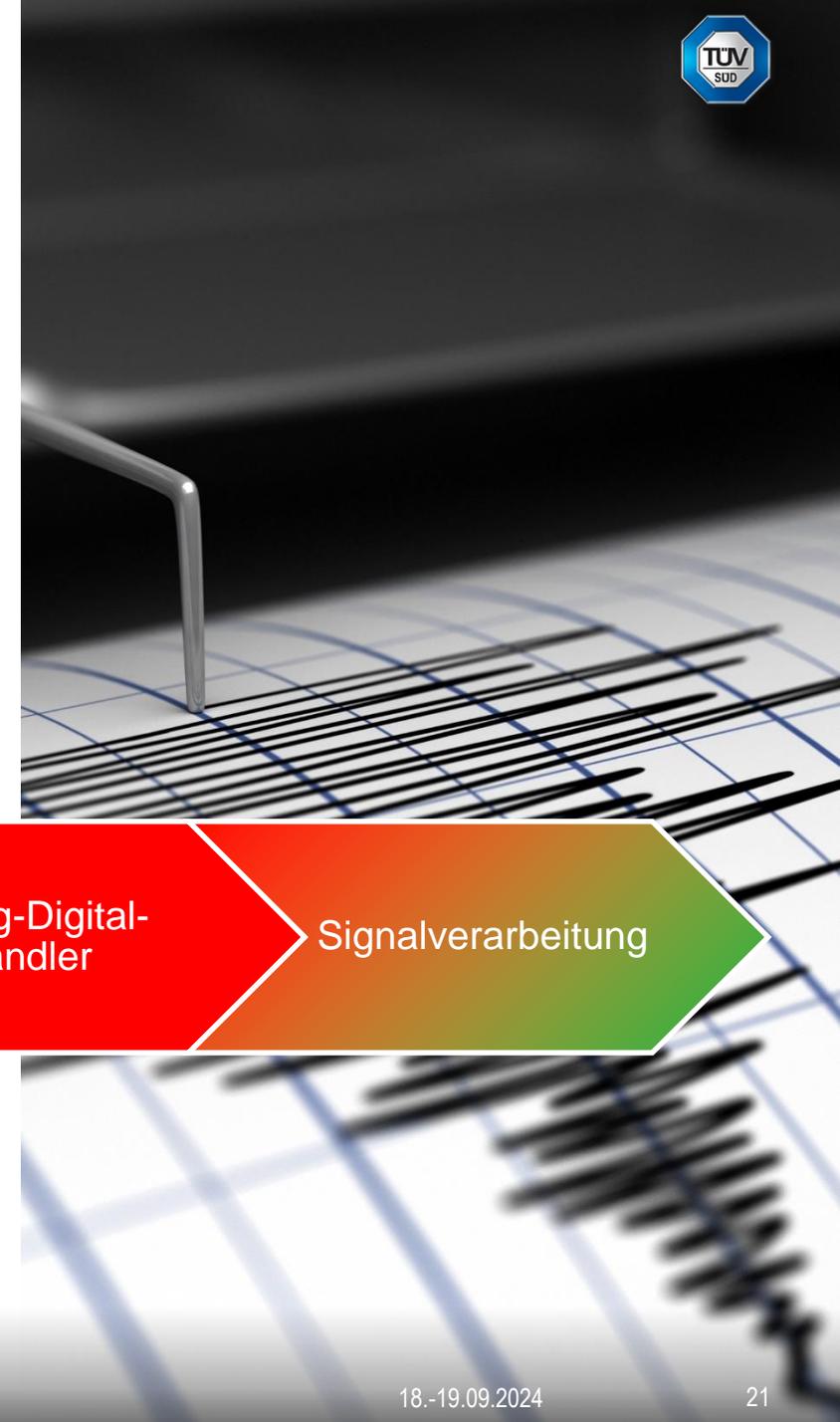
$$\frac{\lambda_{DUmu}}{5} + \lambda_{DUtr} \neq \lambda_{DUmu} + \lambda_{DUtr}$$

**ca. 40% der Fehler werden nicht aufgedeckt!**

# Sinn und Unsinn: Beispiel 1

## Zusammenfassung

- **0,0%** der systematischen Fehler werden aufgedeckt!
  - Max. 60% der zufälligen Fehler können aufgedeckt werden
- **Der systematische Ausfall ist sicher!**
- **Die Ausfallwahrscheinlichkeit auf Grund von zufälligen Fehlern steigt gegenüber einer 100%Prüfung!**



# Sinn und Unsinn: Beispiel 1

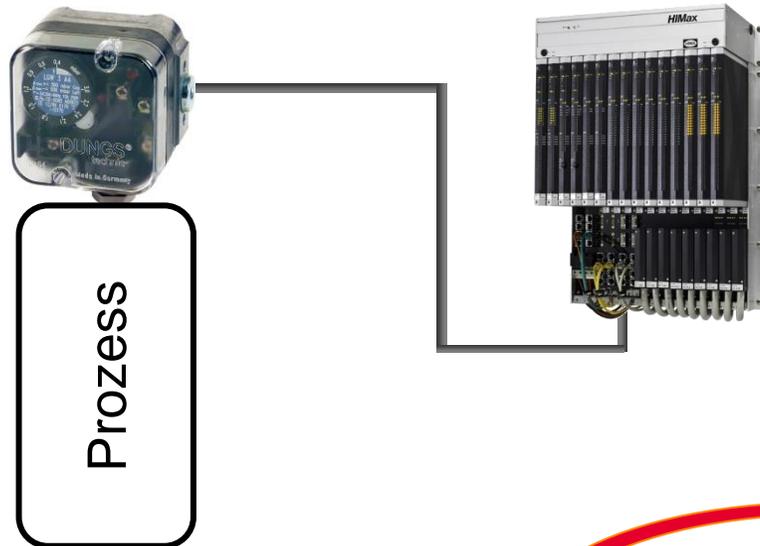
## Zusammenfassung

- **Der systematische Ausfall ist sicher!**



**Zu geringer Luftdruck im Reifen führt zum systematischen (im Experiment reproduzierbar) Versagen des Reifens**

# Sinn und Unsinn: Beispiel 2



- Ein binärer Druckschalter soll geprüft werden

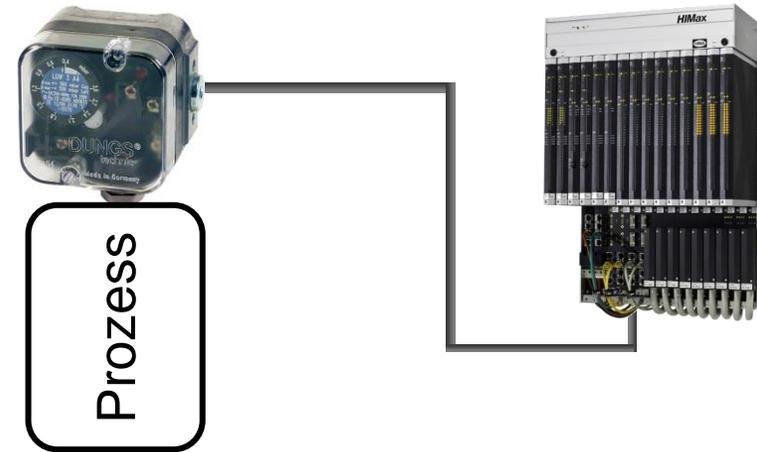
Vorgehen bei der Prüfung

- Verstellen des Grenzwerts am Druckschalter

Wie gut ist das Prüfergebnis?

# Sinn und Unsinn: Beispiel 2

- Druckschalter prüfen durch verstellen des Grenzwerts



# Sinn und Unsinn: Beispiel 2

## Schaltkontakt

- Auslegung
- z.B. bei Maschinen entsprechend der DIN EN ISO 13849-1:2016-06
  - Unterlastet
  - z.B. Bemessungsstrom(Schaltkontakt) = 1,5 x Bemessungsstrom(Sicherung)
- z.B. bei Feuerungsanlagen entsprechend der DIN EN 50156
  - Unterlastet
  - z.B. Bemessungsstrom(Schaltkontakt) x 0,6 = Bemessungsstrom(Sicherung)

**NUR das Bauteil mit der größten Sicherheitsreserve wird geprüft!**



# Sinn und Unsinn: Beispiel 2

Wie gut ist das Prüfergebn?  
**Mangelhaft**



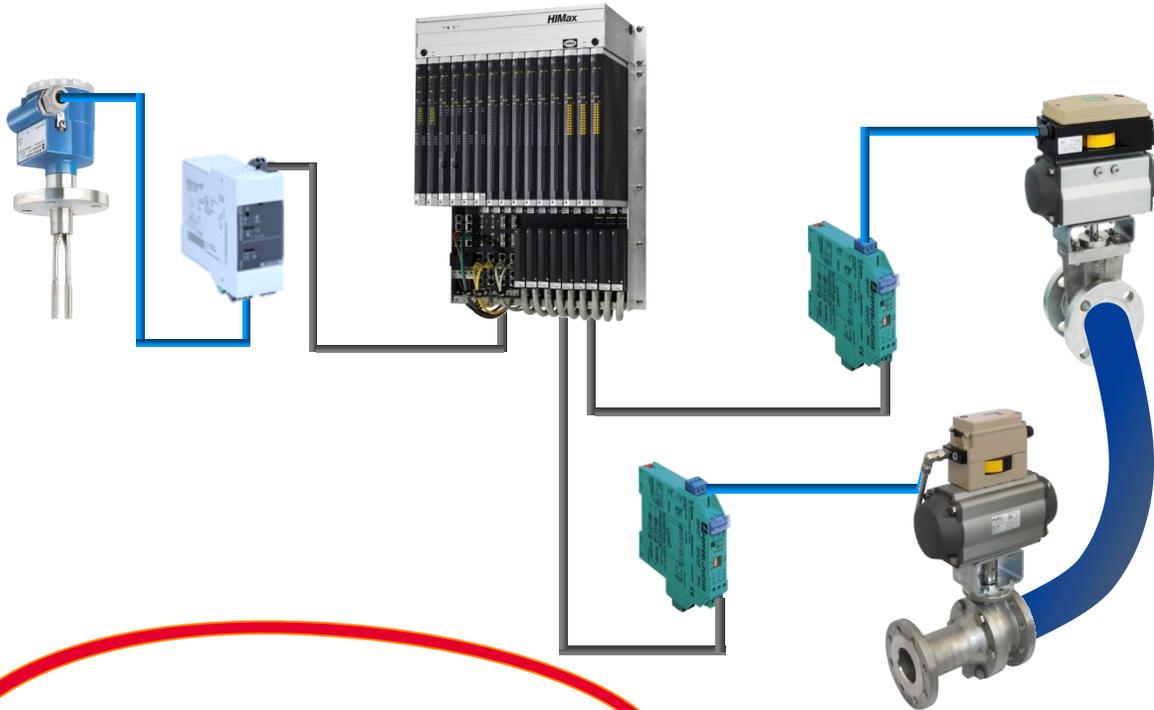
- Schalterpunkt
- Funktion des Messwerks



- Potentialfreier Kontakt



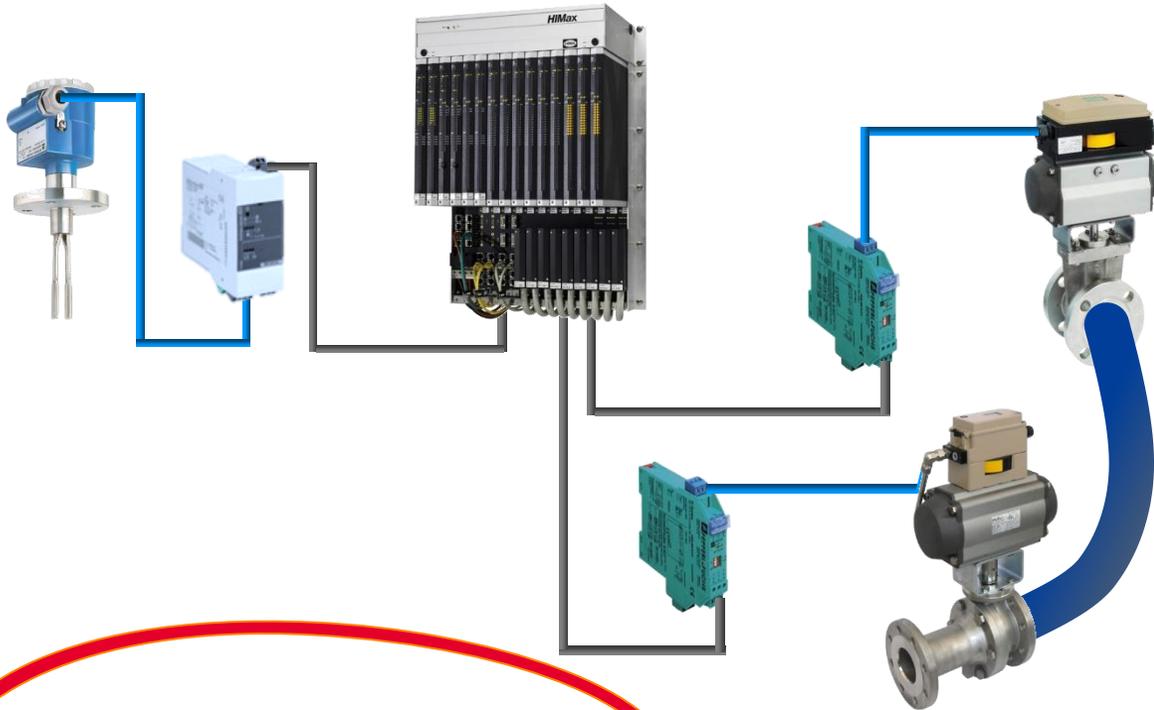
# Durchführung der Prüfung: Beispiel 3 - Sensorik



Wie gut ist das Prüfergebnis?

- Am Tank X ist eine Schwinggabel als Überfüllsicherung montiert. Im Rahmen der wiederkehrenden Prüfung soll geprüft werden, ob die Überfüllsicherung bei Überschreiten des Standes anspricht. Der Prüfer löst die Überfüllsicherung durch Betätigen der Prüftaste am Gerät aus.
- Prüfung vollständig?
- Was muss beachtet werden?

# Durchführung der Prüfung: Beispiel 3 - Aktorik



- Die zur Überfüllsicherung gehörenden Ventile soll geprüft werden
- Um den laufenden Betrieb nicht zu stören, werden die Armatur mechanisch in Offenstellung blockiert
- Zulässig? Sinnvoll? Aussagekräftig?

Wie gut ist das Prüfergebnis?

# Inhalt

1 Was ist eine PLT-Sicherheitsfunktion

2 Rechtlicher Rahmen

3 Fehlerarten

4 Sinn und Unsinn

5 Zusammenfassung

6 Kontakt

# Zusammenfassung

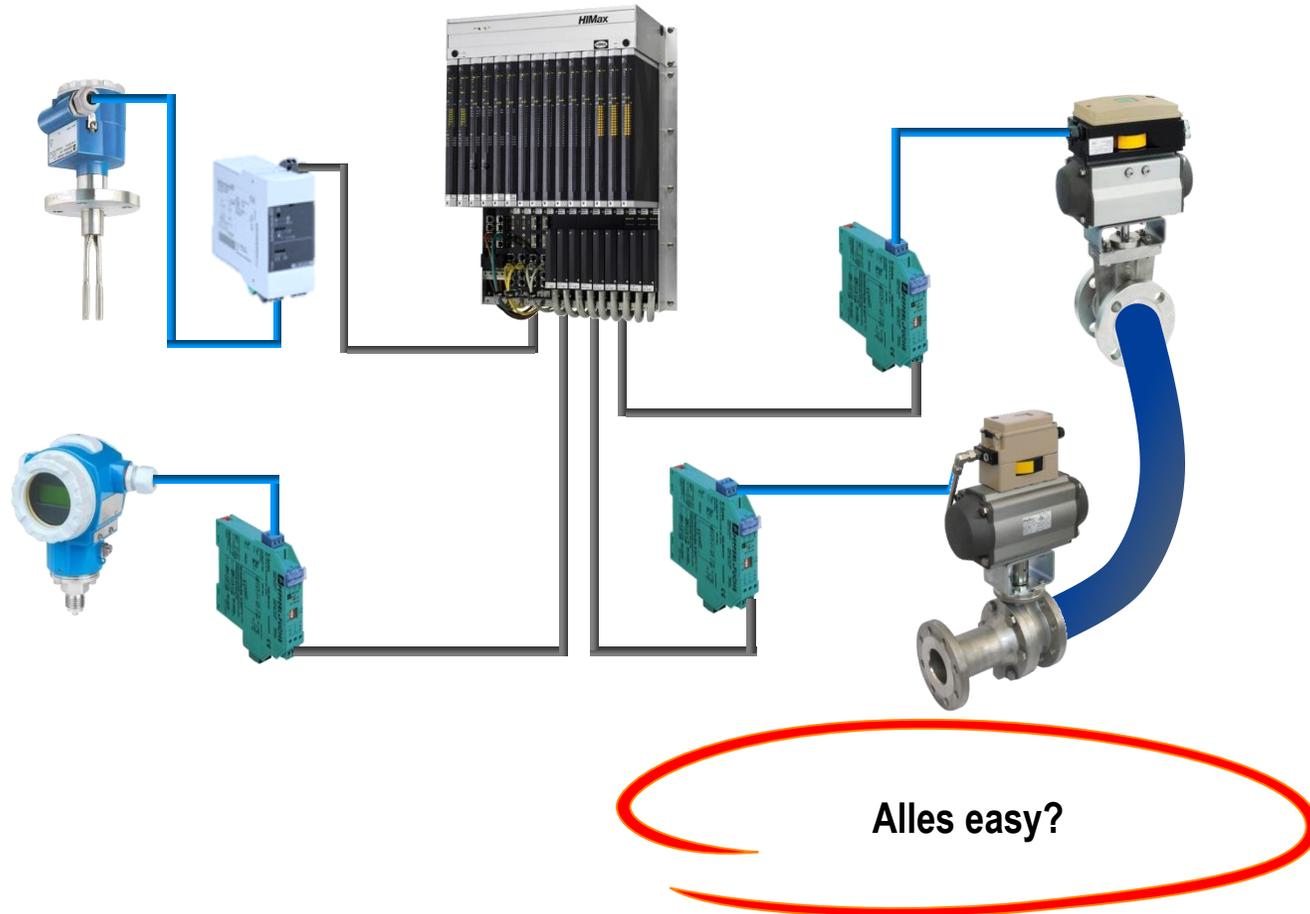
Gibt es Sinn und Unsinn bei  
der wiederkehrenden Prüfung?

**JA**



# Zusammenfassung

Was kann schief gehen?



- Planung der Prüfung
- Prüfvorgang
- Prüfmittel
- Dokumentation der Prüfung
- Vollständigkeit der Prüfung  
Ist die geprüfte Sicherheitseinrichtung wieder aktiv?
- Menschliches Versagen beim Prüfvorgang
- ...

# Inhalt

1 Was ist eine PLT-Sicherheitsfunktion

2 Rechtlicher Rahmen

3 Fehlerarten

4 Sinn und Unsinn

5 Zusammenfassung

6 Kontakt

# Kontakt

**TÜV SÜD Industrie Service GmbH**

---

**Hr. Stefan Krause**

- Experte Funktionale Sicherheit und Feuerungstechnik
- Friedenstr. 6  
93051 Regensburg
- Mobile: +49 151 42463408
- E-Mail: [stefan.krause@tuvsud.com](mailto:stefan.krause@tuvsud.com)

**WARUM MIT DEM  
FASTEN BEGINNEN?**



**BEIM TÜV NIMMT MAN  
JEDEN TAG ETWAS AB.**



**Mehr Wert.  
Mehr Vertrauen.**

**Vielen Dank für Ihre  
Aufmerksamkeit!**



# Mythos SIL-Nachweisberechnung: Warum möchten alle etwas rechnen?

# Persönliche Vorstellung

## **Persönliche Vorstellung:**

Malika Mast

Geschäftsführerin RAMSYS GmbH

- FSCEA (Functional Safety Certified Engineer Application)  
A031\_01255/18 (TÜV Nord)
- FS Eng für Maschinen  
# 14527/17 (TÜV Rheinland)
- FS Eng im Arbeitsgebiet Explosion Protection  
Id.-Nr.: 0328/2019 (TÜV Süd)

## **Kontaktdaten:**

Hervester Straße 36

46286 Dorsten

Tel.: +49 (0)2369 / 74593-10

[m.mast@ramsys.org](mailto:m.mast@ramsys.org)

[www.ramsys.org](http://www.ramsys.org)



# Agenda

## **I. Mythos SIL-Nachweis**

- (1) Brauche ich einen SIL-Nachweis?
- (2) Warum ist ein SIL-Nachweis für alle so interessant?
- (3) Dokumentation der Funktionalen Sicherheit

## **II. Sicht der Norm**

- (1) Fehlerarten
- (2) Welche Fehler betrachtet die SIL-Nachweisrechnung

## **III. Probleme aus der Praxis**

- (1) Struktur bei Konzernen
- (2) Anpassung der HAZOP
- (3) Änderung des Prüfkonzepts

## **IV. Abschluss**

- (1) Alternative Ansätze
- (2) Aufbau FSM
- (3) Fazit

# I. Mythos SIL-Nachweis

- (1) Brauche ich einen SIL-Nachweis
- (2) Warum ist ein SIL-Nachweis für alle so interessant?
- (3) Dokumentation der Funktionalen Sicherheit

# (1) Brauche ich einen SIL-Nachweis

Normauszug:

**DIN EN 61511-1 (VDE 0810-1):2019-02**  
**EN 61511-1:2017 + A1:2017**

## **11.9 Quantifizierung zufälliger Ausfälle**

**11.9.1** Der für jede PLT-Sicherheitsfunktion ermittelte Ausfallwert muss gleich oder besser als der Zielwert des in der Spezifikation der Sicherheitsanforderungen spezifizierten SIL. Dies muss durch eine Berechnung nachgewiesen werden.

## (2) Warum ist ein SIL-Nachweis für alle so Interessant?

- Aus unserer Erfahrung heraus, genießt der SIL-Nachweis in Form einer PFD-Berechnung bei vielen Betreibern bzw. Anlagenverantwortlichen den höchsten Stellenwert im SIL-Bereich. Woran liegt das?
- Es liegt kein oder ein nicht gelebtes FSM vor
- Berechnungen stellen ein eindeutiges Ergebnis da
- Der SIL-Nachweis ist in der Regel das einzige Dokument, in dem abgefragt wird ob eine gewisse SIL-Einstufung erreicht wurde:

<b>Ziel der Prüfung</b>	Durchführung der SIL-Nachweisrechnung
<b>Ergebnis der Prüfung:</b>	Die geforderte SIL 1 Einstufung konnte nachgewiesen werden

# (3) Dokumentation der Funktionalen Sicherheit

Notwendige Dokumentation (Prozessindustrie) nach Durchlaufen des Sicherheitslebenszyklus

Dienstleister	ZÜS / TAS	Interne Prüfung	Geräte-Doku	Betreiber
Nachweis FSM	Abnahme Protokoll	Validierungsberichte	Sicherheitshandbuch	Gefährdungsbeurteilung
Qualifikationsnachweise der Mitarbeiter	Prüfbericht	Verifizierungsberichte	SIL-Zertifikat	Klassifizierung
		Auditberichte	Handbuch	SRS
			Technische Inf.	SIL-Nachweis
			Konformitätserkl.	UW-Matrix
			Bedienungsanleit.	Prüfkonzept
			Montageanleit.	FAT-Doku
				SSPS-Doku

## II. Sicht der Norm

(1) Fehlerarten

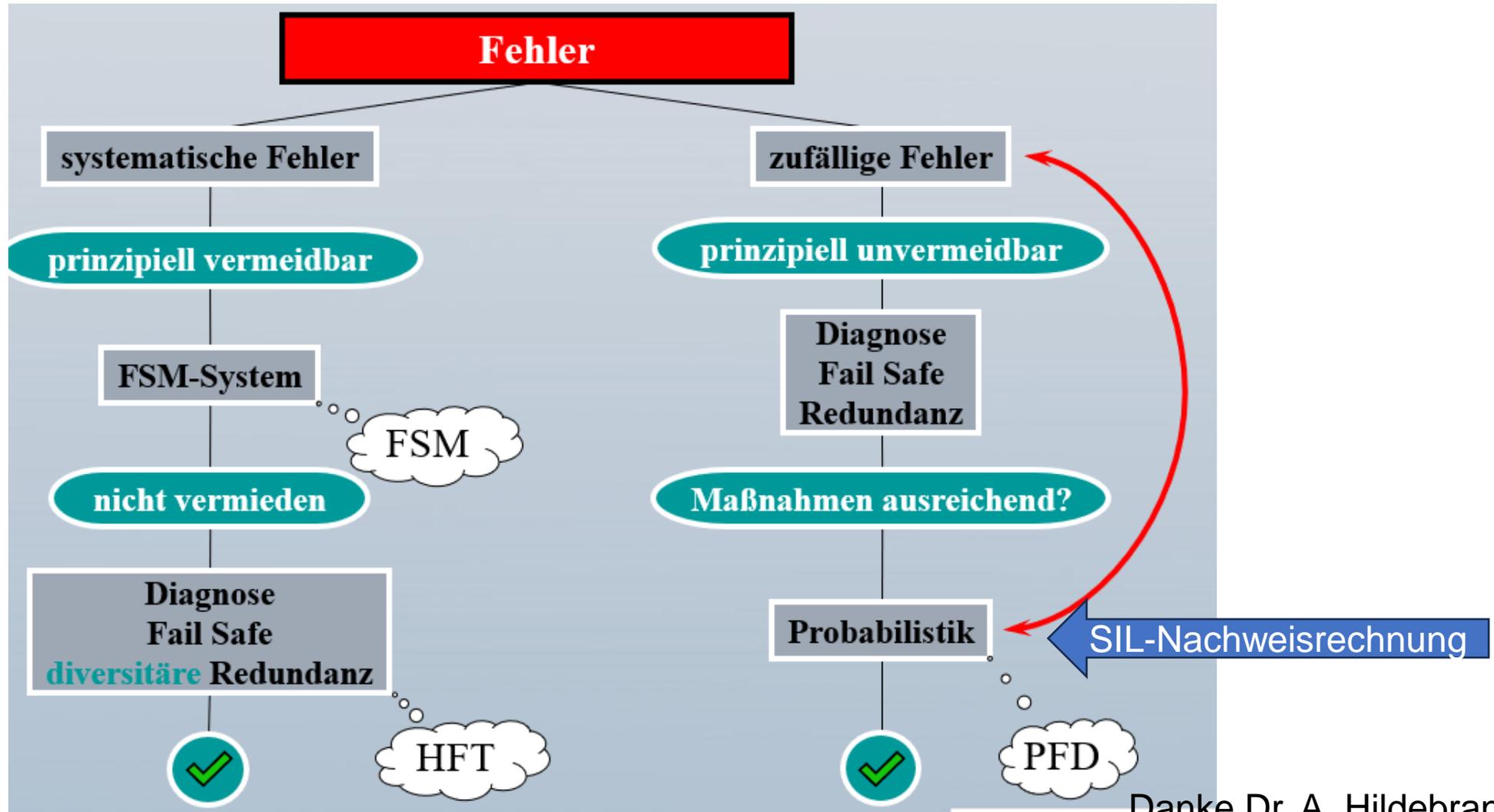
(2) Welche Fehler betrachtet der SIL-Nachweis

# (1) Fehlerarten

▀ Verschiedenen Fehlerarten der Funktionalen Sicherheit

Art der Fehler	---	grob	systematisch	zufällig
				
Abweichung	optimale Verteilung der Messwerte	Aussagen schwer möglich	gering	hoch
Qualität des Mittelwertes			schlecht	gut

(2) Welche Fehler betrachtet die SIL-Nachweisrechnung



Danke Dr. A. Hildebrandt

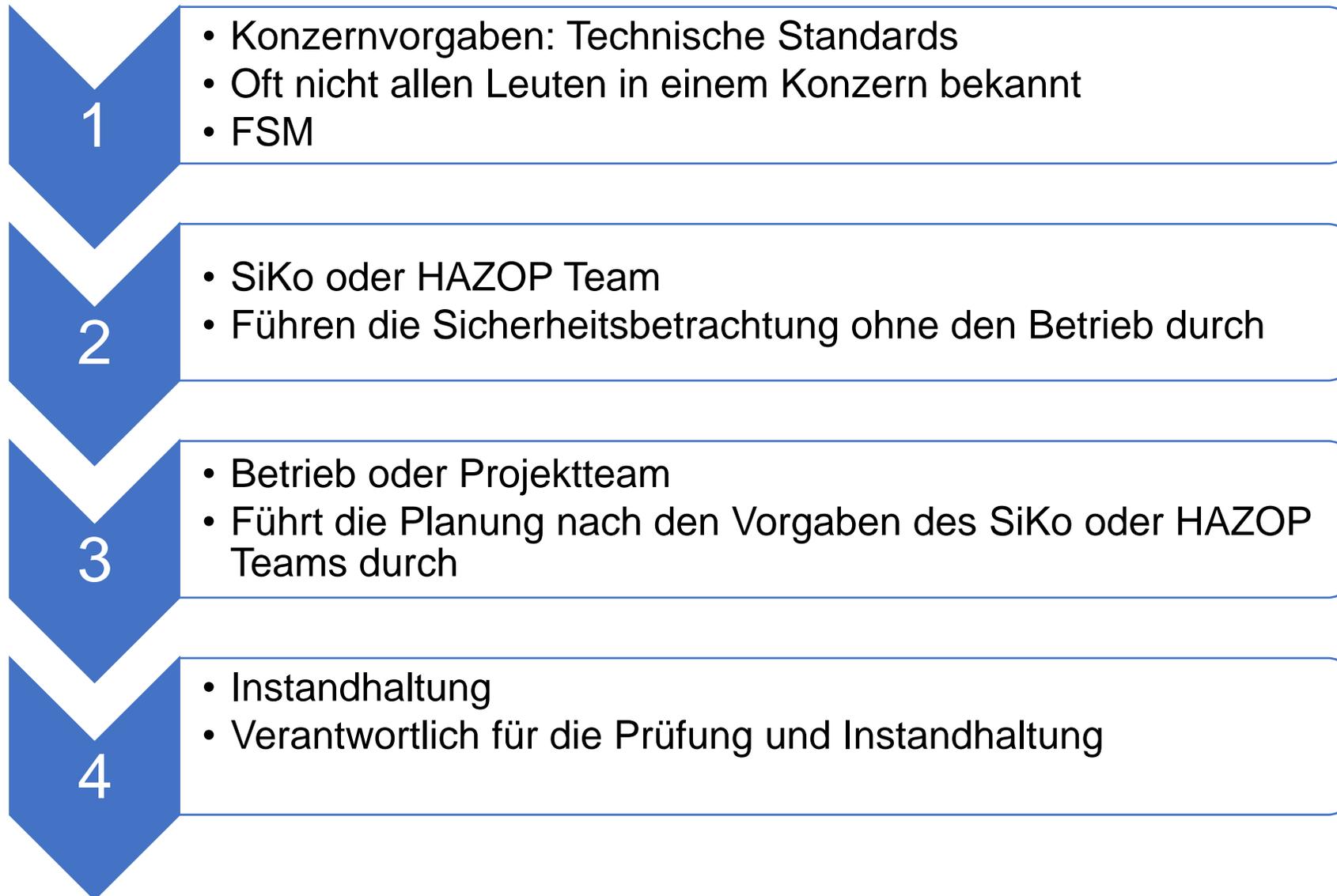
## (2) Welche Fehler betrachtet die SIL-Nachweisrechnung



### III. Probleme aus der Praxis

- (1) Struktur bei Konzernen
- (2) Anpassung der HAZOP
- (3) Änderung des Prüfkonzepts

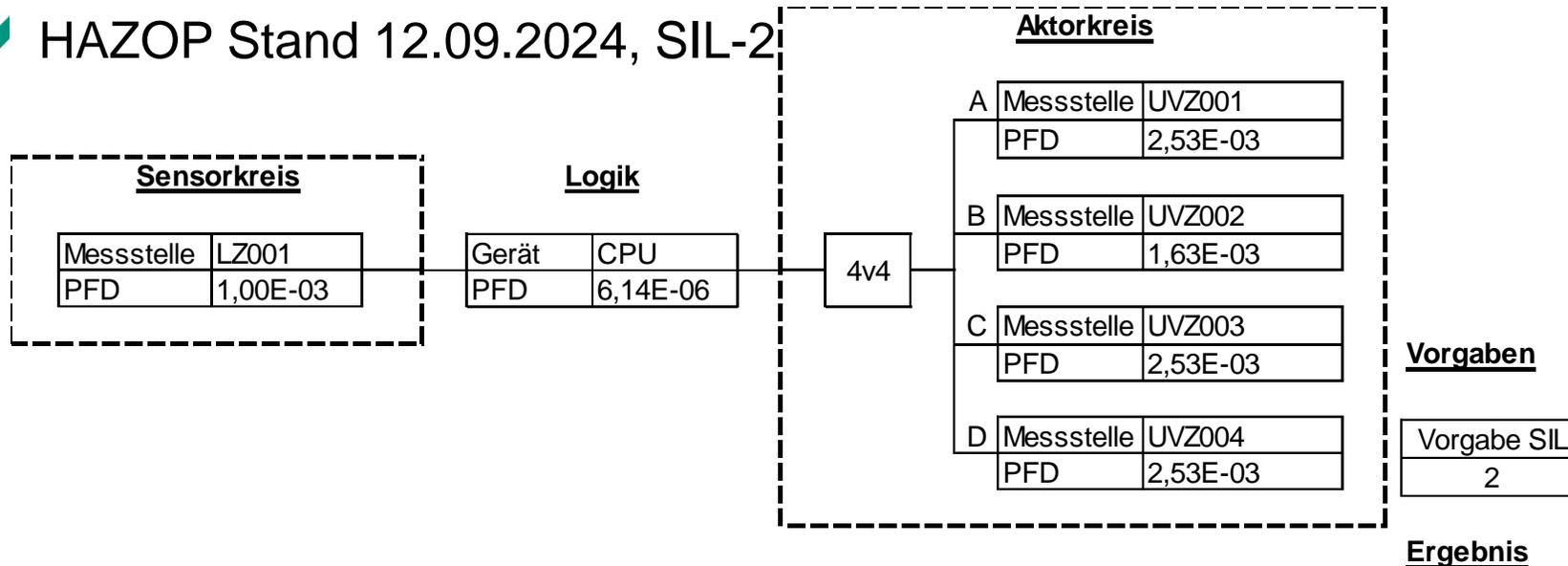
# (1) Kommunikation in Konzernen



SIL-Nachweis

## (2) Anpassung der HAZOP

- Der SIL-Nachweis geht nicht auf, was mache ich jetzt? Beispiel 1:
- HAZOP Stand 12.09.2024, SIL-2

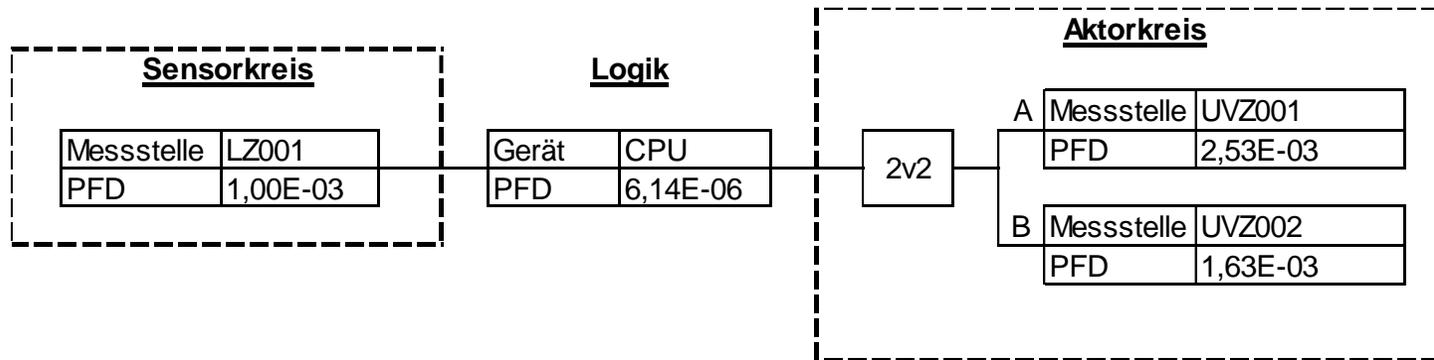


### Ergebnis

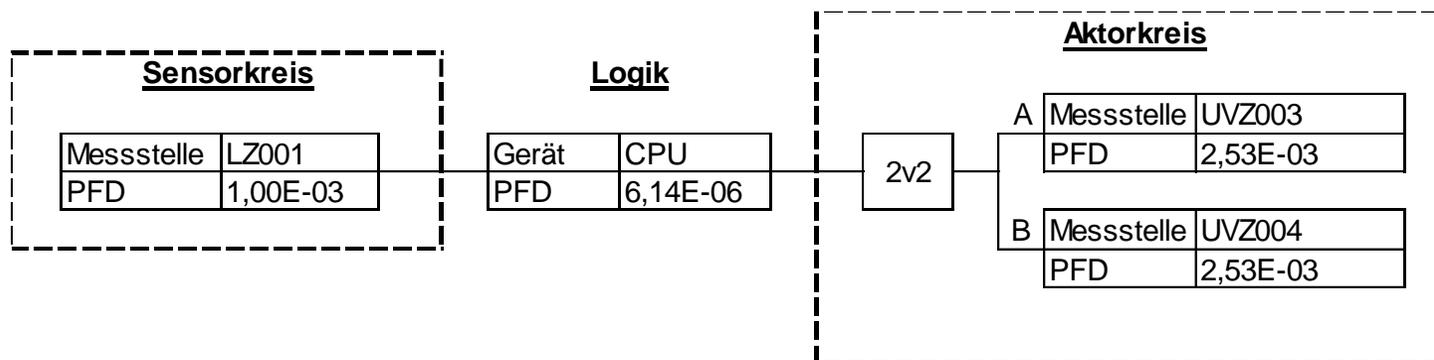
Teil	PFD <sub>avg</sub>	SIL <sub>PFD</sub>	SIL <sub>HFT</sub>	SIL
Sensor	1,00E-03		2	
CPU	6,14E-06		3	
Aktor	9,22E-03		2	
Ergebnis SIF	1,02E-02	1	2	1
Vorgabe erfüllt				<b>Nein</b>

## (2) Anpassung der HAZOP

- Der SIL-Nachweis geht nicht auf, was mache ich jetzt? Beispiel 1:
- HAZOP Stand 13.09.2024: Kreis 1, SIL-2



- HAZOP Stand 13.09.2024: Kreis 2, SIL-2



- Generell kann man eine HAZOP erneut durchführen. Aber der Ansatz meine Berechnung geht nicht auf pass das mal bitte schnell an, ist nicht im Sinne der Norm.

## (3) Änderung des Prüfkonzeppts

- Anpassung der Prüfkonzeppte innerhalb eines SIL-Nachweises
- Die gleiche Armatur wird von mehreren Abschaltungen betätigt und in jedem Kreis wird ein anderes Prüfkonzeppt verwendet. (Kreis 1 = 1 Jahr, Kreis 2 = 5 Jahre, Kreis 3 = 18 Monate)
  - Anpassung ohne Revalidierung des Gesamten Konzepptes
- Reduzierung von Prüfintervallen auf ein nicht mehr praktikables Maß
  - Das Engineering setzt einen Ausbau der Ventile alle 6 Monate an. Solche Vorgaben können von der Instandhaltung nicht gehalten werden

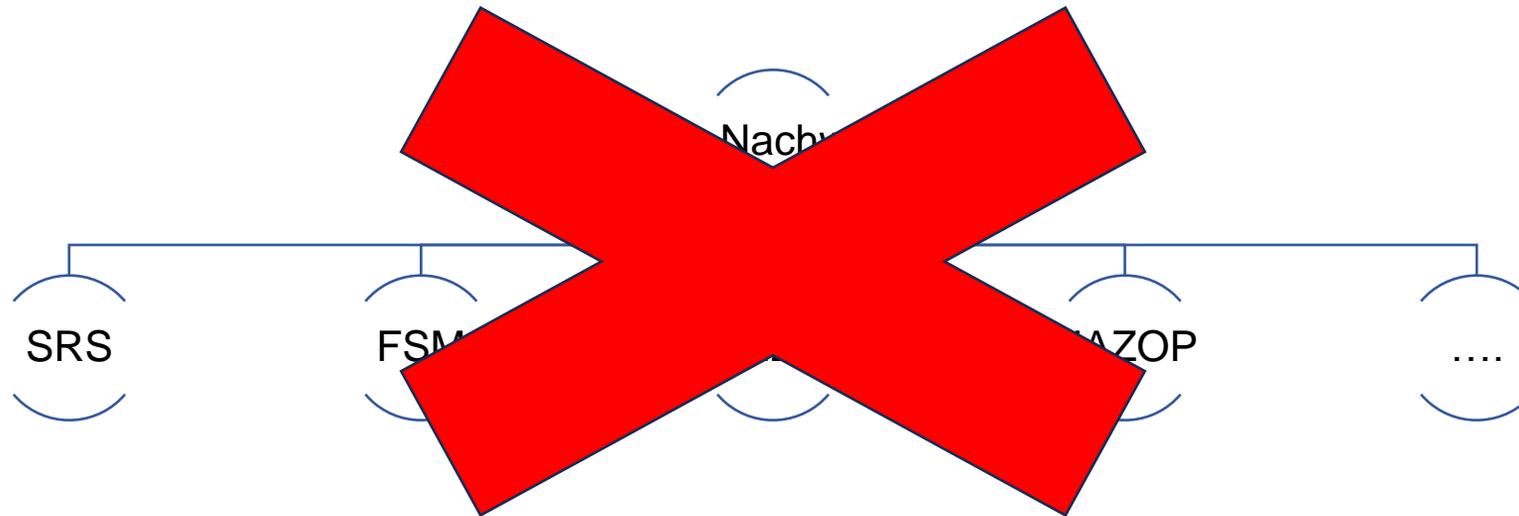
## IV. Abschluss

- (1) Alternative Ansätze
- (2) Aufbau FSM
- (3) Fazit

# (1) Alternative Ansätze

- Erhöhung der Redundanz (wenn möglich) / Austausch von Geräten
- Aufbau einer zusätzlichen bzw. automatischen Diagnose
- Separates Prüfkonzzept
- Es wird immer Fälle geben, bei denen es keine andere Lösung gibt. Für diese Ausnahmen kann eine Einzelfallbetrachtung durchgeführt werden

## (2) Aufbau FSM



## (2) Aufbau FSM



## (3) Fazit

- Rechnen sollte man, aber es ist ein Dokument von vielen und darf NIE als einzelnes und wichtigstes Dokument betrachtet werden
- Normen sind wichtig aber auch diese sollten nicht blind übernommen werden. Der Ingenieursmäßige Sachverstand ist immer relevant.
- Auch im Bereich Funktionale Sicherheit ist Kommunikation das A und O
- Viel Spaß bei der Abendveranstaltung

# Vielen Dank für Ihre Aufmerksamkeit

**Malika Mast Dipl. Ing / Geschäftsführerin**

E-Mail: [M.Mast@ramsys.org](mailto:M.Mast@ramsys.org)

Tel.-Nr.: 0 23 69 / 745 93 10

Mobil: 0171 / 3037392

