3. SIL-Slam am 23.06.2022

Rückblick

08:45 Uhr	Begrüßung
09:00 Uhr	**KI4Safety** (Marco Knödler)
09:30 Uhr	**KI in der Funktionalen Sicherheit** (Michael Kindermann)
10:00 Uhr	**Gedanken zum EU AI-Act** (Holger Laible)
10:30 Uhr	Kaffeepause
10:45 Uhr	**SILusionen** (Fred Stay)
11:15 Uhr	**Klimawandel – Herausforderung für die Funktionale Sicherheit** (Stefan Lauer)
11:45 Uhr	**Verständnis im Bereich der Funktionalen Sicherheit** (Malika Mast)
12:15 Uhr	Mittagspause
13:00 Uhr	**Enhancement of safety communication model** (Frank Schiller)
13:30 Uhr	**Der Analphabet und die Schreibmaschine** (Andreas Hildebrandt)
14:00 Uhr	Ende der Veranstaltung

„BACK TO THE FUTURE“
– DIE FUNKTIONALE SICHERHEIT IN ZUKUNFT

… und was wir heute für morgen lernen können/müssen –

Gedanken zur Gebrauchsdauer von Methodik

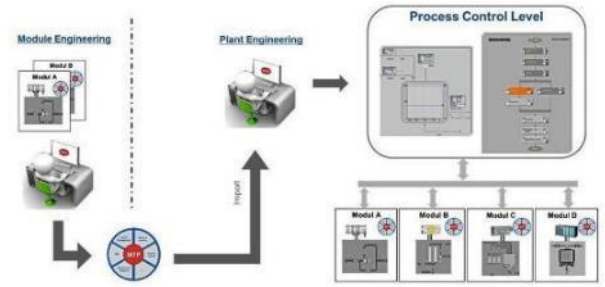
Marco Knödler, Yncoris
– IGR AF-Leitung Funktionale Sicherheit
- NAMUR AK 4.5 – VDI/VDE-GMA FA 6.13
– DIN NA 003-01-01 AA - CEN/TC 69/WG 1
- DKE AK 914.0.11 & STD_1941.0.8 - SCI 4.0,
Expertenrat KI in industriellen Anwendungen

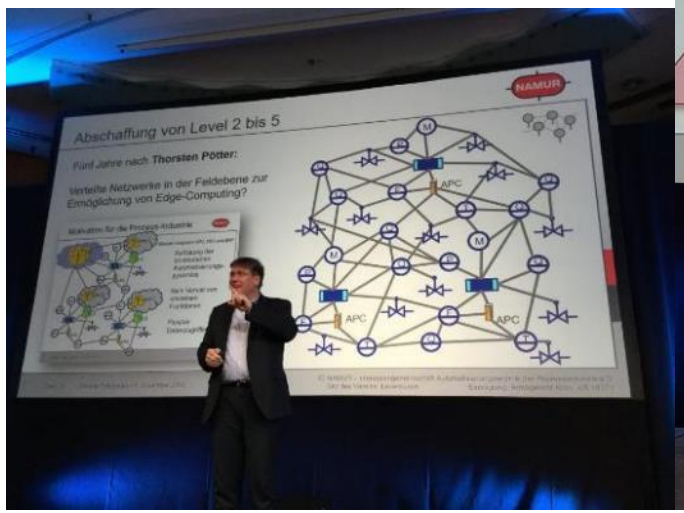
#Systematisch_Richtig_statt_Zufällig_Falsch

FUTURE TRENDS FOR FUNCTIONAL SAFETY IN THE PROCESS INDUSTRY

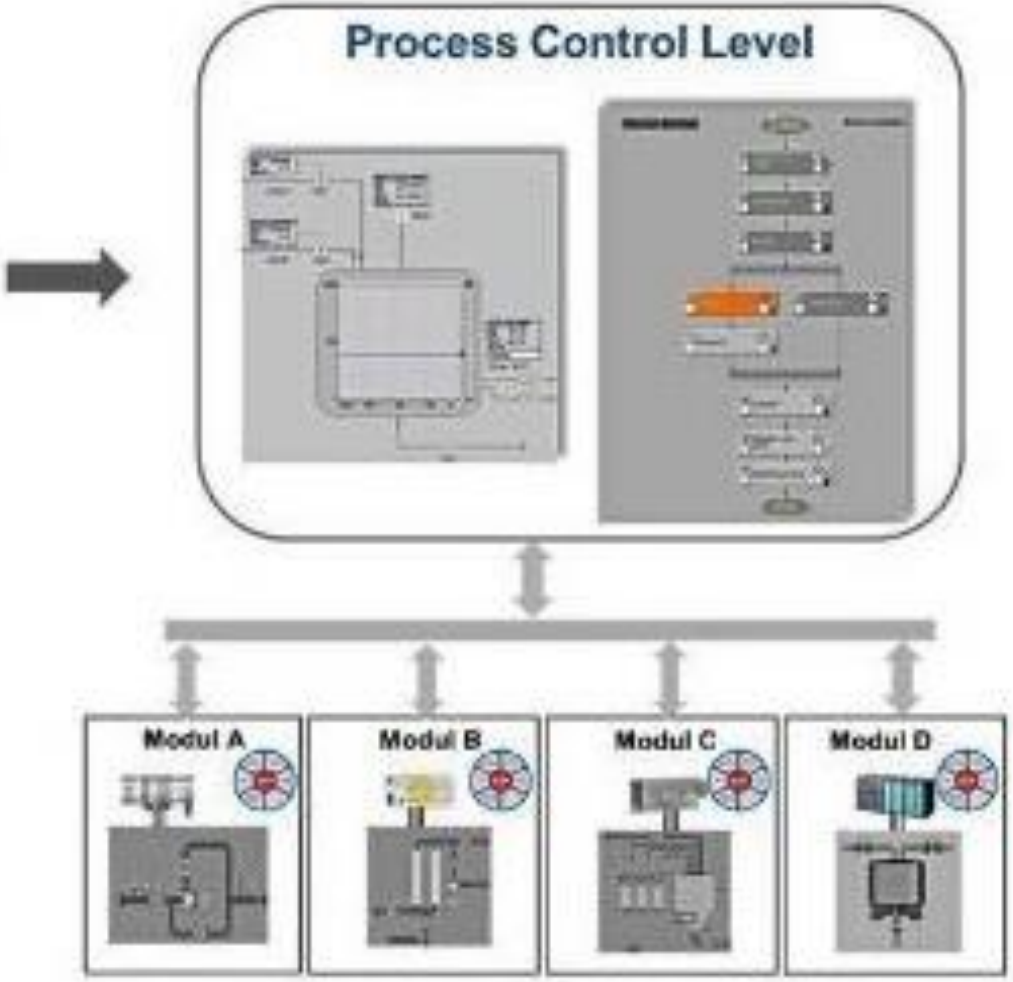
- **Increased connectivity**
- **more data (traffic)**
- **less (simple) hardware**
- **more software**
- **<u>increased complexity</u>**
- **Examples:**
  - APL4Safety
  - MTP-Safety
  - NOA meets/needsSecurity (4Safety)
  - AI4Safety

- **Impressions from NAMUR conventions**





MTP – MODULAR PROCESS PLANT SAFETY



- The **flexibilization** of **modular plants** poses new challenges for risk reduction procedures with Safety Instrumented Systems. In order to reduce losses in flexibility, the entire **Safety Lifecycle** and the activities contained therein must be **adapted** for the requirements of modular automation. In this paper, the existing safety life cycle models from IEC 61508 and IEC 61511 are examined with regard to their suitability for application in modular plants.
- #functional safety #**Functional Safety Orchestration** #modular plants #modular process automation #**modular SIS-Safetylifecycle**
- #Safety-MTP

GARRY KASPAROV

HOME ABOUT GARRY LECTURES & EVENTS KASPAROV CLASS

Home : Man vs Machine

Man vs Machine

https://www.kasparov.com/timeline-event/deep-blue/

NRM KI (1.0) – 80X „SAFETY“ – ABER WORÜBER REDEN/SCHREIBEN WIR DENN WIRKLICH?

Fokus für NRM 2.0

Fokussierung

Risiko

- Entsteht durch KI?
- Wird eingeschätzt durch KI?
- Wird verändert durch KI?
- Wird gemindert durch KI?
- Für wen? die KI?
- Was riskieren wir überhaupt?

Sicherheit

- Safety
- Security
- Zuverlässigkeit
- Privacy
- …

Kontext

- Horizontal – Querschnittsthema, bspw. Zertifizierung
- Vertikalthema – Anwendung in industrieller Automation

NRM KI (1.0) – 80X „SAFETY“ – ABER WORÜBER REDEN/SCHREIBEN WIR DENN WIRKLICH?

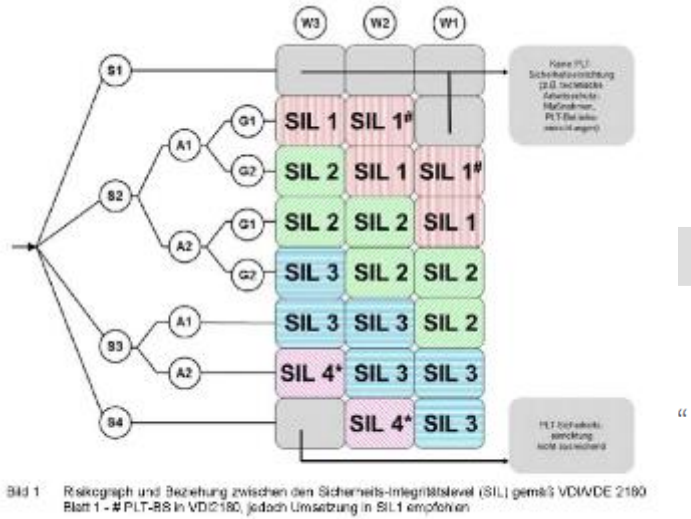
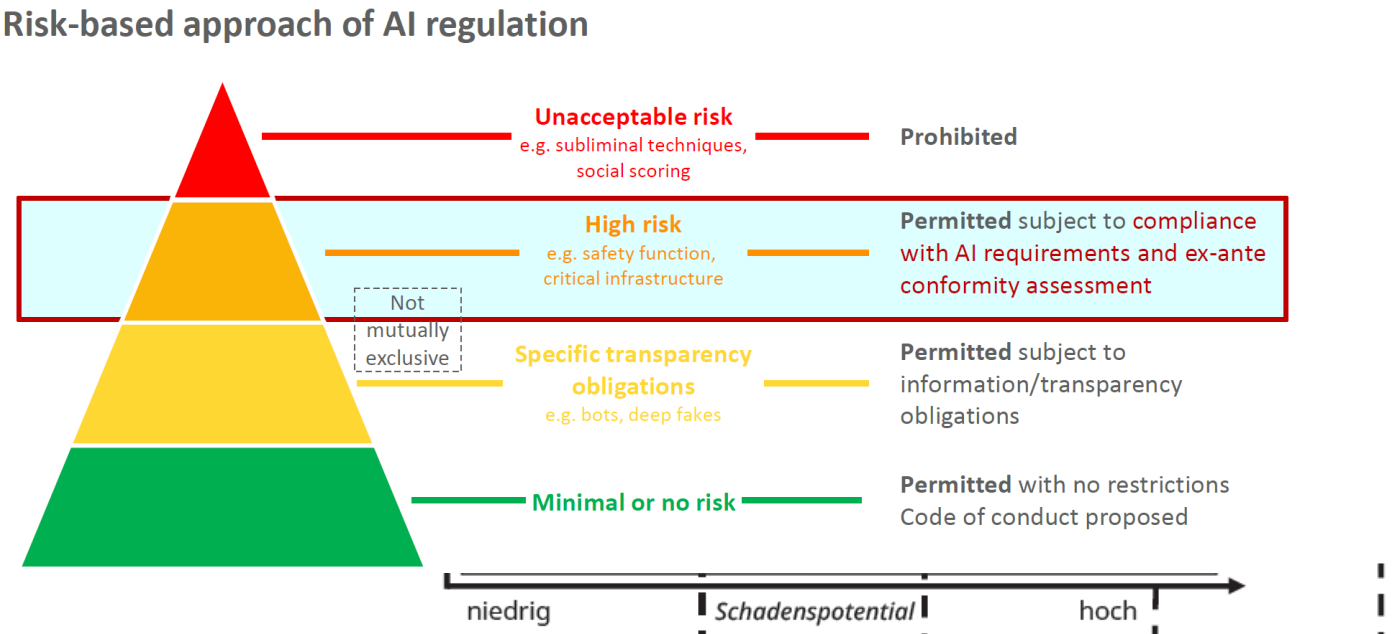
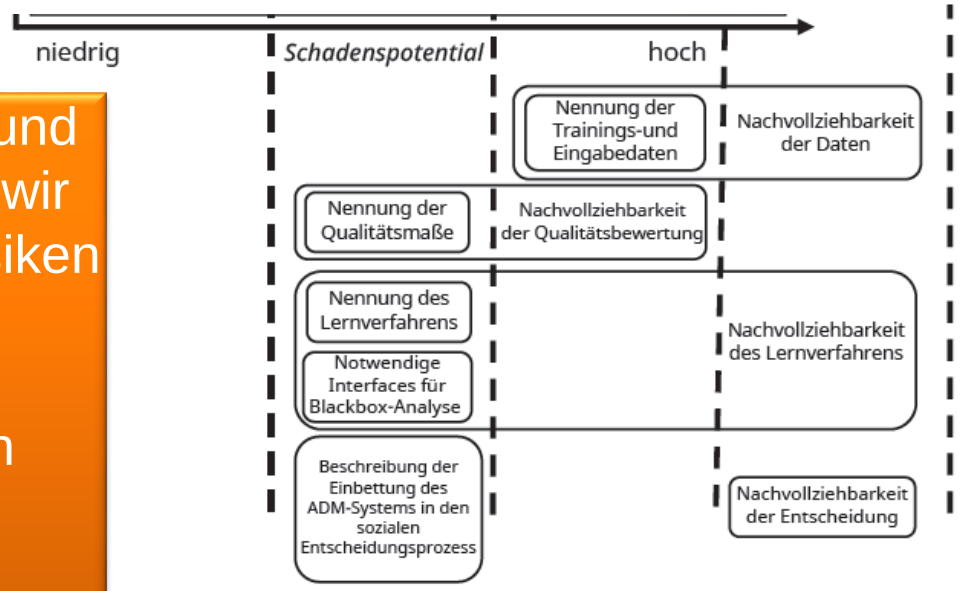


Bild 1 Risikograph und Beziehung zwischen den Sicherheits-Integritätslevel (SIL) gemäß VDI/VDE 2180 Blatt 1 - # PLT-BS in VDI2180, jedoch Umsetzung in SIL1 empfohlen

?





Für die nachhaltige IT-Sicherheit eines KI-Systems muss der gesamte „Life Cycle“ Berücksichtigung finden. Jedes Stadium beinhaltet mögliche Risiken, die analysiert und bewertet werden sollten. Dies beginnt mit der Konzeption und der Entwicklung und erstreckt sich über Test, Training, Verteilung und Betrieb bis zur Stilllegung. Dabei sind sowohl das KI-Modell z. B. mit Maschine Learning als auch die Daten für Test, Training und Betrieb, das Produkt, das IT-Gesamtsystem und die Interaktionen mit der Umgebung in der Risikobetrachtung zu berücksichtigen. Ein Management der IT-Sicherheit, ein KI-System in Bezug auf Safety, Security und Privacy wie beispielsweise mit ISO/IEC 27001 [19] und ISO/IEC 27005 [218] kann große Unterstützung bieten. Inwieweit die Norm für KI-Systeme erweitert werden kann oder sollte, müsste geprüft werden.

Wenn wir von Safety und KI sprechen, müssen wir ein klares Bild der Risiken sowie der risikomindernden Maßnahmen zeichnen Und die KI in diesem Kontext einordnen

https://www.process-worldwide.com/ai-autonomously-runs-chemical-plant-for-35-days-a-1105250/?cmp=nl-317&uuid=916df1653133e8644a95560eb0a0782fc

PROCESS WORLDWIDE

ACHEMA 2022

YNCORIS Industrial Services

Control & Automation | Engineering | Ex Protection & Safety | Pharma & Food | Pumps & Compressors | Topics | PROCESS Milestones | Service

Control & Automation » AI Autonomously Runs Chemical Plant for 35 Days

Next-Gen Control Technology

AI Autonomously Runs Chemical Plant for 35 Days

24.03.2022 | Source: Press release

In a field test, a chemical plant in Japan ran autonomously for 35 days with the assistance of an artificial intelligence (AI) solution developed by Yokogawa and the Nara Institute of Science and Technology. The next-generation control technology is capable of taking into account numerous factors such as quality, yield, energy saving, and sudden disturbances.

Distillation columns at the JSR chemical plant.
(Source: JSR Corporation)

Tokyo/Japan – Yokogawa Electric Corporation and JSR Corporation have recently announced the successful conclusion of a field test in which AI was used to autonomously run a chemical plant for 35 days, a world first. This test confirmed that reinforcement learning AI can be safely applied in an actual plant, and demonstrated that this technology can control operations that have been beyond the capabilities of existing control methods (PID control/APC) and have up to now necessitated the manual operation of control valves based on the judgements of plant personnel. The initiative described here was selected for the 2020 Projects for the Promotion of Advanced Industrial Safety subsidy program of the Japanese Ministry of Economy, Trade and Industry.

Related Companies

YOKOGAWA Deutschland GmbH

AZO.

ILUDEST

TRM Filter PURE TRUST

(KÜNSTLICH) INTELLIGENTE SICHERE MASCHINEN

FACHBEITRÄGE MATTIUZZO/VOCK/MÖSSNER/VOß| Sichere Maschinen

Sichere Maschinen mit – oder trotz – künstlicher Intelligenz

Die Europäische Kommission hat im April nicht nur einen Vorschlag für eine Verordnung zur künstlichen Intelligenz vorgelegt, sondern auch einen Vorschlag für eine Verordnung über Maschinenprodukte mit rechtlich verbindlichen Rahmenbedingungen für die Verwendung künstlicher Intelligenz, welche die Maschinen-Richtlinie 2006/42/EG ablösen soll. Ob diese Rahmenbedingungen vollständige, klare und verifizierbare Anforderungen dafür enthalten, in welchen Fällen und unter welchen Voraussetzungen sicherheitsrelevante Funktionen einer Maschine von Methoden der künstlichen Intelligenz beeinflusst oder automatisiert ausgeführt werden dürfen, muss nun geprüft werden. Dieser Artikel will hierzu einige Hinweise und Anregungen liefern.

https://ec.europa.eu/commission/presscorner/detail/de/QANDA_21_1683#3

Anforderungen an Software für Sicherheitsfunktionen sind in den Normen der Reihe DIN EN 61508[5] sowie in DIN EN 62061:2016-05[6] ***zu finden.*** Auch in den Entwurf der DIN EN ISO 13849-1:2020[7] sind jetzt Anforderungen an Software zum Einsatz für Sicherheitsfunktionen in Maschinen aufgenommen worden. ***Es ist also zu prüfen, ob diese Normen für die Entwicklung von Software, die mit künstlicher Intelligenz ausgestattet ist,***

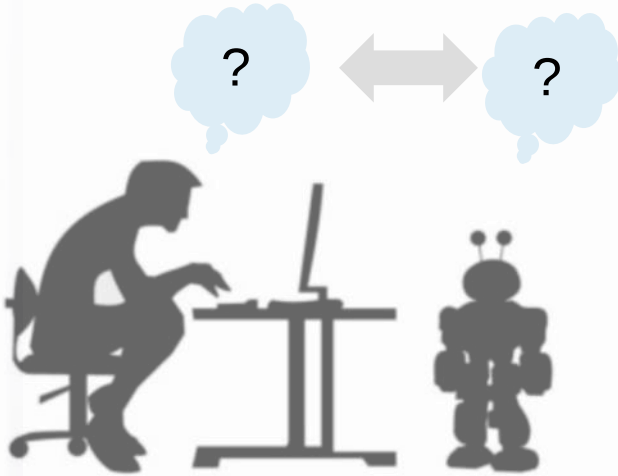
AI 4 (FUNCTIONAL) SAFETY

Usage Level (property of application)

Technique Usage Level \ AI Technology Class →	Class I (1) can be systematically reviewed, as the used methods are fully transparent and understood, and the AI can be unambiguously mapped to the final application.	Class II (1) can be partly reviewed, verified and validated, but the AI is not completely transparent or understood, and/or the AI cannot be unambiguously mapped to the final application.	Class III (1) cannot, or only to a small extend, be reviewed or verified, and the methods are mainly not transparent or understood, and/or the AI cannot be unambiguously mapped to the final application.
Usage Level A1 used in a safety relevant E/E/PE system and automated decision making possible.	application of existing functional safety standards possible	*See clause „ab"*	**Not recommended (or limited) application**
Usage Level A2 used in a safety relevant E/E/PE system and no automated decision making (e.g. used for diagnostic functions).		*See clause „cd"*	
Usage Level B1 used during development of a safety relevant E/E/PE system (offline support tool) and automated decision making possible.		*See clause „ef"*	*See clause „ab"*
Usage Level B2 used during development of a safety relevant E/E/PE system (offline support tool) and no automated decision making.		*See clause „ef"*	*See clause „cd"*
Usage Level C (3) used outside a safety relevant E/E/PE system, but with direct impact to safety relevant operating conditions (e.g. demand rate for safety systems).		*See clause „gh"*	*See clause „ef"*
Usage Level D (1, 2) used outside a safety relevant E/E/PE system, sufficiently segregated and behaviour controlled (e.g. sandbox, hypervised)	No specific functional safety requirements for AI, but safety precautions need investigation. Additionally, other safety aspects (not being addressed with functional safety methods) might be impacted by AI usage.		

1 Static (offline) AI (during development) teaching/learning only
2 Dynamic (online) AI teaching/learning possible
3 AI techniques clearly providing additional risk reduction and their failure is not critical in respect to the level of risk acceptance are included.

Class (property of AI) ~ complexity, explainability



Ideas for a Technical Report (TR5469) for IEC61508 related to„AI4Safety"

(KÜNSTLICH) INTELLIGENTE FUNKTIONALE SICHERHEIT – EIN FALL FÜR DIE PROBABILISTIK?

Neuronalen Netzen muss eine epistemische Unsicherheit zugeordnet werden

An diesem Beispiel zeigt sich auch, dass Machine Learning als „gefühlt-nicht-deterministisch" (Dr. Henrik Putzer) bezeichnet werden kann: Nicht immer liefert eine Syste komponente auf Basis von maschinellem Lernen die erwarteten Ergebnisse. Diese Fehlerm öglichkeit kann mit einer Unsicherheit (uncertainty) beschreiben werden. In der Hardware wird dies du ch die Ausfallrate oder das LAMBDA bezeichnet. Im Gegensatz zu dieser aleatorischen Unsicherheit n der Hardware (kann irgendwann zufällig z. B. durch Alterung ausfallen) muss dem Neuronalen N tz eine epistemische Unsicherheit zugeordnet werden (eine Fehlerkennung eines Fußgängerbildes wird immer wieder gleich fehlerhaft ausfallen, ist aber allgemein nicht vorherzusagen). Genau diese Eigenschaft bereitet dem Sicherheitsdenkenden Probleme. Um dies zu handhaben wird n neuer Kennwert, das LAMBDA-AI, vorgeschlagen (Dr. Henrik Putzer). Doch die Methoden zur Erm tlung des LAMBDA-AI sind noch in der Erforschung. Klar ist, dass der Entwicklungsprozess, die Metrik n und ggfs. auch die Analyse des vom Neuronalen Netz gelernten Wissens eine Rolle spielen werden.

Probabilistik?

Erfurter Tage 2019 - Dr. Henrik Putzer | Melanie Kahl / CEF

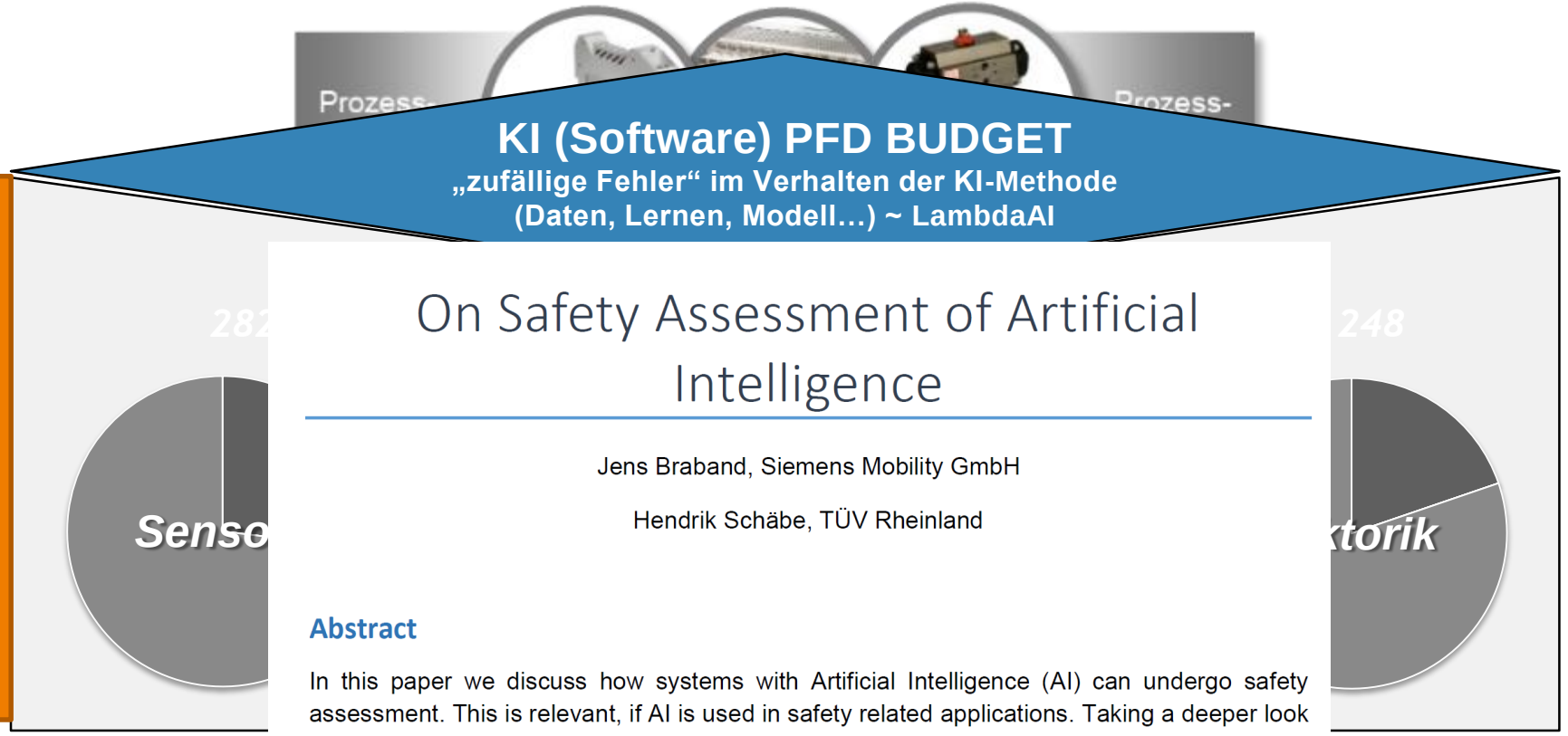
$$PFD_{1oo1,AI} = PTC_0 \lambda_{AI} \frac{T_0}{2} + (PTC_1 - PTC_0) \lambda_{AI} \frac{T_1}{2} + (1 - PTC_1) \lambda_{AI} \frac{T_2}{2}$$

https://www.dke.de/de/news/2019/vde-dke-kongress-funktionale-sicheheit-industrie40-ki

ZUVERLÄSSIGKEIT & PROBABILISTIK = SAFETY?

KI (Software) PFD BUDGET
„zufällige Fehler“ im Verhalten der KI-Methode (Daten, Lernen, Modell…) ~ LambdaAI

IEC 62998 (Safety of machinery - Safety-related sensors used for the protection of persons)
Teil 3 beinhaltet Kapitel mit „machine learning“.



On Safety Assessment of Artificial Intelligence

Jens Braband, Siemens Mobility GmbH

Hendrik Schäbe, TÜV Rheinland

Abstract

In this paper we discuss how systems with Artificial Intelligence (AI) can undergo safety assessment. This is relevant, if AI is used in safety related applications. Taking a deeper look into AI models, we show, that many models of artificial intelligence, in particular machine learning, are statistical models. Safety assessment would then have to concentrate on the model that is used in AI, besides the normal assessment procedure. Part of the budget of dangerous random failures for the relevant safety integrity level needs to be used for the probabilistic faulty behavior of the AI system. We demonstrate our thoughts with a simple example and propose a research challenge that may be decisive for the use of AI in safety related systems.

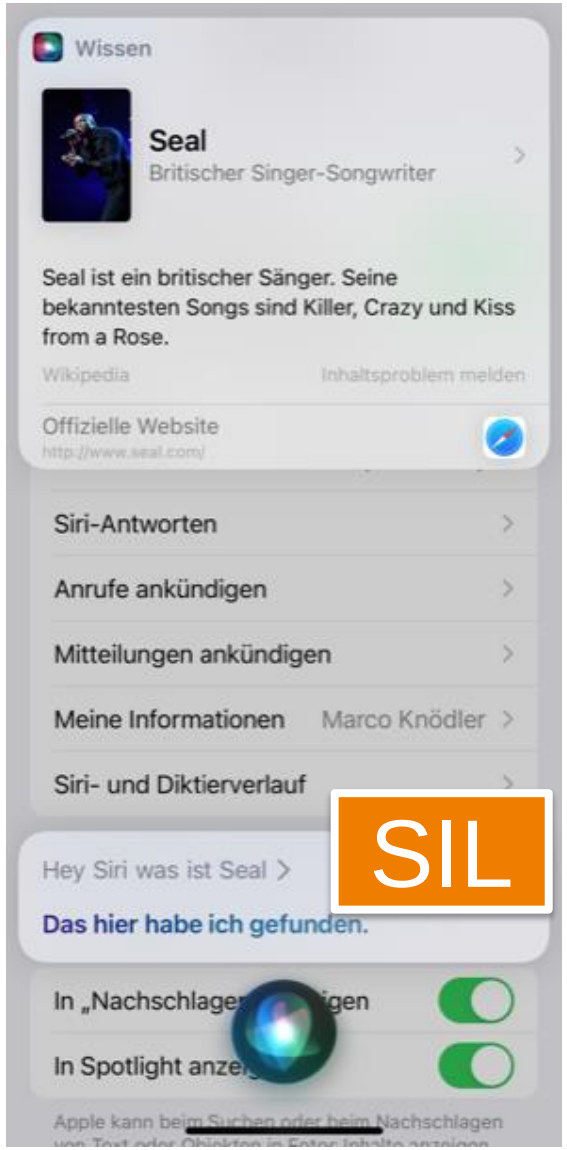
Probabi-listik?

Quelle: Stördaten-Auswertung NAMUR.smart

Zufällige Fehler
Systematische Fehler

(KÜNSTLICH) INTELLIGENTE FUNKTIONALE SICHERHEIT?

YNCORIS Industrial Services



SIL

IGR NAMUR

YNCORIS Industrial Services

Hauptbeitrag

Peer-Review: 14.12.2020

Systematisch richtig, statt zufällig falsch

Stopp dem Erraten von Ausfallraten für Mechanik mit VDI/VDE 2180 Blatt 4

Dirk Hablawetz, BASF; Marco Knödler, YNCORIS; Norbert Matalla, NM-Consulting; Gregor Schmitt-Pauksztat, BAYER

Im neuen Blatt 4 der VDI/VDE 2180 wird beschrieben, welche Besonderheiten bei mechanischen Komponenten als Teil von PLT-Sicherheitseinrichtungen zu beachten sind. Insbesondere wird auf die möglichen auftretenden zufälligen Fehler und deren Berücksichtigung in der PFD-Berechnung sowie deren Bedeutung im Vergleich zu systematischen Fehlern eingegangen. Dieser Artikel fasst die Inhalte des neuen Blatts 4 kurz zusammen und zeigt seinen Nutzen in der praktischen Anwendung.

#SIL #Mechanik #PFD-Rechnung

(KÜNSTLICH) INTELLIGENTE FUNKTIONALE SICHERHEIT

Verstanden?
gleichwertig?
Akzeptiert?

$Code + Code > Code?$

Systematisch richtige Abbildung der Realität

Expertenrat für Künstliche Intelligenz in industriellen Anwendungen
Übersicht der Themen der UAG

STANDARDIZATION COUNCIL INDUSTRIE 4.0

Systematisch richtig: Transfer in Daten und Information, Repräsentanz der Realität in Information, (KI) Analyse

Systematisch richtiger Einfluss auf die Realität

BACK TO THE FUTURE – THE HUMAN FACTOR

THE **PARADOX OF AUTOMATION** SAYS THAT

- THE MORE EFFICIENT THE AUTOMATED SYSTEM,
->THE MORE CRUCIAL THE HUMAN CONTRIBUTION OF THE OPERATORS.

HUMANS ARE LESS INVOLVED, BUT THEIR INVOLVEMENT BECOMES MORE CRITICAL.
LISANNE BAINBRIDGE, A COGNITIVE PSYCHOLOGIST, IDENTIFIED THESE ISSUES NOTABLY IN HER WIDELY CITED PAPER "IRONIES OF AUTOMATION.“

Abstract
This paper discusses the ways in which automation of industrial processes may expand rather than eliminate problems with the human operator. Some comments will be made on methods of alleviating these problems within the ‘classic’ approach of leaving the operator with responsibility for abnormal conditions, and on the potential for continued use of the human operator for on-line decision-making within human-computer collaboration.

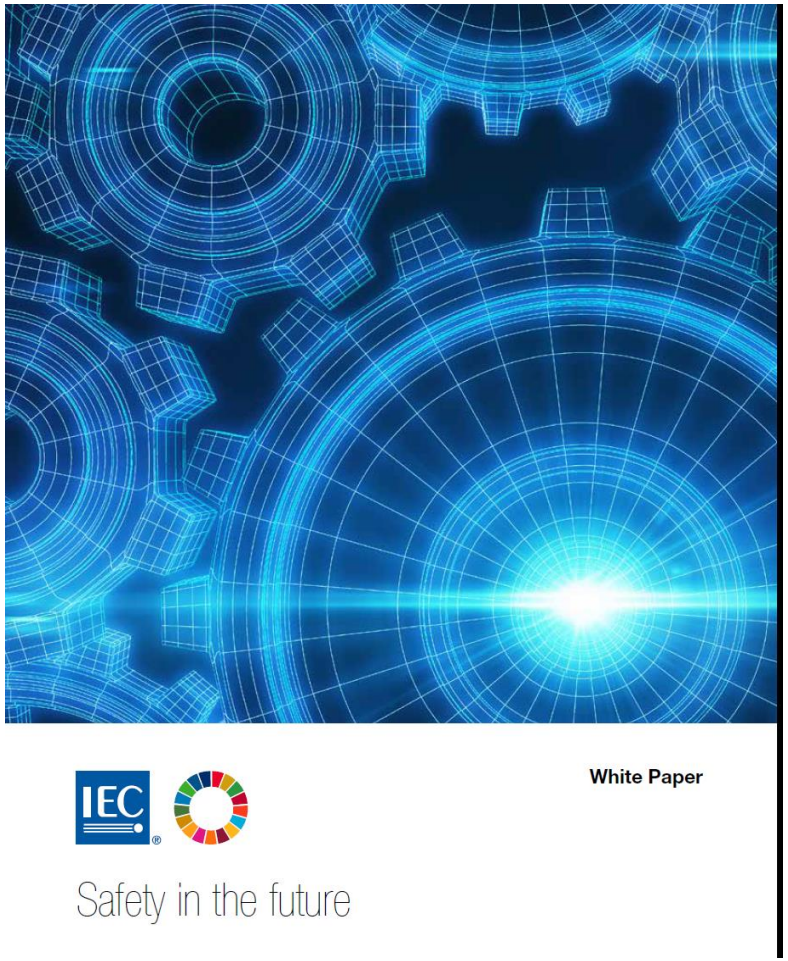
Ironies of automation☆ Author LisanneBainbridge†
†Department of Psychology, University College London, London WC1E 6BT, U.K.

Received 16 December 1982, Revised 23 May 1983, Available online 10 February 2003.

THE HUMAN FACTOR

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

IEC WP Safety in the future:2020-10(en)



DANKE FÜR EURE AUFMERKSAMKEIT!

Die SIL-Sprechstunde – Fragen und Antworten rund um die funktionale Sicherheit

Das Thema SIL ist zuweilen Gegenstand von Missverständnissen und offenen Fragen. Lassen Sie sich Ihre Frage(n) zu SIL jetzt beantworten!

Gebrauchs-dauer

Die Eckdaten zur 13. SIL-Sprechstunde:

- **Schwerpunkt**: Gebrauchsdauer
- **Termin**: 28. bis 29. September 2022
- **Ort**: Pepperl+Fuchs, Mannheim
- **Teilnehmerfragen**: können zu jedem beliebigen Thema rund um die funktionale Sicherheit gestellt werden

Reichen Sie Ihre individuelle Frage ein. Sie können jederzeit weitere Fragen einreichen.

„BACK TO THE FUTURE“ – DIE FUNKTIONALE SICHERHEIT IN ZUKUNFT

… und was wir heute für morgen lernen können/müssen –

Gedanken zur Gebrauchsdauer von Methodik

Marco Knödler, Yncoris
– IGR AF-Leitung Funktionale Sicherheit
- NAMUR AK 4.5 – VDI/VDE-GMA FA 6.13
– 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

#Systematisch_Richtig_statt_Zufällig_Falsch

Was auch immer die Zukunft bringt: lieber #Systematisch_Richtig_statt_Zufällig_Falsch

Artificial Intelligence in Safety Relevant Applications

SIL slam 2022
2022-June-23

Content

1. About me
2. Are there any known applications in industry?
3. To which standards could AI be evaluated already? Any criteria?
4. Difficulties with the disciplines…
5. Online learning or not?
6. Any effects on the involved parties?
7. On the road from the simple emergency shutdown to the collaborating robot…

About the presenter

Dipl. Ing. Michael Kindermann

Degree in Electrical Engineering (Automation) @ University of Kaiserslautern

10 years R&D @ Pepperl + Fuchs

Design of functionally safe devices since 2001 (EN 954-1 and EN 61508)

3 years of certification in hazardous locations @ UL International

Certified Functional Safety Engineer in HW/SW design by TÜV Rheinland

Since 2011 **Head of Functional Safety Management @ Pepperl+Fuchs**

- ***Supervising the work of standard experts*** *for functional safety*
- ***Responsible for processes*** *linked to functional safety*
- ***Functional Safety Manager*** *for design projects*
- ***Committee Work*** *GK 914 (FS), AK 225.1 (Machines and FS), K132.0.1 (FMEA), K241 (Ex and FS)*
- ***Committee Moderator GAK 914.0.3*** *(Safe Software in 61508),* ***AK 914.0.9*** *(Statistical Evaluation of FS Software) and* ***AK 9014.0.11*** *(AI and FS)*

Are there any known applications in industry???

My contact at Bayer

September 2020: Don’t worry, nothing yet

June 2021: Can you check my article about AI in Industrial applications?

Source: Bayer

Das ist Bayers neue Expertin für Künstliche Intelligenz

Die Amerikanerin Fei-Fei Li zieht in den Aufsichtsrat von Bayer ein. Sie hat einen kritischen Blick auf die neue Technologie.

Source: Handelsblatt

About the new expert for AI in the supervisory board of Bayer

… aim to substitute humans in high working cost countries

Are there any known applications in industry???

My contact at BASF

Oct. 2020: Don’t worry, nothing yet

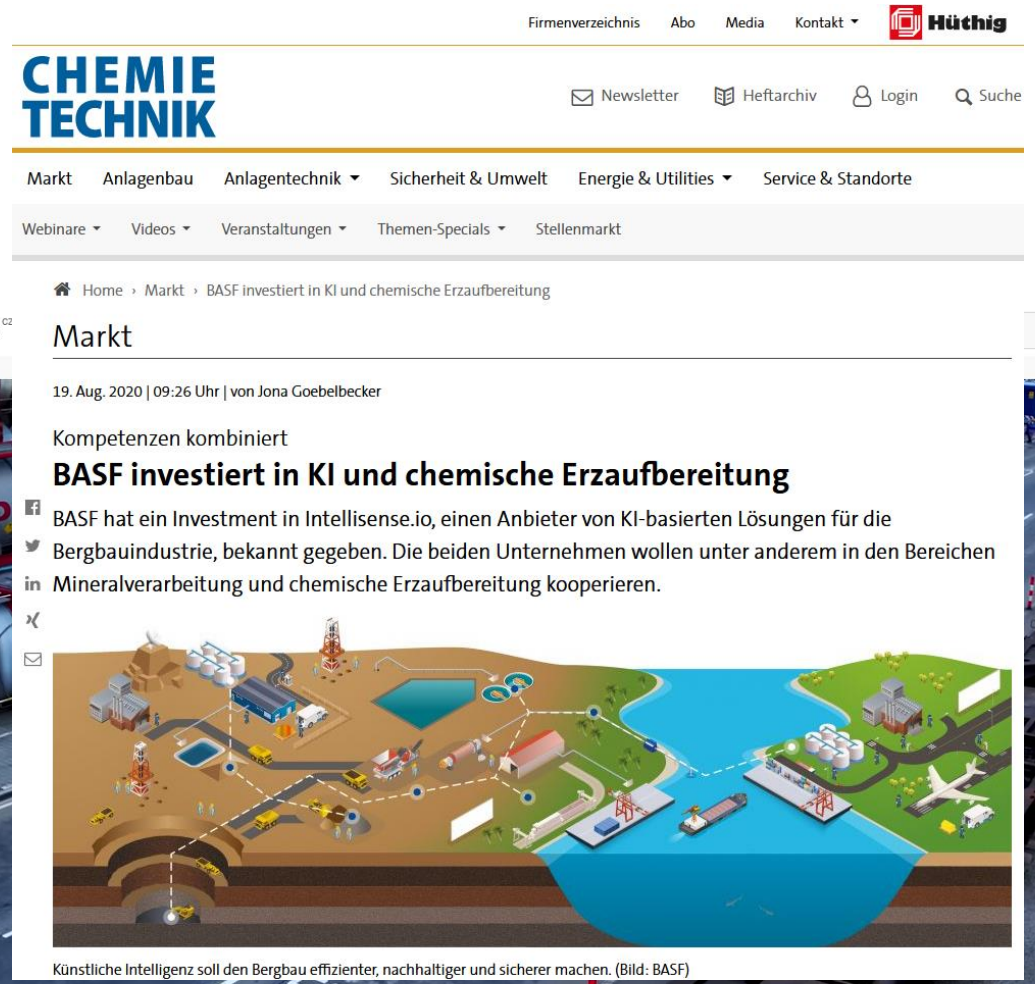
Found application from 2017: AGVs. Discussed.

Nov. 2021: Self driving vehicles allowed on public roads between two parts of the company (platooning)

Dec. 2021: Do you have the draft of the technical report for AI and safety?

Source: Hüthig Verlag

About BASF investing in AI company for ore processing



Source: https://www.youtube.com/watch?v=yxqTtN--IAU

Are there any criteria for the use of AI in industry?

What does EN/IEC 61508 say?

Now (Edition 2, 2010):

4b	Graceful degradation	C.3.6	R	R	HR	HR
5	Artificial intelligence - fault correction	C.3.9	---	NR	NR	NR
6	Dynamic reconfiguration	C.3.10		NR	NR	NR

Source: IEC 61508-2:2010

Mostly the “not recommended” is read like “Don’t!”

Proposed (Edition 3):

IEC 61508-3 / Table A.2 / Technique 5

5	Artificial intelligence	C.3.9	---	---	---	---

Source: Committee draft IEC 61508-2 Edition 3

… just wait for edition 4?

Timeline

Wait for edition 4???

This year the CD comes

Release 2028!!!

	Q1/22	Q2/22	Q3/22	Q4/22	Q1/23	Q2/23	Q3/23	Q4/23	Q1/24	Q2/24	Q3/24	Q4/24	Q1/25	Q2/25	Q3/25	Q4/25	Q1/26	q2/26	Q3/26	Q4/26	Q1/27	Q2/27	Q3/27	Q4/27	Q1/28
Programme with draft CD, CD1 and CD2																									
Relase questionaire																									
Release RR/draft CD		X																							
Receive NC comments on RR/draft CD			X																						
Prepare CD1				CD1																					
Release CD1							X																		
Secretariat translation																									
Secretariat circulate CD1 with translation									X																
Receive NC CD1 comments										X															
Prepare CD2										CD2															
Release CD2													X												
Receive NCCD2 comments														X											
Prepare CDV															CDV										
Release CDV																		X							
Secretariat polishing of CDV																									
Secretariat circulate CDV with translation																			X						
Receive NC CDV comments/ballot																				X					
Prepare FDIS																					FDIS				
Release FDIS																						X			
Receive NC comments FDIS																							X		
Implement editorial updated																									
Release Ed 3 to secretariat																									X
Alternative porgramme if no need for CD2																									
Prepare CDV										CDV															
Release CDV													X												
Secretariat polishing of CDV																									
Secretariat circulate CDV with translation														X											
Receive NC CDV comments/ballot															X										
Prepare FDIS																FDIS									
Release FDIS																	X								
Receive NC comments FDIS																		X							
Implement editorial updated																									
Release Ed 3 to secretariat																				X					

Source: 65A_ DRAFT REVIEW REPORT IEC 61508 Parts 1-7 ED2 20220326 draft v3

Edition 2 in 2010, Edition 3 in 2028 – makes Edition 4 in 2046

Are there any criteria for the use of AI in industry?

TR 5469 AI classification table

Application

Usage Level	AI Technology Class =>		
Usage Level A1 AI technique used in a safety relevant E/E/PE system and automated decision making possible.		See clause „ab“	Not recommen… applicatio…
Usage Level A2 AI technique used in a safety relevant E/E/PE system and no automated decision making (e.g. used for diagnostic functions).		See clause…	
Usage Level B1 AI technique used during development of a safety relevant E/E/PE system (offline support tool) and automated decision making possible.		See …	See …
Usage Level B2 AI technique used during development of a safety relevant E/E/PE system (offline support tool) and no automated decision making.		…use „ef“	…se „cd“
Usage Level C 3 AI technique used outside a safety relevant E/E/PE system, but with direct impact to safety relevant operating conditions (e.g. demand rate for safety systems).		…e clause „gh“	…e clause „ef“
Usage Level D 1, 2 AI technique used outside a safety relevant E/E… system, sufficiently segregated and behaviou… …d (e.g. sandbox, hypervised)		No …nctional safety req… …for AI, Additionally, ot… …y preautions need… …ion. …aspects (not bein… …d with functional safety …ds) might be impa… …usage.	

1 offline AI (during development) teaching… …only
2 online AI teaching/learning possible
3 AI techniques clearly providing additional risk reduction and their failure is not critical in respect to … risk acceptance are included.

AI?

Can be systematically analysed

Something in between

Cannot be systematically analysed

Interesting: AI doesn’t directly mean “learning online!”

Source: Draft ISO/IEC TR 5469

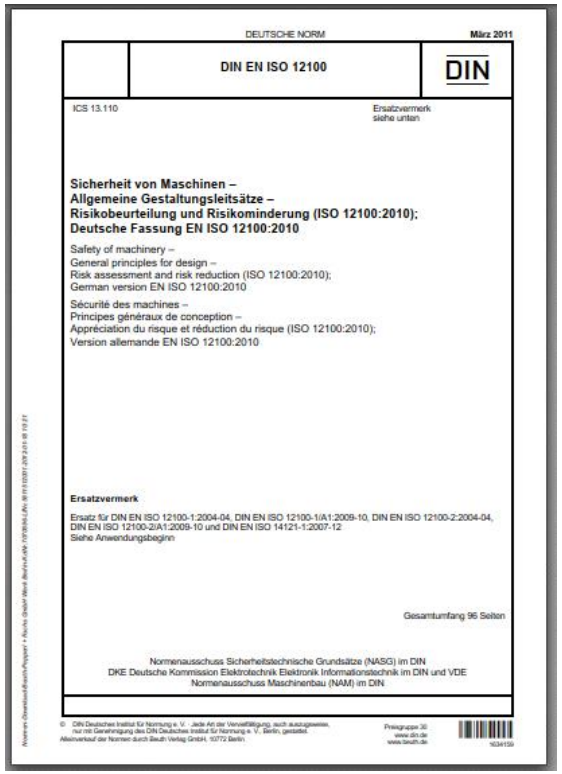
Quelle: MT 61508-3 Task Group N

Are there any criteria for the use of AI in industry?

What can you do already?

Possibility: use a risk assessment standard like ISO 12100!

(I was happy to see it is used in the mining business)



DEUTSCHE NORM März 2011

DIN EN ISO 12100

DIN

ICS 13.110

Ersatzvermerk siehe unten

Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (ISO 12100:2010); Deutsche Fassung EN ISO 12100:2010

Safety of machinery – General principles for design – Risk assessment and risk reduction (ISO 12100:2010); German version EN ISO 12100:2010

Sécurité des machines – Principes généraux de conception – Appréciation du risque et réduction du risque (ISO 12100:2010); Version allemande EN ISO 12100:2010

Ersatzvermerk

Ersatz für DIN EN ISO 12100-1:2004-04, DIN EN ISO 12100-1/A1:2009-10, DIN EN ISO 12100-2:2004-04, DIN EN ISO 12100-2/A1:2009-10 und DIN EN ISO 14121-1:2007-12
Siehe Anwendungsbeginn

Gesamtumfang 96 Seiten

Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
Normenausschuss Maschinenbau (NAM) im DIN

Source: DIN EN ISO 12100

Cooking Receipe:

- **Determine the risk within the application without the AI device**
- **Determine the risk within the application with the AI device**
- **Compare and look whether the use is justified**

Probable outcome: AI contains unacceptable lacks in predictability but is welcomed to support and improve things the conventional methods don’t do comparably well.

Are there any criteria for the use of AI in industry?

Too many ideas – Catalogs of Criteria

“Trustworthy Industrial AI systems” by DNV-GL

based on characteristics (purpose, ability to perform, capacity to verify actions …)

“Trusted AI” by TÜV Austria

based on eleven “challenges” with main chapters security / function / ethics

“Towards an AI Safety Landscape – an overview” by Espinoza et al (2019)

based on life cycle activities, promoted by ai-safety.org

“KI-Prüfkatalog” by Fraunhofer IAIS (Bonn)

based on “dimensions” fairness, control, transparency, data quality, …

“Whitepaper Zertifizierung KI-Systeme, www.platform-lernende-systeme.de

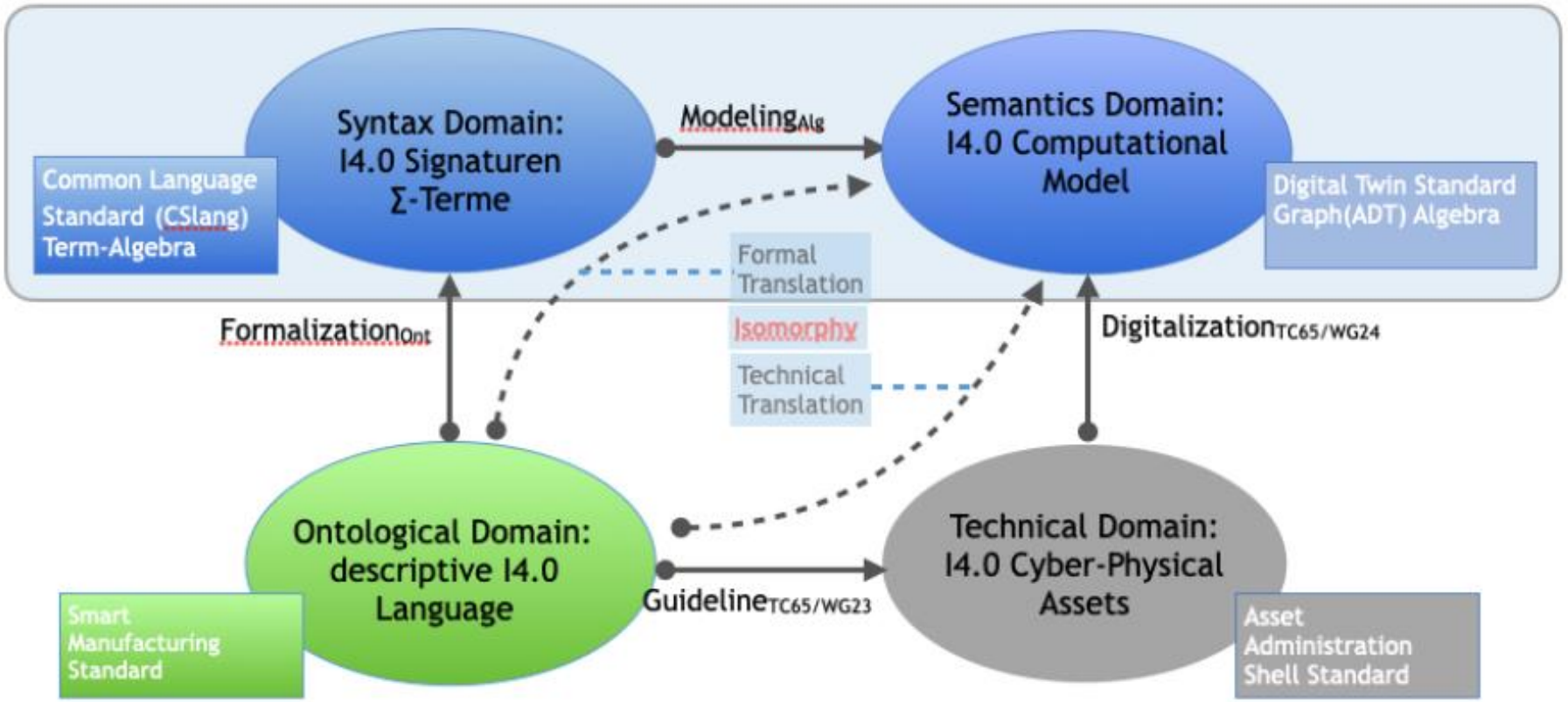
based on a big questionnaire about safety /reliability / fairness …

“Safety Assurance Objctives for Autonomous Systems” By SCSC

based on three levels computation / architecture / platform

Are there any criteria for the use of AI in industry?

Possibility: modeling



Source: Semantics for I4.0 Smart Manufacturing from Jan B. de Meer, 2020, published online at researchgate.net

…it's just that simple!

Speaking the same language? AI and safety experts

Negative example: Compared to a human…

AI expert: we are better in reaction than a human.

Safety expert: doesn‘t make me happy.

Lightcurtain

- Will detect people in the door
- Will detect people in the door
- Will detect people in the door
- Will detect people in the door
- Will detect people in the door

Maybe fails once in two years

Serviced twice a year

Source: Pixabay

Conductor

- Will look on the cell phone
- Will be tired from the screaming baby at night
- Will have private topics distracting him
- Will be distracted talking
- Will be distracted otherwise

Probably fails several times per day

Needs food and beverage and a cigarette and …

Speaking the same language? AI and safety experts

Positive example: Autonomous braking

Human:

1 second reaction time

Decision taking process

Perhaps wrong decision

Algorithm:

Input in milliseconds

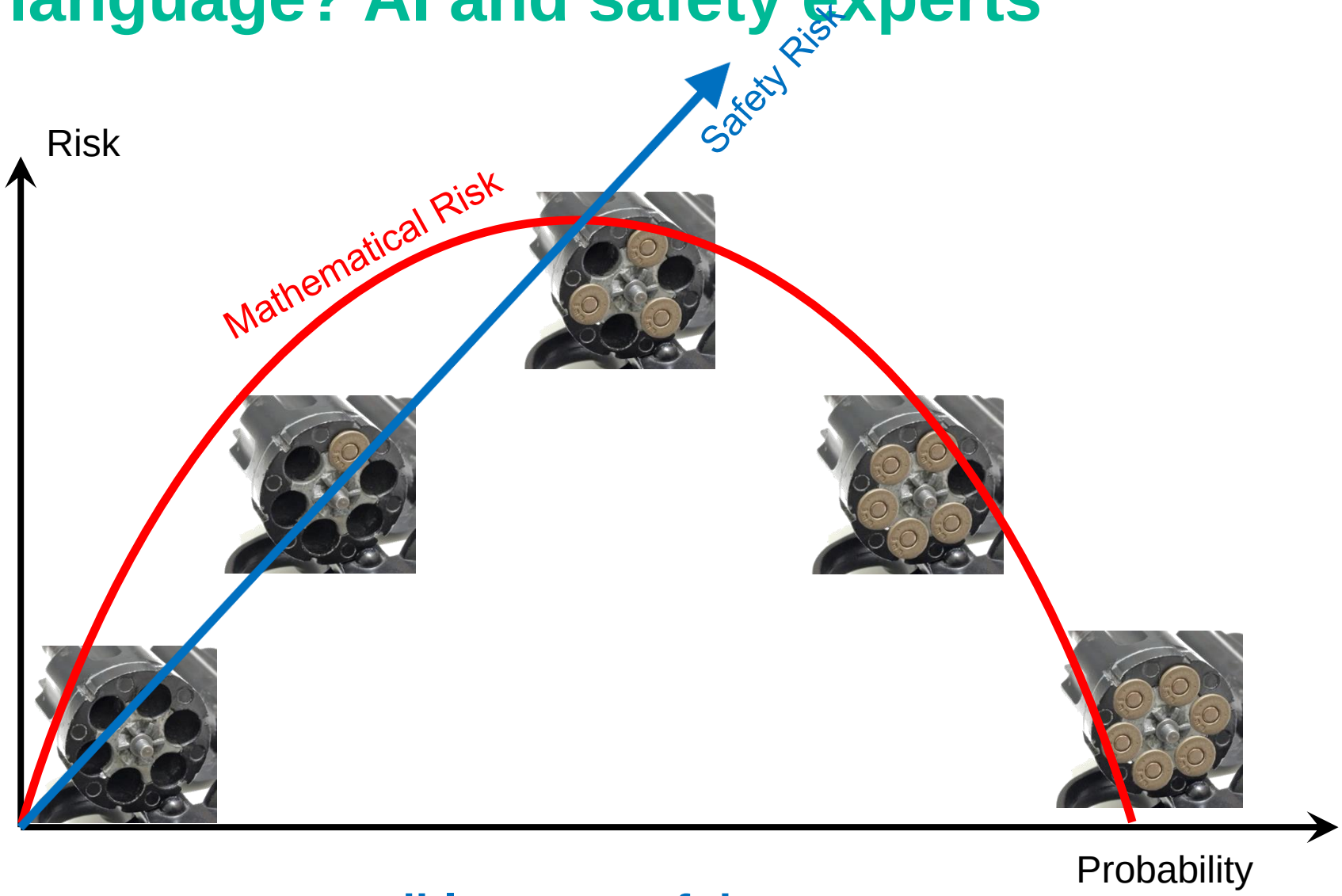
Compared

Standard scenario chosen

Source: Pixabay

Speaking the same language? AI and safety experts

Terms: Risk

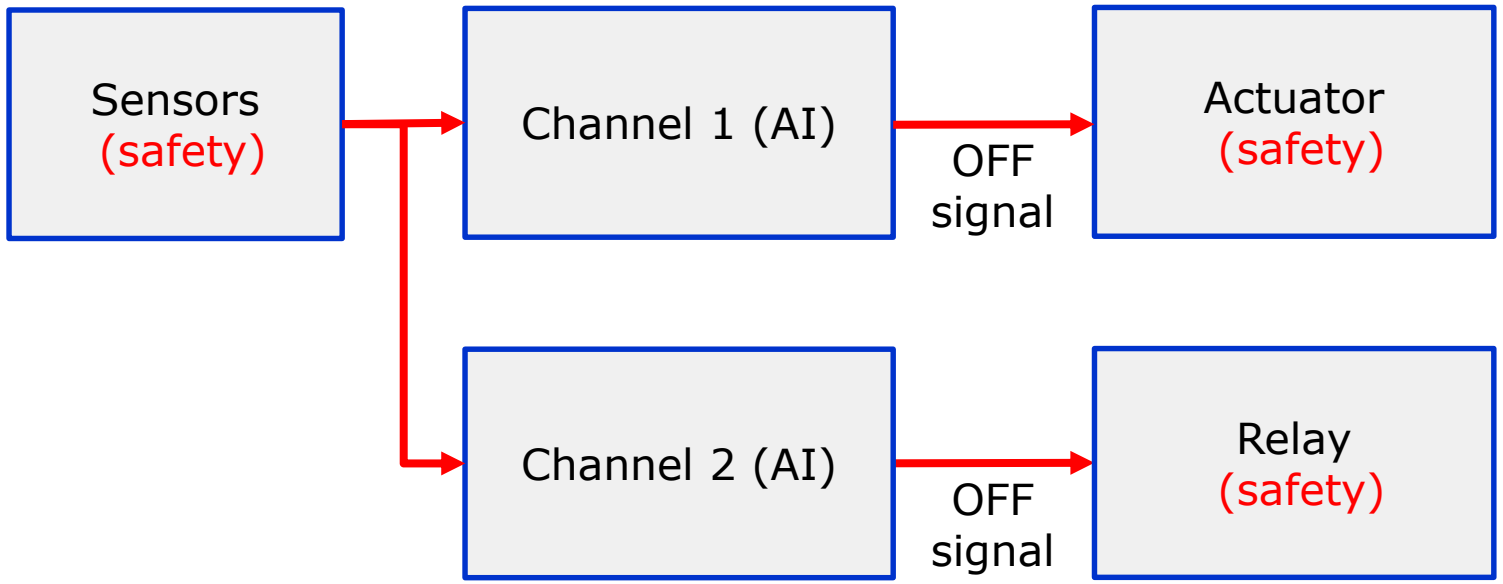


Safety risk: Probability of occurrence x possible extent of damage

Online learning?

Just use redundancy

Safety thinking: if you want to improve safety just use redundancy

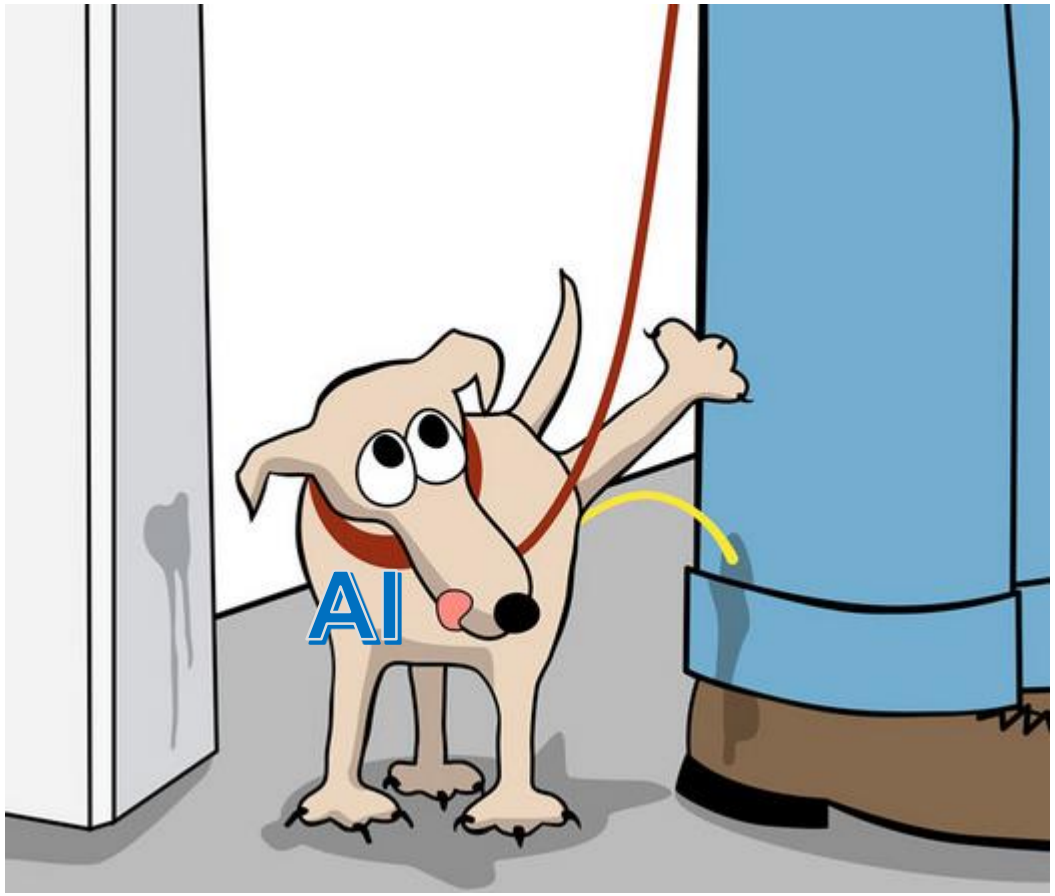


„Funny. The two AI engines have learnt the same wrong behaviour…“

Online learning?

Who is responsible?

„Oh. Sorry, the AI engine never did that before“



Source: bestehunde.de

With conventional technology the supplier or the planner are responsible for the behaviour (function) of the device (or the user in negligence of duties).

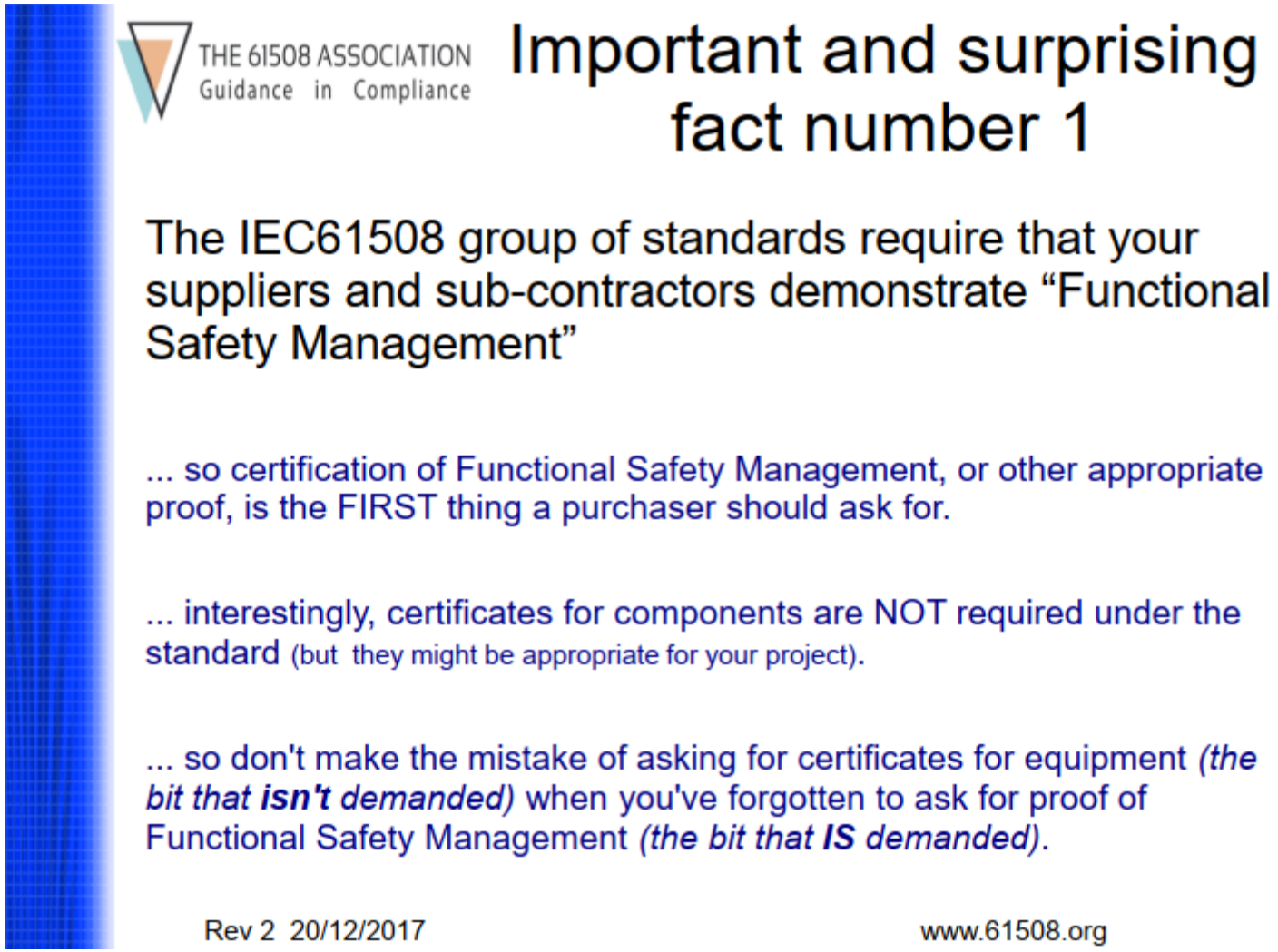
When learning it could be the user!!!

See the EU AI act

(58) Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as regard the need to ensure proper monitoring of the performance of an AI system in a real-life setting, it is appropriate to set specific responsibilities for users. Users should in particular use high-risk AI systems in

Users rather want a certificate!

A certificate?



Summary

Who is better?

Now:
Why was the application only observed by an AI engine?
An operator would have been more reliable in preventing the accident!

Then:
Why didn‘t you use an AI engine instead of an operator?
The AI engine would have been more reliable in preventing the accident!

The task: find the right moment to turn the key…

Source: Pixabay

Summary

Shake hands with the lion…

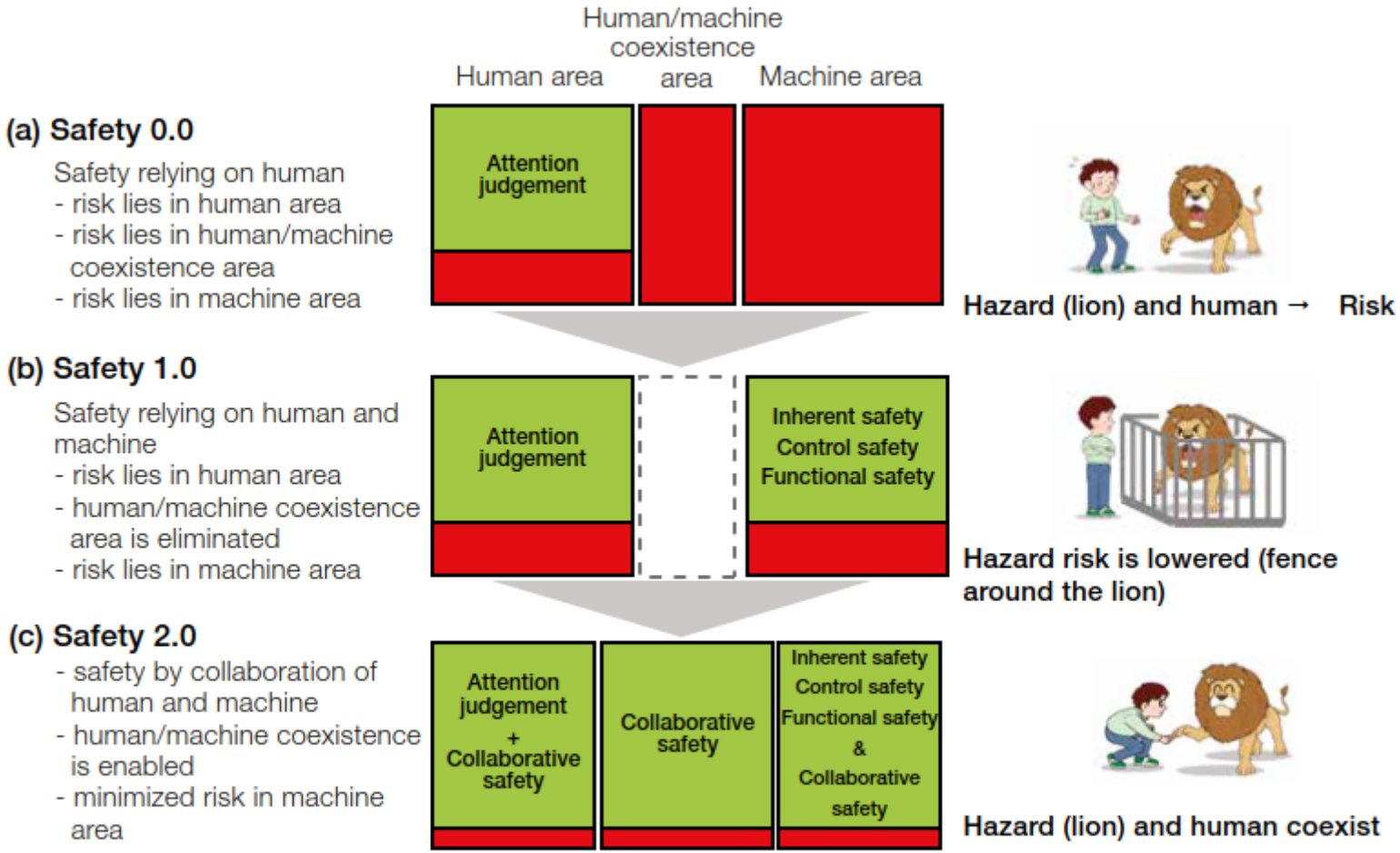


Figure 2-5 | Three ages in the development of (machine) safety

Source: IEC white paper „Safety in the future“ 2020-10

Looking forward…

Useful lifetime?

ISO 13849-1 proposes a mi

So our safety function uses t

You smell and hear when it needs to be serviced

Robus

Motor not overdimensioned

You hear when danger approaches

Reliable

Looking forward…

Useful lifetime?

So what do we talk about – systematic faults or probabilities?

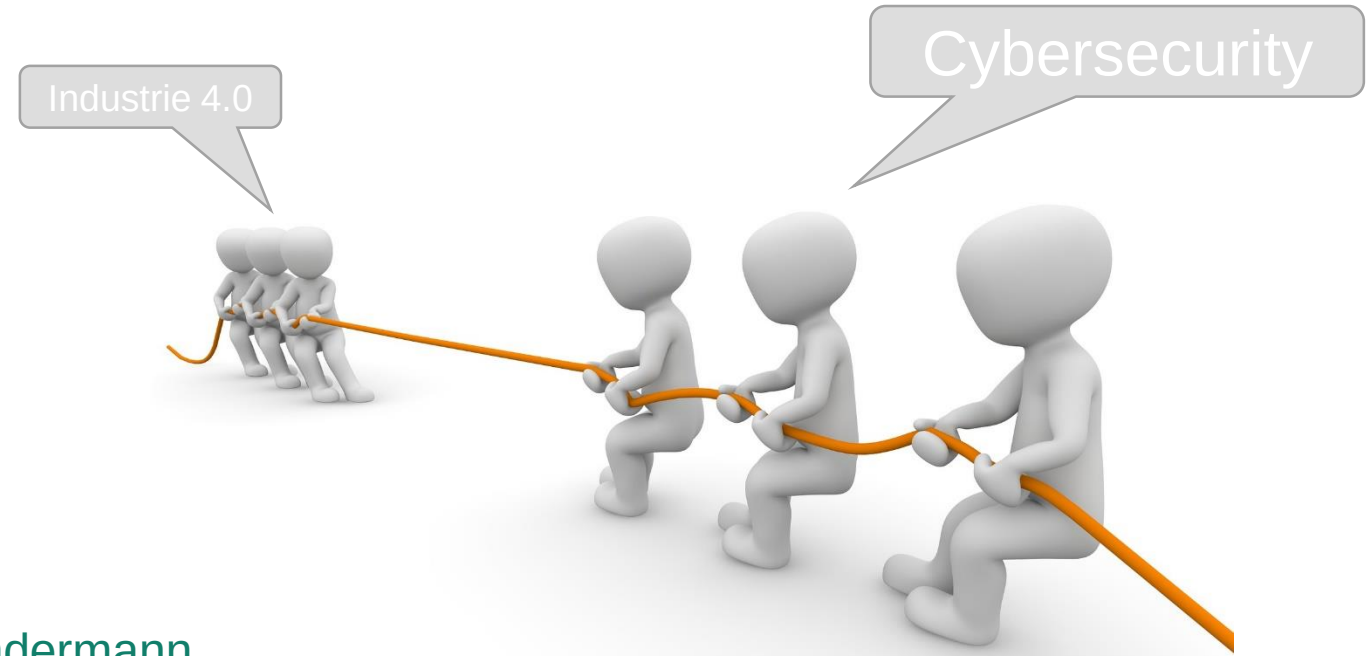
Do you know el. devices with such a lifetime in private and would you trust it?

Where are the limits?

Probably necessary for running a plant so what do we provide?

Looking forward to the discussion!

Industrie 4.0 versus Cybersecurity



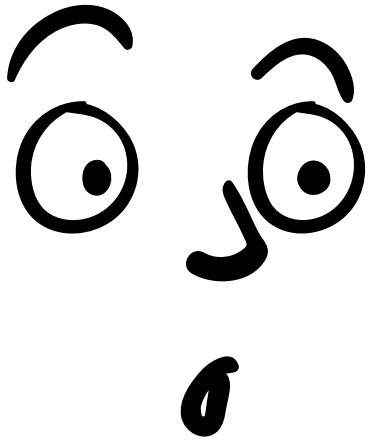
Michael Kindermann
Pepperl+Fuchs SE
mkindermann@de.pepperl-fuchs.com

Source: Hildebrandt, P+F

Gedanken zum EU AI-Act

Dipl-Ing. (FH) Holger Laible

EUROPEAN
COMMISSION



Brussels, 21.4.2021
COM(2021) 206 final

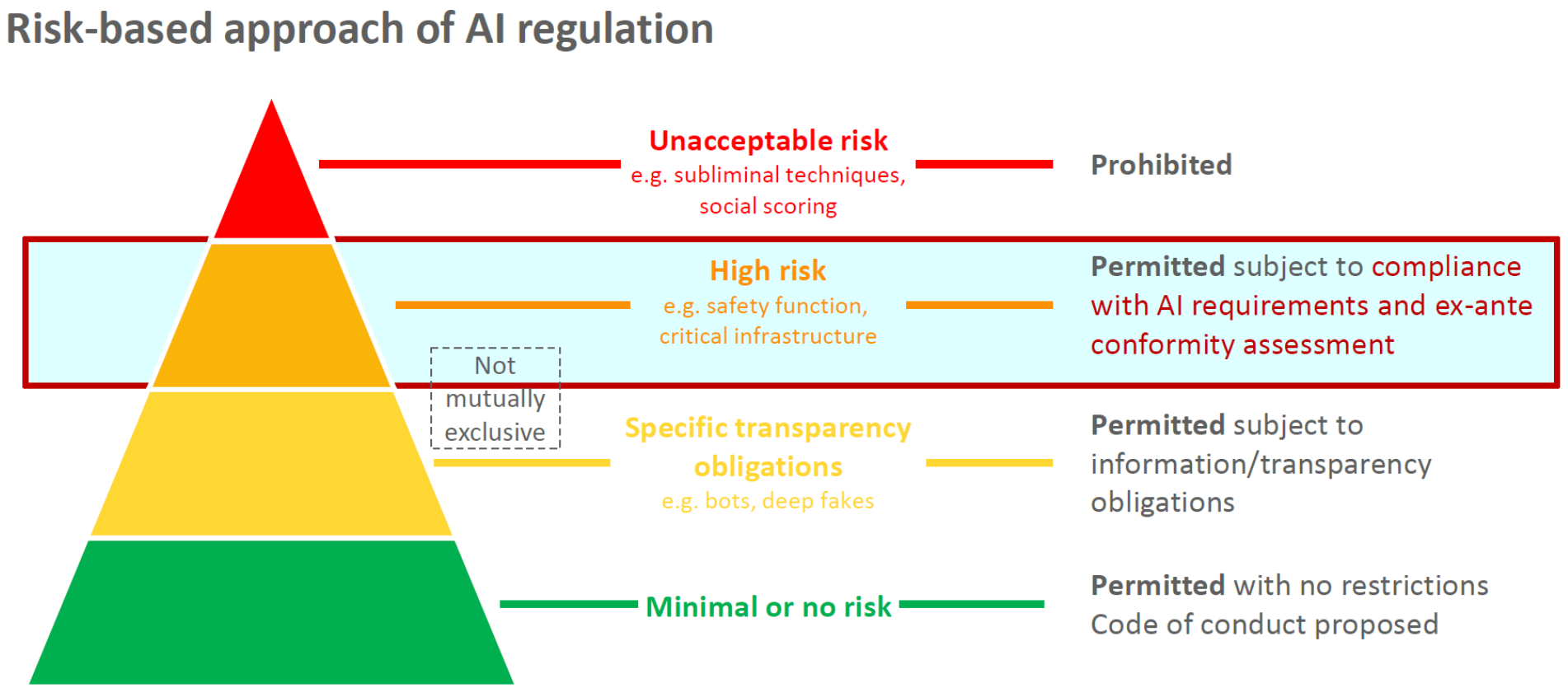
2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

Was ist „high risk“ und wie geht man damit um?



“The proposal lays down a solid risk methodology to define “high-risk” AI systems that pose significant risks to the **health and safety or fundamental rights of persons**.”

Welche Anforderungen gibt es an High-Risk Anwendungen?

a) diese Anwendungen sollten **resilient gegen Risiken** sein, welche mit den Systemgrenzen zusammenhängen (z.B. errors, faults, inconsistencies, unexpected situations)

b) Diese Anwendungen sollten **gegen böswillige Aktivitäten geschützt werden**, die zu gefährlichem oder anderweitig ungewünschtem Verhalten führen.

c) Es wird Horizontale Anforderungen und ein **Zulassungsverfahren** für “trustworthy AI” in der EU geben.

d) Es ist Übereinstimmung zu erzeugen mit **Datenschutz, Verbraucher-Schutz, Nicht-Diskriminierung und Gender-Gleichstellung**.

e) Es wird ein **Register für High-Risk Applikationen** und eine Nachverfolgung geben.

Gedanken dazu:

- Können umsetzbare, widerspruchsfreie Anforderungen dazu in naher Zukunft für KI überhaupt erstellt werden? Insbesondere nachdem es eine sehr breite Definition von KI gibt.
- Benötigen **alle** High-Risk AI Anwendungen generell eine **Safety Betrachtung**?
- Wird Safety zum Standard für High-Risk AI? Was bedeutet dies in der Praxis?

Konkrete Angaben zu High-Risk Applikationen

“The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:

(a) the AI systems are **intended to be used in any of the areas listed** in points 1 to 8 of Annex III;

(b) the AI systems pose a **risk of harm to the health and safety, or a risk of adverse impact on fundamental rights**, that is, in respect of its severity and probability of occurrence, **equivalent to or greater** than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.”

Gedanken dazu:

- Sollten Grundrechtsfragen überhaupt risikobewertet werden? Gibt es überhaupt Low-Risk?
- Der betroffene Bürger ist im Entwurf gar nicht erwähnt. Welche Einflussnahme ist möglich?

Welches sind High-Risk Anwendungen nach Anhang III?

1) Biometrische Identifikation und Kategorisierung natürlicher Personen
2) Management und Betrieb von Kritischer Infrastruktur
   => **Safety Components**
3) Ausbildung und Spachtraining
4) Beschäftigungsverhältnis, Arbeiter Management und Zugang zu Selbstständigkeit
   => Auswahl, Bewertung der Perfomance und des Verhaltens, Arbeitszuteilung, Kündigung
5) Zugang und Genuss von essentiellen privaten und öffentlichen Dienstleistungen und Vergünstigungen
   => *Bewilligung, Reduzierung, Widerrufung, Rückforderung von Leistungen*
   => *Kreditwürdigkeit / Credit Score*
   => *Priorisierung von Feuerwehr und medizinischem Dienst*
6) Strafverfolgung
7) Migration, Asyl und Management der Grenzkontrollen
8) Administration von Justiz und demokratischen Prozessen

Gedanken dazu:

=> Das bedeutet: Alle diese Anwendungen sind angedacht und sollen erlaubt werden!

=> Wie defintieren sich „Safety Components“, wenn die Verfügbarkeit von krit. Infrastruktur wichtig ist?

=> Sind Punkte 4 und 5 nicht gleichbedeutend mit Social Credit Systemen?

=> Ist es überhaupt möglich diese Anwendungen in Übereinstimmung mit den Grundrechten umzusetzen?

„The development of full artificial intelligence could spell the end of the human race".

„AI is likely to be either the best or the worst thing to happen to humanity."

Stephen Hawking

„Once you trust a self-driving car with your life,
you pretty much will trust artificial intelligence with anything."

Dave Waters

SILusionen
der Funktionalen Sicherheit

Referent

Fred Stay

Senior Safety Consultant / Director Safety Consulting

Phone: +49 6202 5770 -130

f.stay@hima.com

HIMA Paul Hildebrandt GmbH

Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone: +49 6202 709-0
Fax: +49 6202 709-107

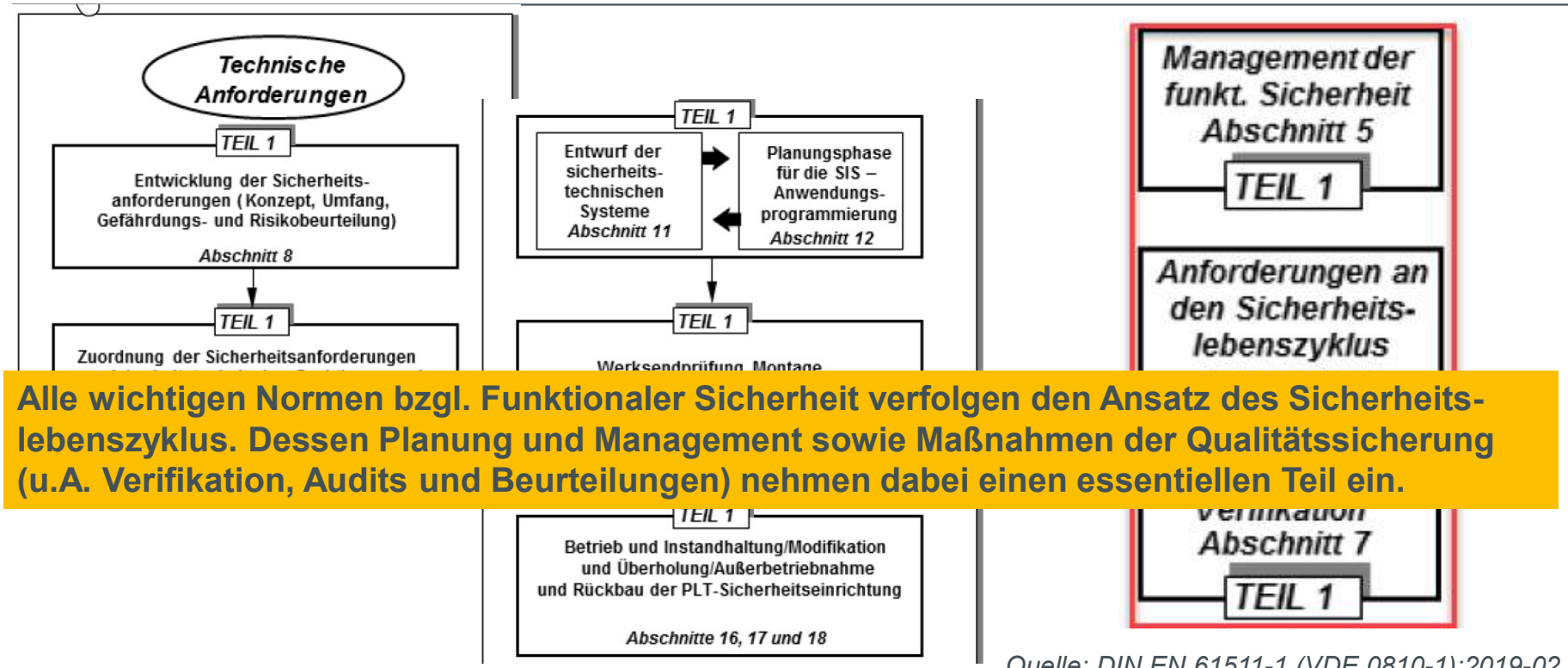
E-mail: info@hima.com
Internet: www.hima.com

SILusionen

Quelle: YouTube

SIL …
der Weg ist das Ziel

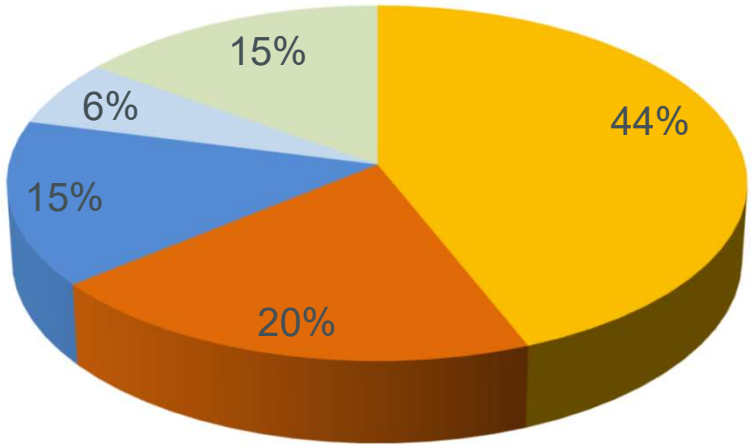
SILusion:
“SIL Normen beschreiben vor allem technische Inhalte”



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

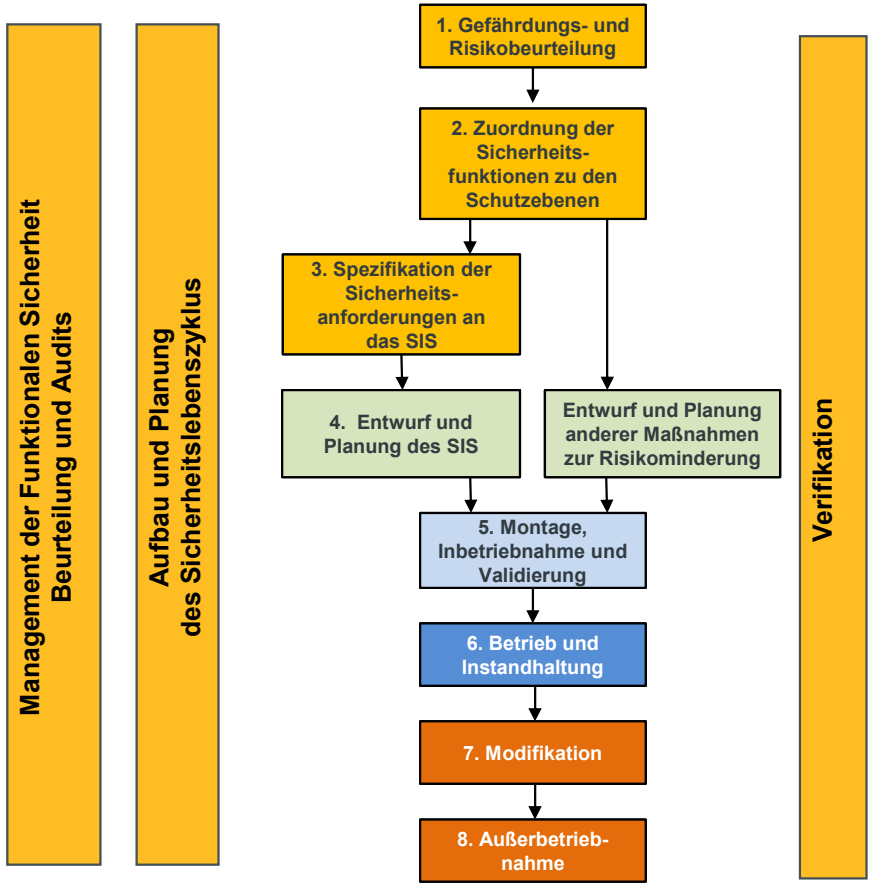
Quelle: DIN EN 61511-1 (VDE 0810-1):2019-02

Lebenszyklus und Fehlerhäufigkeit



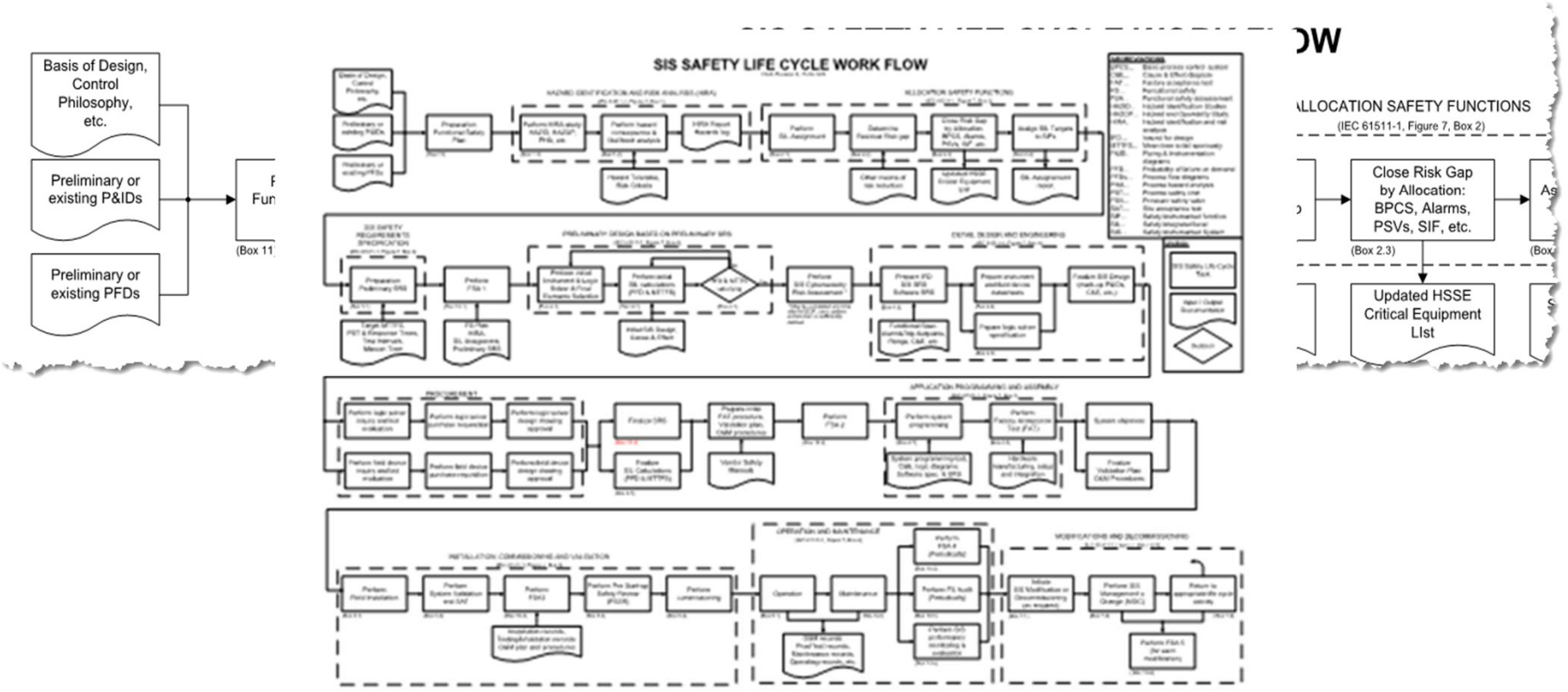
- Spezifikation
- Änderung nach Inbetriebnahme
- Betrieb und Wartung
- Installation und Inbetriebnahme
- Design und Implementierung

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

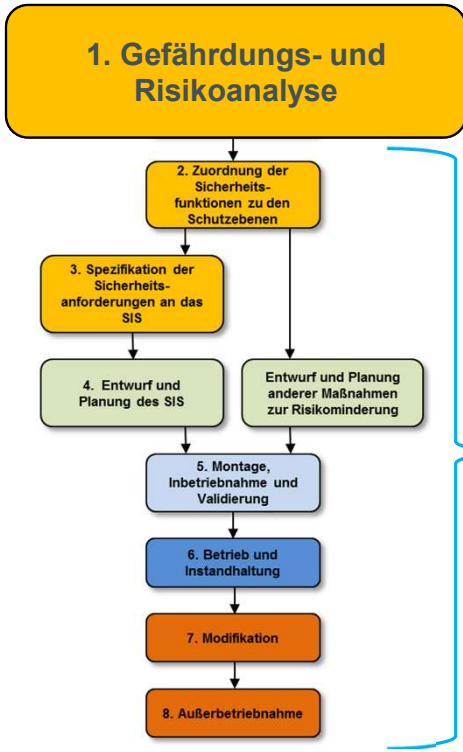


Quelle: DIN EN 61511-1 (VDE 0810-1):2019-02

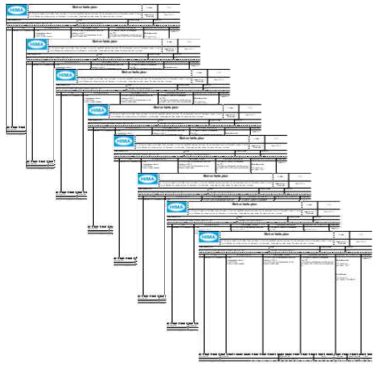
Der Weg ist das Ziel



Kein SIL-Ziel ohne Safety Plan



Beschreibung der Details pro Phase

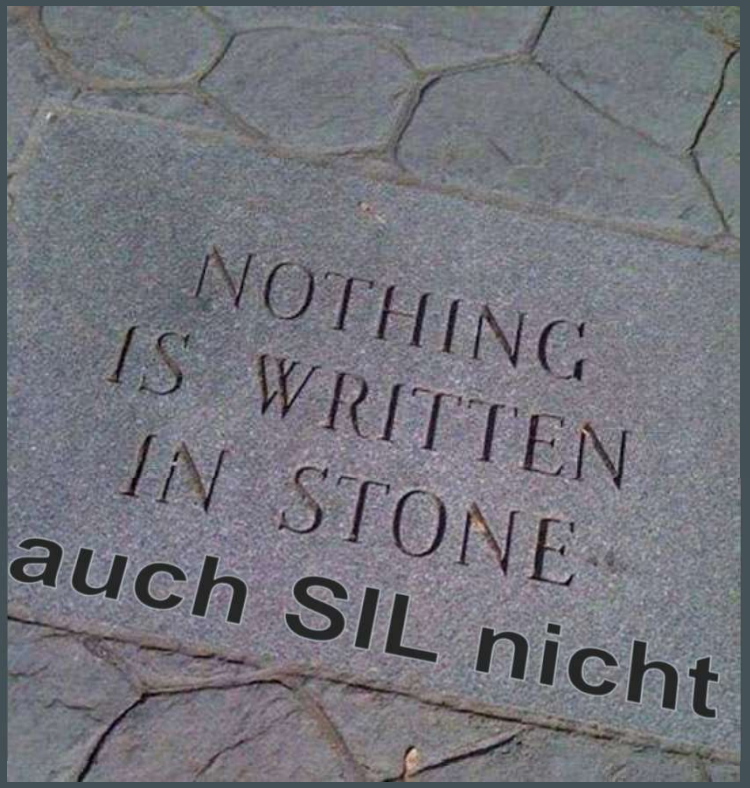


- Titel der Phase
- Erforderliche Info (Eingangsdokumente)
- Zielvorgabe / Aktion
- Geforderte Ergebnisse
- Verantwortlichkeiten / Ausführung durch
- benötigte Kompetenzen
- Anforderungen aus …

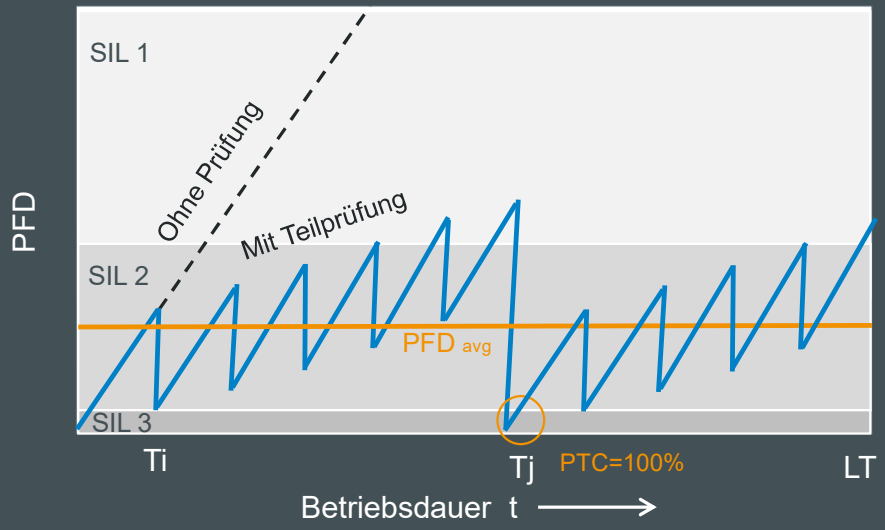
In der Praxis können unterschiedliche individuelle Lebenszyklen definiert werden für Betreiber, Errichter, Integratoren, Planer, Entwickler für Hardware / Software …

Einmal SIL immer SIL

SILusion: “Einmal SIL immer SIL”



SILusion: “Einmal SIL immer SIL”



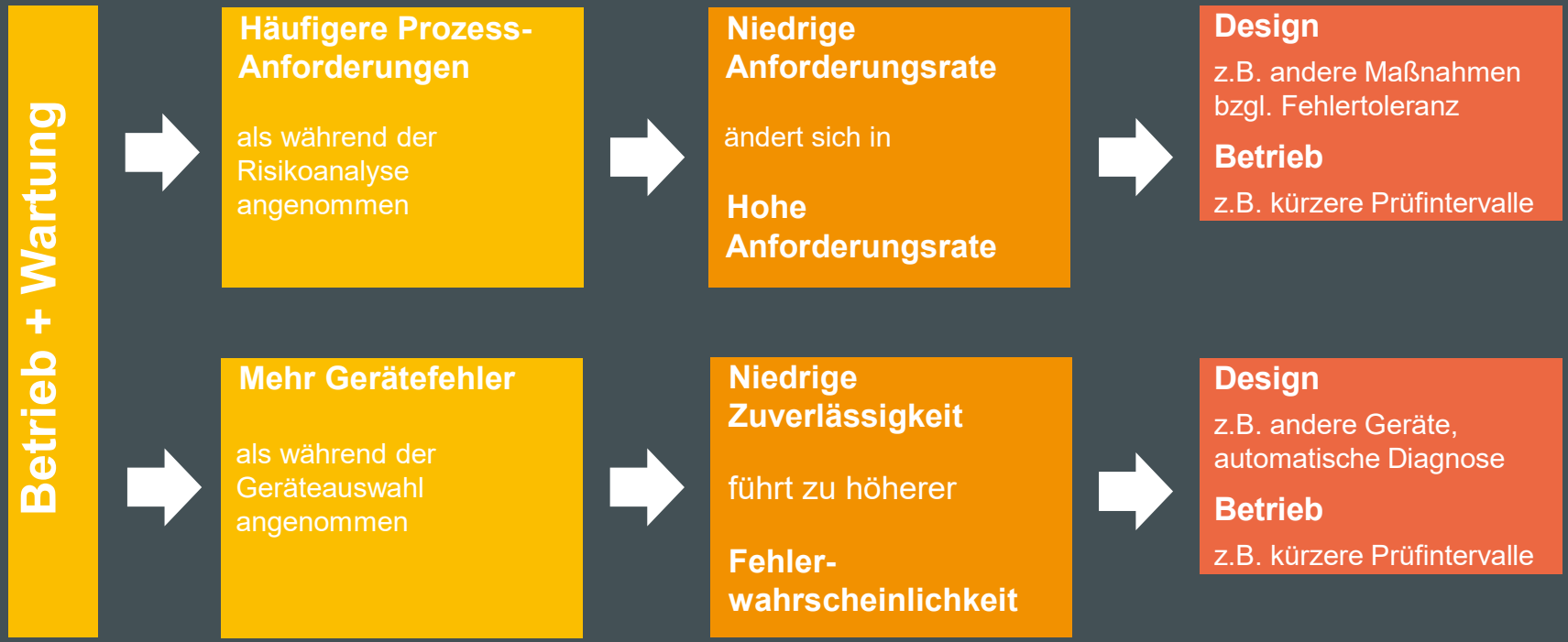
$PFD_{avg} \approx \frac{1}{2} \lambda_{du} \times Ti \times PTC + \frac{1}{2} \lambda_{du} \times Tj \times (1 - PTC)$

PTC – Prüftiefe , Ti – Testintervall (Teilprüfung) , Tj – Testintervall (Vollprüfung)

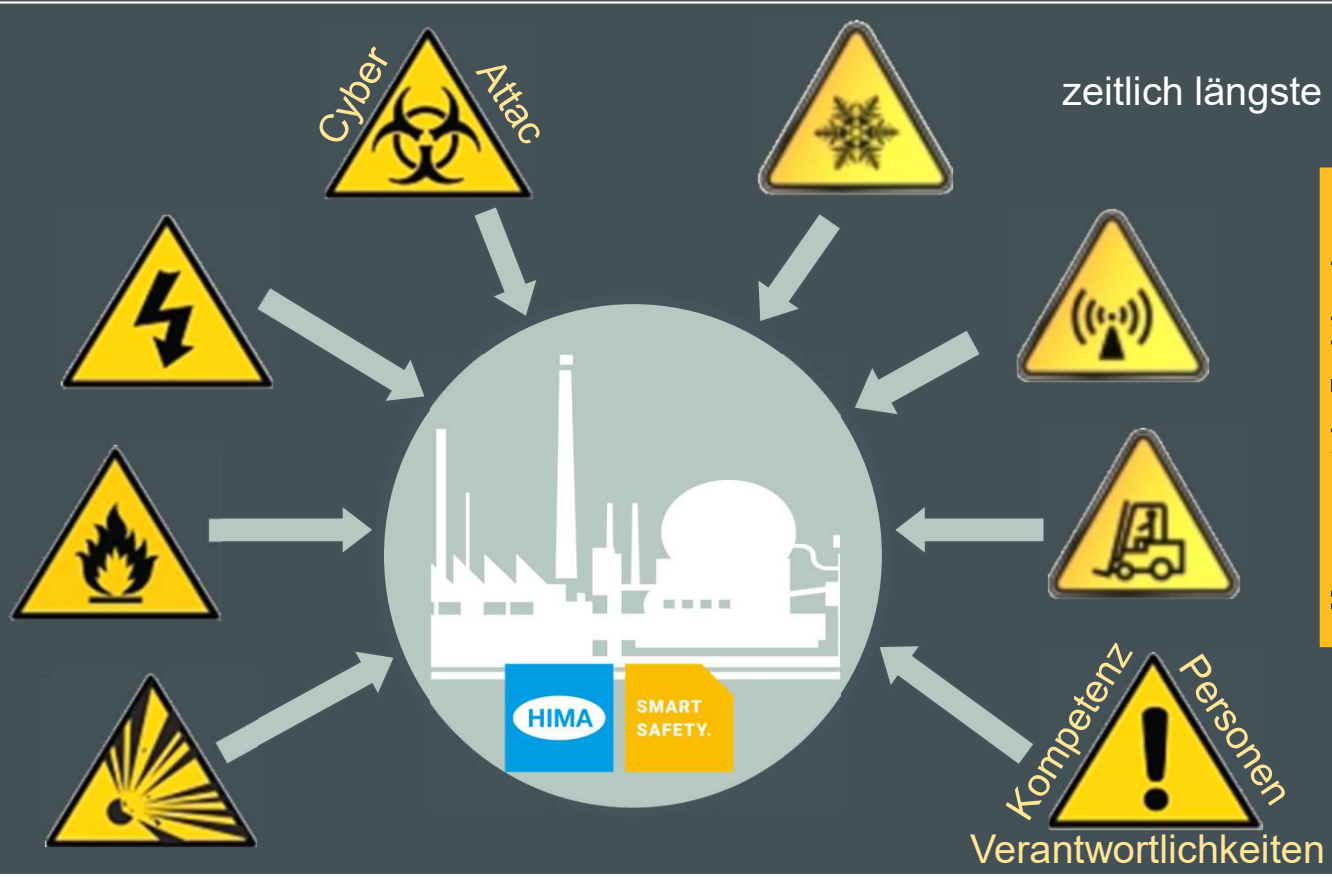
„Die Zuverlässigkeit der Sicherheitsfunktion lässt sich berechnen“…zu kurz gedacht!

Überwachung der Leistungsfähigkeit

Konsequenzen bei Abweichungen zu Planungsdaten



Integrität der SIF – Erhalt im Betrieb



zeitlich längste Phase!

Sicherheits-lebenszyklus Phasen 1-5

Management der Funktionalen Sicherheit Beurteilung und Audits

Aufbau und Planung des Sicherheitslebenszyklus

6. Betrieb und Instandhaltung

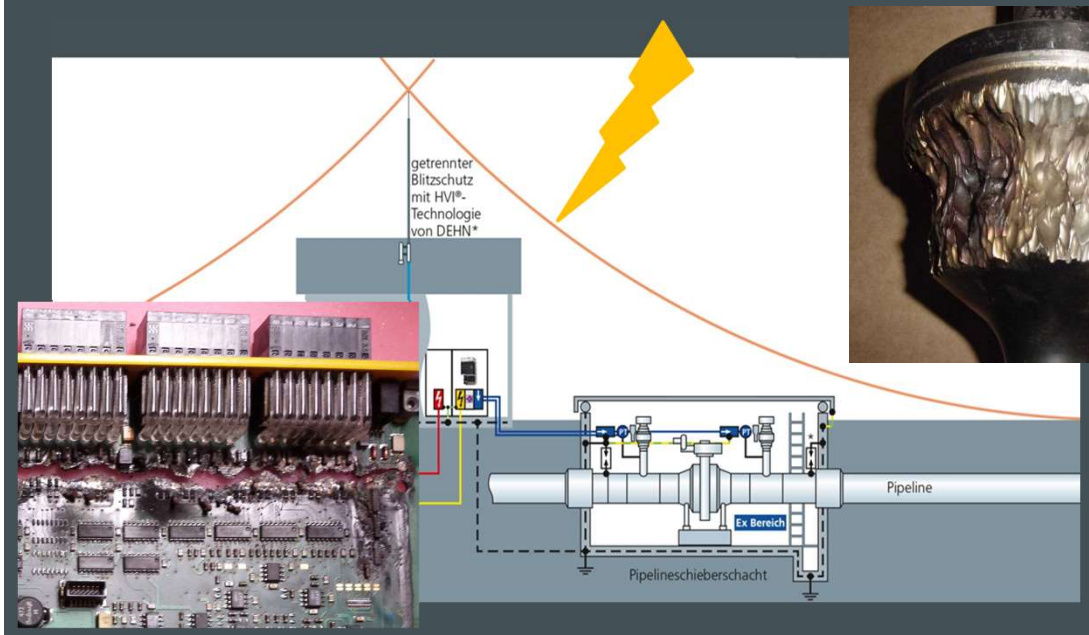
7. Modifikation

8. Außerbetrieb-nahme

Verifikation

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.



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

Thank You.

Fred Stay

Senior Safety Consultant / Director Safety Consulting

f.stay@hima.com

HIMA Paul Hildebrandt GmbH

Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone: +49 6202 5770 -130
Mobile: +49 1624250759

E-mail: info@hima.com
Internet: www.hima.com

Klimawandel - Herausforderung für die funktionale Sicherheit?

SIL Slam 23.06.2022

Klimawandel - Herausforderung für die funktionale Sicherheit?

Klimawandel

- ...Treibhauseffekt...
- ...seit Industrialisierung CO_2 um 48% erhöht...
- ...2020 eines der drei wärmsten Jahre...
- ...Erderwärmung Ende 2100 2,5 – 5°C...
- ...Gletscher und Meereis der Arktis schrumpfen...
- ...der Meeresspiegel steigt...
- ...extreme Wetterlagen nehmen zu...

Bildquelle: Pixabay

Klimawandel - Herausforderung für die funktionale Sicherheit?

Definition Klima und Klimawandel

- *Klima:*
  Langjähriges Mittel der meteorologischen Verhältnisse
  - in einer Region oder weltweit
  - Temperatur
  - Niederschlag
  - Wind
  - “Langjährig”: Jahrzenhnte oder länger (Typ. 30 Jahre)
- *Klimawandel:*
  Durchschnittswerte und Schwankungsbreiten der o.a. Größen ändern sich – dies dauerhaft und statistisch nachweisbar.
- Achtung, diese Definition sagt nichts über die Ursachen und Zusammenhänge aus!

Bildquelle: Pixabay

Klimawandel - Herausforderung für die funktionale Sicherheit?

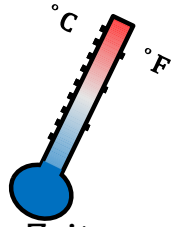
- Mit welchen Aspekten des Klimawandels müssen wir rechnen?
- Wie kommen sie zustande?
- Haben diese Aspekte einen Einfluss auf Sicherheitsfunktionen?
- Wenn ja, welchen?
- Wie sind diese Aspekte dann zu berücksichtigen?

Klimawandel - Herausforderung für die funktionale Sicherheit?

Temperaturanstieg – in Deutschland und weltweit, sowie Prognosen

Ist Stand:

- In Deutschland: Das Jahresmittel der Lufttemperatur ist seit Beginn der Wetteraufzeichnungen 1881 bis 2018 um **1,5°C** angestiegen. *(1)*
- Die globale Erwärmung seit der vorindustriellen Zeit wird mit **1,2°C** angegeben (2021). *(3)*



Prognose:

- Weltweit wird die globale Erwärmung bis 2100 **1,6°C – 4,7°C** im Vergleich zur vorindustriellen Zeit betragen, je nach den zukünftigen Treibhausgasemissionen. *(2)*
- Erwärmung von Landmassen und **von hohen nördlichen Breiten stärker ausgeprägt** als der Rest *(2)*

1. Quelle speziell für Deutschland: Zweiter Fortschrittsbericht zur Deutschen Anpassungsstrategie an den Klimawandel inkl. Aktionsplan 2020 z.B. Umweltbundesamt oder BMUV, https://www.bmuv.de/download/zweiter-fortschrittsbericht-zur-deutschen-anpassungsstrategie-an-den-klimawandel
2. https://www.umweltbundesamt.de/themen/klima-energie/klimawandel/zu-erwartende-klimaaenderungen-bis-2100
3. Climate Action Tracker, Globale Erwärmung bis Ende 2100 unter Berücksichtigung verschiedener Faktoren, z.B. Einhaltung Klimaziele von 32 Staaten, https://climateactiontracker.org/

Klimawandel - Herausforderung für die funktionale Sicherheit?

Meteorologische Extremereignisse

- Zukünftige Zunahme von Hitzewellen*
- Vermehrtes Auftreten von Tornados**
- Zukünftige Zunahme der Häufigkeit von **Starkniederschlägen***
  - Kurzzeitige, heftige Starkregen eher im Sommerhalbjahr*
  - Wiederkehrzeit von vergleichbaren Niederschlagsereignissen ist im Süden Deutschlands kleiner
  - Quellen: KLIWA Kurzbericht Starkregen 07/2019 z.B. www.kliwa.de Forschungsbericht zur TRAS 320, Mai 2016, z.B. www.bmuv.de
  - Beispiele 2014 Münster, 2016 Braunsbach, 2021 Ahrtal,...
  - Kann auch als Schnee fallen Bsp. Februar 2022 Athen

Bildquelle: Pixabay

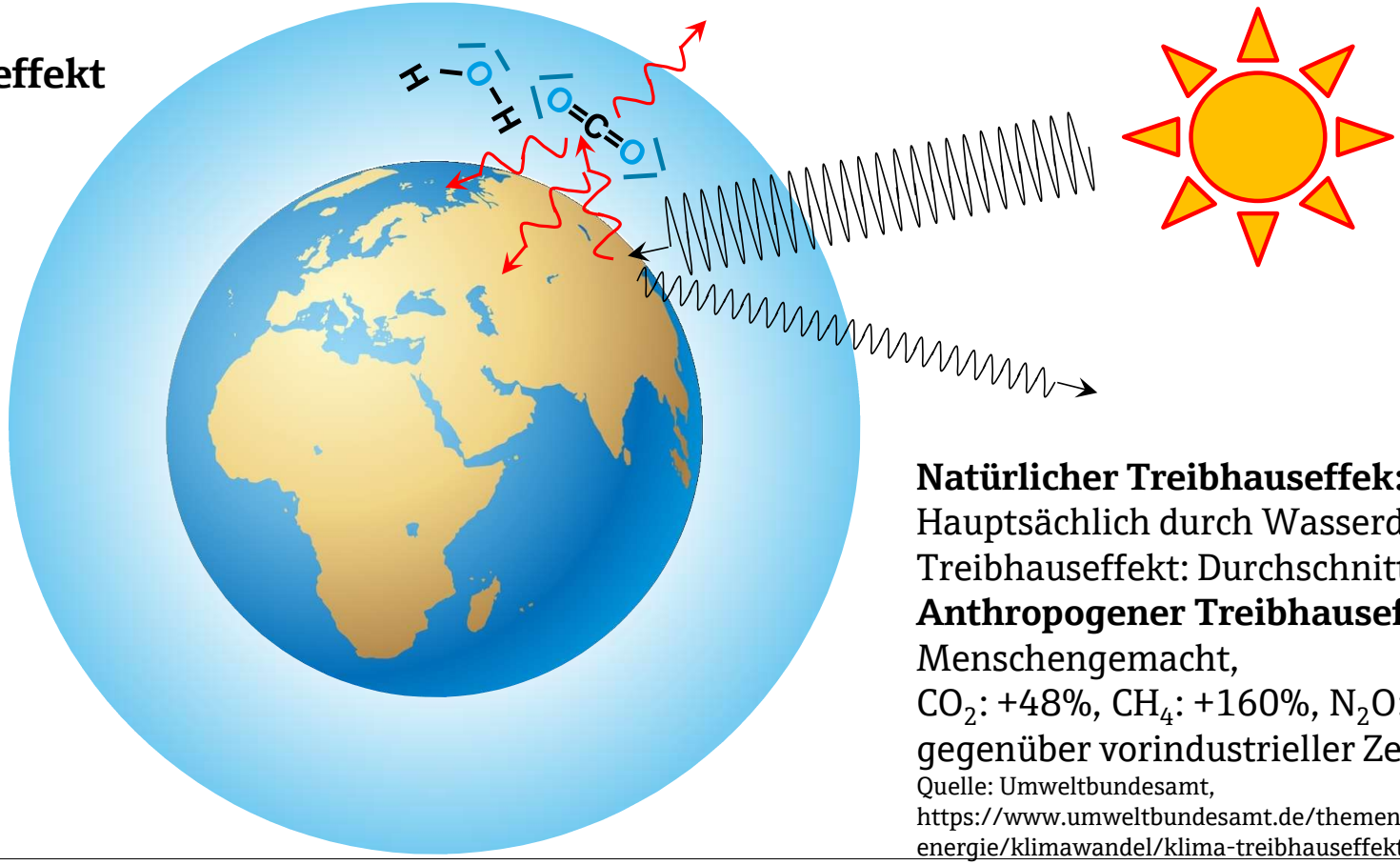
* „Generell sind im Themenfeld noch viele Aussagen mit großen Unsicherheiten behaftet, oder es ist auf Basis der vorliegenden Datengrundlage noch keine Aussage möglich!“ (KLIWA Kurzbericht Starkregen 07/2019 z.B. www.kliwa.de)

** Hinweise als Folge des Klimawandels, Forschungsbericht zur TRAS 320, Mai 2016

Klimawandel - Herausforderung für die funktionale Sicherheit?

Treibhauseffekt

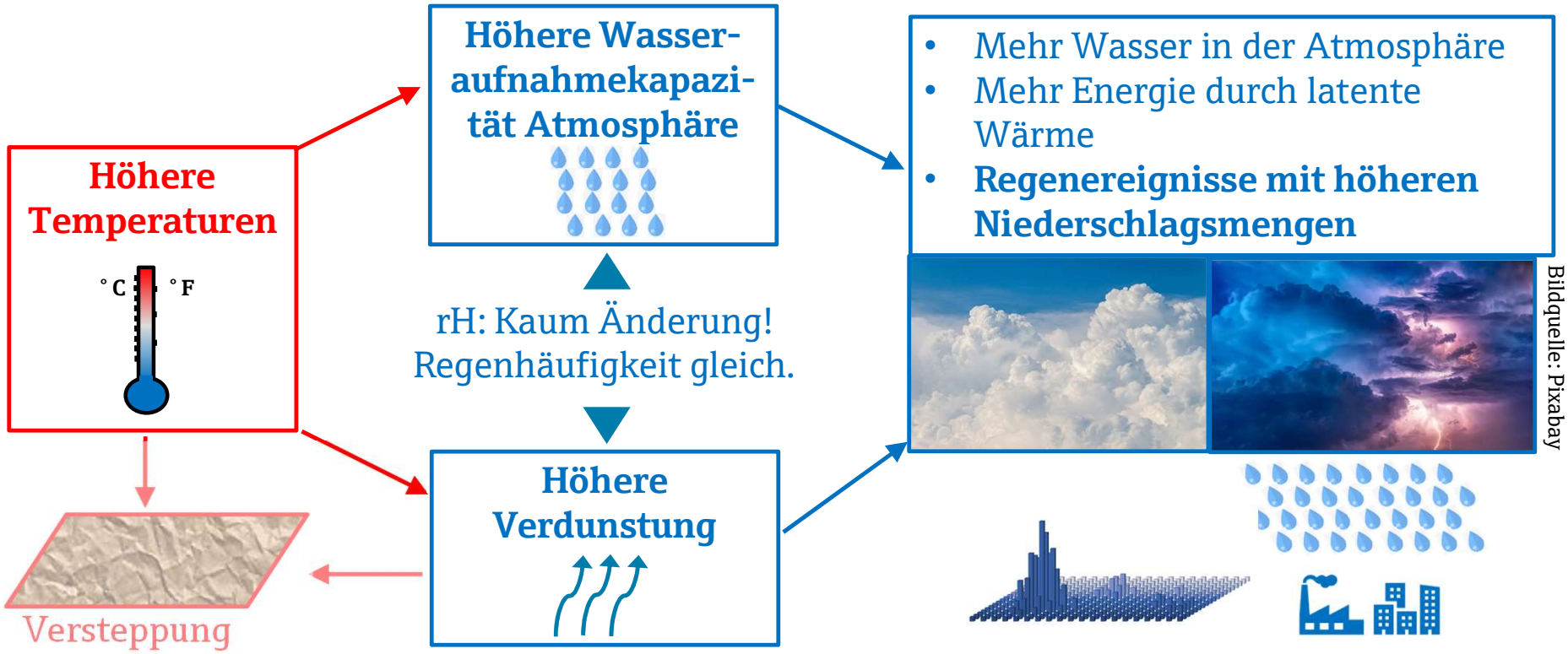
- CO_2
- H_2O
- CH4
- NO_x
- FCKW
- ...



Natürlicher Treibhauseffek:
Hauptsächlich durch Wasserdampf, ohne Treibhauseffekt: Durchschnittlich -18°C!
Anthropogener Treibhauseffekt:
Menschengemacht,
CO_2: +48%, CH_4: +160%, N_2O: +23% gegenüber vorindustrieller Zeit
Quelle: Umweltbundesamt, https://www.umweltbundesamt.de/themen/klima-energie/klimawandel/klima-treibhauseffekt#grundlagen

Klimawandel - Herausforderung für die funktionale Sicherheit?

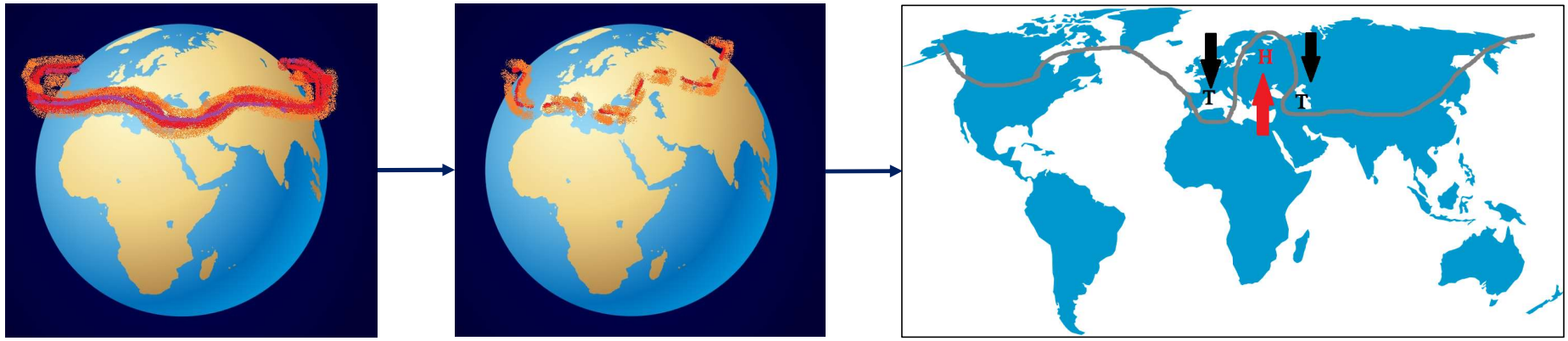
Zustandkommen von Starkregenereignissen und vermuteter Einfluss des Klimawandels I



Klimawandel - Herausforderung für die funktionale Sicherheit?

Zustandkommen von Starkregenereignissen und vermuteter Einfluss des Klimawandels II

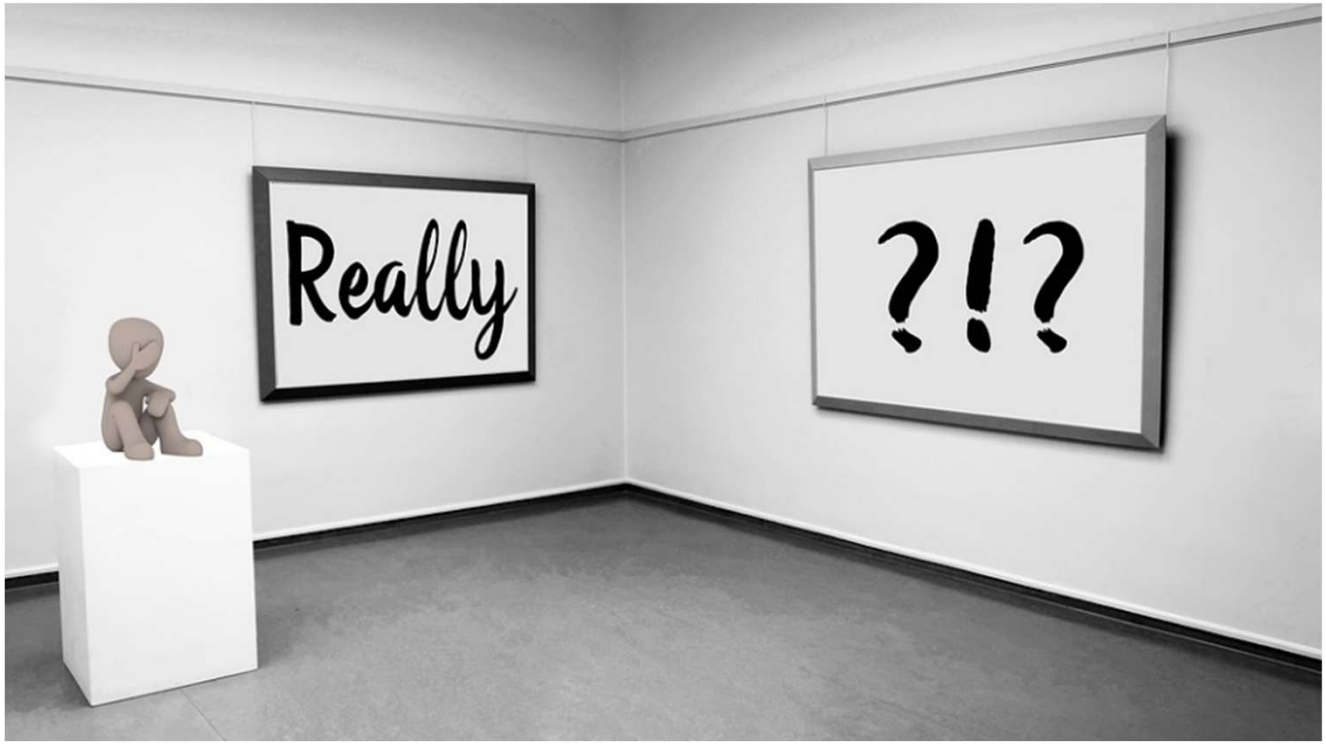
- Zeitweise abgeschwächter Jetstream sorgt für Störung der in unseren Breiten vorhandenen westlichen Strömung
- Stationäres Verbleiben (lokaler) Tiefdruckgebiete an einem Ort
- Evtl. Ursache: Stärkere Erwärmung der Arktis als der Rest der Nordhalbkugel*



* wird kontrovers diskutiert, zu wenig statistische Sicherheit

Klimawandel - Herausforderung für die funktionale Sicherheit?

- Haben diese Aspekte einen Einfluss auf die funktionale Sicherheit?



Bildquelle: Pixabay

Klimawandel - Herausforderung für die funktionale Sicherheit?

Zufällige Fehler: Temperaturerhöhung - Verkürzung der Gebrauchsdauer bzw. Erhöhung der Ausfallraten?

- Arrheniusgleichung, Eyringgleichung oder MIL HDBK 217F

$$t_E = t_Q \cdot e^{\frac{E_A}{k}\cdot\left(\frac{1}{T_E}-\frac{1}{T_Q}\right)}$$

$$\lambda_E = \lambda_Q \cdot e^{-\frac{E_A}{k}\cdot\left(\frac{1}{T_E}-\frac{1}{T_Q}\right)}$$

Base Failure Rate -

T_A (°C)	Stress .1	.3	.5
0	.0021	.0032	.0049
10	.0023	.0036	.0056
20	.0025	.0040	.0064
30	.0028	.0045	.0072
40	.0031	.0050	.0082
50	.0034	.0056	.0093
60	.0037	.0063	.011
70	.0041	.0070	.012
80	.0045	.0079	.014

MIL-HDBK-217F
2 DECEMBER 1991

MILITARY HANDBOOK

RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT

-> Erhöhung der Umgebungstemperatur um wenige Grad Celsius bringt nur vernachlässigbaren Beitrag zu Ausfallraten

- Lokale Eigenerwärmung durch Verlustleistung der Bauteile bringt hier immer noch den wesentlichen Beitrag, Deratingkurven der Komponenten sind zu berücksichtigen.

Systematische Fehler sind wie so oft entscheidender.

Klimawandel - Herausforderung für die funktionale Sicherheit?

Warum geht von Starkregen ein hohes Risiko aus?

- **Extrem kurze Vorwarnzeit** => Hohe Gefahr
- Wirkt sich außerhalb und unabhängig von Gewässern aus => potenziell **alle** Regionen können von Starkregen betroffen sein
- Starkregenereignisse werden in Folge des Klimawandels zunehmen
- **Treten sehr lokal auf** => schwere Vorhersage, durch große Wetterstationen oft nicht messbar
- Wenig Daten => Räumliche Betroffenheit kann nicht abgeleitet werden

-> Massnahmen des Hochwasserschutzes!

Bildquelle: Pixabay

Klimawandel - Herausforderung für die funktionale Sicherheit?

Hochwasserschutz – Rechtliche Vorgaben

Hochwasser-risikomanagement-Richtlinie HWRM-RL

Wasserrahmen-richtlinie

Hochwasserrisikomanagement-Richtlinie:
- Übergeordnete Richtlinie auf EU-Ebene
- Verpflichtet die Mitgliedstaaten zum Hochwasserrisikomanagement
- Keine Verpflichtung zum tech. Hochwasserschutz. Richtlinie soll das Bewusstsein für die Gefahren von Hochwasser schaffen

Wasserrahmenrichtlinie:
- Verpflichtet zur Erreichung eines „guten ökologischen Zustandes“ der Oberflächengewässer

Wasserhaushalts-gesetz des Bundes

Wasserhaushaltsgesetzt (WHG):
- Ausweisung von Überschwemmungsgebieten (Gebiete, die bei einem HQ100 überschwemmt werden)
- Umsetzung der EU-Richtlinie in nationales Recht

Wassergesetz der Länder

Wassergesetz der Länder
- Umsetzung des Wasserhaushaltsgesetzes des Bundes in Länderrecht
- Basis für kommunalen Hochwasserschutz

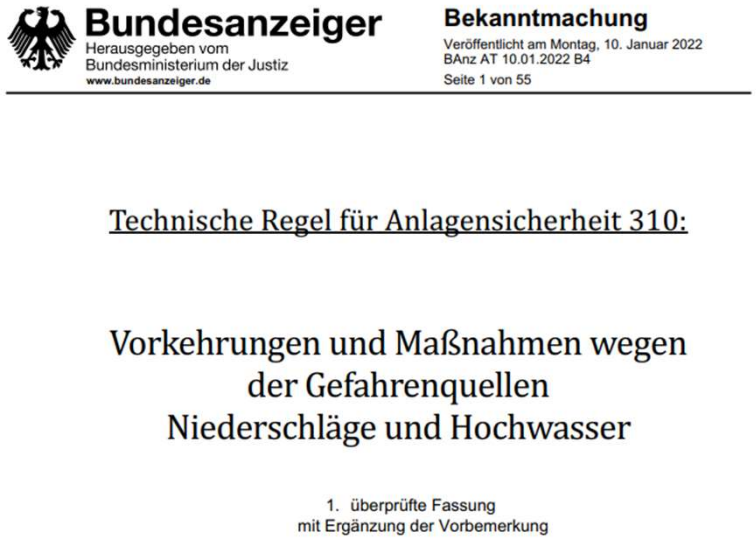
Kommune

- Hochwasserschutz im Rahmen allgemeiner Daseinsvorsorge
- Hochwasserschutz in der Bauleitplanung (Ausweisung Baugebiet)
- Bereitstellung von Informationen zum Thema Hochwasserschutz an die Bevölkerung (keine rechtliche Verankerung, jedoch dringende Empfehlung)

Klimawandel - Herausforderung für die funktionale Sicherheit?

Was sagt das technische Regelwerk zum Klimawandel?

- Bei Betrieben, die dem Wasserhaushaltsgesetz oder der Störfallverordnung unterliegen, ist das nichts neues, sie müssen auch in Bezug auf Hochwasserrisiken regelmässig überprüfen und minimieren.
- Technische Regeln zur Anlagensicherheit TRAS 310, TRAS 320
- Technische Regel zur Anlagensicherheit TRAS 310: “Vorkehrungen und Massnahmen wegen der Gefahrenquellen Niederschläge und Hochwasser” **Januar 2022**



Bundesanzeiger
Herausgegeben vom Bundesministerium der Justiz
www.bundesanzeiger.de

Bekanntmachung
Veröffentlicht am Montag, 10. Januar 2022
BAnz AT 10.01.2022 B4
Seite 1 von 55

Technische Regel für Anlagensicherheit 310:

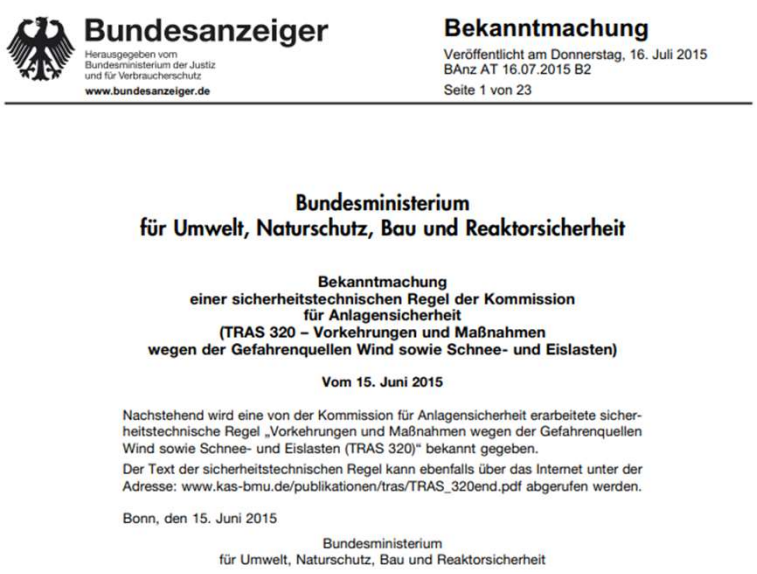
Vorkehrungen und Maßnahmen wegen der Gefahrenquellen Niederschläge und Hochwasser

1. überprüfte Fassung
mit Ergänzung der Vorbemerkung

Klimawandel - Herausforderung für die funktionale Sicherheit?

Was sagt das technische Regelwerk zum Klimawandel?

- Bei Betrieben, die dem Wasserhaushaltsgesetz oder der Störfallverordnung unterliegen, ist das nichts neues, sie müssen auch in Bezug auf Hochwasserrisiken regelmässig überprüfen und minimieren.
- Technische Regeln zur Anlagensicherheit TRAS 310, TRAS 320
- Technische Regel zur Anlagensicherheit TRAS 320: “Vorkehrungen und Massnahmen wegen der Gefahrenquellen Wind sowie Schnee- und Eislasten” Juli 2015



Bundesanzeiger
Herausgegeben vom Bundesministerium der Justiz und für Verbraucherschutz
www.bundesanzeiger.de

Bekanntmachung
Veröffentlicht am Donnerstag, 16. Juli 2015
BAnz AT 16.07.2015 B2
Seite 1 von 23

**Bundesministerium
für Umwelt, Naturschutz, Bau und Reaktorsicherheit**

**Bekanntmachung
einer sicherheitstechnischen Regel der Kommission
für Anlagensicherheit
(TRAS 320 – Vorkehrungen und Maßnahmen
wegen der Gefahrenquellen Wind sowie Schnee- und Eislasten)**

Vom 15. Juni 2015

Nachstehend wird eine von der Kommission für Anlagensicherheit erarbeitete sicherheitstechnische Regel „Vorkehrungen und Maßnahmen wegen der Gefahrenquellen Wind sowie Schnee- und Eislasten (TRAS 320)“ bekannt gegeben.

Der Text der sicherheitstechnischen Regel kann ebenfalls über das Internet unter der Adresse: www.kas-bmu.de/publikationen/tras/TRAS_320end.pdf abgerufen werden.

Bonn, den 15. Juni 2015

Bundesministerium
für Umwelt, Naturschutz, Bau und Reaktorsicherheit

Klimawandel - Herausforderung für die funktionale Sicherheit?

Was sagt das technische Regelwerk zum Klimawandel?

-> Aus der TRAS 310 Abschnitt 2 Grundlagen:

- Bezüglich der naturbedingten Gefahrenquellen, wie Hochwasser und Niederschläge, hat sich der allgemeine Kenntnisstand vor dem Hintergrund des Klimawandels weiter entwickelt. Unbestritten ist, dass sich mit dem Anstieg der globalen Temperatur der Wasserhaushalt in der Atmosphäre verändert und **die Wahrscheinlichkeit von Starkniederschlägen zunimmt**.
- Damit steigen zugleich auch die Gefahren durch Hochwasser bzw. Überflutungen.
- **Diese neuen Erkenntnisse sind bei der Bewertung der naturbedingten Gefahrenquellen zu beachten.**
- Januar 2022

Quelle: TRAS 310, z.B. https://www.kas-bmu.de/app.php/nachricht/tras-310.html

Klimawandel - Herausforderung für die funktionale Sicherheit?

Was sagt das technische Regelwerk zum Klimawandel?

-> Aus der TRAS 310 Abschnitt 2 Grundlagen:

- Vor diesem Hintergrund weist die **Deutsche Anpassungsstrategie an den Klimawandel (DAS)** darauf hin, dass bei Betriebsbereichen, in denen gefährliche Stoffe bei Extremereignissen freigesetzt werden könnten, **die bisherigen Sicherheitsanforderungen und das Sicherheitsmanagement** entsprechend des wissenschaftlichen Erkenntnisfortschritts und der Betreiberpflichten gemäß Störfall-Verordnung zu **überprüfen und gegebenenfalls** anzupassen sind.
- Dabei: Beachtung der Gebiete mit signifikantem Hochwasser-Risiko, unter Zuhilfenahme der Hochwasser- und Starkregen gefahren und risikokarten der Kommunen
- Januar 2022

Quelle: TRAS 310, z.B. https://www.kas-bmu.de/app.php/nachricht/tras-310.html

Klimawandel - Herausforderung für die funktionale Sicherheit?

Was sagt das technische Regelwerk zum Klimawandel?

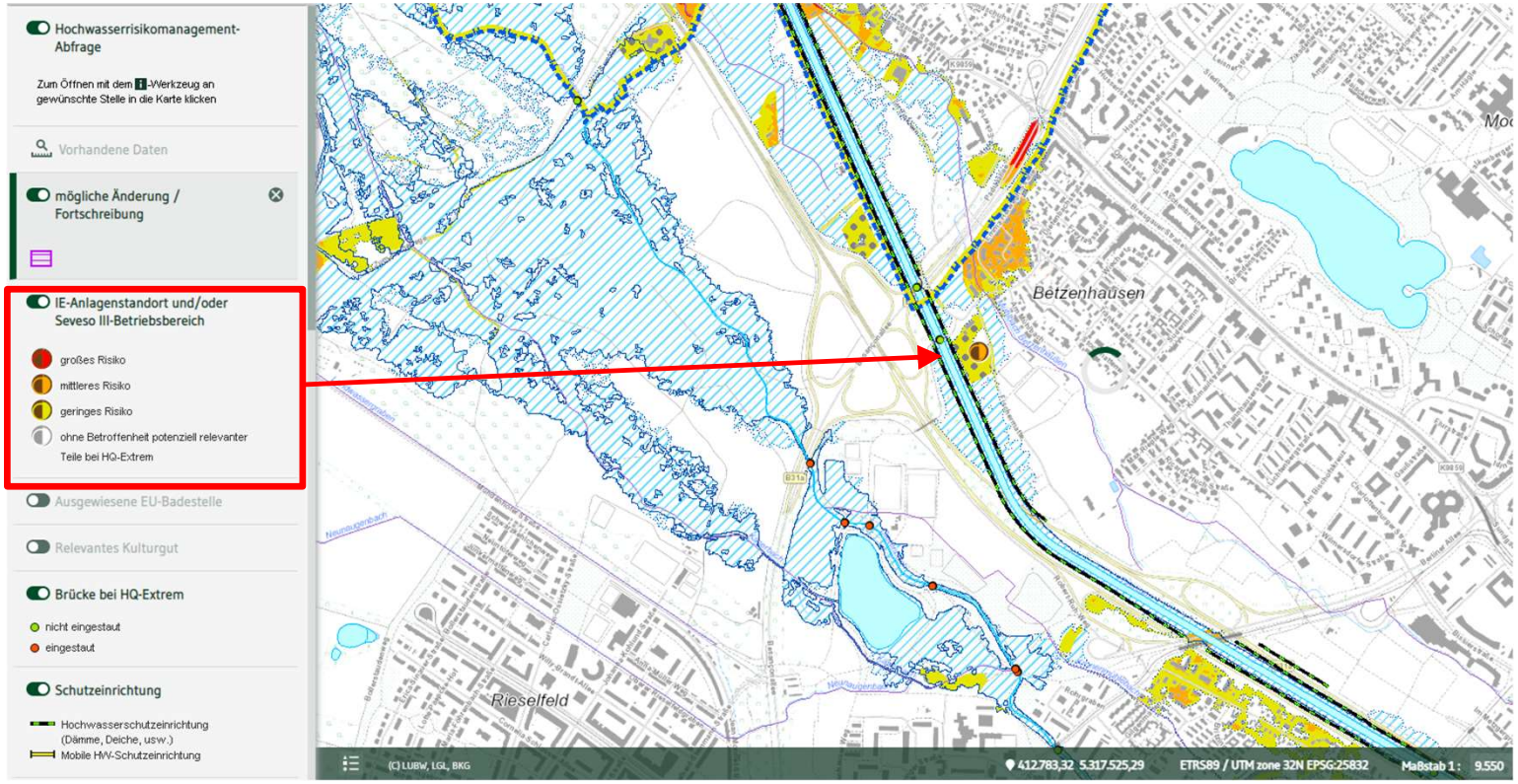
-> Aus der TRAS 310 Abschnitt 2 Grundlagen:

- Betreiber von allen Betriebsbereichen haben **Änderungen von (Hochwasser-)Gefahren- und Risikokarten sowie Starkregengefahren- und -risikokarten** im Rahmen der Aktualisierung von Konzepten zur Verhinderung von Störfällen (§ 8 Absatz 4 Störfall- Verordnung) sowie bei der systematischen Überprüfung und Bewertung von Konzepten zur Verhinderung von Störfällen und Sicherheitsmanagementsystemen (Anhang III Nummer 2 Buchstabe g Störfall-Verordnung) umzusetzen.

Quelle: TRAS 310, z.B. https://www.kas-bmu.de/app.php/nachricht/tras-310.html

Klimawandel - Herausforderung für die funktionale Sicherheit?

- Hochwasserrisikobewertungskarten https://www.hochwasser.baden-wuerttemberg.de/



Endress+Hauser

Klimawandel - Herausforderung für die funktionale Sicherheit?

Was sagt das technische Regelwerk zum Klimawandel?

-> Aus der TRAS 310 Abschnitt 2 Grundlagen:

- **Als Auslegungsgröße für Schutzmaßnahmen soll grundsätzlich ein Klimaänderungsfaktor von 1,2** herangezogen werden, um die Folgen des Klimawandels von 2010 bis zum Jahr 2050 zu berücksichtigen (siehe Kapitel 7.3 und Anhang I), sofern von den zuständigen Behörden gemäß §§ 72 bis 81 WHG die Folgen des Klimawandels nicht bereits in den (Hochwasser-)Gefahren- und Risikokarten berücksichtigt wurden.
- Z.B. als Bemessungsfaktor bei Berücksichtigung von Hochwasserabfluss

Quelle: TRAS 310, z.B. https://www.kas-bmu.de/app.php/nachricht/tras-310.html

Klimawandel - Herausforderung für die funktionale Sicherheit?

Fazit aus dem technischen Regelwerk:

- Regelmässiges Überprüfen der Situation, dabei bei der Gefahrenquellenanalyse bzw. im Sicherheitskonzept auch Aspekte des Klimawandels und deren Einfluss berücksichtigen.
- Anpassen der vorhandenen Gefährdungsbeurteilungen, nicht nur Überschwemmungen durch Flüsse, sondern auch Starkregen berücksichtigen, ggf. häufiger und intensiver auftretend.
- TRAS 320, TRAS 310 berücksichtigen (TRAS 310: Klimaanpassungsfaktor 1,2)
- Regelmässige Überprüfung nach Störfallverordnung ohnehin erforderlich.
- Weil die Häufigkeit dieser Ereignisse sehr wahrscheinlich zunehmen wird: Evtl. auch für andere Anlagen und Betriebe, welche zwar nicht der Störfallverordnung unterliegen, aber Sicherheitseinrichtungen betreiben*
- Dazu gibt es viele Hilfestellungen seitens der Umweltämter, der Landkreise und der Kommunen.

* TRAS 310 gilt für Betriebsbereiche im Anwendungsbereich der Störfall-Verordnung. Es wird aber in Abschnitt 3 “Anwendungsbereich” der TRAS 310 empfohlen, diese ausweitend anzuwenden, wo Freisetzung gefährlicher Stoffe, Brände oder Explosionen drohen!

Klimawandel - Herausforderung für die funktionale Sicherheit?

Hochwasser- und Starkregen Frühwarnsystem im Hochschwarzwald (Lenzkirch) im Test

- Autarkes Radar (FWR30, batteriegespeist, online-Anbindung) misst Flusspegel
- Grenzwertalarmierung via E-Mail
- Weiterentwicklungen des Systems in Arbeit (Kombination mit weiteren Sensoren + KI)

Micropilot FWR30

Video: https://www.youtube.com/watch?v=PVBqVmLz-fo

Klimawandel - Herausforderung für die funktionale Sicherheit?

Herzlichen Dank für Ihre Aufmerksamkeit!

RAMSYS
DAS machen Ingenieure

Verständnis im Bereich Funktionale Sicherheit

Kann Funktionale Sicherheit nach Schema „F“ bearbeitet werden?

Persönliche Vorstellung

Kontaktdaten:
Hervester Straße 36
46286 Dorsten
Tel.: +49 (0)2369 / 74593-10
Mob: 0171 / 3037392
m.mast@ramsys.org
www.ramsys.org

- Malika Mast
- Geschäftsführerin
  - 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)

Inhaltsverzeichnis

RAMSYS
DAS machen Ingenieure

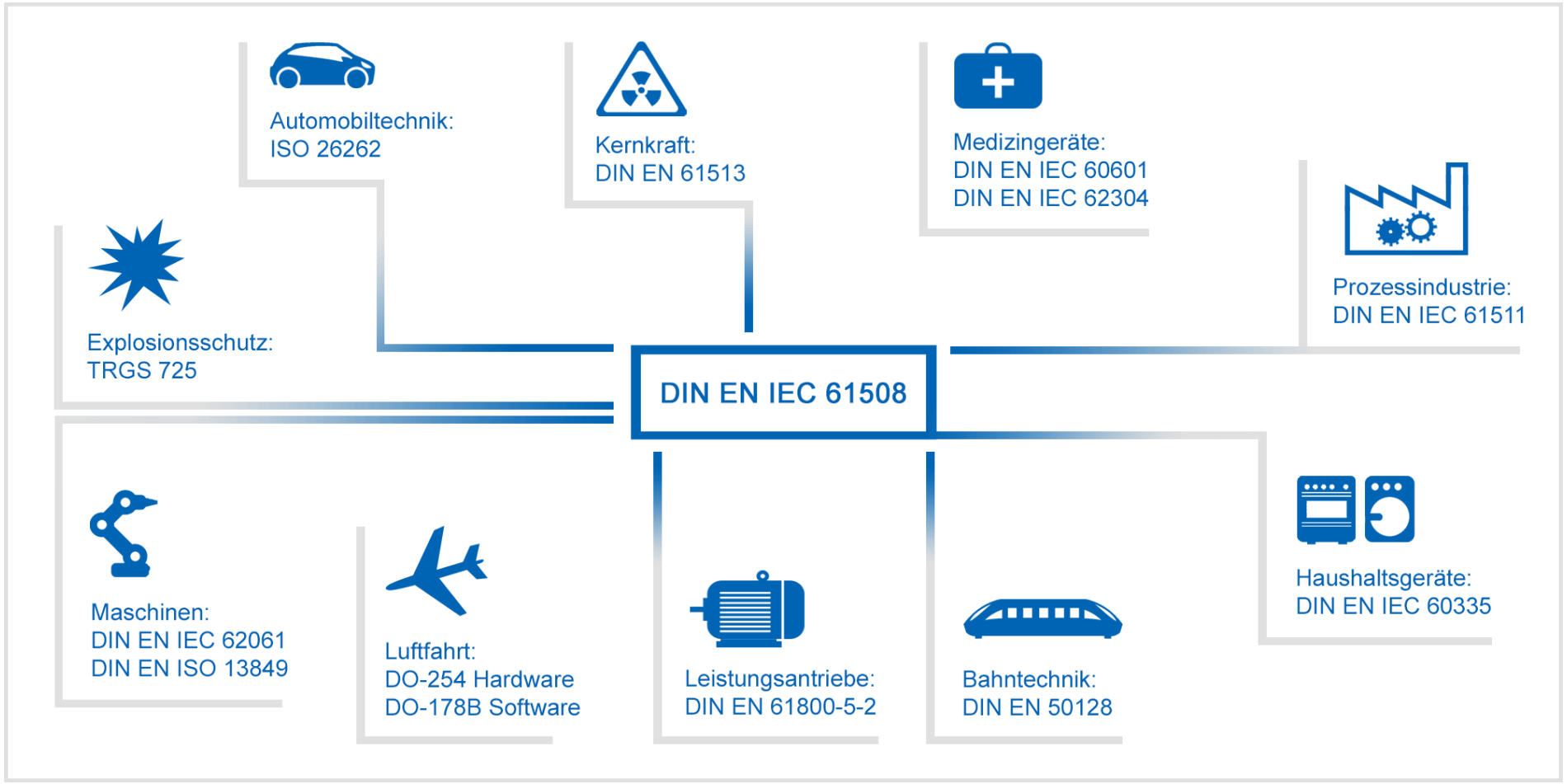
I. Grundlagen FuSi

(1) Normenübersicht

(2) Sicherheitslebenszyklus

(3) FSM

(1) Normenübersicht

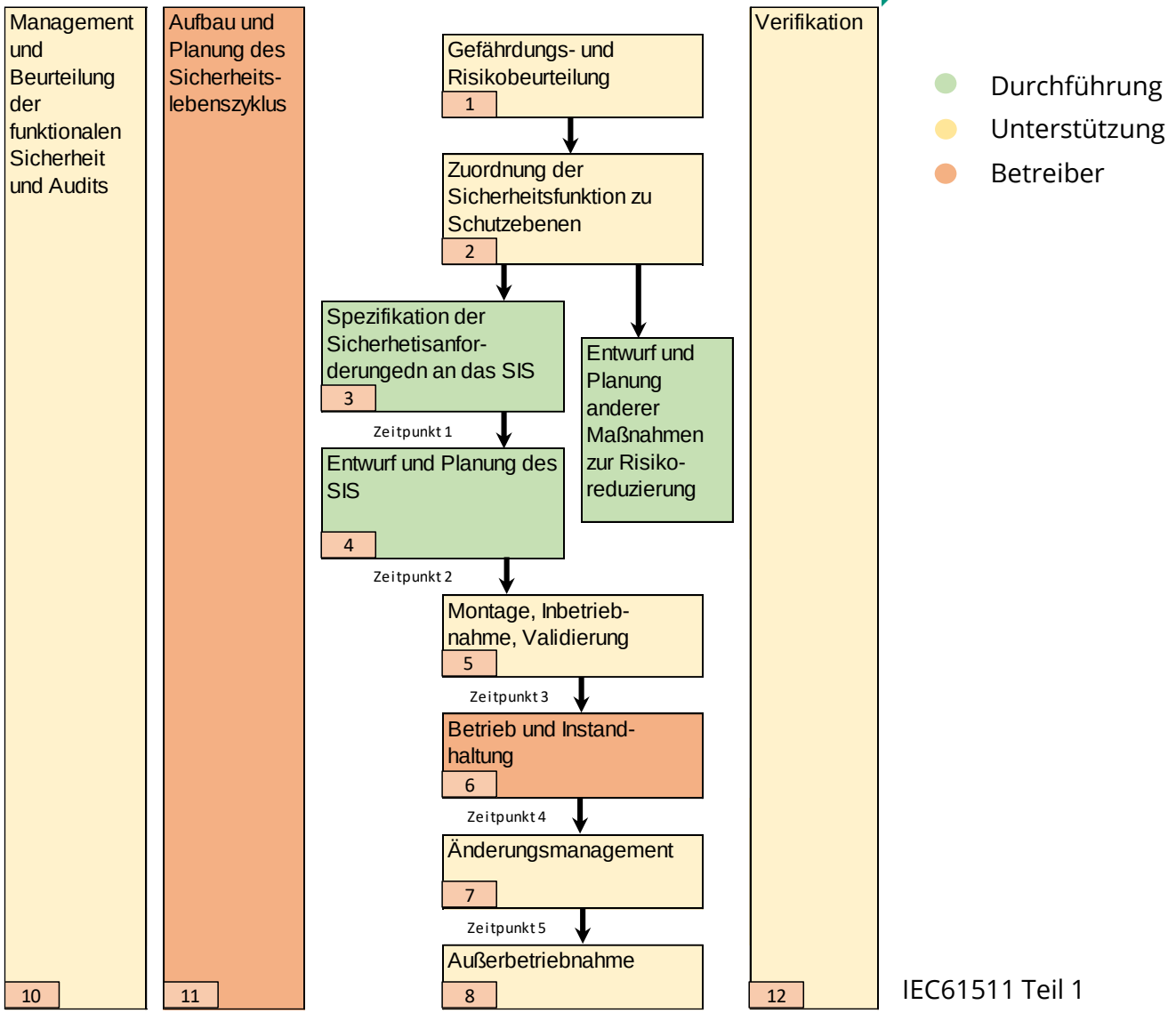


https://www.vde.com/tic-de/dienstleistungen/funktionale-sicherheit

(2) Sicherheitslebenszyklus

- Lebenszyklus nach IEC 61511-1 (2003), EU Standard

- Schema F?



(3) FSM

- Regelt den Ablauf des Sicherheitslebenszyklus im einem Unternehmen
  - Arbeitsanweisungen
  - Prozessbeschreibungen
  - Formblätter
  - Etc.

BESCHEINIGUNG ◆ ATTESTATION ◆ 证明书 ◆ СВИДЕТЕЛЬСТВО ◆ CONSTANCIA ◆ ATTESTAZIONE

TÜV SÜD Industrie Service

BESCHEINIGUNG

Hiermit wird bescheinigt, dass das Unternehmen

RAMSYS GmbH
Hervester Straße 36
46286 Dorsten
Deutschland

für die durch das Unternehmen durchgeführten Tätigkeiten, die den Sicherheitslebenszyklus eines Sicherheitstechnischen Systems betreffen, insbesondere

Planung, Programmierung, Montagebegleitung sowie Inbetriebnahmeunterstüzung

ein Managementsystem der Funktionalen Sicherheit gem.

DIN EN 61511-1, Abschnitt 5 u.
DIN EN 61508-1, Abschnitt 6

eingeführt hat und anwendet.

Dauer der Gültigkeit

siehe Auditbericht Br-ET-2946-2019-01 vom 23.09.2019

TÜV SÜD Industrie Service GmbH
Niederlassung Regensburg
Abteilung Elektro- und Gebäudetechnik

Regensburg, 2019-09-23

Christian Eberle

TÜV®

RAMSYS
DAS machen Ingenieure

II. Beispiel 1: Risikobeurteilung

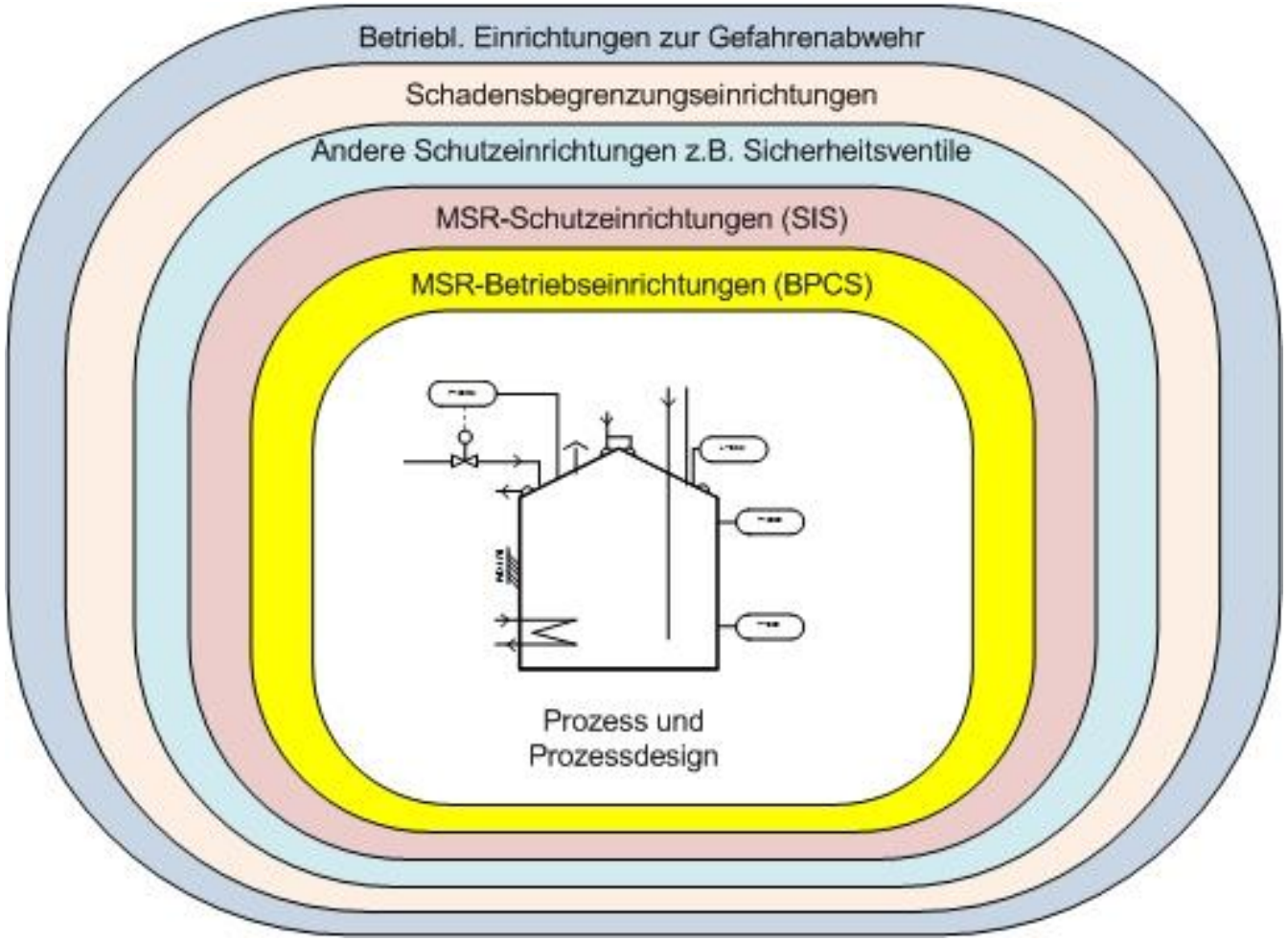
(1) Risikobeurteilung: LOPA

(2) Beispiel

(3) Ergebnis

(1) Risikobeurteilung

- LOPA
  - Layer of Protection Analysis
  - Baut auf eine von dem Unternehmen vorgegeben Risikomatrix mit fest beschriebenen Parametern und Einzelszenarien auf
  - Unterscheidet meistens zwischen Mensch / Umwelt und Wirtschaftlichkeit



https://www.leipholz.biz/lopa/

(2) Beispiel

- LOPA Szenario: Explosion Im Ofenraum
- Ursache: Falsche Verbrennung
- Einstufung:

Konsequenz auf	Kategorie	Beschreibung	TMEL (/yr)
Sicherheit	E	Ereignis führt zu 1 oder 2 Todesfällen	1,0E-04
Umwelt	H	Örtlich begrenzte Umweltschäden im BP Gelände, die in Wochen beseitigt werden	1,0E-01
Wirtschaftlichkeit	G	$50k -$500k	1,0E-01

- Ziel ist eine Risikoreduzierung von 1,0E-04

(2) Beispiel

- Gegenmaßnahmen (übertriebene Darstellung):
  - Betriebliche Abschaltung vorhanden (BPCS) = 1,0E-01
  - Geschultes Personal = 1,0E-01
  - Standardgeräte im Einsatz = 1,0E-01
  - Zusätzliche Diagnose (Stellungsrückmeldung) = 1,0E-01

- Damit ist der geforderte Wert von 1,0E-04 erreicht ohne eine PLT-Sicherheitseinrichtung

Konsequenz auf	Kategorie	Beschreibung	TMEL (/yr)
Sicherheit	E	Ereignis führt zu 1 oder 2 Todesfällen	1,0E-04
Umwelt	H	Örtlich begrenzte Umweltschäden im BP Gelände, die in Wochen beseitigt werden	1,0E-01
Wirtschaftlichkeit	G	$50k -$500k	1,0E-01

(3) Ergebnis

- Nach unserer Erfahrung sind zwei Dinge passiert, die mit einer anderen Methode nicht passiert wären
  - Das Kriterium Wirtschaftlichkeit wurde immer als erstes und mit höchster Priorität betrachtet.
  - Wie im Beispiel zu sehen, kann ich in einer LOPA a
    Katastrophe ohne eine Sicherheitsfunktion auskom
    entsprechend die Parameter vorher definiert habe

https://www.leipholz.biz/lopa/

RAMSYS
DAS machen Ingenieure

III. Weitere Beispiele

(1) Klassifizierungen

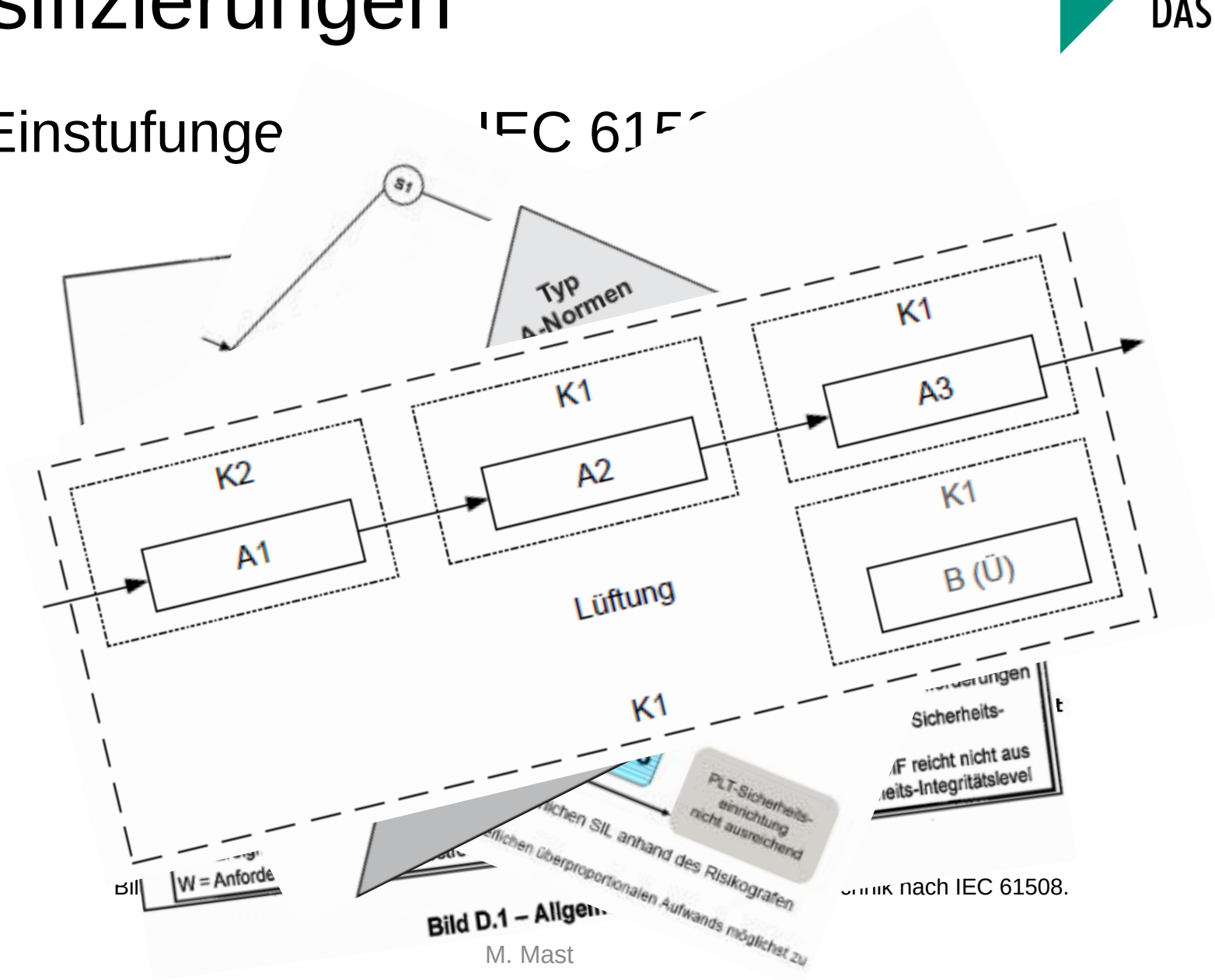
(2) Prüffristen

(3) SIL-Nachweisberechnung

(1) Klassifizierungen

- Standard Einstufunge IEC 61F

TRGS 725



nach IEC 61508.

(2) Prüffristen

- Meine PTC-Berechnung hat ergeben das ich “nur” alle 6 Jahre prüfen muss

Richtlinien / Normen / etc.	Angaben zur Wiederholungsprüfung
BetrSichV. (Ex-Schutz)	Anhang 2, Kapitel 5.2: alle 3 Jahre
Druckgeräterichtlinie	Alle 5 Jahre (Abweichung: Je nach Geräteart und Medium)
WHG	Jährliche Prüfung
NE130 / NE93	Jährliche Prüfung
TRGS 725	Alle 3 Jahre, mit Verweis auf BetrSichV.
DGUV	Paragraph 5: Alle 4 Jahre

- Sind die 6 Jahre immer noch in Ordnung?

(3) SIL-Nachweisberechnung

RAMSYS
DAS machen Ingenieure

- Bei der Bestellung und Planung werden oft Punkte übersehen
  - Verschaltung der Geräte und die geforderte Redundanz bei SIL-3
  - Der Prozessanschluss und die dazugehörigen Verfahrensdaten müssen passen, nicht nur das einzelne Geräte
  - Gibt es besondere Anforderungen des Herstellers
  - Erreicht meine Schaltung Insgesamt den geforderten SIL? SIL ist keine Geräte Eigenschaft

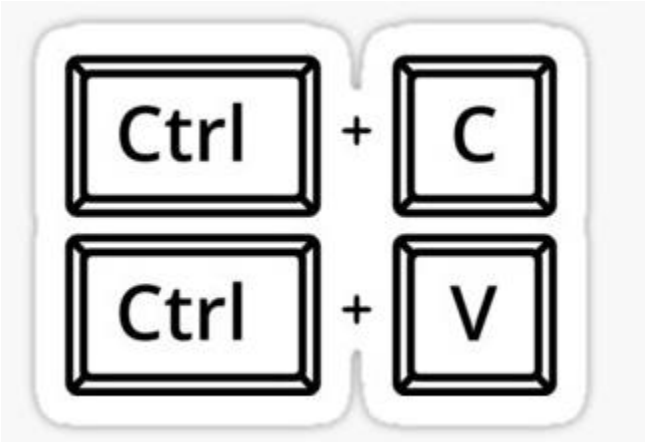
IV. Was bedeutet das?

(1) Fazit

(1) Fazit

- Gibt es Funktionale Sicherheit nach Schema “F” ?
  - In der Funktionalen Sicherheit sollte man nicht einfach kopieren
    - Die Funktionale Sicherheit entwickelt sich ständig weiter
  - Nichts alleine entscheiden (4 Augen-Prinzip)
  - Es gibt kein Schema „F“!

Arbeiten im Büro



RAMSYS
DAS machen Ingenieure

Danke für Ihre Aufmerksamkeit

Malika Mast

Geschäftsführerin

E-Mail: M.Mast@RAMSYS.org

Tel.-Nr.: +49 23 69 / 745 93 10

Mobil: 0171 3037395

BECKHOFF

Enhanced Channel Model for Safety Communication*

— Preserving the Black Channel —

Frank Schiller[1], Dan Judd[2], Peerasan Supavatanakul[3],
Tina Hardt[4], Felix Wieczorek[5]

[1]Beckhoff Automation GmbH & Co. KG; [2]Arlington Laboratory Corp.;
[3]TÜV SÜD Japan Ltd.; [4]Arendar IT-Security GmbH; [5]Siemens AG, Cybersecurity

based on: Schiller, F. et al.: Enhancement of Safety Communication Model – Preserving the Black Channel Concept, Automatisierungstechnik (at), vol. 70, no. 1.

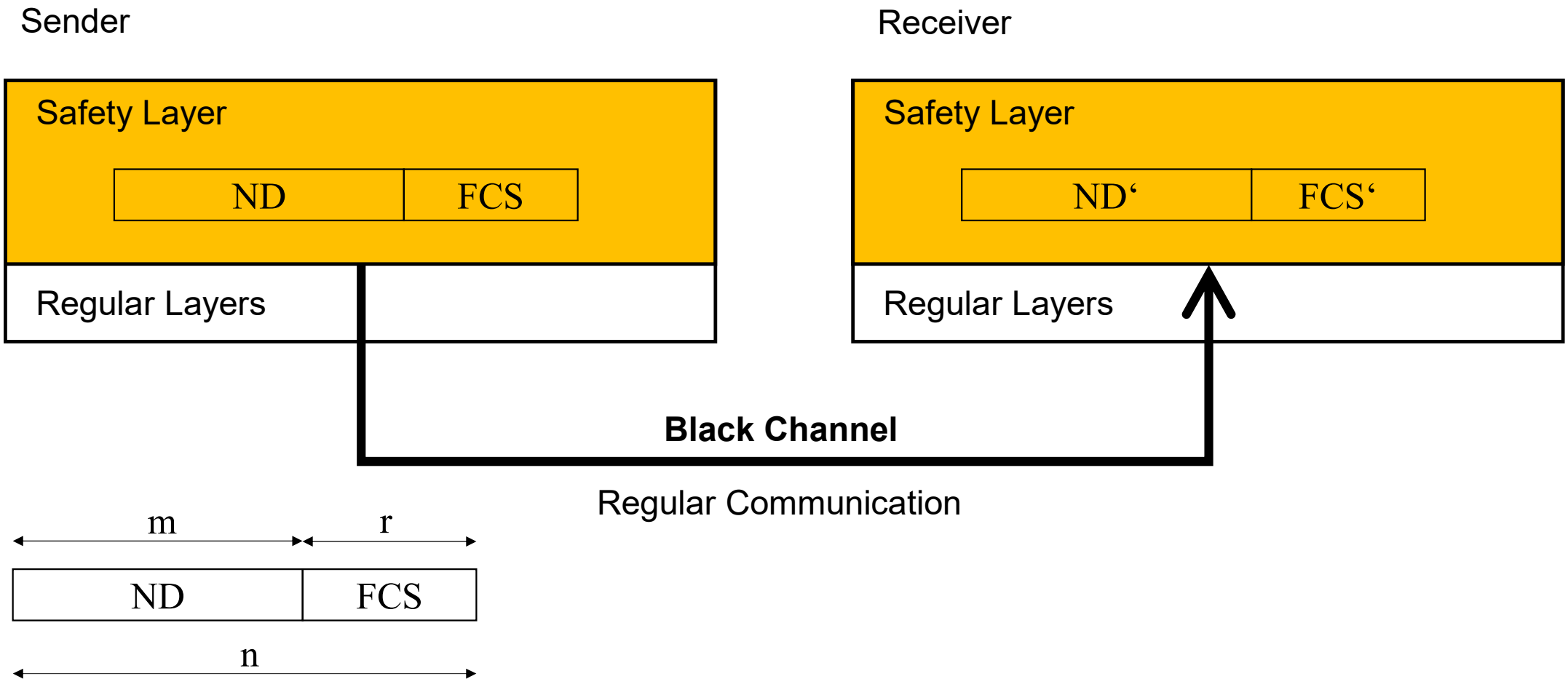
Enhanced Channel Model for Safety Communication

BECKHOFF

- Introduction
- Binary Symmetric Channel (BSC)
- Further Error Types
- Uniformly Distributed Segments (UDS)
- Result
- Conclusion

Introduction – Safety Communication

BECKHOFF



Enhanced Channel Model for Safety Communication

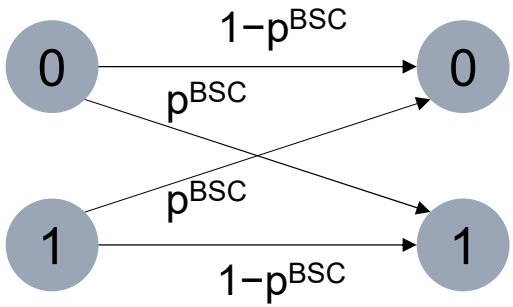
BECKHOFF

- Introduction
- Binary Symmetric Channel (BSC)
- Further Error Types
- Uniformly Distributed Segments (UDS)
- Result
- Conclusion

Binary Symmetric Channel

BECKHOFF

- **Binary Symmetric Channel (BSC)**
  - Each bit is erroneous independently of the others.
  - Each bit is erroneous with the same probability, the bit error probability p^{BSC}.
  - The falsification from value 0 to value 1 and the falsification from value 1 to value 0 occur with same probability.
  - For the probability p^{BSC}, $0 \leq p^{BSC} \leq 0.5$ holds.
  - IEC 61784-3 [1]: $0 \leq p^{BSC} \leq 0.01$
  - BSC is accepted if additional deterministic criteria are fulfilled:
    - Hamming Distance
    - Detection of complete zero-messages
    - Detection of complete one-messages
    - Detection of inverted messages
    - …



Enhanced Channel Model for Safety Communication

BECKHOFF

- Introduction
- Binary Symmetric Channel (BSC)
- Further Error Types
- Uniformly Distributed Segments (UDS)
- Result
- Conclusion

Further Error Types

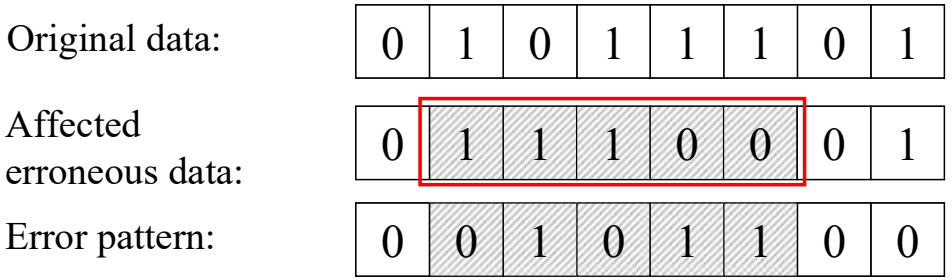
BECKHOFF

- **Non-BSC Errors by Origin**
  - Burst errors
  - Overwrite errors
  - Shift errors
  - Message length errors
  - Bit slipping errors
  - Masquerade errors

Further Error Types

BECKHOFF

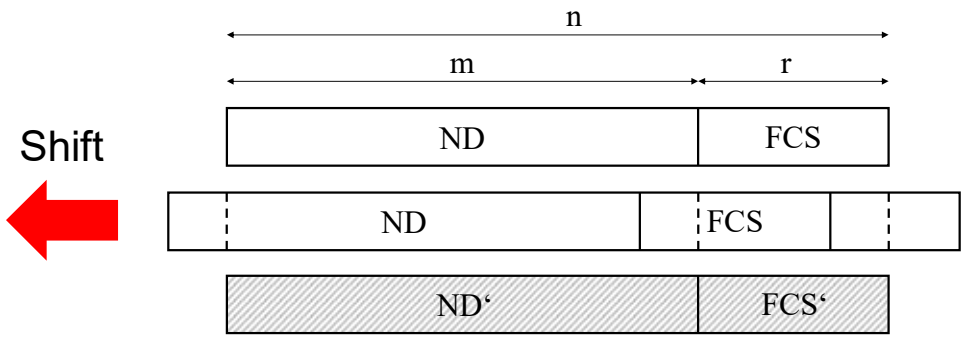
- **Non-BSC Errors by Origin**
  - Burst errors
  - Overwrite errors
  - Shift errors
  - Message length errors
  - Bit slipping errors
  - Masquerade errors



Further Error Types

BECKHOFF

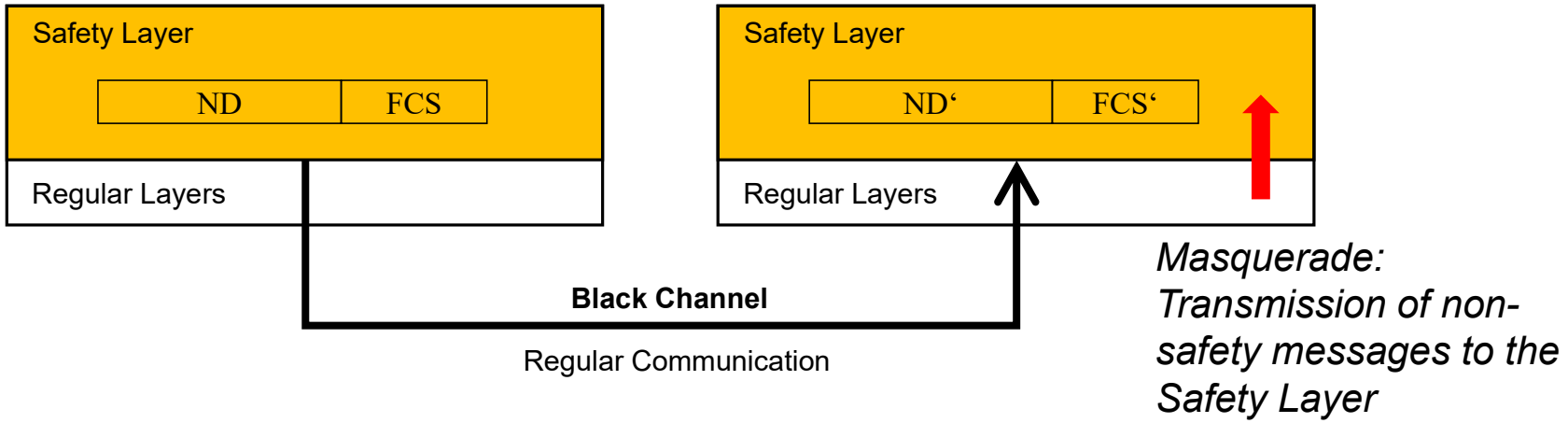
- **Non-BSC Errors by Origin**
  - Burst errors
  - Overwrite errors
  - Shift errors
  - Message length errors
  - Bit slipping errors
  - Masquerade errors



Further Error Types

BECKHOFF

- **Non-BSC Errors by Origin**
  - Burst errors
  - Overwrite errors
  - Shift errors
  - Message length errors
  - Bit slipping errors
  - Masquerade errors

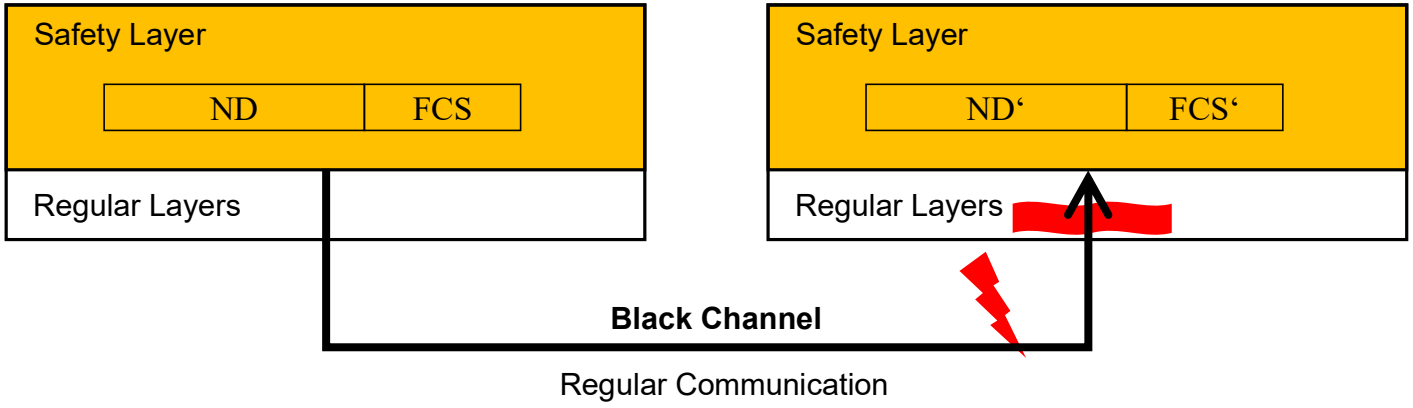


Further Error Types

BECKHOFF

- **Non-BSC Errors as result of data processing in the channel**
  - Data errors before bit destuffing
  - Data errors before symbol decoding
  - Data errors before decompression
  - Data errors before error correction
  - Data errors before decryption

BSC errors are modified by algorithms such that they are no BSC errors anymore.

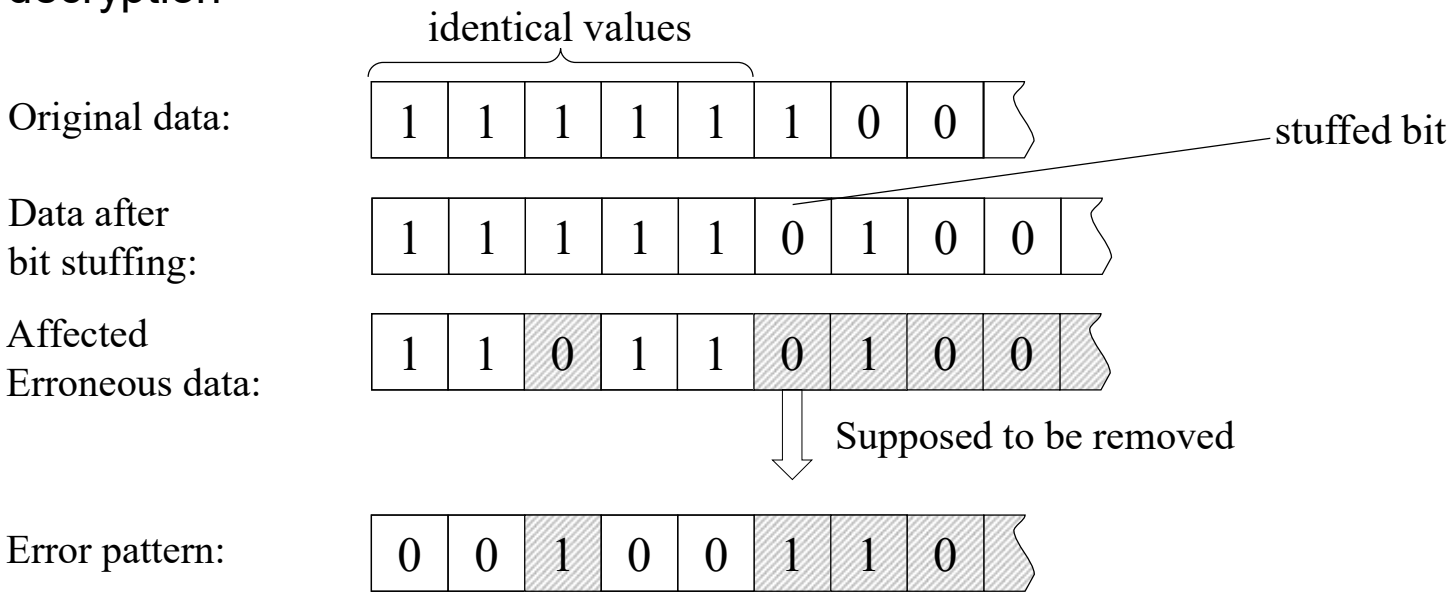


Further Error Types

BECKHOFF

- **Non-BSC Errors as result of data processing in the channel**
  - Data errors before bit destuffing
  - Data errors before symbol decoding
  - Data errors before decompression
  - Data errors before error correction
  - Data errors before decryption

BSC errors are modified by algorithms such that they are no BSC errors anymore.

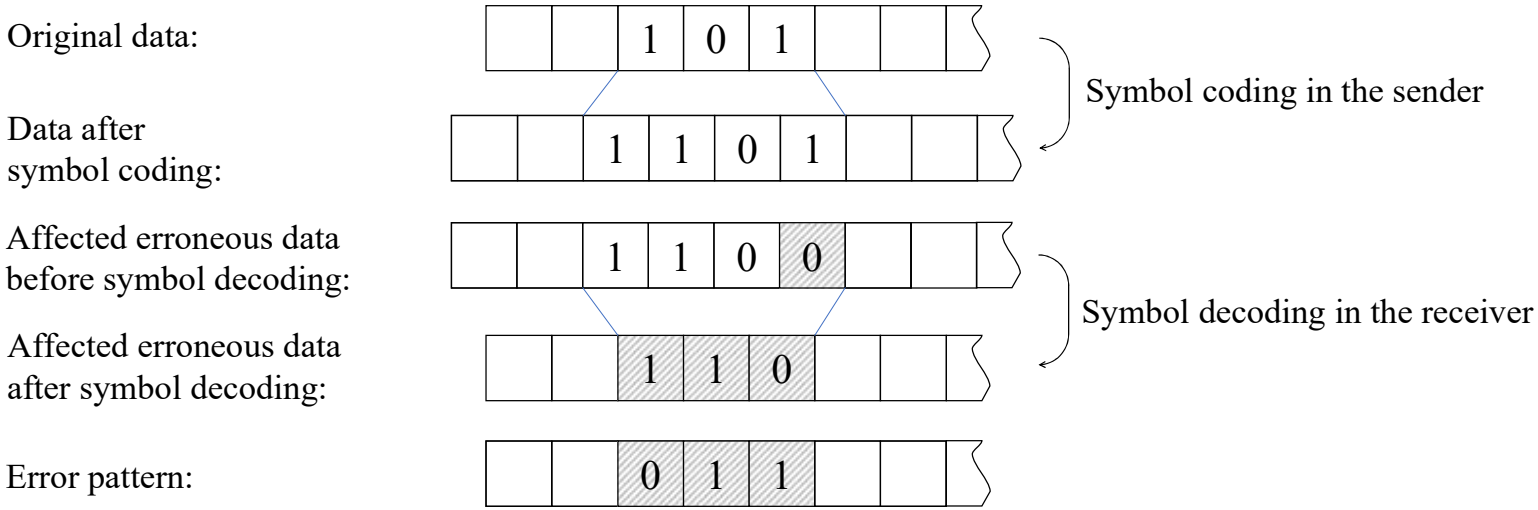


Further Error Types

BECKHOFF

- **Non-BSC Errors as result of data processing in the channel**
  - Data errors before bit destuffing
  - Data errors before symbol decoding
  - Data errors before decompression
  - Data errors before error correction
  - Data errors before decryption

BSC errors are modified by algorithms such that they are no BSC errors anymore.



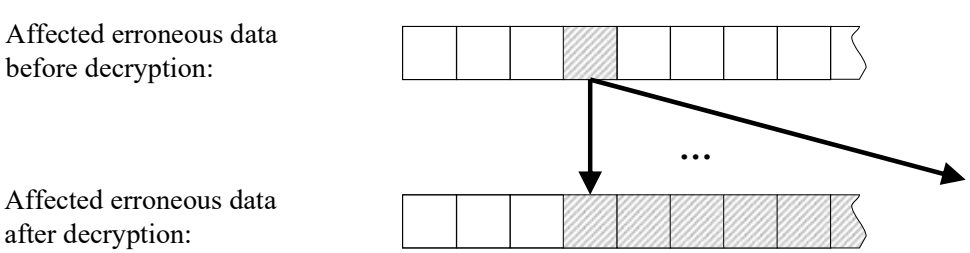
Further Error Types

BECKHOFF

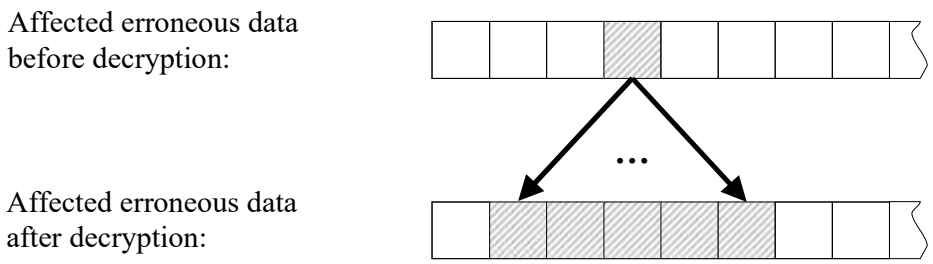
- **Non-BSC Errors as result of data processing in the channel**
  - Data errors before bit destuffing
  - Data errors before symbol decoding
  - Data errors before decompression
  - Data errors before error correction
  - Data errors before decryption

The affected parts are uniformly distributed on purpose, i.e., BSC errors are no BSC errors anymore.

Chained decryption:



Block cipher:



Enhanced Channel Model for Safety Communication

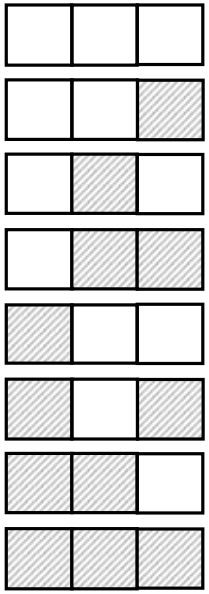
BECKHOFF

- Introduction
- Binary Symmetric Channel (BSC)
- Further Error Types
- Uniformly Distributed Segments (UDS)
- Result
- Conclusion

Uniformly Distributed Segments

BECKHOFF

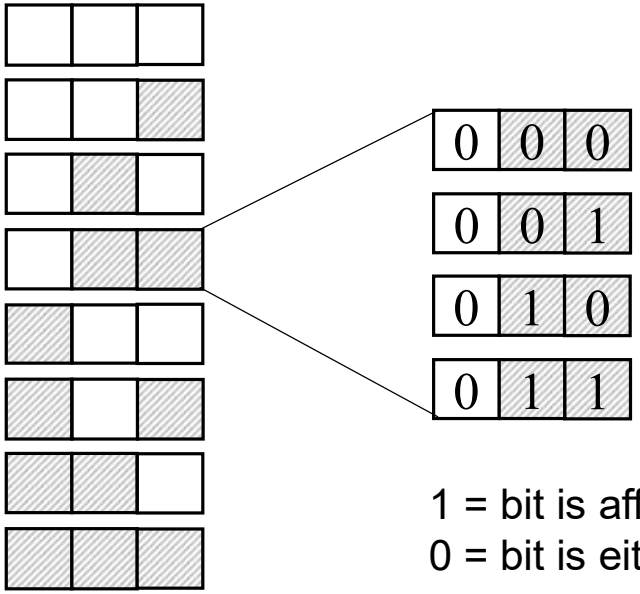
- All possible combinations of numbers, lengths, and positions of the segments occur with equal probability, such that the patterns of affected bits in the received message are uniformly distributed.



Uniformly Distributed Segments

BECKHOFF

- All possible combinations of numbers, lengths, and positions of the segments occur with equal probability, such that the patterns of affected bits in the received message are uniformly distributed.
- The error patterns within the affected segments of the patterns of affected bits caused are uniformly distributed.



1 = bit is affected and erroneous
0 = bit is either not affected or affected and correct

Enhanced Channel Model for Safety Communication

BECKHOFF

- Introduction
- Binary Symmetric Channel (BSC)
- Further Error Types
- Uniformly Distributed Segments (UDS)
- Result
- Conclusion

Result

BECKHOFF

- Residual Error Probability (cf. [2]):

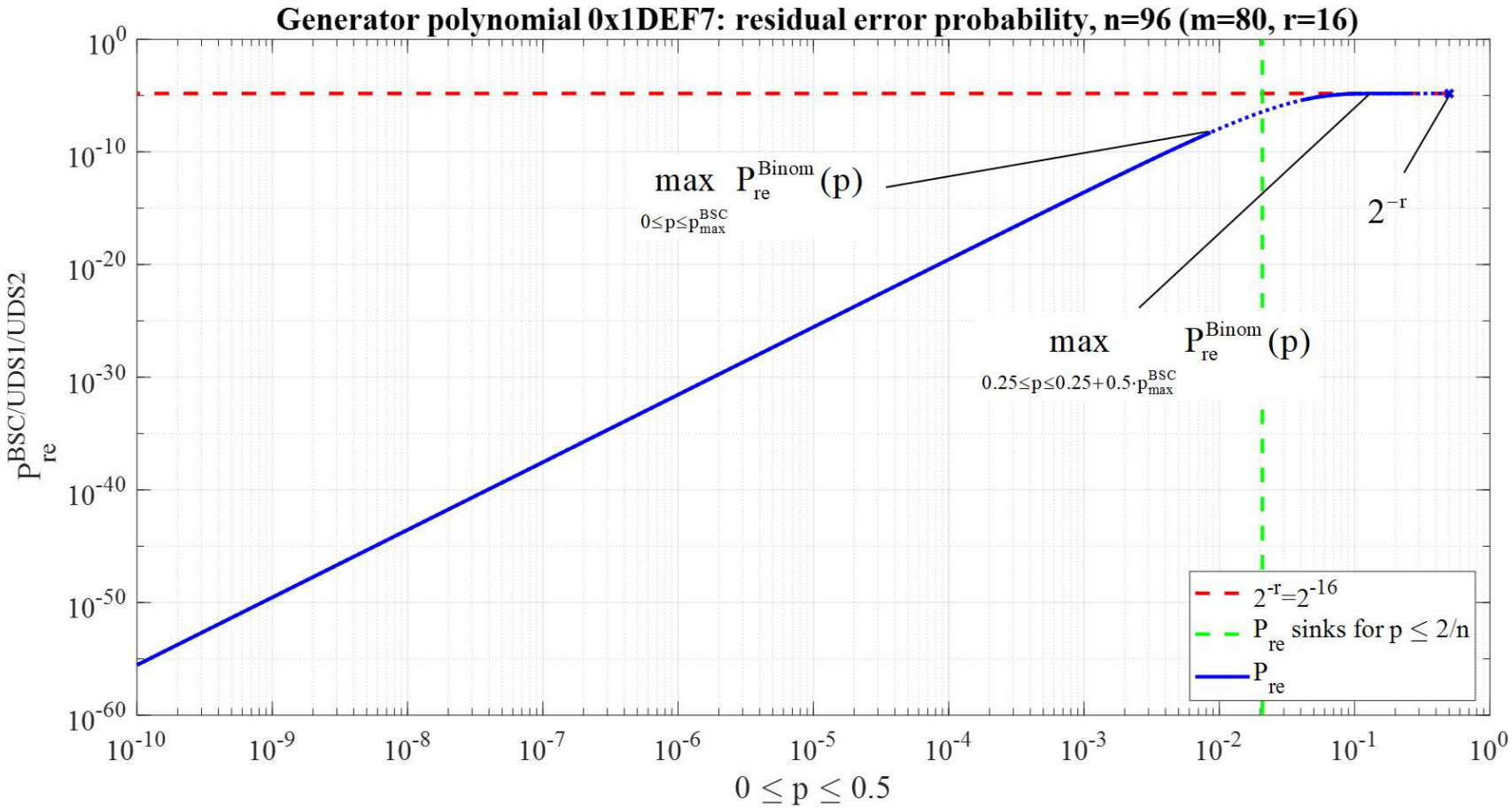
$$P_{re} \leq \max_{0 \leq p \leq p_{max}^{BSC}} P_{re}^{Binom}(p) \cdot (1 - P(f^{UDS})) + \max_{0 \leq p \leq 0.5} P_{re}^{Binom}(p) \cdot P(f^{UDS})$$

- Residual Error Probability if probability of occurrence of UDS faults is unknown (cf. [2]):

$$P_{re} \leq \max_{0 \leq p \leq 0.5} P_{re}^{Binom}(p) \qquad \Leftrightarrow P_{re} \leq \max_{0 \leq p^{BSC} \leq 0.5} P_{re}^{BSC}(p^{BSC})$$

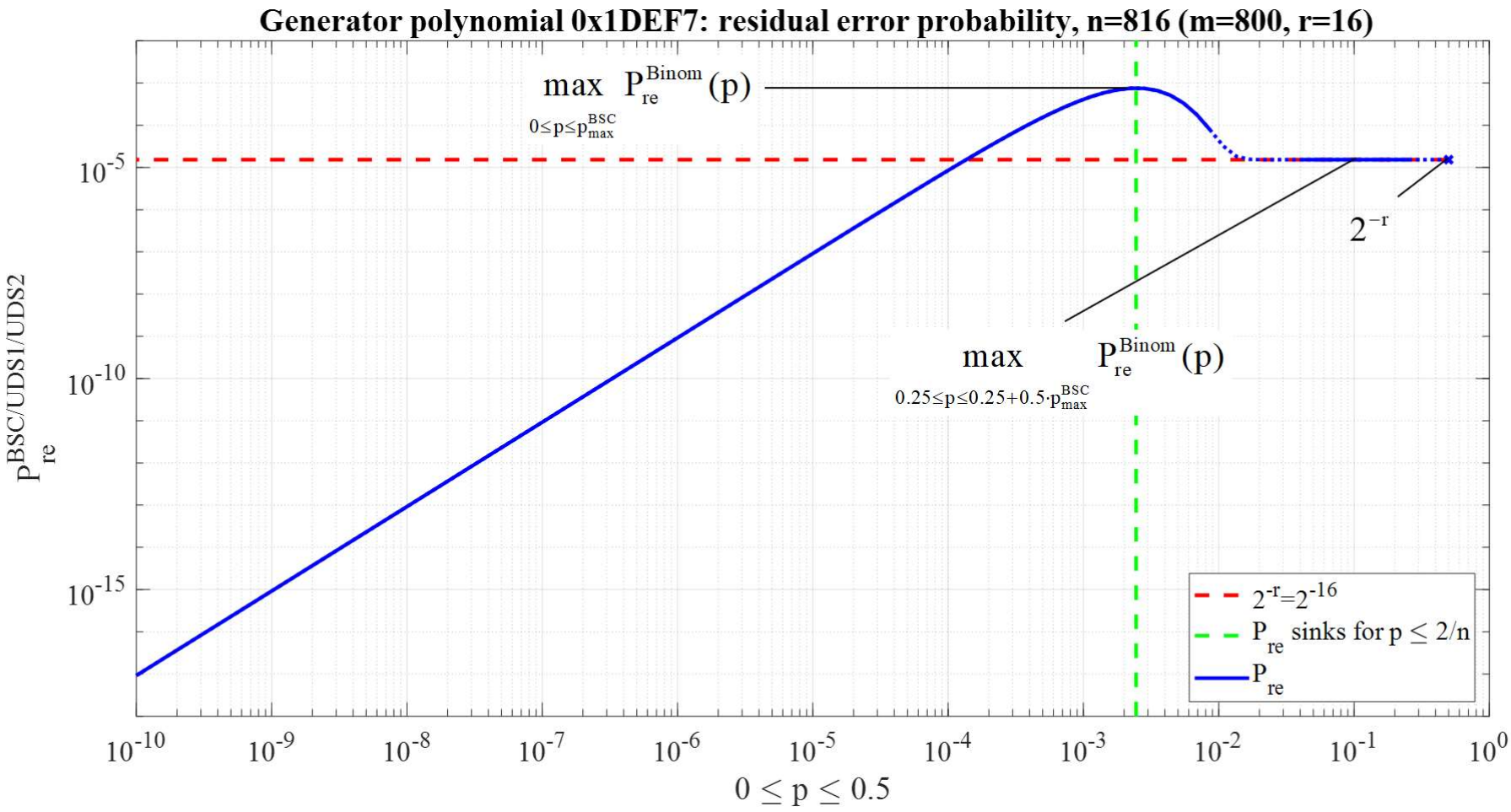
Result

BECKHOFF



Result

BECKHOFF



Enhanced Channel Model for Safety Communication

BECKHOFF

- Introduction
- Binary Symmetric Channel (BSC)
- Further Error Types
- Uniformly Distributed Segments (UDS)
- Result
- Conclusion

Conclusion

BECKHOFF

- The communication error model has to be broadened acc. to technical progress concerning implementations within the Black Channel.
- The model of Uniformly Distributed Segments (UDS) considers additional relevant error types.
- The resulting Residual Error Probability is practically identical to that one of BSC with bit error probability up to 0.5.
- Note, even if the BSC formula is applied, additional error types beyond BSC errors are included. The application of the parameter corresponding to bit error probability up to 0.5 ensures their inclusion. For example, value 0.5 does not mean that each second bit is erroneous!

References

BECKHOFF

[1] IEC 61784-3, Functional Safety Fieldbuses – General Rules and Profile Definitions, 2021

[2] Schiller, F., Judd, D., Supavatanakul, P., Hardt, T., and Wieczorek, F.: Enhancement of Safety Communication Model – Preserving the Black Channel Concept, Automatisierungs-technik (at), vol. 70, no. 1, Online ISSN: 2196-677X, Print ISSN: 0178-2312, pp. 38-52, https://doi.org/10.1515/auto-2021-0098, De Gruyter, 2022

[3] Schiller, F., Judd, D., Supavatanakul, P., Hardt, T., and Wieczorek, F.: A Broadened Channel Model for Safety-related Communication Errors, safe.tech – Funktionale Sicherheit in der Bahntechnik, Automatisierung und Automobiltechnik, TÜV SÜD Akademie, München, 2022

Der Analphabet und die Schreibmaschine

Achtung - Kalauer!

- „Verkäufer des Jahres“ eines Büromaschinen-Händlers zum Kunden:
  - *Gerade weil Sie nicht schreiben können brauchen Sie ja eine Schreib-MASCHINE …*

„Maschinen“ für die PFD-Berechnung

- Software-Tools für die PFD-Berechnung
  - *liefern immer ein Ergebnis*
  - *erzeugen oft beeindruckende Ausgaben mit vielen Seiten und bunten Bildern*
  - *bieten oft nicht die Möglichkeit, Ergebnisse im Detail nachzuvollziehen*
  - *müssen vom Anwender vollständig verstanden werden, um richtig angewendet zu werden*
  - *können in der Regel nur bestimmte Strukturen unter bestimmten Randbedingungen berechnen*
  - *verführen zuweilen dazu, Ergebnisse kritiklos zu akzeptieren*
  - *etc.*

Beispiel

- Eine nach ISO 13849 qualifizierte Logikeinheit soll in der Prozesstechnik eingesetzt werden
- Alle Angaben nach ISO 13849 liegen vor:
  - *Architektur entsprechend Kategorie 3*
  - *Diagnose-Deckungsgrad „mittel“*
  - *$MTTF_D$ = 13,4 Jahre*
  - *CCF wird erfüllt*
  - *PFH = 9,21E-7 1/h*
  - *Performance Level d*

Anwendung eines Tools zur PFD-Berechnung

Mission Time [years]	15
Startup Time [hours]	24
Demand Rate	Low Demand
Comments and Assumptions	

Navigation

Safety Instrumented Function Results

PFDavg Contribution

Achieved Safety Integrity Level	TBD
Safety Integrity Level (PFDavg)	TBD
Safety Integrity Level (Architectural Constraints)	TBD
Safety Integrity Level (Systematic Capability)	TBD
Average Probability of Failure on Demand (PFDavg)	0.00E+00
Risk Reduction Factor (RRF)	0
Mean Time to Failure Spurious (MTTFS) [years]	∞

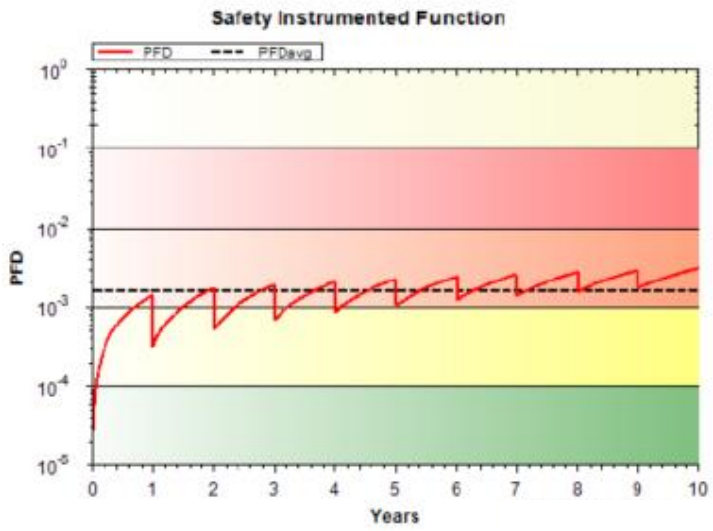
MTTFS Contribution

	PFDavg	MTTFS [years]	SIL PFDavg	SIL Limits	
				Arch. Const.	Sys. Cap.
Sensor Part	8.84E-03	6.78	TBD	2	0
Logic Solver Part	2.63E-04	963.9		3	3
Final Element Part	0.00E+00	∞		TBD	TBD

Final Element Part Incomplete

Group

Group Name	CVMS Element Voltage Deviation
Reuse this Group [Group used 1 time(s)]	MTTR [hours] 24
Group Voting: 1oo1	Proof Test: Interval [months] 12, Performed: Offline
	Coverage [%] 95

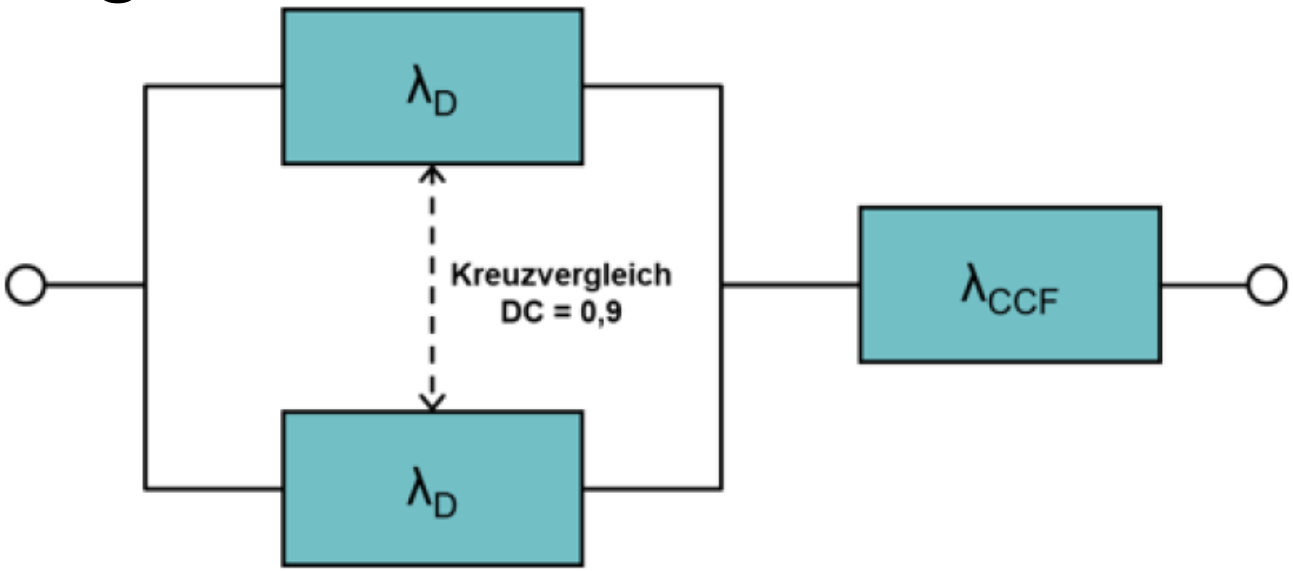


$PFD_{avg}=8{,}84\cdot10^{-3}$

Was bedeuten die Angaben nach ISO 13849?

- Eine nach ISO 13849 qualifizierte Logikeinheit soll in der Prozesstechnik eingesetzt werden
- Alle Angaben nach ISO 13849 liegen vor:
  - *Architektur entsprechend Kategorie 3 (Redundant mit Kreuzvergleich)*
  - *Diagnose-Deckungsgrad „mittel“ (DC = 90%)*
  - *$MTTF_D$ = 13,4 Jahre ($MTTF_D$ eines Kanals)*
  - *CCF wird erfüllt (β = 2%)*
  - *PFH = 9,21E-7 1/h (PFH = PFD(t = 20 Jahre) / 20 Jahre)*
  - *Performance Level d (Risikominderung entspricht SIL 2)*

Richtige Lösung



$$PFD_{avg}(T) := 2 + \frac{4\cdot\lambda_{DU}^{2}\cdot\left(1 - e^{-\lambda_D\cdot T}\right) - \lambda_D^{2}\cdot\left(1 - e^{-2\cdot\lambda_{DU}\cdot T}\right)}{2\cdot\lambda_D\cdot\lambda_{DU}\cdot\left(\lambda_D - 2\cdot\lambda_{DU}\right)\cdot T} - \frac{\left(1 - e^{-\lambda_{CCF}\cdot T}\right)}{\lambda_{CCF}\cdot T}$$

mit $\lambda_D := \frac{1-\beta}{MTTF_d}$ $\lambda_{DU} := (1 - DC)\cdot\lambda_D$ $\lambda_{CCF} := \frac{\beta}{MTTF_d}$

Ende gut, alles gut

Bild: Mohamed Hassan, Pixabay

Dr. Andreas Hildebrandt

Leiter Schulung / Gremienarbeit
Telefon +49 621 776-1454
Mobil +49 151-16222436
E-Mail ahildebrandt@de.pepperl-fuchs.com

Pepperl+Fuchs SE
Lilienthalstraße 200 | 68307 Mannheim | Deutschland

www.pepperl-fuchs.com