Die Präsentationen

Online-SIL-Slam am 30. September 2020

Programm

- **VDI/VDE 2180 Blatt 4** (Dirk Hablawetz, Marco Knödler, Gregor Schmitt-Pauksztat)
- **Zufällige Fehler bei der Mechanik** (Johann Ströbl)
- **Erfahrungen aus der Prüfpraxis** (Christoph Theilen)
- **Unabhängigkeit zwischen PLT-Betriebs- und Sicherheitseinrichtungen** (Jürgen Bode, Thorsten Lasrich)
- **Fehlersichere Kommunikation** (Frank Schiller)
- **Security** (Udo Menck)
- **KI in der funktionalen Sicherheit** (Michael Kindermann)
- **Sicherheitsfunktion bei UL-Drachen** (Stefan Lauer)
- **Ganzheitliches Risikomanagement** (Peter Sieber)
- **SIL aus Sicht eines Ingenieurbüros** (Malika Mast)
- **Reduzierungsstufe versus SIL** (Martin Herrmann)
- **Verfügbarkeit von Systemen** (Ivo Hanspach)
- **SIL im Maschinenbau** (Pascal Staub-Lang)
- **Falsche Symmetrisierungsformel** (Andreas Hildebrandt)

VDI/VDE 2180-4

Lieber systematisch richtig statt zufällig falsch!

2020-09-30

Hablawetz // Knödler // Schmitt-Pauksztat

Neulich…

SIL eines Fahrradschlosses

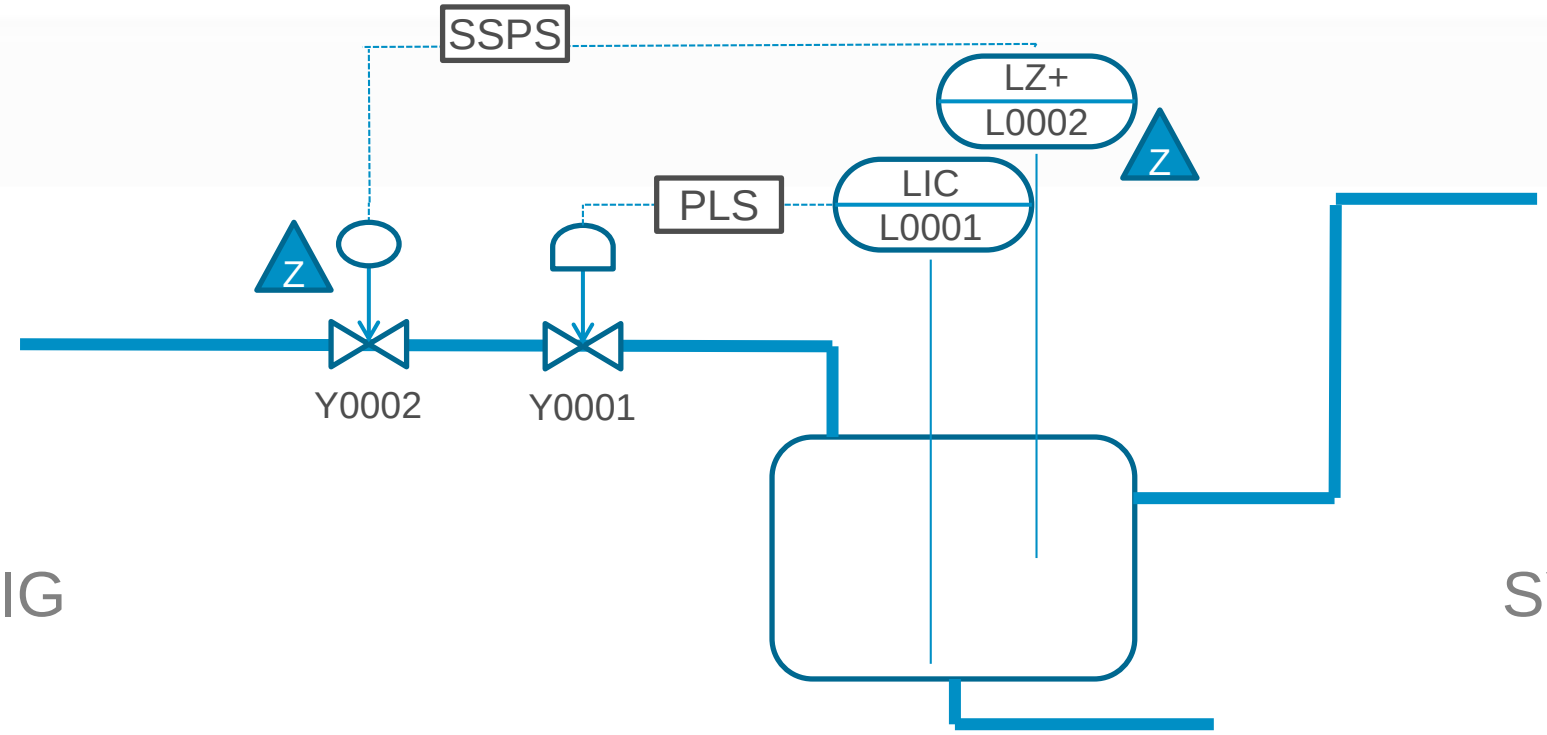
SIL (Safety Integrity Level) als Ordnungszahl der Risikoreduktion durch eine PLT-Sicherheitseinrichtung

SIL- jeweils als 10er-Potenz „sicherer“, ausgehend von zufällig verteilten Ereignissen

SIL	SIL 1	SIL 2	SIL 3	SIL 4
minimale Risikoreduktion (RRF)	10	100	1000	10000
maximale Ausfallwahrscheinlichkeit auf Anforderung (PFD)	1/10	1/100	1/1000	1/10000
in Worten: „eine von ... Sicherheitseinrichtungen würde im Anforderungsfall nicht funktionieren“	**zehn**	**hundert**	**tausend**	**zehntausend**

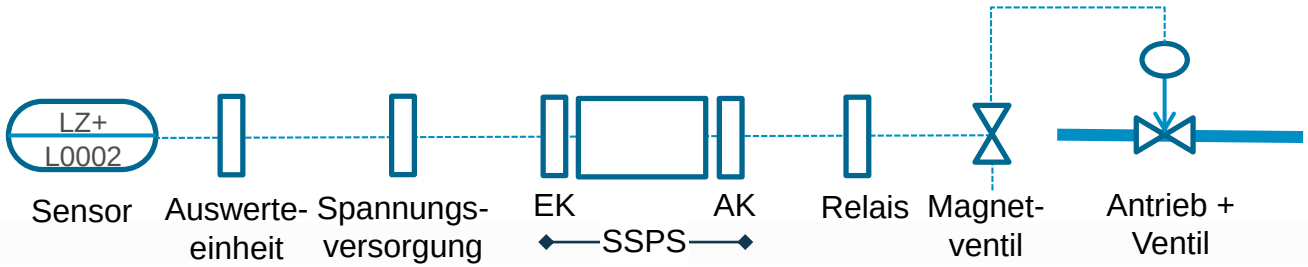
Annahme Anforderungsmodus (Probability of Failure on Demand):
Anforderung weniger als 1x pro Jahr (1 Jahr = 8760 Stunden)

Welche Fehler treten auf?

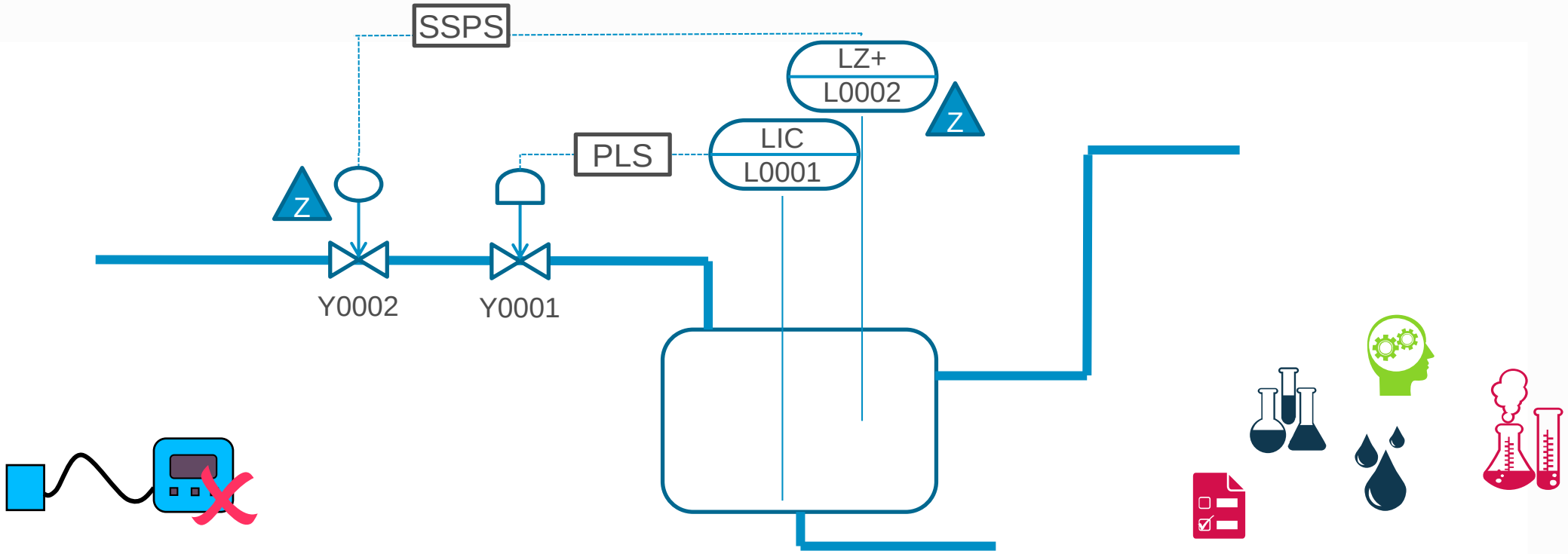


ZUFÄLLIG

SYSTEMATISCH



Systematisch oder zufällig?



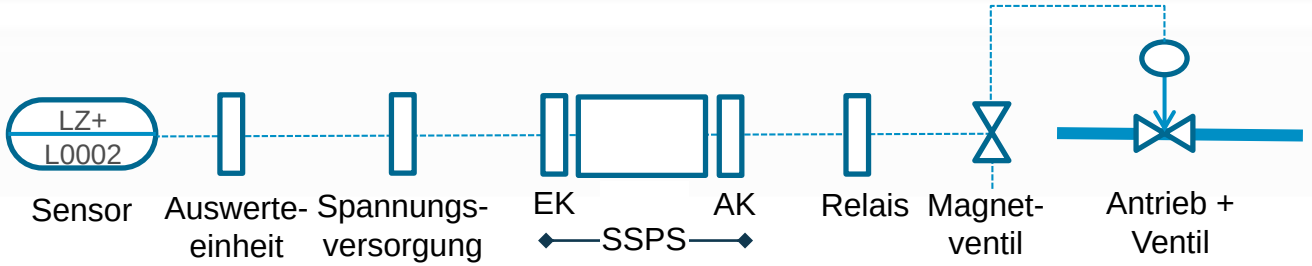
ZUFÄLLIG

SYSTEMATISCH

Zuordnung in NAMUR.smart

	Fehlerbilder	Fehlerursache		
#	Deutsch	Zufällig	Systematisch Engineering	Systematisch Betrieb
1	Interner Gerätefehler (nicht durch Medium verursacht)	x		
2	Alterung / Verschleiß	x		
3	Leitungsbruch/ Leitungsschluss	x		
4	Signal eingefroren	x		
5	Sonstiger zufälliger Fehler	x		
6	EMV		x	
7	Planungsfehler		x	
8	Montagefehler		x	
9	Produkteinflüsse		x	
10	Umwelteinflüsse		x	
11	Softwarefehler / Programmierfehler		x	
12	Konstruktionsfehler		x	
13	Sonstiger systematischer Fehler Engineering		x	
14	Korrosion			x
15	Bedienungsfehler			x
16	Unbefugter Eingriff / Manipulation			x
17	Nicht entfernte Überbrückung			x
18	Fehlerhafte Prüfanweisung			x
19	Zu hohe Messungenauigkeit, Signaldrift			x
20	Undichtigkeit im Durchgang			x
21	Undichtigkeit nach aussen			x
22	Blockieren der Mechanik			x
23	Sonstiger systematischer Fehler Instandhaltung			x

Rumrechnen



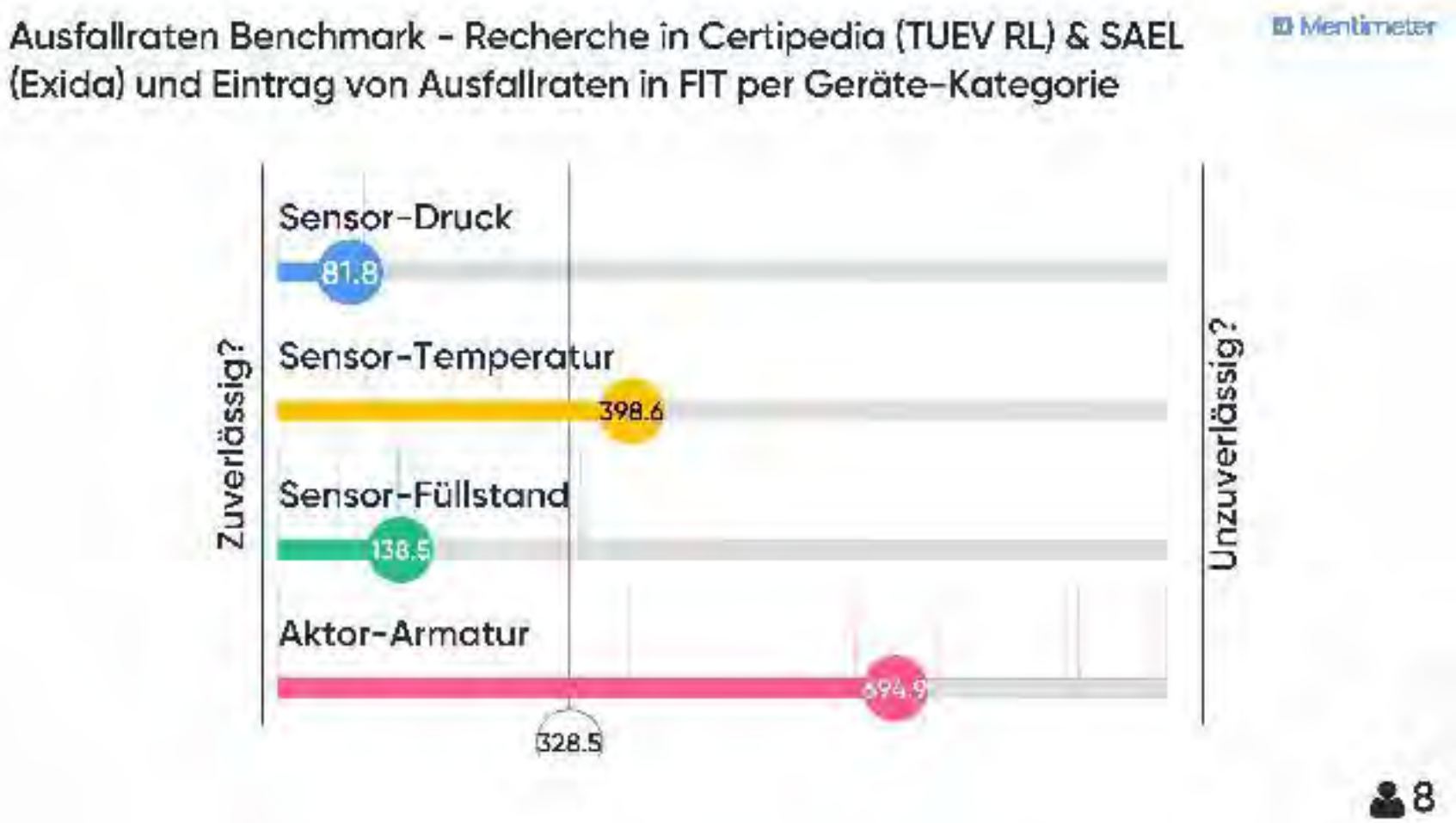
$$PFD_{1oo1,Gerät} = PTC_0 \boldsymbol{\lambda_{DU}} \frac{T_0}{2} + (PTC_1 - PTC_0) \boldsymbol{\lambda_{DU}} \frac{T_1}{2} + (1 - PTC_1) \boldsymbol{\lambda_{DU}} \frac{T_2}{2}$$

λ_{DU} = Rate gefährlicher (Dangerous) und unentdeckter (Undetected) Ausfälle in Failures In Time [FIT] = Ausfälle pro 10^9 Stunden

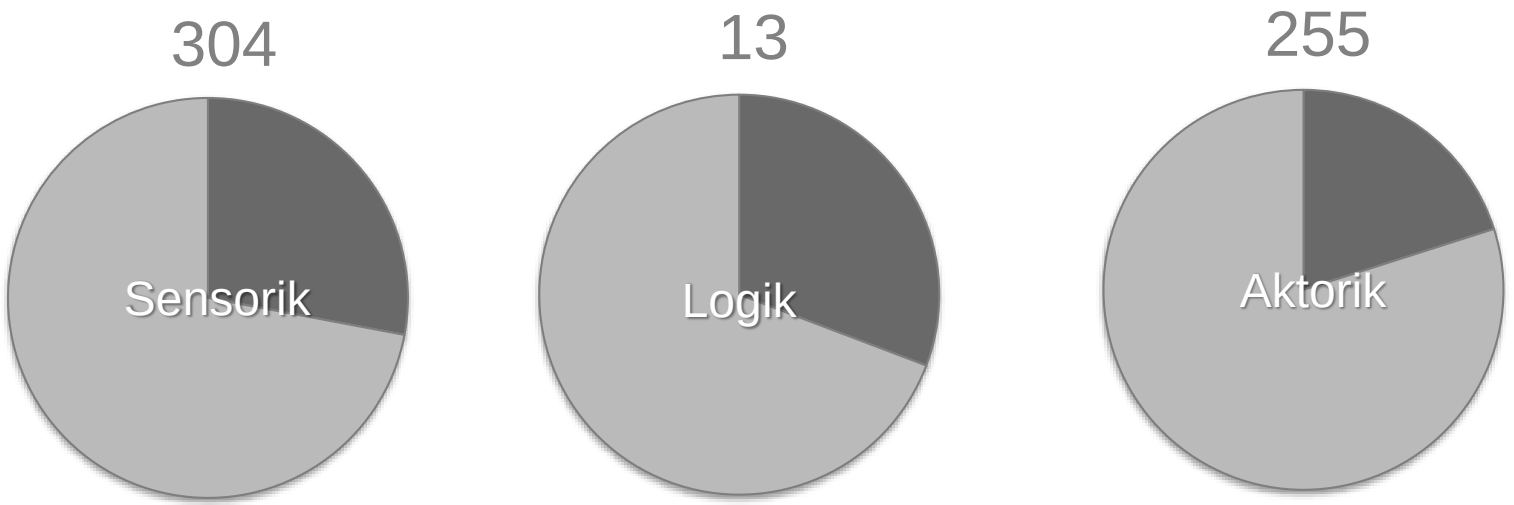
(1 Jahr = 8760 Stunden, 10^9 Stunden = 114.155,25 Jahre)

Annahme Anforderungsmodus (Probability of Failure on Demand):
Anforderung weniger als 1x pro Jahr

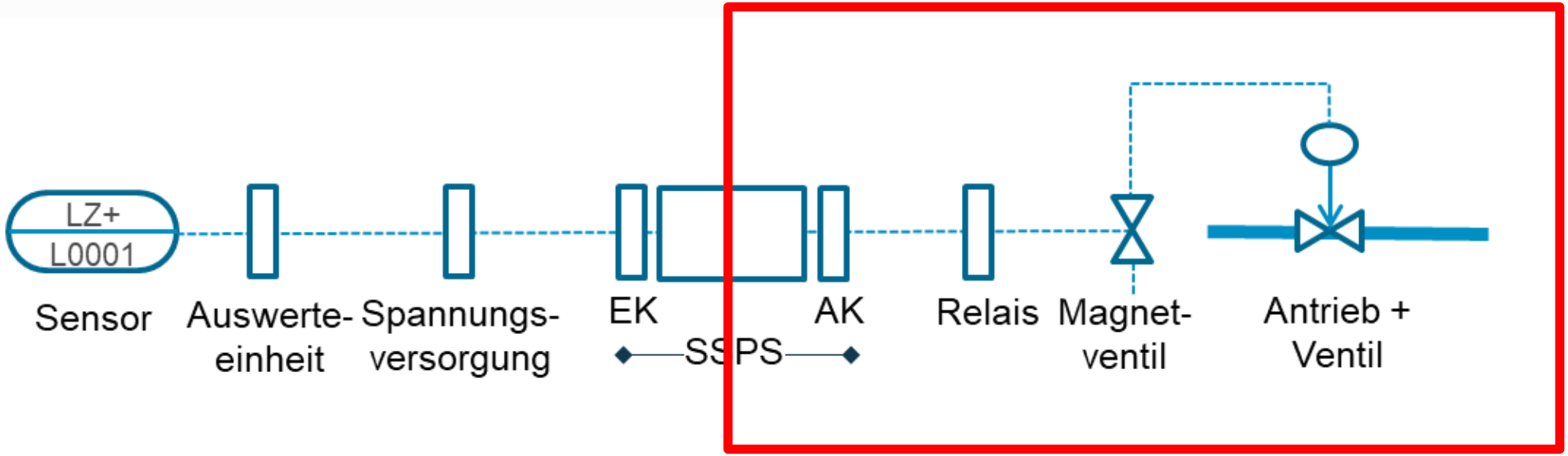
Literaturwerte



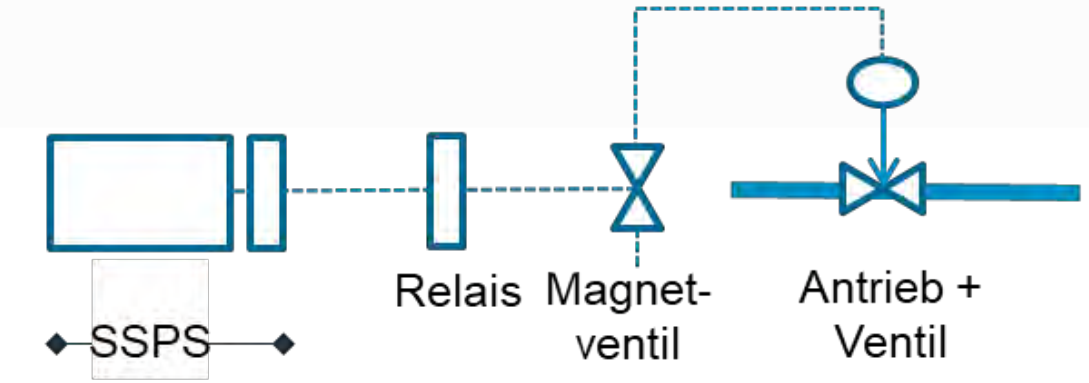
Realität



Neue VDI/VDE 2180-4



Neue VDI/VDE 2180-4



PFD von Hersteller

λ_{DU} von Hersteller

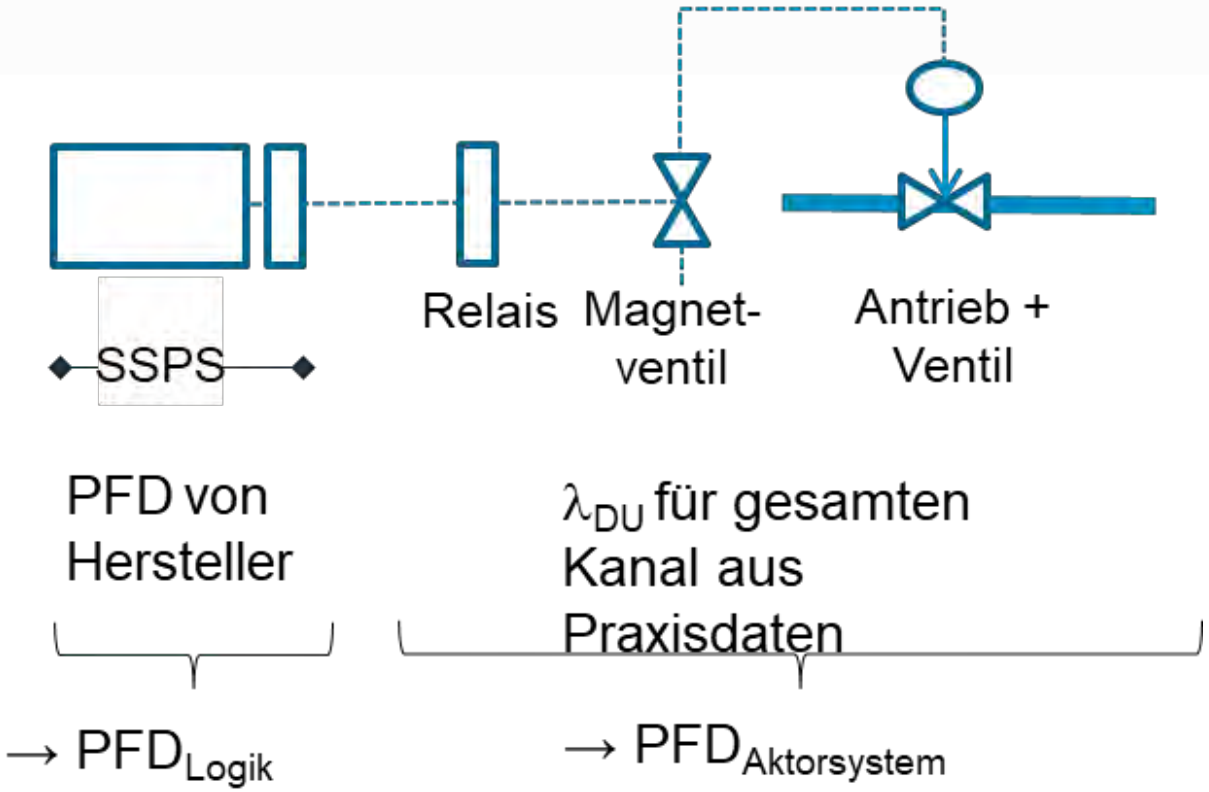
λ_{DU} von Hersteller

λ_{DU} von Hersteller

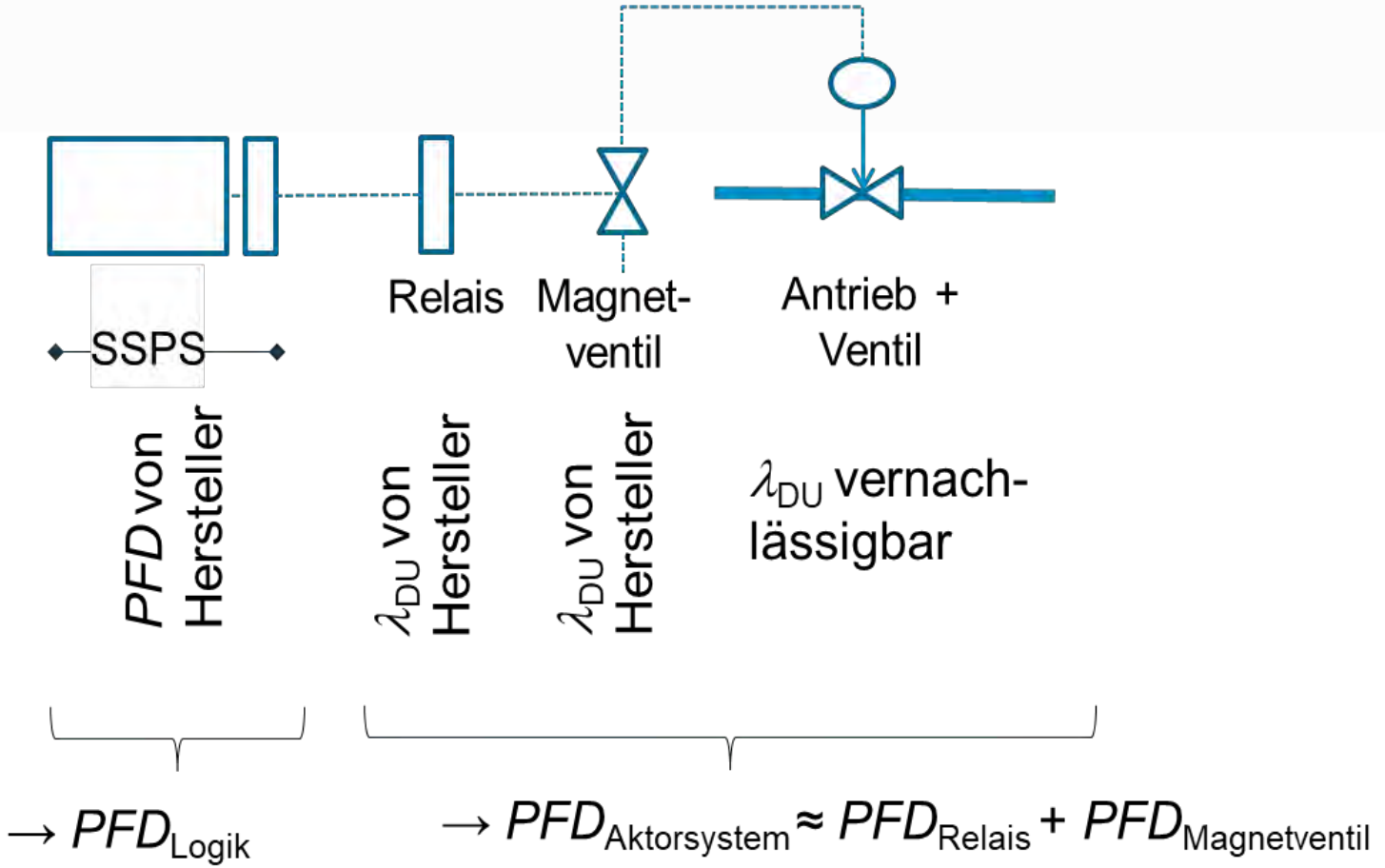
$\rightarrow PFD_{Logik}$

$\rightarrow PFD_{Aktorsystem} = PFD_{Relais} + PFD_{Magnetventil} + PFD_{Antrieb+Ventil}$

Neue VDI/VDE 2180-4



Neue VDI/VDE 2180-4



Lieber systematisch richtig als zufällig falsch!

Danke // Thanks

NAMUR@LinkedIN

NAMUR Homepage

Mechanische Komponenten in Sicherheitskreisen der Prozessindustrie

Die neue VDI 2180-4

Johann Ströbl

30. September 2020

Dipl. Ing. (FH) Johann Ströbl

Beratung Funktionale Sicherheit und
Sicherheit in der Feuerungstechnik

Gremienarbeit:

FA6.13	VDI/VDE 2180
ABS PG1	TRBS xxx „Funktionale Sicherheit“

Mobil 01520 2911795
mail to: johann.stroebl@online.de

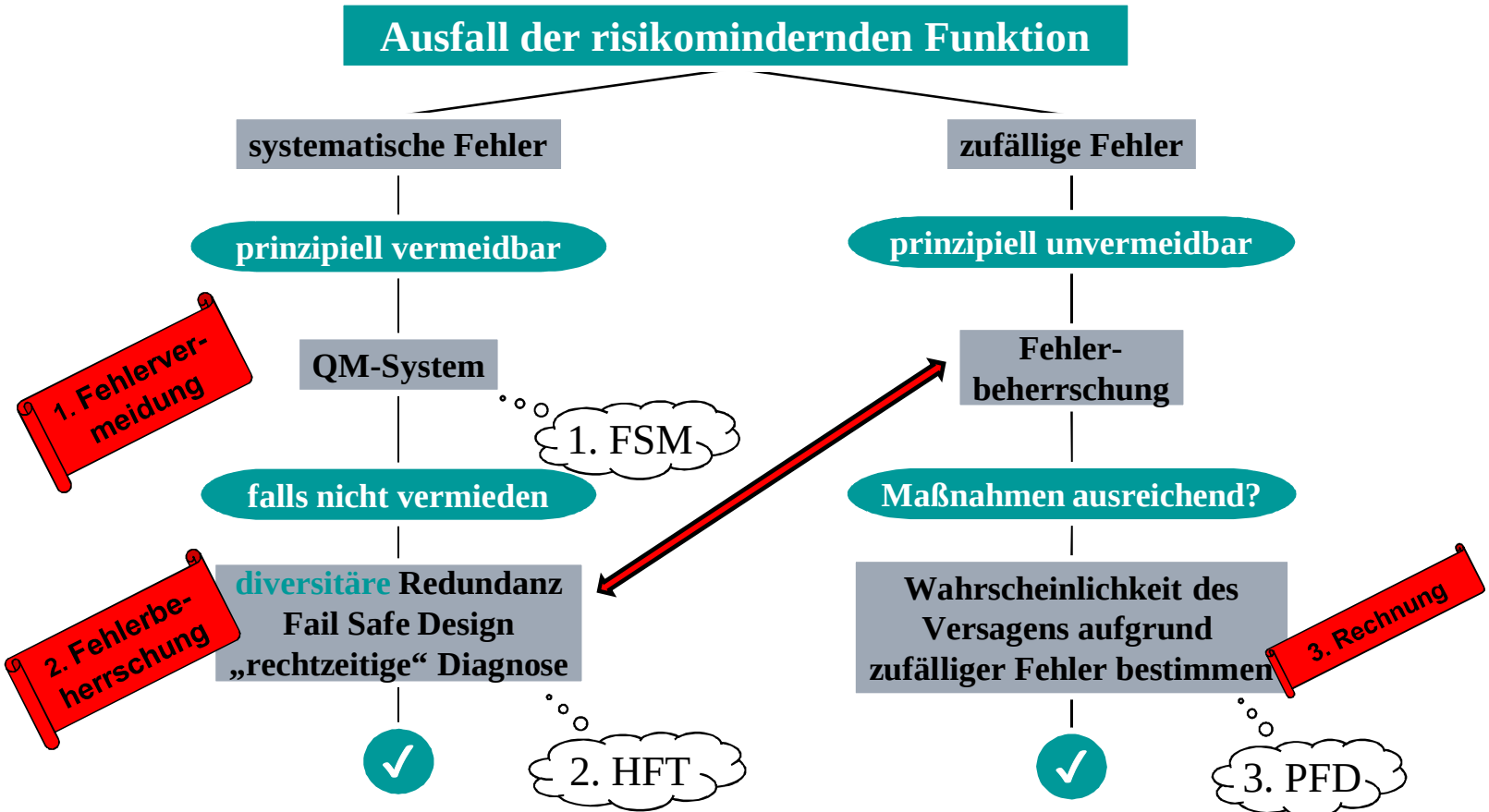
Fehlerdefinition nach VDI 2180 - 1

Fehler
Zustand in einer Funktionseinheit, durch den sie unfähig ist, eine geforderte Funktion zu erfüllen

- systematischer Fehler
Fehler mit grundsätzlich bestimmbarer und reproduzierbarer Ursache

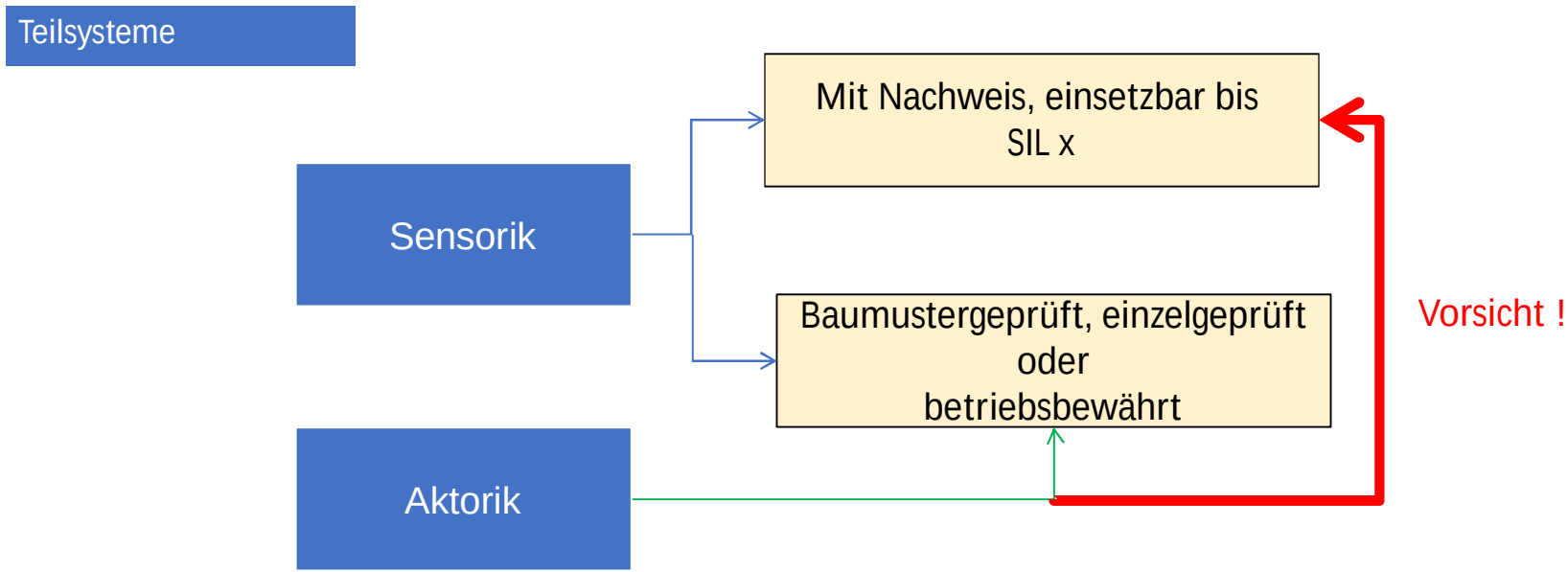
- zufälliger Fehler
Fehler mit nicht reproduzierbarer Ursache

Versagensursachen



Quelle: Dr. Andreas Hildebrandt, Pepperl+Fuchs

Welche Geräte sind geeignet?



Mögliche Eignungsnachweise für mechanische Komponenten in „SIL-Kreisen“

Baumustergeprüft, einzelgeprüft oder betriebsbewährt

Voraussetzungen für Einsatz von Geräten mit Baumusterprüfung, Einzelprüfung oder Betriebsbewährung

- Eignungsnachweis muss unter betriebs- oder betriebsähnlichen Bedingungen erbracht worden sein
- Ausfallsrichtung im Fehlerfall muss für das Gerät bekannt sein
- einkanalig einsetzbar in Sicherheitskreisen bis SIL 2, ab SIL 3 wird Redundanz erforderlich
- bei nachgewiesener Eignung und bestimmungs-gemäßem Einsatz ist Fehlerausschluss möglich. Keine Rechnung erforderlich – PFD=O

Dipl.-Ing. Univ. Christoph Theilen

Vertrieb, Bereichsentwicklung, Business Development

TÜV SÜD Industrie Service GmbH
Region Bayern
Friedenstraße 6
93051 Regensburg
Germany

Tel. 0941/9910 401
Fax 0941/9910 470
Mobil 0160 704 3804
mail to: christoph.theilen@tuev-sued.de

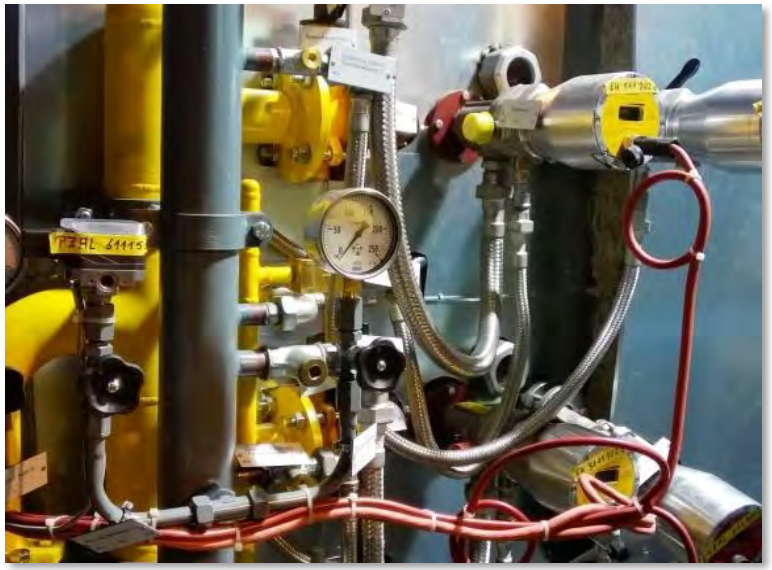
SIL SLAM

Letzte Möglichkeit Fehler zu finden bevor vielleicht ….

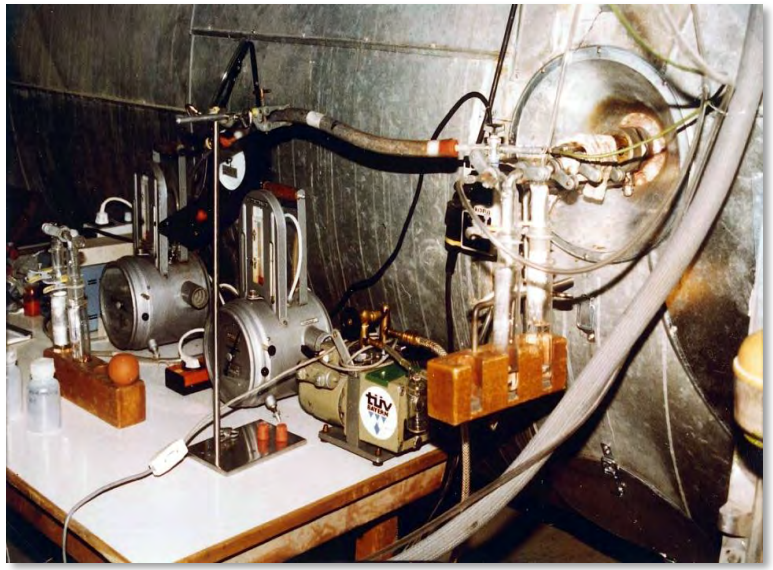
100 % Prüfung der Schutzeinrichtungen vom Sensor bis zum Aktor

visuelle Prüfungen

Funktionsprüfungen



Messungen



Grundlagenermittlung

1. visuelle Prüfung

Überprüfung der geforderten Merkmale und Eigenschaften der gelieferten Ausrüstungsteile und Bauelemente nach dem Einbau, wie z.B. :

- korrekte Komponenten
- spannungsfreier Einbau von Komponenten
- korrekte Einbaulage
- geeignete Dichtmaterialien
- Eignung für die Umgebungsbedingungen

2. Funktionsprüfungen

Überprüfung der korrekten Funktion der Sicherheitskreise:

- Prüfung so betriebsnah wie möglich durchführen
- Grenzwerte anfahren oder geeignet simulieren
- Berücksichtigung der Auflagen des zur Komponente gehörenden safety manual
- Prüfung vom Sensor bis zum Aktor

3. Messungen

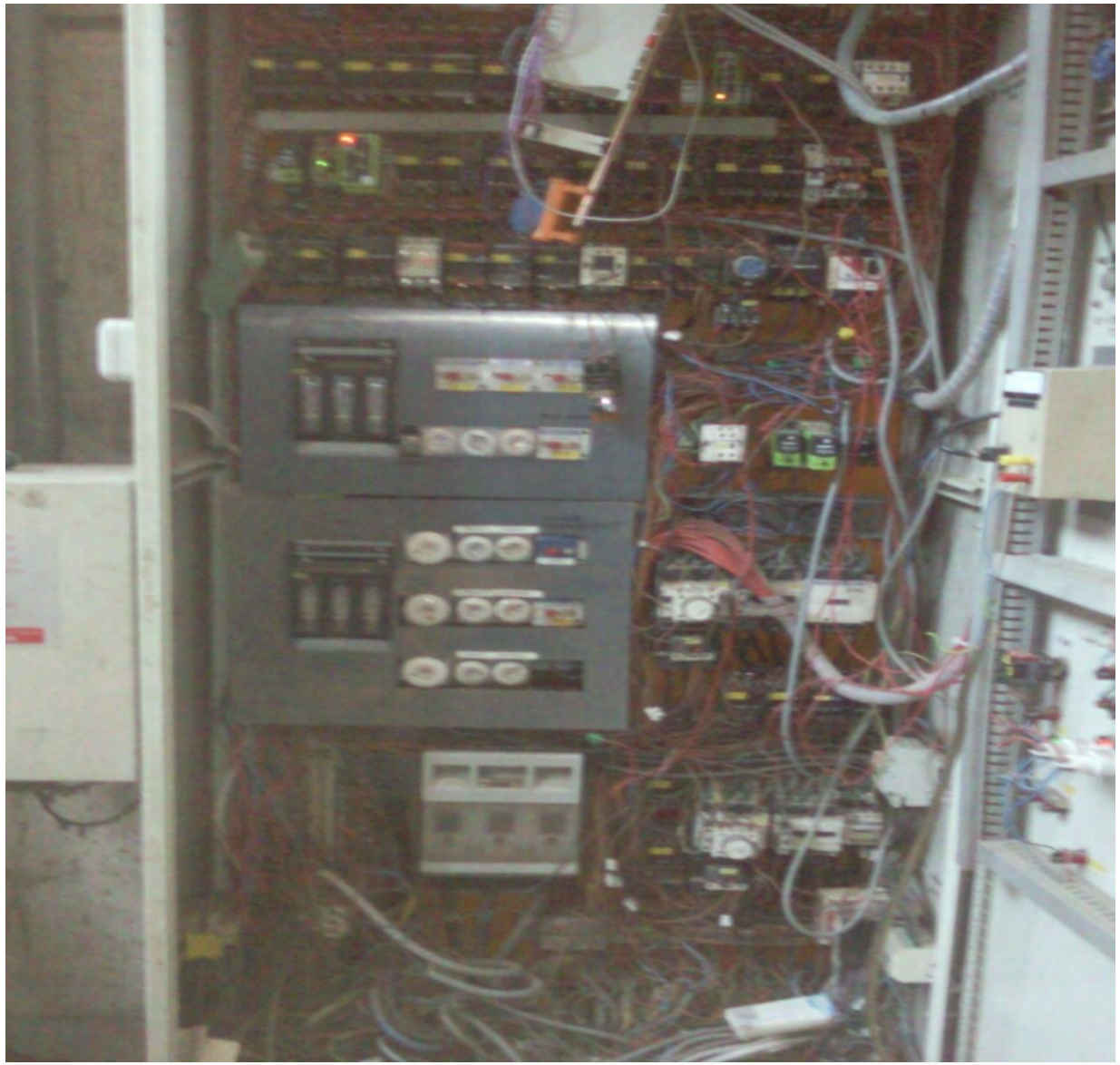
Überprüfung der spezifizierten Grenzwerte um die korrekte Funktion zu gewährleisten:

- z.B. Messung der Einbauposition der Überfüllsicherung

- z.B. Messung des MaxMax Schaltpunktes

- z.B. Messung der Schließzeit der Absperreinrichtungen

Damit bei Ihnen keine Schraube locker ist.

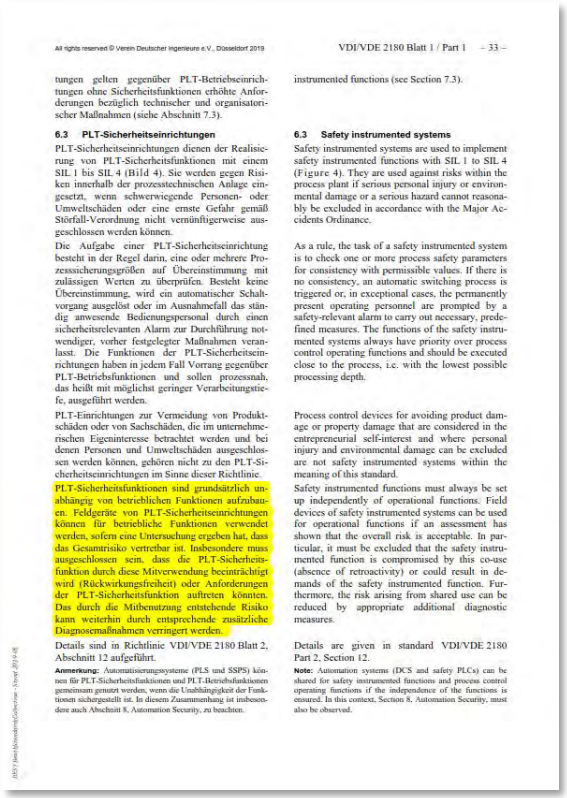


Anforderungen an die Unabhängigkeit von betrieblichen PLT-Einrichtungen und PLT-Sicherheitseinrichtungen

TÜV NORD
InfraChem

VDI / VDE 2180

- Blatt 1 (Stand 04/2019)
  6.3 PLT-Sicherheitseinrichtungen
  - sind grundsätzlich unabhängig von betrieblichen Funktionen aufzubauen.
  - Feldgeräte können für betriebliche Funktionen verwendet werden, sofern eine Untersuchung ergeben hat, dass das Gesamtrisiko vertretbar ist.
  - dürfen nicht durch die Mitverwendung beeinträchtigt werden (Rückwirkungsfreiheit).
  - dürfen nicht durch die Mitverwendung angefordert werden.



tungen gelten gegenüber PLT-Betriebseinrichtungen ohne Sicherheitsfunktionen erhöhte Anforderungen bezüglich technischer und organisatorischer Maßnahmen (siehe Abschnitt 7.3).

6.3 PLT-Sicherheitseinrichtungen

PLT-Sicherheitseinrichtungen dienen der Realisierung von PLT-Sicherheitsfunktionen mit einem SIL 1 bis SIL 4 (Bild 4). Sie werden gegen Risiken innerhalb der prozesstechnischen Anlage eingesetzt, wenn schwerwiegende Personen- oder Umweltschäden oder eine ernste Gefahr gemäß Störfall-Verordnung nicht vernünftigerweise ausgeschlossen werden können.

Die Aufgabe einer PLT-Sicherheitseinrichtung besteht in der Regel darin, eine oder mehrere Prozesssicherungsgrößen auf Übereinstimmung mit zulässigen Werten zu überprüfen. Besteht keine Übereinstimmung, wird ein automatischer Schaltvorgang ausgelöst oder im Ausnahmefall das ständig anwesende Bedienungspersonal durch einen sicherheitsrelevanten Alarm zur Durchführung notwendiger, vorher festgelegter Maßnahmen veranlasst. Die Funktionen der PLT-Sicherheitseinrichtungen haben in jedem Fall Vorrang gegenüber PLT-Betriebsfunktionen und sollen prozessnah, das heißt mit möglichst geringer Verarbeitungstiefe, ausgeführt werden.

PLT-Einrichtungen zur Vermeidung von Produktschäden oder von Sachschäden, die im unternehmerischen Eigeninteresse betrachtet werden und bei denen Personen und Umweltschäden ausgeschlossen werden können, gehören nicht zu den PLT-Sicherheitseinrichtungen im Sinne dieser Richtlinie.

PLT-Sicherheitsfunktionen sind grundsätzlich unabhängig von betrieblichen Funktionen aufzubauen. Feldgeräte von PLT-Sicherheitseinrichtungen können für betriebliche Funktionen verwendet werden, sofern eine Untersuchung ergeben hat, dass das Gesamtrisiko vertretbar ist. Insbesondere muss ausgeschlossen sein, dass die PLT-Sicherheitsfunktion durch diese Mitverwendung beeinträchtigt wird (Rückwirkungsfreiheit) oder Anforderungen der PLT-Sicherheitsfunktion auftreten könnten. Das durch die Mitbenutzung entstehende Risiko kann weiterhin durch entsprechende zusätzliche Diagnosemaßnahmen verringert werden.

Details sind in Richtlinie VDI/VDE 2180 Blatt 2, Abschnitt 12 aufgeführt.

Anmerkung: Automatisierungssysteme (PLS und SSPS) können für PLT-Sicherheitsfunktionen und PLT-Betriebsfunktionen gemeinsam genutzt werden, wenn die Unabhängigkeit der Funktionen sichergestellt ist. In diesem Zusammenhang ist insbesondere auch Abschnitt 8, Automation Security, zu beachten.

instrumented functions (see Section 7.3).

6.3 Safety instrumented systems

Safety instrumented systems are used to implement safety instrumented functions with SIL 1 to SIL 4 (Figure 4). They are used against risks within the process plant if serious personal injury or environmental damage or a serious hazard cannot reasonably be excluded in accordance with the Major Accidents Ordinance.

As a rule, the task of a safety instrumented system is to check one or more process safety parameters for consistency with permissible values. If there is no consistency, an automatic switching process is triggered or, in exceptional cases, the permanently present operating personnel are prompted by a safety-relevant alarm to carry out necessary, predefined measures. The functions of the safety instrumented systems always have priority over process control operating functions and should be executed close to the process, i.e. with the lowest possible processing depth.

Process control devices for avoiding product damage or property damage that are considered in the entrepreneurial self-interest and where personal injury and environmental damage can be excluded are not safety instrumented systems within the meaning of this standard.

Safety instrumented functions must always be set up independently of operational functions. Field devices of safety instrumented systems can be used for operational functions if an assessment has shown that the overall risk is acceptable. In particular, it must be excluded that the safety instrumented function is compromised by this co-use (absence of retroactivity) or could result in demands of the safety instrumented function. Furthermore, the risk arising from shared use can be reduced by appropriate additional diagnostic measures.

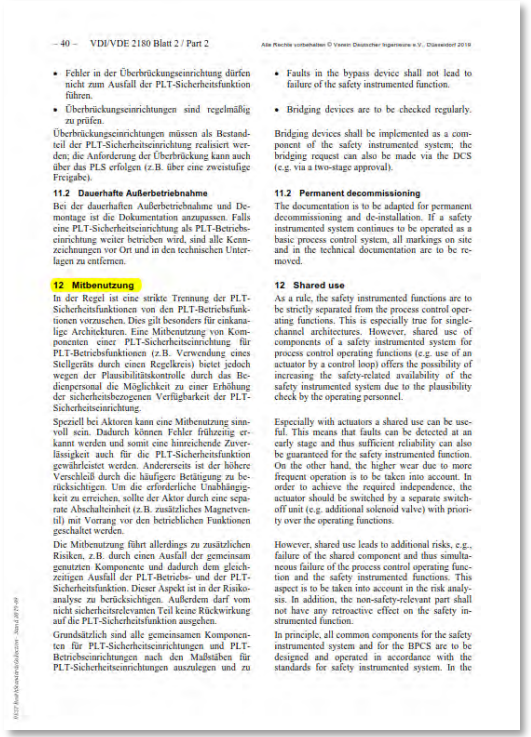
Details are given in standard VDI/VDE 2180 Part 2, Section 12.

Note: Automation systems (DCS and safety PLCs) can be shared for safety instrumented functions and process control operating functions if the independence of the functions is ensured. In this context, Section 8, Automation Security, must also be observed.

TÜV NORD InfraChem

VDI / VDE 2180

- Blatt 2 (Stand 09/2019)
  12 Mitbenutzung
  - I.d.R. strikte Trennung, insbesondere bei einkanaligen Architekturen.
  - kann bei entsprechender Diagnose die sicherheitsbezogene Verfügbarkeit erhöhen.
  - kann zu erhöhtem Verschleiß führen
  - kann zu zusätzlichen Risiken führen



– 40 – VDI/VDE 2180 Blatt 2 / Part 2

- Fehler in der Überbrückungseinrichtung dürfen nicht zum Ausfall der PLT-Sicherheitsfunktion führen.
- Überbrückungseinrichtungen sind regelmäßig zu prüfen.

Überbrückungseinrichtungen müssen als Bestandteil der PLT-Sicherheitseinrichtung realisiert werden; die Anforderung der Überbrückung kann auch über das PLS erfolgen (z.B. über eine zweistufige Freigabe).

11.2 Dauerhafte Außerbetriebnahme

Bei der dauerhaften Außerbetriebnahme und Demontage ist die Dokumentation anzupassen. Falls eine PLT-Sicherheitseinrichtung als PLT-Betriebseinrichtung weiter betrieben wird, sind alle Kennzeichnungen vor Ort und in den technischen Unterlagen zu entfernen.

12 Mitbenutzung

In der Regel ist eine strikte Trennung der PLT-Sicherheitsfunktionen von den PLT-Betriebsfunktionen vorzusehen. Dies gilt besonders für einkanalige Architekturen. Eine Mitbenutzung von Komponenten einer PLT-Sicherheitseinrichtung für PLT-Betriebsfunktionen (z.B. Verwendung eines Stellgeräts durch einen Regelkreis) bietet jedoch wegen der Plausibilitätskontrolle durch das Bedienpersonal die Möglichkeit zu einer Erhöhung der sicherheitsbezogenen Verfügbarkeit der PLT-Sicherheitseinrichtung.

Speziell bei Aktoren kann eine Mitbenutzung sinnvoll sein. Dadurch können Fehler frühzeitig erkannt werden und somit eine hinreichende Zuverlässigkeit auch für die PLT-Sicherheitsfunktion gewährleistet werden. Andererseits ist der höhere Verschleiß durch die häufigere Betätigung zu berücksichtigen. Um die erforderliche Unabhängigkeit zu erreichen, sollte der Aktor durch eine separate Abschalteinheit (z.B. zusätzliches Magnetventil) mit Vorrang vor den betrieblichen Funktionen geschaltet werden.

Die Mitbenutzung führt allerdings zu zusätzlichen Risiken, z.B. durch einen Ausfall der gemeinsam genutzten Komponente und dadurch dem gleichzeitigen Ausfall der PLT-Betriebs- und der PLT-Sicherheitsfunktion. Dieser Aspekt ist in der Risikoanalyse zu berücksichtigen. Außerdem darf vom nicht sicherheitsrelevanten Teil keine Rückwirkung auf die PLT-Sicherheitsfunktion ausgehen.

Grundsätzlich sind alle gemeinsamen Komponenten für PLT-Sicherheitseinrichtungen und PLT-Betriebseinrichtungen nach den Maßstäben für PLT-Sicherheitseinrichtungen auszulegen und zu

- Faults in the bypass device shall not lead to failure of the safety instrumented function.
- Bridging devices are to be checked regularly.

Bridging devices shall be implemented as a component of the safety instrumented system; the bridging request can also be made via the DCS (e.g. via a two-stage approval).

11.2 Permanent decommissioning

The documentation is to be adapted for permanent decommissioning and de-installation. If a safety instrumented system continues to be operated as a basic process control system, all markings on site and in the technical documentation are to be removed.

12 Shared use

As a rule, the safety instrumented functions are to be strictly separated from the process control operating functions. This is especially true for single-channel architectures. However, shared use of components of a safety instrumented system for process control operating functions (e.g. use of an actuator by a control loop) offers the possibility of increasing the safety-related availability of the safety instrumented system due to the plausibility check by the operating personnel.

Especially with actuators a shared use can be useful. This means that faults can be detected at an early stage and thus sufficient reliability can also be guaranteed for the safety instrumented function. On the other hand, the higher wear due to more frequent operation is to be taken into account. In order to achieve the required independence, the actuator should be switched by a separate switch-off unit (e.g. additional solenoid valve) with priority over the operating functions.

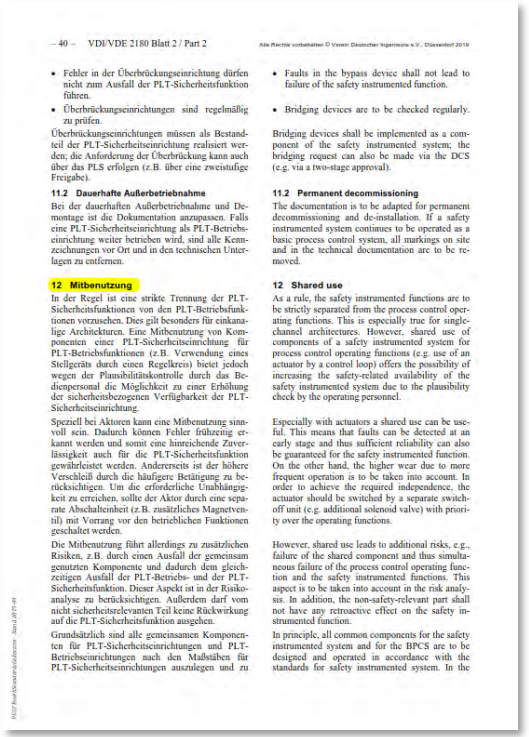
However, shared use leads to additional risks, e.g., failure of the shared component and thus simultaneous failure of the process control operating function and the safety instrumented functions. This aspect is to be taken into account in the risk analysis. In addition, the non-safety-relevant part shall not have any retroactive effect on the safety instrumented function.

In principle, all common components for the safety instrumented system and for the BPCS are to be designed and operated in accordance with the standards for safety instrumented system. In the

TÜV NORD InfraChem

VDI / VDE 2180

- Blatt 2 (Stand 09/2019) Fortsetzung
  12 Mitbenutzung
  - Ein Gerät einer PLT-Sicherheitsfunktion darf nur für betriebliche Funktionen verwendet werden, wenn ein Ausfall dieses Gerätes nicht zu einer Anforderung dieser PLT-Sicherheitsfunktion führt.



– 40 – VDI/VDE 2180 Blatt 2 / Part 2

- Fehler in der Überbrückungseinrichtung dürfen nicht zum Ausfall der PLT-Sicherheitsfunktion führen.
- Überbrückungseinrichtungen sind regelmäßig zu prüfen.

Überbrückungseinrichtungen müssen als Bestandteil der PLT-Sicherheitseinrichtung realisiert werden; die Anforderung der Überbrückung kann auch über das PLS erfolgen (z.B. über eine zweistufige Freigabe).

11.2 Dauerhafte Außerbetriebnahme

Bei der dauerhaften Außerbetriebnahme und Demontage ist die Dokumentation anzupassen. Falls eine PLT-Sicherheitseinrichtung als PLT-Betriebseinrichtung weiter betrieben wird, sind alle Kennzeichnungen vor Ort und in den technischen Unterlagen zu entfernen.

12 Mitbenutzung

In der Regel ist eine strikte Trennung der PLT-Sicherheitsfunktionen von den PLT-Betriebsfunktionen vorzusehen. Dies gilt besonders für einkanalige Architekturen. Eine Mitbenutzung von Komponenten einer PLT-Sicherheitseinrichtung für PLT-Betriebsfunktionen (z.B. Verwendung eines Stellgeräts durch einen Regelkreis) bietet jedoch wegen der Plausibilitätskontrolle durch das Bedienpersonal die Möglichkeit zu einer Erhöhung der sicherheitsbezogenen Verfügbarkeit der PLT-Sicherheitseinrichtung.

Speziell bei Aktoren kann eine Mitbenutzung sinnvoll sein. Dadurch können Fehler frühzeitig erkannt werden und somit eine hinreichende Zuverlässigkeit auch für die PLT-Sicherheitsfunktion gewährleistet werden. Andererseits ist der höhere Verschleiß durch die häufigere Betätigung zu berücksichtigen. Um die erforderliche Unabhängigkeit zu erreichen, sollte der Aktor durch eine separate Abschalteinheit (z.B. zusätzliches Magnetventil) mit Vorrang vor den betrieblichen Funktionen geschaltet werden.

Die Mitbenutzung führt allerdings zu zusätzlichen Risiken, z.B. durch einen Ausfall der gemeinsam genutzten Komponente und dadurch dem gleichzeitigen Ausfall der PLT-Betriebs- und der PLT-Sicherheitsfunktion. Dieser Aspekt ist in der Risikoanalyse zu berücksichtigen. Außerdem darf vom nicht sicherheitsrelevanten Teil keine Rückwirkung auf die PLT-Sicherheitsfunktion ausgehen.

Grundsätzlich sind alle gemeinsamen Komponenten für PLT-Sicherheitseinrichtungen und PLT-Betriebseinrichtungen nach den Maßstäben für PLT-Sicherheitseinrichtungen auszulegen und zu

- Faults in the bypass device shall not lead to failure of the safety instrumented function.
- Bridging devices are to be checked regularly.

Bridging devices shall be implemented as a component of the safety instrumented system; the bridging request can also be made via the DCS (e.g. via a two-stage approval).

11.2 Permanent decommissioning

The documentation is to be adapted for permanent decommissioning and de-installation. If a safety instrumented system continues to be operated as a basic process control system, all markings on site and in the technical documentation are to be removed.

12 Shared use

As a rule, the safety instrumented functions are to be strictly separated from the process control operating functions. This is especially true for single-channel architectures. However, shared use of components of a safety instrumented system for process control operating functions (e.g. use of an actuator by a control loop) offers the possibility of increasing the safety-related availability of the safety instrumented system due to the plausibility check by the operating personnel.

Especially with actuators a shared use can be useful. This means that faults can be detected at an early stage and thus sufficient reliability can also be guaranteed for the safety instrumented function. On the other hand, the higher wear due to more frequent operation is to be taken into account. In order to achieve the required independence, the actuator should be switched by a separate switch-off unit (e.g. additional solenoid valve) with priority over the operating functions.

However, shared use leads to additional risks, e.g., failure of the shared component and thus simultaneous failure of the process control operating function and the safety instrumented functions. This aspect is to be taken into account in the risk analysis. In addition, the non-safety-relevant part shall not have any retroactive effect on the safety instrumented function.

In principle, all common components for the safety instrumented system and for the BPCS are to be designed and operated in accordance with the standards for safety instrumented system. In the

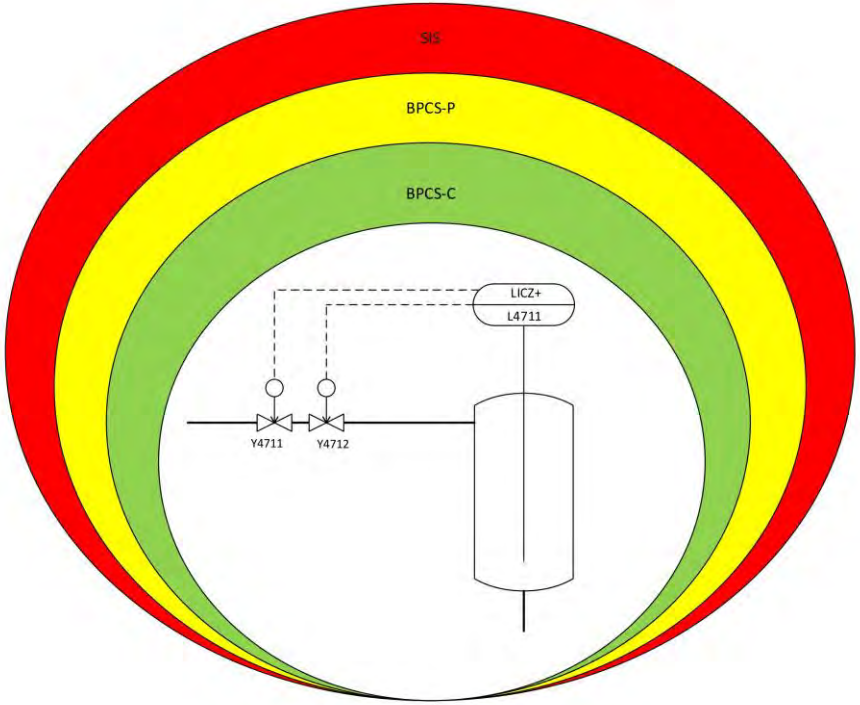
TÜV NORD InfraChem

Prinzip der unabhängigen Schutzebenen

BPCS-C = basic process control system – control

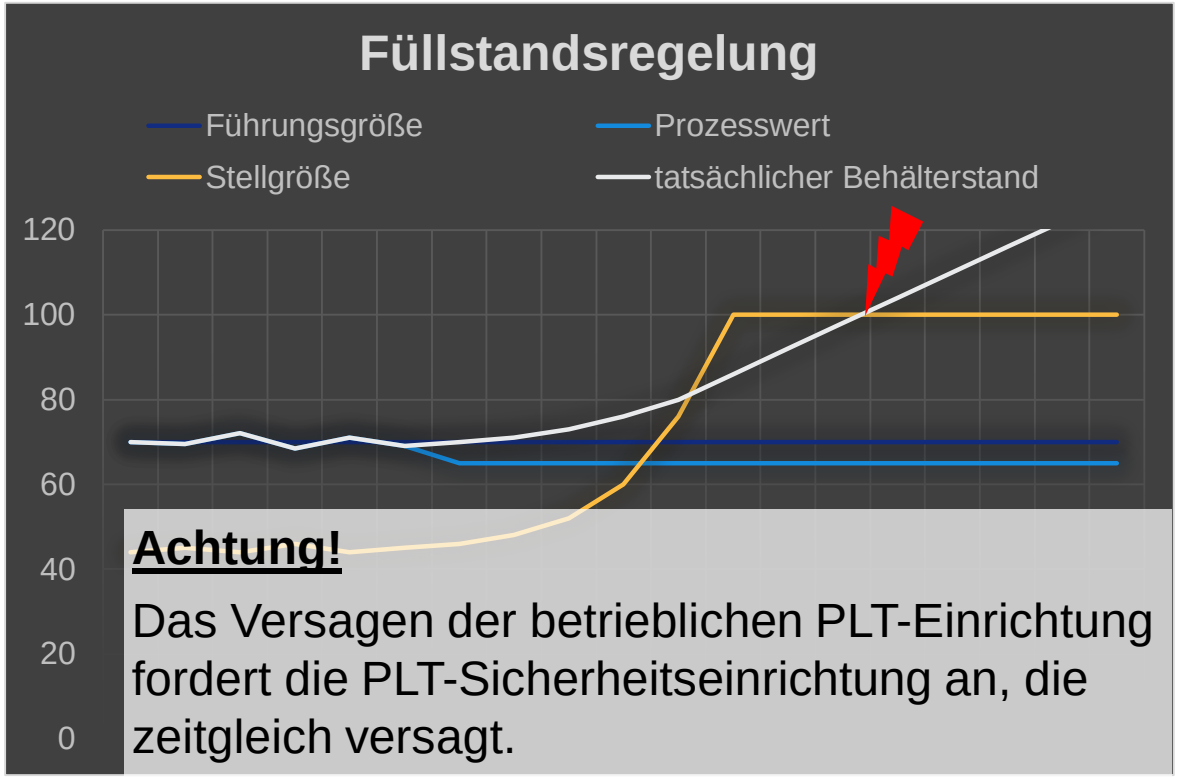
BPCS-P = basic process control system – protection

SIS = safety instrumented system



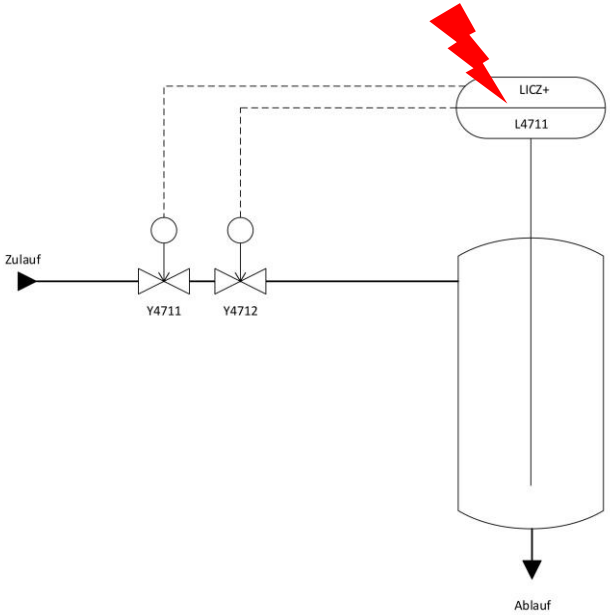
TÜV NORD InfraChem

Fall 1: Mitbenutzung Sensor



Achtung!

Das Versagen der betrieblichen PLT-Einrichtung fordert die PLT-Sicherheitseinrichtung an, die zeitgleich versagt.



TÜV NORD InfraChem

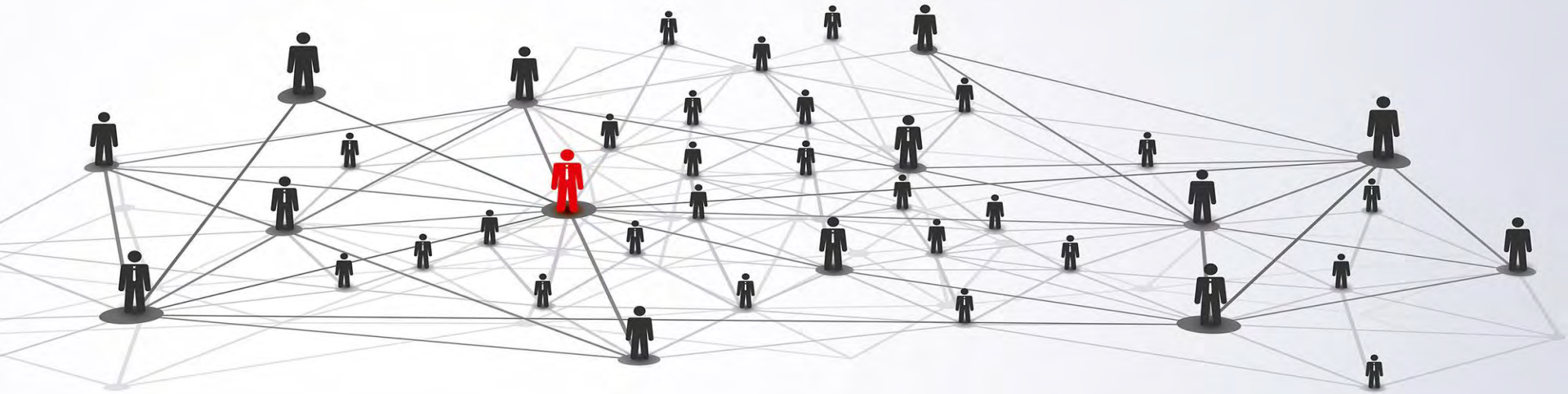
Fazit

- Ein einzelner Fehler darf nicht zum gleichzeitigen Versagen der PLT-Betriebs- und -Sicherheitsfunktion führen.
- Mitbenutzung in einkanaligen Systemen ist grundsätzlich zu vermeiden.
- Nur in begründeten Einzelfällen ist die Mitbenutzung in einkanaligen Systemen möglich und nur dann, wenn kein kausaler Zusammenhang zwischen Ausfall der Betriebsfunktion und Ansprechen der Sicherheitsfunktion besteht.
- Eine Mitbenutzung von Sensoren oder Aktoren in mehrkanaligen Systemen ist aufgrund von Diagnosemöglichkeiten (z.B. Gleichlaufüberwachung, Endlagen) und der damit verbundenen Fehleraufdeckung einfacher zu begründen.

Fragen?!?

Vielen Dank für die Aufmerksamkeit!

TÜV NORD InfraChem



Jürgen Bode
jbode@tuev-nord.de
Mobil +49 160 888 5132

Bei Fragen sprechen Sie uns an!

Thorsten Lasrich
tlasrich@tuev-nord.de
Mobil +49 160 888 2461

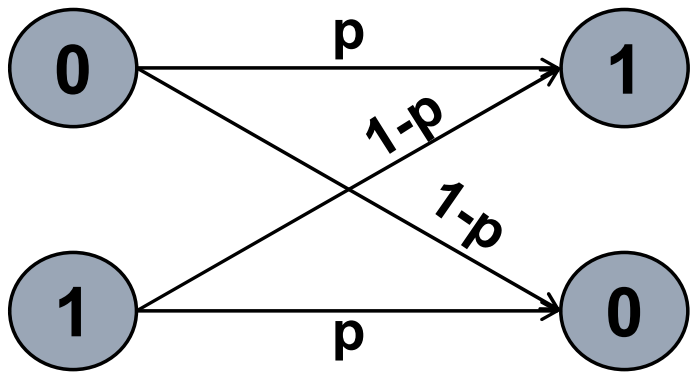
Current Discussions about Safety Communication Models

BECKHOFF

Current Model: Binary Symmetric Channel (BSC)

BECKHOFF

1. Each bit is falsified independently of the other bits.
2. Each bit is falsified with equal probability.
3. The falsification from 1 to 0 and the falsification from 0 to 1 occurs the equal probability (Bit Error Probability).



- Bit Error Probabilities > 0.5 are not considered.
  - If Bit Error Probability > 0.5 then an inverter can be applied.

    error 0 → 1 with 0.6, with inverter: → 0; correct 0 → 1 with 0.4

    error 1 → 0 with 0.6, with inverter: → 1; correct 1 → 0 with 0.4
  - No reasonable communication is possible with more than a half of erroneous bits.

Current Practice: Binary Symmetric Channel (BSC)

BECKHOFF

IEC 61784-3:

1. Binary Symmetric Channel
2. No reasonable communication is possible for Bit Error Probability > 10^{-4}.
   Safety margin: consider Bit Error Probability ≤ 10^{-2}

Additional deterministic criteria can be analyzed:

- Hamming Distance
- Detection of odd bit errors
- Detection of burst errors
- Detection of complete zero-messages
- Detection of complete one-messages
- Detection of completely inverted messages
- …

The deterministic criteria are independent of the assumption of the Binary Symmetric Channel!

Questioned: Validity of Binary Symmetric Channel

BECKHOFF

Questions in the past about:

- Bit stuffing
- Symbol coding / symbol decoding
- Data compression / data decompression
- Error correction

Recently, questions include effects of security measures:

- Encryption / decryption, e.g. Block Cipher

Discussions within IEC SC65C WG12 Task Force 1

BECKHOFF

Discussion 1:

- Discussion about discussion:

  Do we need to make any change?

Discussion 2:

- Keeping BSC:

  Do we need to consider Bit Error Probability up to 0.5 or can we keep the limit of 10^{-2} ?

Discussion 3:

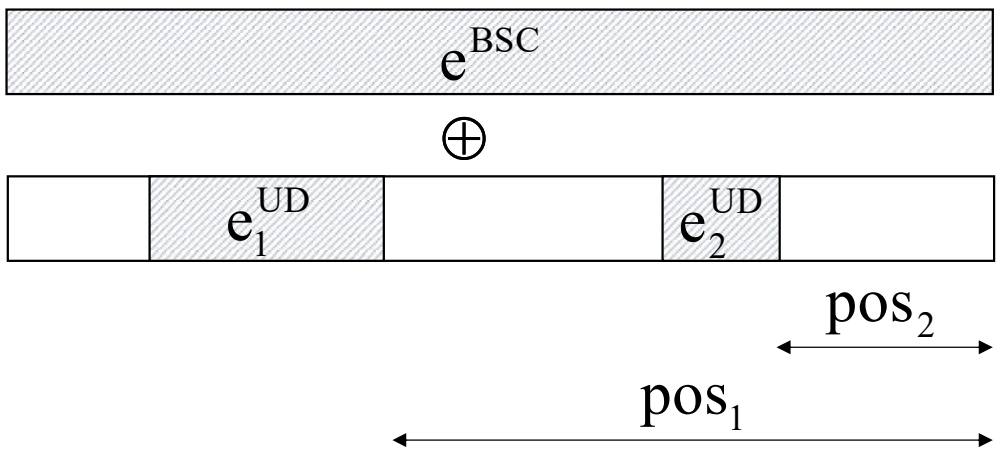
- Superimposition of BSC and uniformly distributed segments:

  Parameters:

  - Bit Error Probability (includes Discussion 2)
  - Probability of Occurrence of uniformly distributed segments

Discussion3: Superimposition of BSC and Uniformly Distributed Segments

BECKHOFF



BSC

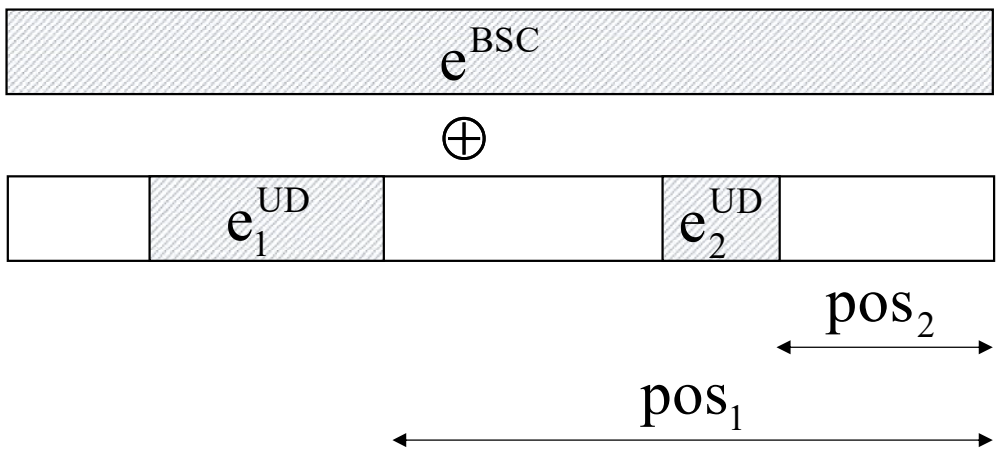
Bitwise XOR

Uniformly Distributed Segments

CRC: $$(e^{BSC} \oplus e_1^{UD} \cdot x^{pos_1} \oplus e_2^{UD} \cdot x^{pos_2}) \bmod g \stackrel{?}{=} 0$$

Discussion3: Superimposition of BSC and Uniformly Distributed Segments

BECKHOFF



BSC

Bitwise XOR

Uniformly Distributed Segments

CRC,
presumed Residual Error Probability:

$$P_{re} \overset{?}{\approx} 2^{-r} \cdot P_{occ}^{UD} + P_{re}^{CRC,BSC} \cdot (1 - P_{occ}^{UD})$$

Contact

BECKHOFF

Beckhoff Automation GmbH & Co. KG
Headquarters
Huelshorstweg 20
33415 Verl
Germany

Phone: +49 5246 963-0
Fax: +49 5246 963-198
E-Mail: info@beckhoff.com
Web: www.beckhoff.com

SIL SLAM

Cyber – Security
im Bereich der Produktion

OT Security

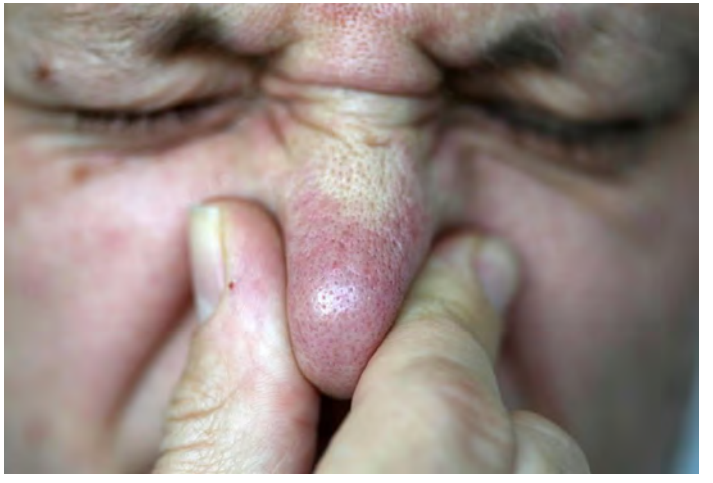
Wahrscheinlich denken Sie jetzt an:

- Richtlinien die nicht helfen
- Aufwendige Assessments
- teure Tools
  - die nie „up to date sind“
  - die nur durch Experten bedienbar sind
  - Wahrscheinlich doch nicht funktionieren

NEVER ENDING STORY

Es ist Freitag der 13. und folgendes passiert um 22:30 Uhr in einer Meßwarte …

Freitag der 13. / 22:30 Uhr



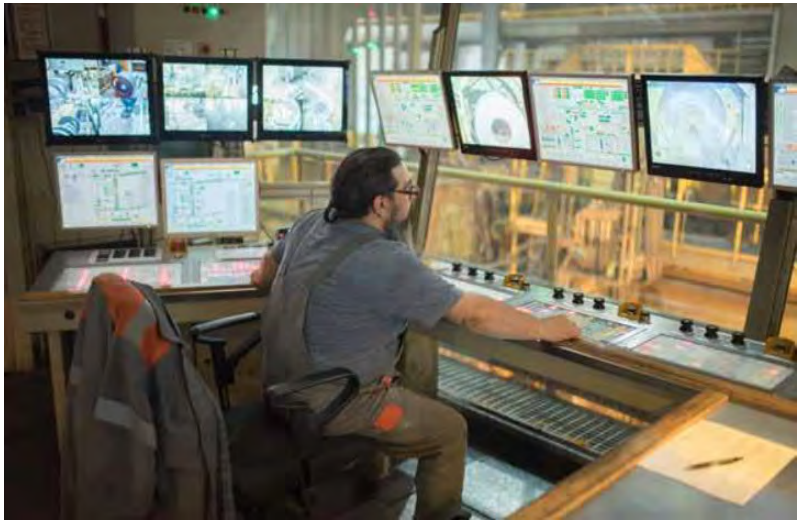
Ein Operator kommt in die Meßwarte:

„Draußen riecht es merkwürdig“

Ein zweiter Operator kommt in die Meßwarte:

„Der Kompressor läuft irgendwie unruhig und sehr hochtourig“

Freitag der 13. / 22:45 Uhr



Der verantwortliche Anlagenbediener schaut auf seinen Bildschirm:

„Hmm … mein Bildschirm zeigt nichts bemerkenswertes an. Aber irgendwie funktioniert etwas nicht. Ich kann nichts bedienen und die Werte sind eingefroren“

Er geht an einen weiteren Bedienplatz:

„Wir haben ein Problem. Auf diesem Bildschirm ist es ebenso. Ich bekomme keine neuen Werte und kann nichts bedienen“

Freitag der 13. / 23:00 Uhr

Meldung an den Schichtleiter.

Schichtleiter:

„Rufen Sie den Bereitschaftsdienst an.
Es ist Wochenende und hier ist niemand mehr, der uns helfen kann“.

Operator:

„Ich kann die Bereitschaftsliste auf dem Server nicht öffnen.
Der Computer zeigt hier etwas in Englisch an.“

Freitag der 13. / 23:00 Uhr

Schichtleiter:

„Rufen Sie mal den Ingenieur Meier an.
Die Nummer habe ich im Kopf … 0123-45678“.

Operator:

„Irgendwie funktioniert das Telefon nicht.
Da steht was von IP Verbindung fehlt“

Freitag der 13. / 23:15 Uhr

Draußen wird es lauter, der Kompressor läuft in ungewöhnlich hoher Drehzahl.

Ein weiterer Operator kommt in die Meßwarte und berichtet über knackende Geräusche am Boiler.

Schichtleiter:

„Wir müssen die Anlage abfahren. Drucken Sie den Notfallplan aus“

Operator:

„Geht nicht … ich kann den PC nicht bedienen“

Freitag der 13. / 23:30 Uhr

Ein Ordner mit dem Notfallplan wurde gefunden. Der Schichtleiter folgt dem Plan.

Schichtleiter:

„In Abhängigkeit von den Temperaturen, Drücken und der Drehzahl müssen wir unterschiedliche Schritte ausführen.“

Operator:

„Das Leitsystem funktioniert nicht mehr. Wie kann ich jetzt den Notfallplan ausführen?“

Freitag der 13. / 23:45 Uhr

Schichtleiter:

„Gehen Sie in den Schaltraum und schalten Sie den Kompressor von dort aus. Eine Schaltberechtigung haben Sie ja.“

Operator:

„Ich bin mir nicht mehr sicher, welche Schalter das waren.?“

Schichtleiter:

„Im Schaltraum müssten Pläne liegen“

Freitag der 13. / 23:55 Uhr

Operator:

„Ich kann die Tür zum Schaltraum mit meiner Chipkarte nicht mehr öffnen“

Und nun kommen Sie:

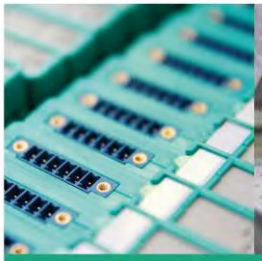
Sind sie überrascht?

So etwas kann bei uns nicht passieren, weil …

… oder vielleicht doch!?

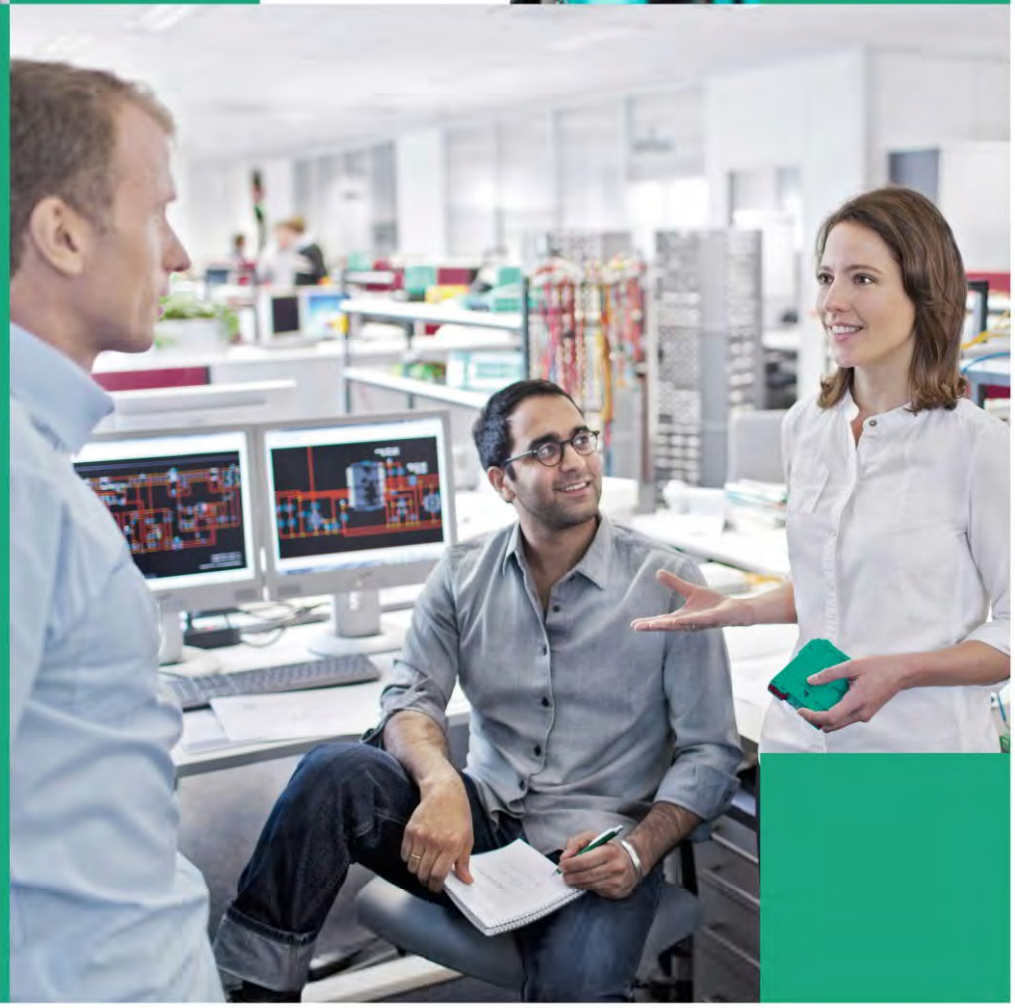
Welche Geräte sind wirklich „Cyber-Sicher“ ?

Was müssen wir vorhalten, um im Falle eines boshaften Cyberangriffs (Mensch und Umwelt) handlungsfähig zu bleiben?





Your automation, our passion.



PEPPERL+FUCHS

PEPPERL+FUCHS

SIL Slam: FS und KI

PEPPERL+FUCHS

Zweck des Internets

PEPPERL+FUCHS

Zweck des Internets

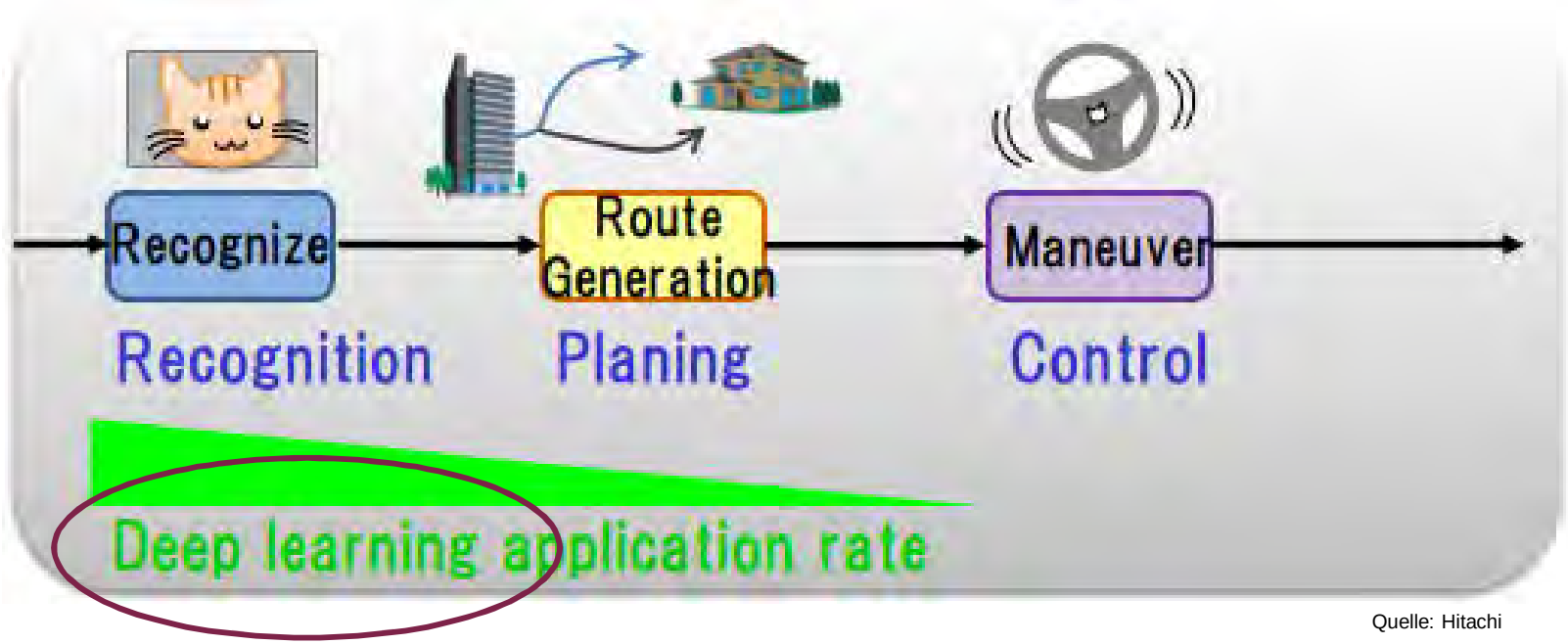
Niedliche Katzenvideos

https://www.youtube.com/watch?v=AguUewSmsNU

Zweck von KI

Katzenbilder erkennen

Quelle: Pixabay



Quelle: Hitachi

Was ist überhaupt KI?

Quelle: publicdomainpictures.net

„Cool things that Computers can't do"

„Cool things that Computers can do"

Adaptivity - the ability to improve performance by learning from experience.

Source: P+F / infoteam

Kognitive Systeme

Machine Learning

Starke / Schwache KI

PEPPERL+FUCHS

Keine Definition im Bereich Safety???

Quelle: publicdomainpictures.net

MT 61508-3 Task Group Ref N

AK 914.0.11

ISO 12100-5 TC189

ISO JTC1 SC42

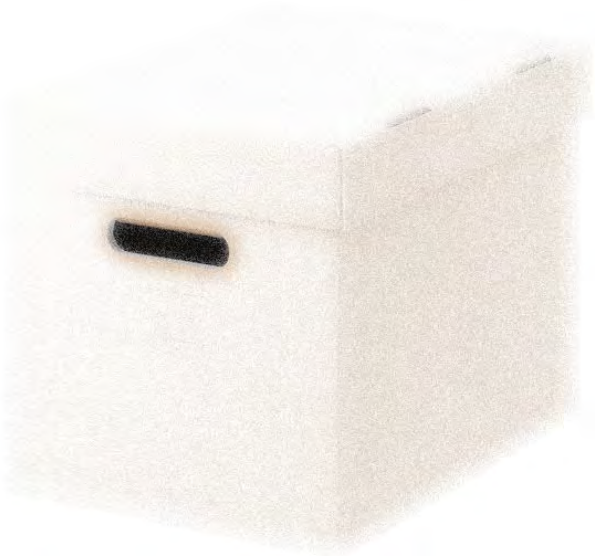
EASA AI task force

AK 801.0.8

Safety of Autonomous Systems Working Group SASWG

Kein Problem…

White Box



Grey Box

Black Box

Source: P+F / infoteam

PEPPERL+FUCHS

AI classification table



Quelle: debilder.net

AI Technology Class => Usage Level			
Usage Level A1 AI technique used in a safety relevant E/E/PE system and automated decision making possible.	KI?	*See clause „ab*	Not recomm applica
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 claus*	
Usage Level B1 AI technique used during development of a safety relevant E/E/PE system (offline support tool) and automated decision making possible.	appli existing functic standards ble	*See ef“*	*Se „ab“*
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“*	*ause „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“*	*See clause „ef“*
Usage Level D 1, 2 AI technique used outside a safety relevant E/E/PE sy sufficiently segregated and behaviour controlled (e.g sandbox, hypervised)	No sp unctional safety re s for AI, but sa ty preautions nee tion. Additionally, other safety aspects (not being ad n functional safety methods) might be impacted ge.		

Can be systematically analysed

Something in between

Cannot be systematically analysed

1 offline AI (during development) teaching/learning only
2 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.

PEPPERL+FUCHS

Alles wie immer…


Quelle: Pixabay

Annex C defines the following desirable properties:

I. Completeness with respect to safety
II. Correctness with respect to safety
III. Freedom from intrinsic specification faults, including freedom from ambiguity
IV. Understandability of safety requirements (Explainability)
V. Freedom from adverse interference of non-safety functions with the safety needs
VI. Capability of providing a basis for verification and validation

Kein zusätzlicher Spielraum für KI

PEPPERL+FUCHS

Keine Metriken

Quelle: VDE-AR-E 2842-61

Figure 9 – Aspects forming the meta-term "Trustworthiness"

Quelle: Pixabay

source of uncertainty	HW	SW	AI
systematic failures	✓	✓	✓
„random" failures	λ	– –	λ_{AI}

Quelle: infoteam

PEPPERL+FUCHS

Die Automobilisten wollen rechnen

Idealer Fall (nur statistisch unabhängige Unfallereignisse):

- Strecke ca. 100 Mio. km => Kosten mehrere 100 Mio. €
- Bei jeder Veränderung erneute Dauerlaufprüfung notwendig

Quelle: Pixabay

Realität ist aber noch schlimmer

- Testabdeckung immer noch gering (etwas mehr als 1 $^{o}/_{oo}$ der jährlichen Fahrleistungen in D), potentielle „pathologische“ Fälle bleiben verborgen
- Große Länderunterschiede
  - USA ca. 127 Mio. km/fatal crash (nach Shladover 2009)
- Komponentenkombinationen (Grenzmusterverhalten)

Referenz ISO 26262

- Erlaubte Rate nicht entdeckter Ausfälle mit potentiellem Schaden für Gesundheit und Leben: 10^{-8}/h => ca. $50 \cdot 10^{8}$ km = 5 Mrd. km

Quelle: Prof. Winner, “Absicherung automatischen Fahrens”,
6. FAS-Tagung, 2013, Vortrag der TU Darmstadt

Vergleich: Reaktion Mensch

1 Sekunde Reaktionszeit
Entscheidung 1: Sch… rufen
Entscheidung 2: Bremse betätigen

Quelle: Pixabay

PEPPERL+FUCHS

Vergleich: Reaktion KI

100 ms: alle Philosophen von Platon bis Kant bewerten
Entscheidung für Cato: …Carthaginem esse delendam
Entscheidung für Ausweichen

Quelle: 2 x Pixabay

PEPPERL+FUCHS

Problemstellung

Vorwurf derzeit:
Der Mensch hätte sicher ohne Automatik den Unfall vermieden

Worauf es hinläuft:
Die KI hätte sicher besser reagiert als der Mensch

Quelle: Pixabay

PEPPERL+FUCHS

Mögliche Richtungen

Grundsatz: KI nur dann einsetzen wenn ein Vorteil gegenüber deterministischen Verfahren nachweisbar.

EN/IEC 61508 ist Industriestandard

Einleitung

– legt Anforderungen für die Vermeidung und Beherrschung von systematischen Fehlern fest, die auf Erfahrungen und Urteilsvermögen beruhen, die durch praktische Erfahrung in der Industrie gewonnen wurden. Wenn auch die Wahrscheinlichkeit des Auftretens systematischer Ausfälle im Allgemeinen nicht quantifiziert werden kann, erlaubt die Norm jedoch für eine festgelegte Sicherheitsfunktion den Anspruch zu erheben, dass der mit der Sicherheitsfunktion verbundene Ausfallgrenzwert als erreicht betrachtet werden kann, wenn alle Anforderungen dieser Norm erfüllt worden sind,

PEPPERL+FUCHS

Mögliche Richtungen

Will / sollte die EN/IEC 61508 wirklich die ‚Basic Safety Publication‘ sein???

PEPPERL+FUCHS

About the presenter

Dipl. Ing. Michael Kindermann

- Degree in Electrical Engineering (Automation) @ University of Kaiserslautern
- 10 years R&D @ Pepperl + Fuchs
- **Design of functional safety devices since 2001** (EN 954-1 und EN 61508)
- 3 years of certification in hazardous locations @ UL International
- Certified FS-Engineer in HW/SW design
- 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 (61508), AK 225.1 (Machines and FS), K132.0.1 (FMEA), K241 (Ex and FS)
  - **Committee Moderator GK 914.0.3** (Safe Software in 61508) and **GK 914.0.9** (Statistical Evaluation of Software)

PEPPERL+FUCHS

THE END…

Michael Kindermann

mkindermann@de.pepperl-fuchs.com

Pepperl+Fuchs Inc.
Twinsburg · Ohio · USA
Tel. +1 330 425 3555
E-Mail: sales@us.pepperl-fuchs.com

Pepperl+Fuchs GmbH
Mannheim · Germany
Tel. +49 621 776 0
E-Mail: info@de.pepperl-fuchs.com

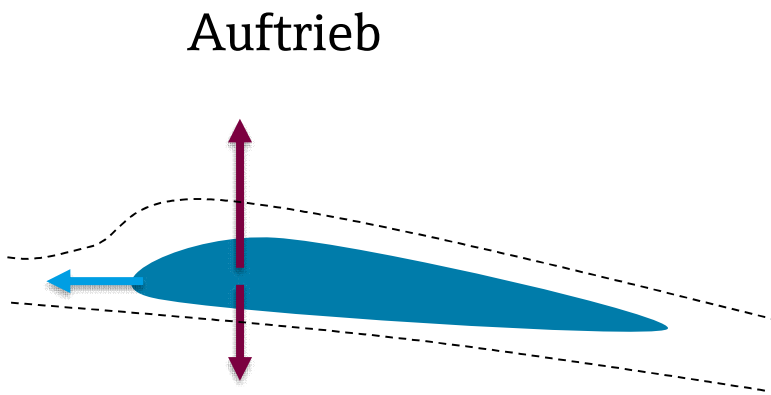
Pepperl+Fuchs PTE Ltd.
Singapore
Tel. +65 677 99091
E-Mail: sales@sg.pepperl-fuchs.com

PEPPERL+FUCHS

Die Sicherheitsfunktion

Anforderungen und Spezifikationen
Ein - hoffentlich unterhaltsamer - Vergleich aus dem Flugsport

Beispiel „Sicherheitsfunktion“ – aus dem Flugsport



Bildquelle: www.dhv.de

Beispiel „Sicherheitsfunktion“ – aus dem Flugsport

~~Auftrieb~~

Unkontrollierbarer Flugzustand, Absturz droht!

Bildquelle: www.dhv.de

Beispiel „Sicherheitsfunktion“ – aus dem Flugsport

- Rettungsschirm, Reserve
  … Anforderungen?

Bildquelle: www.dhv.de

Die klassische Sicherheitsfunktion

Definition der klassischen Sicherheitsfunktion aus den gängigen Sicherheitsnormen

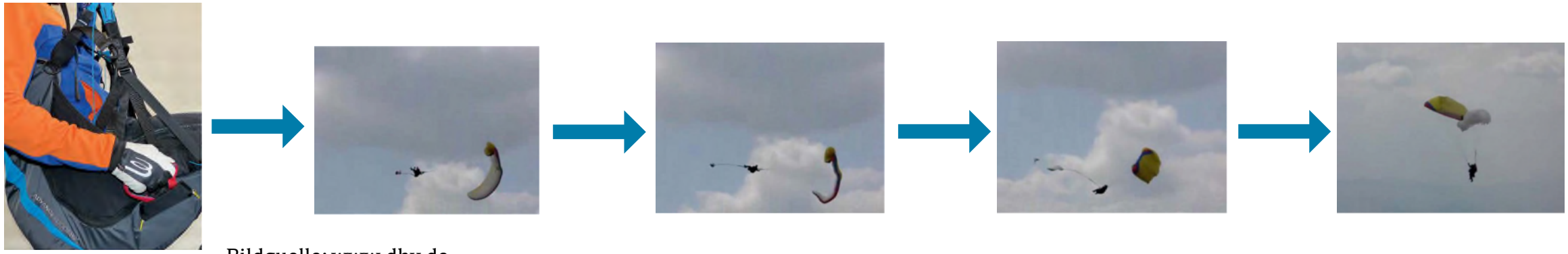
- DIN EN 61508-4, DIN EN 61511-1: Eine Sicherheitsfunktion hat die Aufgabe, einen sicheren Zustand zu erreichen oder aufrecht zu erhalten, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls.
- DIN EN ISO 13849-1: Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos führen kann.

-> Vergleich mit der „Sicherheitsfunktion“ aus dem Flugsport?

Beispiel „Sicherheitsfunktion“

Anforderungen an die „Sicherheitsfunktion“

- Zuverlässigkeit!
  Wie zuverlässig muss die Sicherheitsfunktion sein? Es gibt keine 100% Sicherheit.
  Statistik -> Wie oft fliegt man, welche Risiken geht man dabei ein, wie gut ist die Reserve,…
- DIN EN 61508-4, DIN EN 61511-1: Eine Sicherheitsfunktion hat die Aufgabe, einen sicheren Zustand zu erreichen oder aufrecht zu erhalten, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls.
- DIN EN ISO 13849-1: Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos führen kann.



Bildquelle: www.dhv.de

Beispiel „Sicherheitsfunktion“

Anforderungen an die „Sicherheitsfunktion“:

→ Schnelle Auslösung bei geringem Bodenabstand!
Öffnungszeit des Rettungsschirms?

- Auch die klassische Sicherheitsfunktion braucht Zeit, um den fatalen Ausgang zu verhindern
- Zeitverhalten der Schutzeinrichtung ist zu beachten!
- Beispiel: Schließzeiten von Ventilen, Zeiten bis zur Erkennung eines gefährlichen Fehlers im Verhältnis zur Anforderungsrate.

Bildquelle: Eigener Fundus

Bildquelle: www.dhv.de

Beispiel „Sicherheitsfunktion“

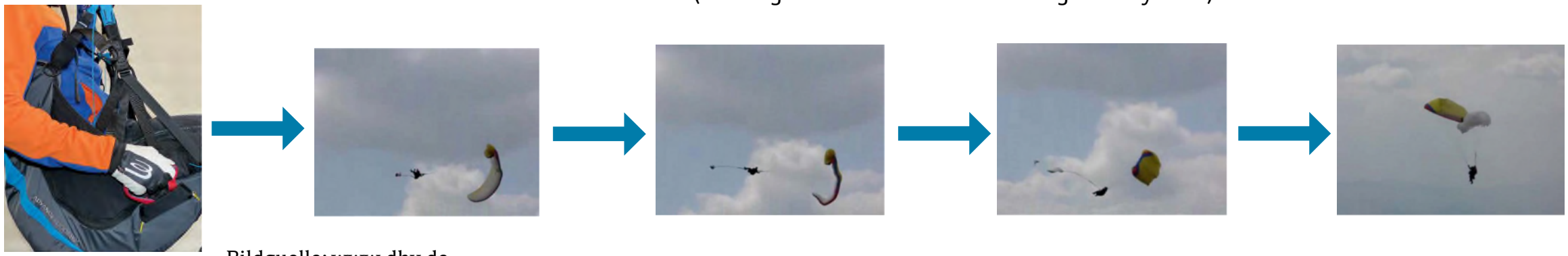
Anforderungen an die „Sicherheitsfunktion“:

→ Eignung für das Einsatzgebiet und bestimmungsgemäße Verwendung

- SIL-Eignung der Komponenten
- Eignung der Komponenten der Sicherheitsfunktion für den Einsatzzweck (Betriebsmodus, sicherheitsrelevante Prozessparameter,…)

→ Das Rettungsgerät wurde speziell zur Verwendung als Rettungsgerät für Gleitschirmflieger entwickelt. Jeglicher Gebrauch für andere Flugsportarten wie Fallschirmspringen, Base-Jumping etc. ist verboten.
→ Das Rettungsgerät darf gemäß EN 12491 nur bis zu Maximalgeschwindigkeiten von 32m/s oder 115 km/h verwendet werden.
→ Das Rettungsgerät muss alle 6 Monate gelüftet und neu gepackt werden.
→ Nach einer Rettungsschirmöffnung muss das Rettungsgerät vom Hersteller oder einem autorisierten Instandhaltungsbetrieb für Rettungsgeräte überprüft werden.
→ Das Rettungsgerät muss nach 10 Jahren ausgetauscht werden, auch wenn es nie verwendet wurde.

(Auszug aus der Betriebsanleitung Fa. Skywalk)



Bildquelle: www.dhv.de

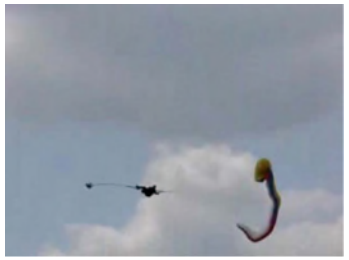
Beispiel „Sicherheitsfunktion“

Anforderungen an die „Sicherheitsfunktion“

→ Kompatibilitätsprüfung: Passt der Retter zum Gurtzeug? Auslösbarkeit?

- Vermeidung systematischer Fehler!
- Allgemein: Passen die Komponenten zu den äußeren Gegebenheiten? (Umgebungsbedingungen, Temperatur, Feuchte, Vibration, EMV, Prozessmedien…)

+



Bildquelle: www.dhv.de

Endress+Hauser

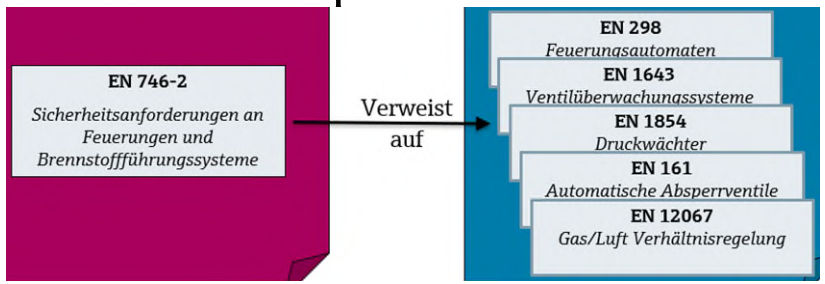
Beispiel „Sicherheitsfunktion“

Anforderungen an die „Sicherheitsfunktion“

→ Anwendung von Normen!

Musterprüfungen, Zulassungsverfahren, Mindest-Sinkgeschwindigkeiten, Anhängelasten, Belastungsanforderungen,…

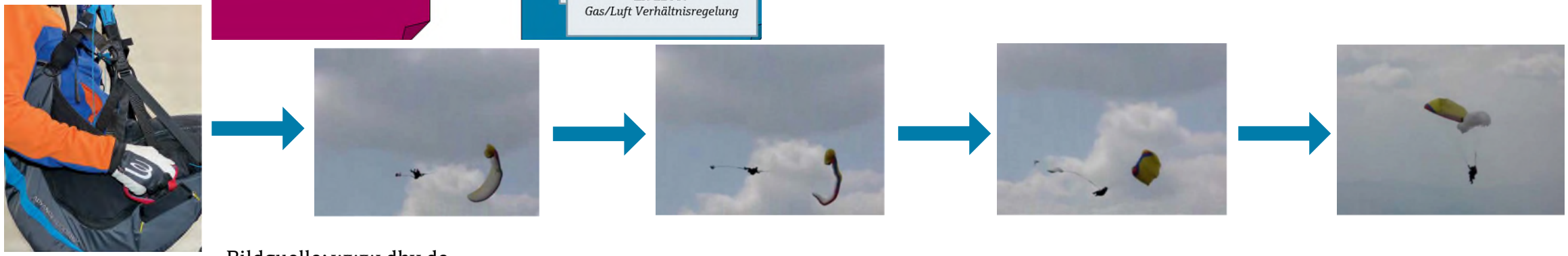
- Produktnormen für Komponenten



DIN EN 12491:2016-02

Ausrüstung für das Gleitschirmfliegen - Rettungsfallschirme - Sicherheitstechnische Anforderungen und Prüfverfahren; Deutsche Fassung EN 12491:2015

Englischer Titel:
Paragliding equipment - Emergency parachutes - Safety requirements and test methods; German version EN 12491:2015



Bildquelle: www.dhv.de

Endress+Hauser

Beispiel „Sicherheitsfunktion“

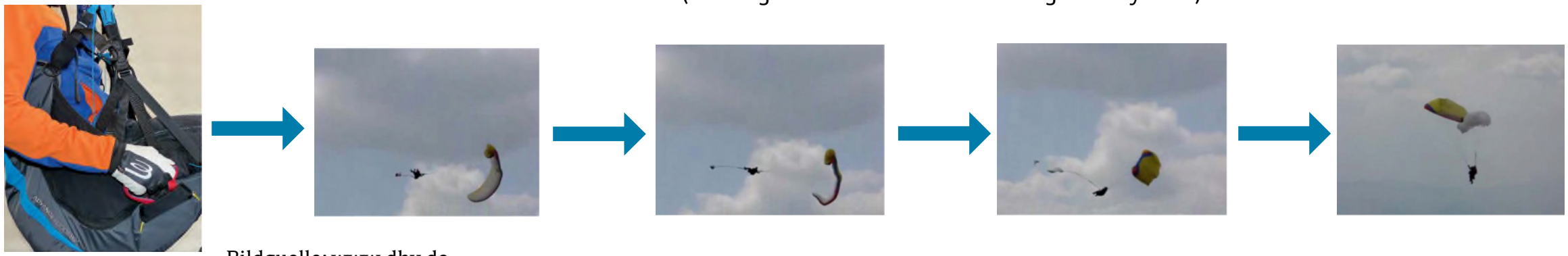
Anforderungen an die „Sicherheitsfunktion“

→ Regelmässige Prüfungen!

- Wiederkehrende Prüfungen von Schutzeinrichtungen

→ Das Rettungsgerät wurde speziell zur Verwendung als Rettungsgerät für Gleitschirmflieger entwickelt. Jeglicher Gebrauch für andere Flugsportarten wie Fallschirmspringen, Base-Jumping etc. ist verboten.
→ Das Rettungsgerät darf gemäß EN 12491 nur bis zu Maximalgeschwindigkeiten von 32m/s oder 115 km/h verwendet werden.
→ Das Rettungsgerät muss alle 6 Monate gelüftet und neu gepackt werden.
→ Nach einer Rettungsschirmöffnung muss das Rettungsgerät vom Hersteller oder einem autorisierten Instandhaltungsbetrieb für Rettungsgeräte überprüft werden.
→ Das Rettungsgerät muss nach 10 Jahren ausgetauscht werden, auch wenn es nie verwendet wurde.

(Auszug aus der Betriebsanleitung Fa. Skywalk)



Bildquelle: www.dhv.de

Beispiel „Sicherheitsfunktion“

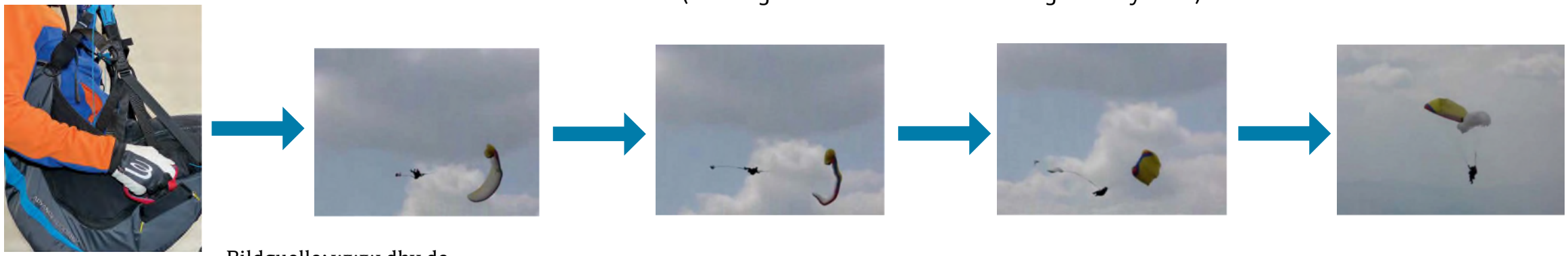
Anforderungen an die „Sicherheitsfunktion“

→ Gebrauchsdauer beachten!

- Useful lifetime…

→ Das Rettungsgerät wurde speziell zur Verwendung als Rettungsgerät für Gleitschirmflieger entwickelt. Jeglicher Gebrauch für andere Flugsportarten wie Fallschirmspringen, Base-Jumping etc. ist verboten.
→ Das Rettungsgerät darf gemäß EN 12491 nur bis zu Maximalgeschwindigkeiten von 32m/s oder 115 km/h verwendet werden.
→ Das Rettungsgerät muss alle 6 Monate gelüftet und neu gepackt werden.
→ Nach einer Rettungsschirmöffnung muss das Rettungsgerät vom Hersteller oder einem autorisierten Instandhaltungsbetrieb für Rettungsgeräte überprüft werden.
→ Das Rettungsgerät muss nach 10 Jahren ausgetauscht werden, auch wenn es nie verwendet wurde.

(Auszug aus der Betriebsanleitung Fa. Skywalk)



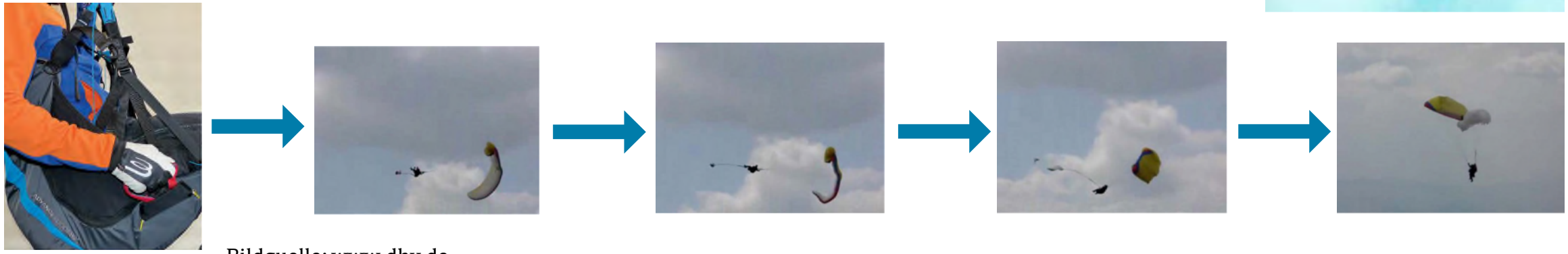
Bildquelle: www.dhv.de

Beispiel „Sicherheitsfunktion“

Anforderungen an die „Sicherheitsfunktion“

→ Viele Test-, „Acro-“ oder Wettbewerbspiloten haben 2 Retter dabei.

- HFT > 0, ggf. Redundanz
- Höhere Sicherheit bei Vorhandensein eines höheren Risikos und Versagen der ersten Sicherheitsfunktion



Bildquelle: www.dhv.de

Beispiel „Sicherheitsfunktion“

Unterschiede zur echten Sicherheitsfunktion

- Problem: Viele Unfälle passieren, weil der Retter zu spät oder gar nicht ausgelöst wird.
- Auslösung „von Hand“ problematisch
- Reaktion des Menschen muss passen
- Unterschied zur „echten“ Sicherheitsfunktion: Automatische Auslösung durch Sensor, Logik und Aktor!

Bildquelle: www.dhv.de

Beispiel „Sicherheitsfunktion“

Unterschiede zur echten Sicherheitsfunktion

- Die systematische Eignung der Rettungsgeräte wird entsprechend der geltenden Regeln überprüft, aber:
- Kein rechnerischer „SIL-Nachweis“

Betriebsordnung für Luftfahrtgerät (LuftBO)

Erster Abschnitt
Allgemeine Vorschriften

§ 3 Grundregel für den Betrieb

(1) Der Halter hat das Luftfahrtgerät in einem solchen Zustand zu erhalten und so zu betreiben, daß kein anderer gefährdet, geschädigt oder mehr als nach den Umständen unvermeidbar behindert oder belästigt wird.
(2) Luftsportgeräte dürfen nur mit einem zugelassenen Rettungsgerät betrieben werden. Luftsportgeräteführer und Fluggast müssen einen geeigneten Kopfschutz zur Abwehr von Verletzungen bei Unfällen oder sonstigen Störungen tragen. Der Beauftragte kann Ausnahmen zulassen. Absatz 1 bleibt unberührt.
(3) Luftfahrtgeräte nach § 1 Abs. 4 der Luftverkehrs-Zulassung-Ordnung dürfen nur betrieben werden, wenn die Lufttüchtigkeit nach der Verordnung zur Prüfung von Luftfahrtgerät nachgewiesen worden ist.

Bildquelle: Pixabay

PLT-Schutzkreisberechnung nach VDE 2180-3 SIL 0006 11/DE/01.20

Endress+Hauser
People for Process Automation

Anforderung an Schutzfunktion: SIL 2
Summe aller PFD- Werte:

Sensorik:		Einzelwert: [PFD]	
Sensor 1.1	Deltapilot	1,00E-03	
Signalwandler 1.1	Messumformer	4,96E-04	
Summe Sensorik:		+	1,50E-03
Steuerung:			
Verarbeitung 1.1			
Verarbeitung 1.2			
Verarbeitung 1.3			
Verarbeitung 1.4			
Summe Steuerung:		+	0,00E+00
Aktor:			
Aktor 1.1	Schütz	4,38E-04	
Aktor 1.2			
Aktor 1.3			
Aktor 1.4			
Summe Aktor:		+	4,38E-04
Summe: [PFD]		+	1,93E-03

Safety Integrity Level SIL Endress+Hauser

Der berechnete PFD- Wert entspricht SIL 2 Die Schutzfunktion SIL 2 ist erfüllt.

Anmerkung:
Die mittlere Versagenswahrscheinlichkeit wurde mit den Formeln der VDE 2180-4 mit einer Prüftiefe von 100 % ohne Berücksichtigung einer Reparaturdauer (MTTR) berechnet.

Grenzwerte:	SIL1:	≥10E-2 < 10E-1	SIL2:	≥10E-3 < 10E-2	SIL3:	≥10E-4 < 10E-3	SIL4:	≥10E-5 < 10E-4

Weil am Rhein, 27.03.2020 erstellt: i.a. M. Vinzenz Digital unterschrieben von Markus Vinzenz Datum: 2020.03.27 07:23:07 +01'00' geprüft: i.A. Stefan Lauer Digital signiert von: Stefan Lauer Datum: 2020.03.27 08:41:09 +01'00'

Beispiel „Sicherheitsfunktion“

Unterschiede zur echten Sicherheitsfunktion

- Verhalten der Sicherheitsfunktion bei aktiven Fehlern (Auslösung der Sicherheitsfunktion ohne die aufgabengemäß festgelegten Bedingungen)
- Sollte genauso gefahrlos sein wie der Normalbetrieb!

- … obwohl, bei manchen echten Sicherheitsfunktionen…

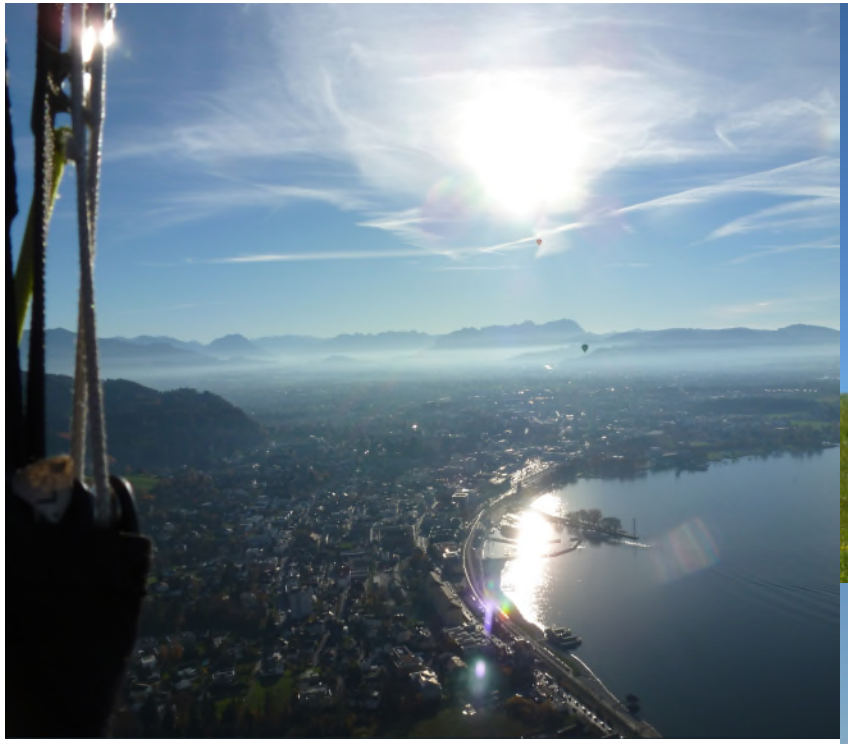
Die **Reaktorschnellabschaltung** (kurz **RESA** oder **Scram**, engl. für „abhauen“, „Leine ziehen“), auch **Reaktortrip**,[1] ist eine Sicherheitsmaßnahme bei Kernreaktoren. Die RESA kann in Störfällen manuell vom Bedienungspersonal oder automatisch durch ein Reaktorschutzsystem beim Überschreiten bestimmter Grenzwerte ausgelöst werden.[2] Um Fehlalarme möglichst zu vermeiden, ermittelt das Reaktorschutzsystem Messwerte mehrfach redundant, bevor es die Abschaltung auslöst.

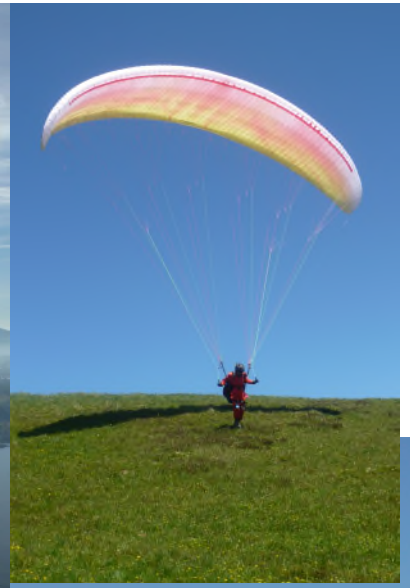
Bei der Nuklearkatastrophe von Tschernobyl kam es aufgrund konstruktiver Besonderheiten der RBMK-Steuerstäbe nach Auslösung des RESA-Schalters (russisch Аварийная Защита 5-й категории (АЗ-5), *Awarijnaja Saschtschita 5-j kategorii (AZ-5)*, „Notfallschutz der 5. Kategorie“) trotzdem zu einer kurzfristigen Leistungs*steigerung*, die den Reaktor prompt überkritisch machte und so seine Zerstörung mit schwersten Folgen auslöste.

Quelle: Wikipedia

Bildquelle: www.dhv.de

Herzlichen Dank für Ihre Aufmerksamkeit!





Bildquelle: Eigener Fundus

Ganzheitliches Riskomanagement

Peter Sieber

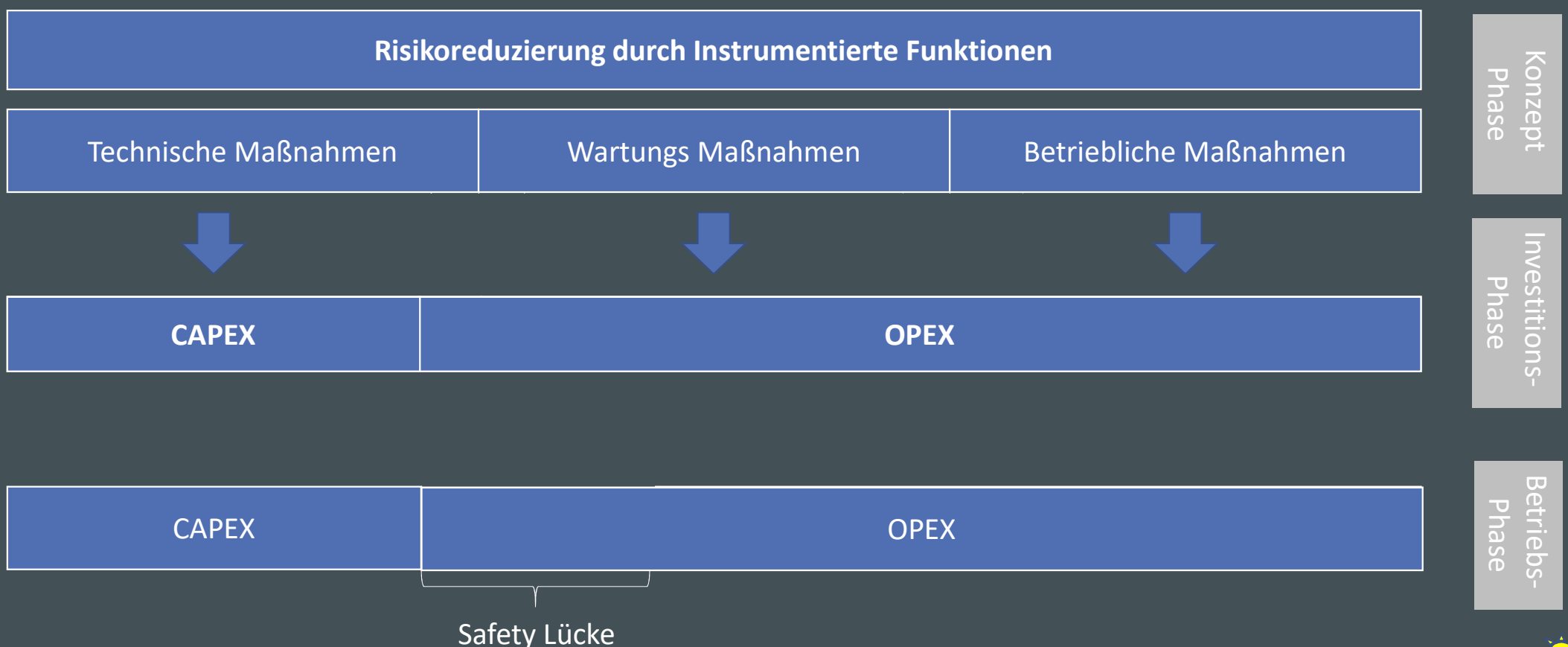
HIMA

Sicherheit und Kosten während des Lebenszyklus

CAPEX werden reduziert durch:

- Reduktion im Safety Engineering
- Reduktion der Produktkosten
- Reduktion des Testaufwandes

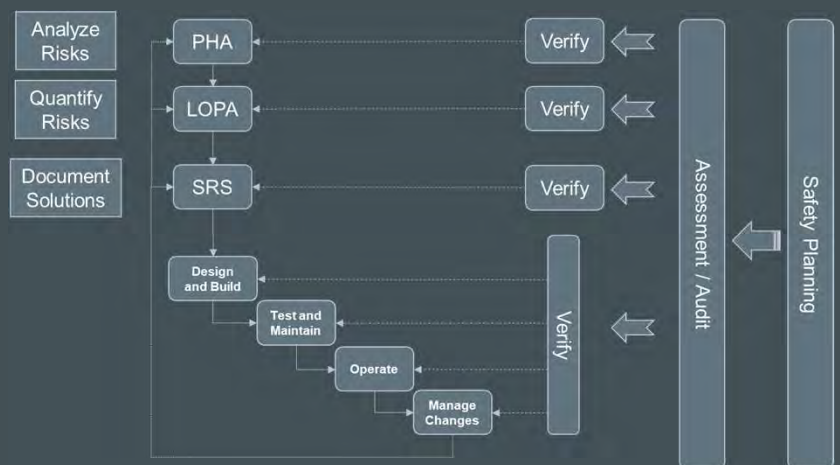
Sicherheit und Kosten während des Lebenszyklus



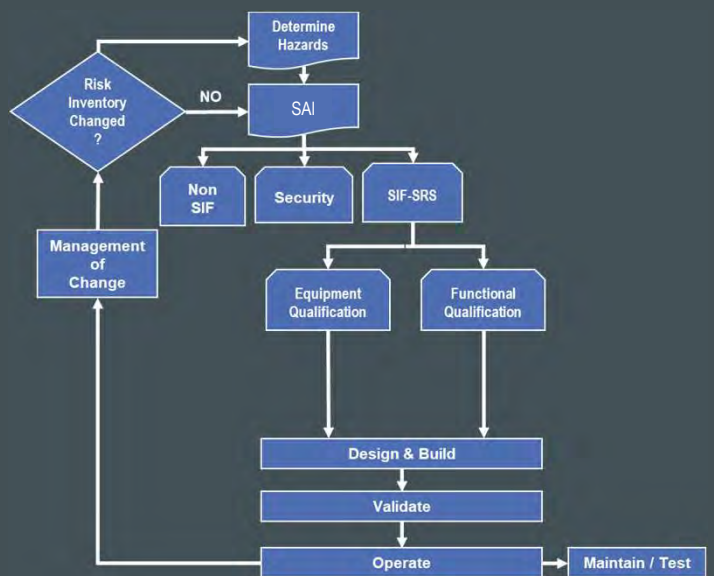
Die Beherrschung der Safety Lücke

Worum müssen wir uns kümmern?

Was wir tun?



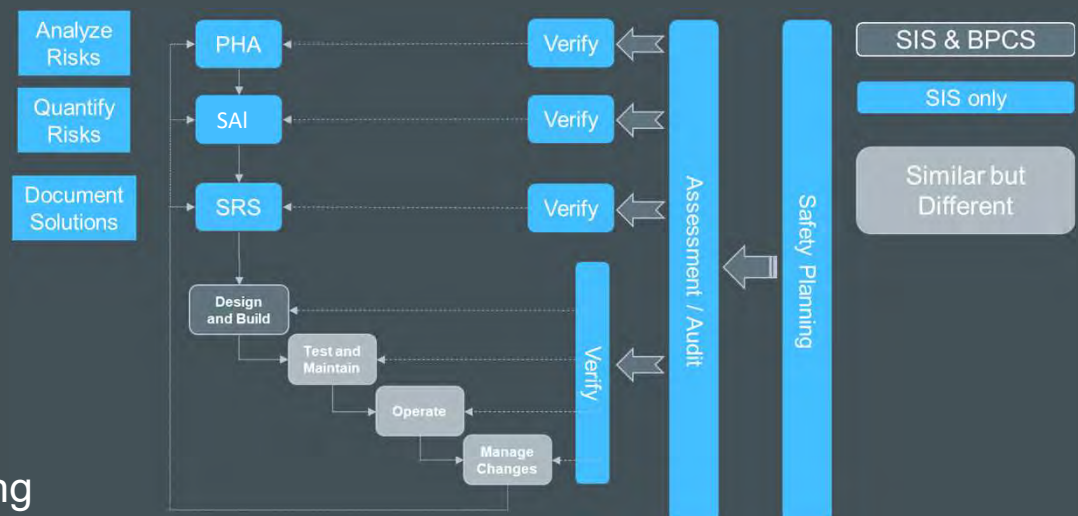
Wie wir es tun?



Für effiziente funktionale Sicherheit müssen wir uns um das “Was” und das “Wie” kümmern

Was wir tun.....

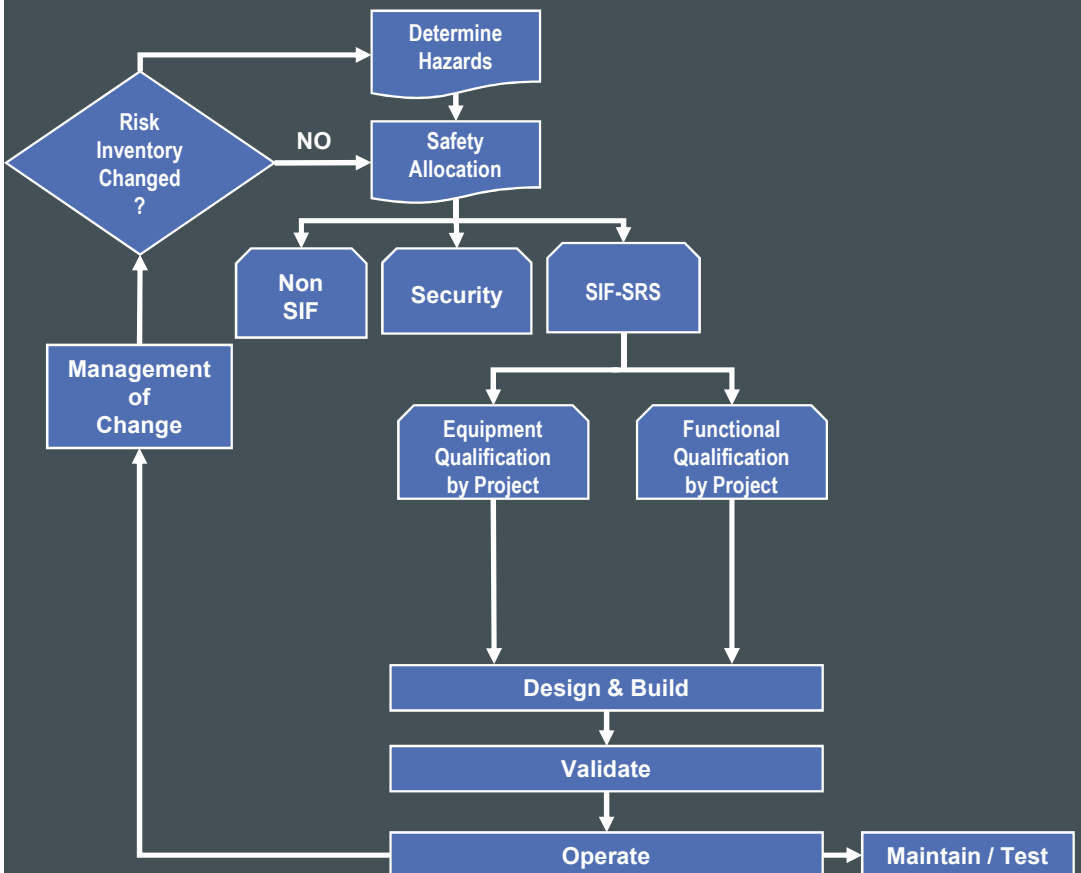
- Der eigentliche Systembau ist identisch
- Testen, Wartung, Betrieb und Änderung sind ähnlich, aber anders
- Alle anderen Schritte beziehen sich ausschließlich auf SIS



Zusammenfassung:

1. SIS Engineering ist nicht wie BPCS Engineering
2. Es gibt nur begrenzte Überlappungen
3. Wenn wir nach mehr Effizienz streben, müssen wir Safety Engineering als eigenständigen Prozess verstehen

Wie wir es tun ……



Bearbeiten der “Safety Basis”

- Nutzung spezifischer Werkzeuge
- H&RA und Safety Allocation werden (häufig) mit unterschiedlichen Werkzeugen gemacht
- Non-SIF/ Non-Safety/SIF-SRS werden unterschiedlich geplant

Equipment Qualifikation
Funktions Qualifikation

- projektspezifisch
- Ohne Werkzeugunterstützung
- Ohne Berücksichtigung der Wartungsprozeduren

Design und Build

- Verwendung der BPCS Prinzipien

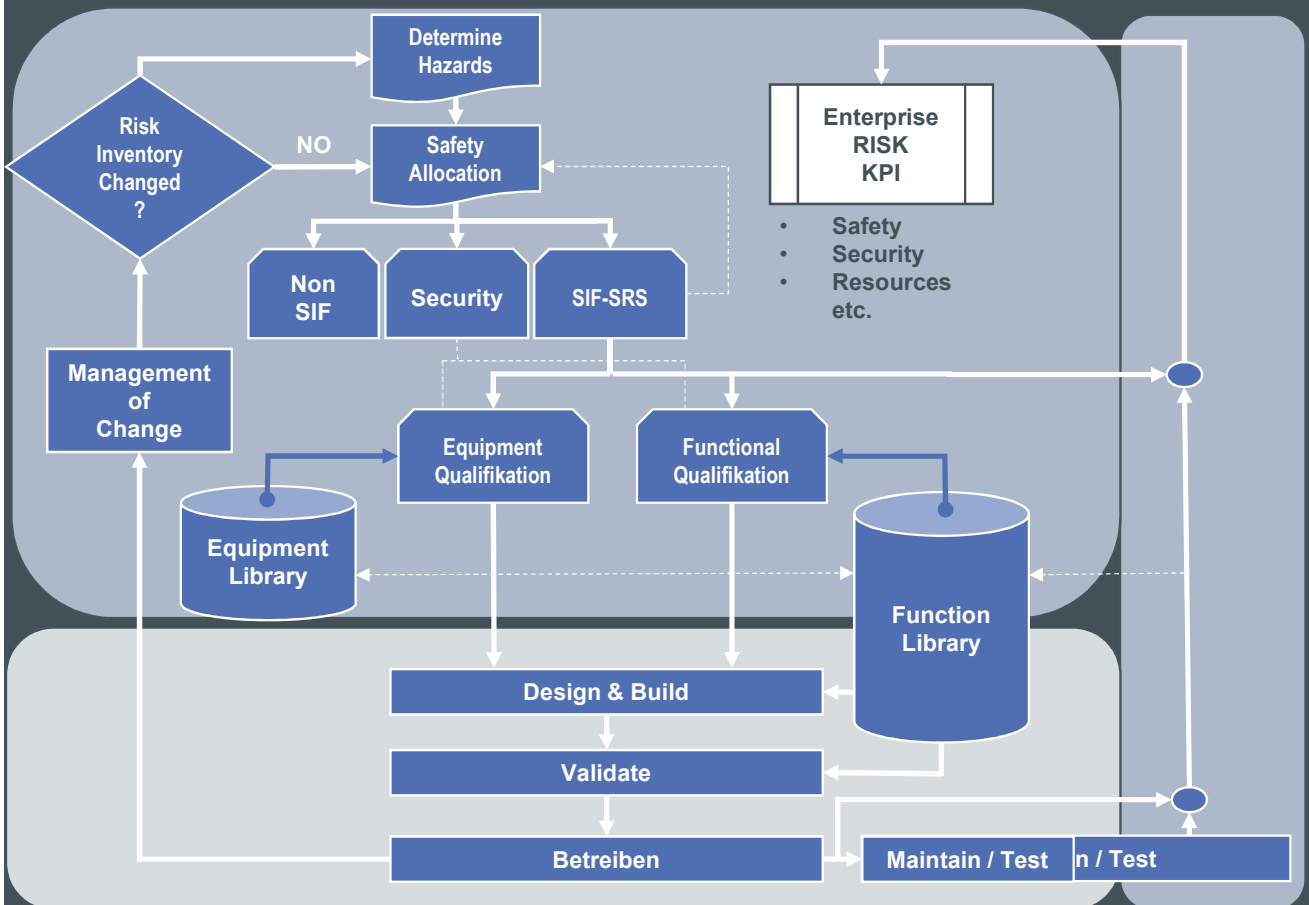
Maintenance & Testing

- Unter Nutzung des ERP

Management of Change

- Manueller Prozess

How We Do It More Efficiently ……



Nutzung einer Informationsplattform für

- Alle Sicherheitsaspekte
- Automatische Referenzierung der Aktivitäten
- Unterstützung von Teamwork
- Management of Change während des Engineering

Nutzung vor-qualifizierter Komponenten

- Incl. deren Funktionsbeschreibung
- Incl. zertifizierter Funktionen
- Incl. zertifizierter Test Prozeduren

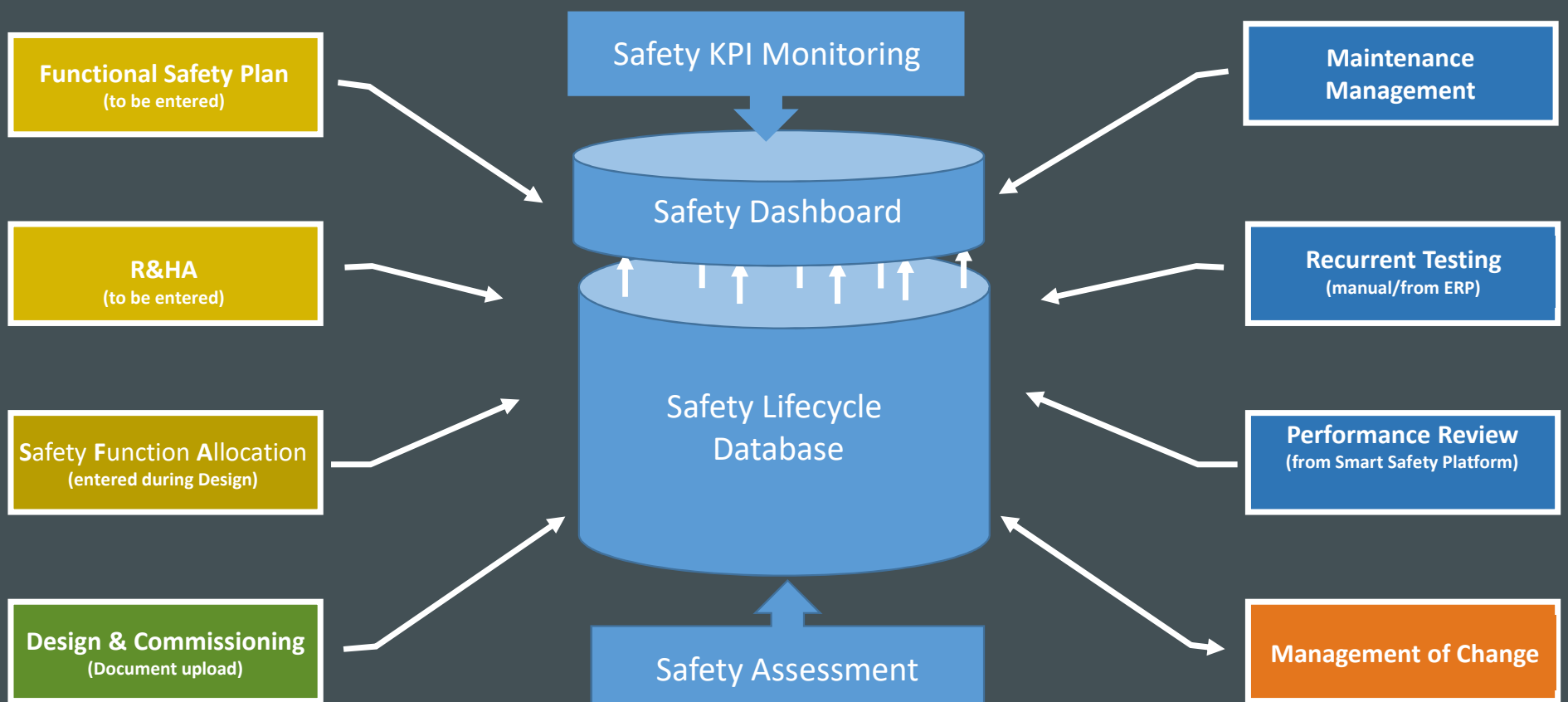
Nutzung einer zertifizierten Engineering Plattform

- Tools tauschen Daten aus
- Automatischer Informationstransfer
- Unterstützung automatischer Tests

Erlaubt aktives Risiko Management

- Für das gesamte Unternehmen
- Basierend auf frei definierbaren KPI

I 4.0 Umgebung für funktionale Sicherheit



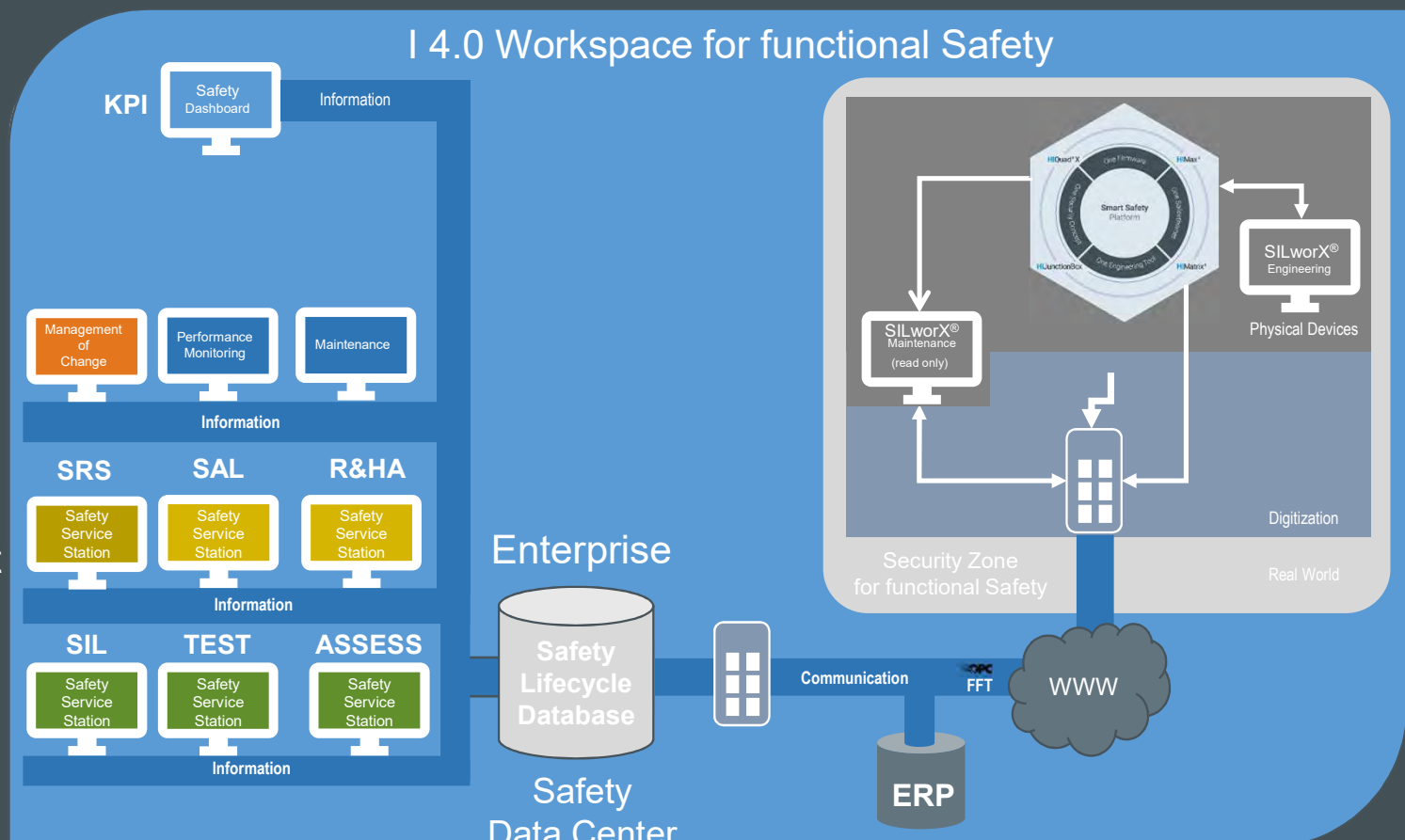
I 4.0 Workspace for functional Safety

Integration d. Sicherheitsdaten
(ohne Konfigurationsänderung)

- Alle Diagnosen
- Alle Brücken
- Alle Alarme
- Alle Abschaltungen
- Alle Wartungsarbeiten (z.B. vom SAP)

Anzeigen von

- Status aller SIF
- Brückungschalter Management
- Performance Information
- Wartungsplanung für funktionale Sicherheit
- Dokumentation von Wartungs-arbeiten



“Die Welt ist ein gefährlicher Platz; allerdings nicht wegen böser Leute, sondern wegen denen, die nichts dagegen tun.”

Albert Einstein

Also: Lassen Sie uns etwas unternehmen!

Peter Sieber

Thank You.
谢谢

HIMA (Shanghai) Industrial Automation Co., Ltd.
希马（上海）工业自动化有限公司
7th Floor, Building2, No.615, Ningqiao Road,
Jinqiao Export Processing Zone, Pudong, Shanghai,
201206, P.R.China
上海市浦东新区金桥出口加工区宁桥路615号2幢7层

RAMSYS
DAS machen Ingenieure

Warum benötigen wir Funktionale Sicherheit, 30.09.2020

Agenda

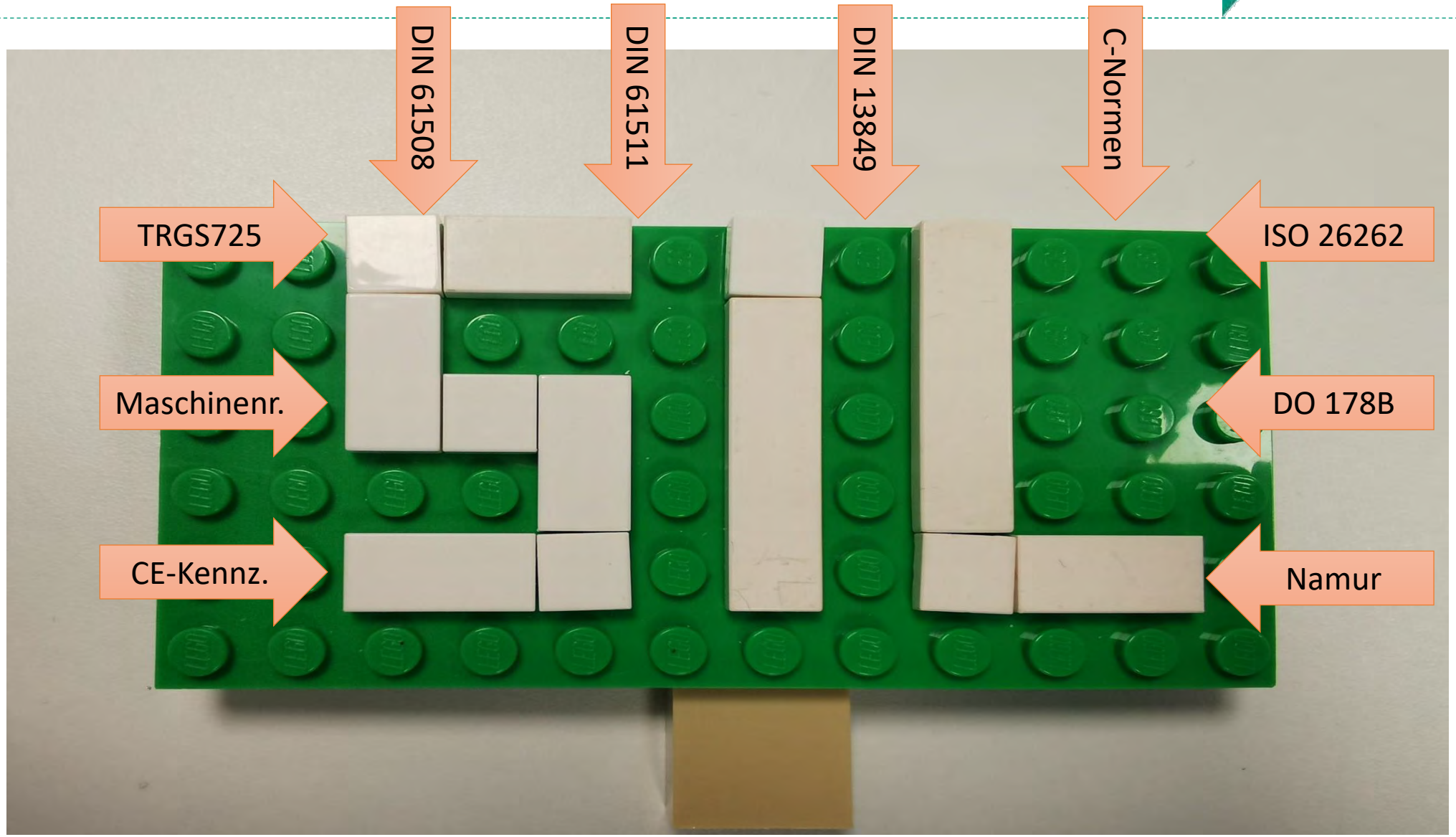
- Wo brauchen wir Funktionale Sicherheit?
- Stetige Weiterentwicklung
- Personelle Einsatzgebiete der Funktionalen Sicherheit
- Dokumentationsflut händeln

Wo brauchen wir Funktionale Si.

Stetige Weiterentwicklung

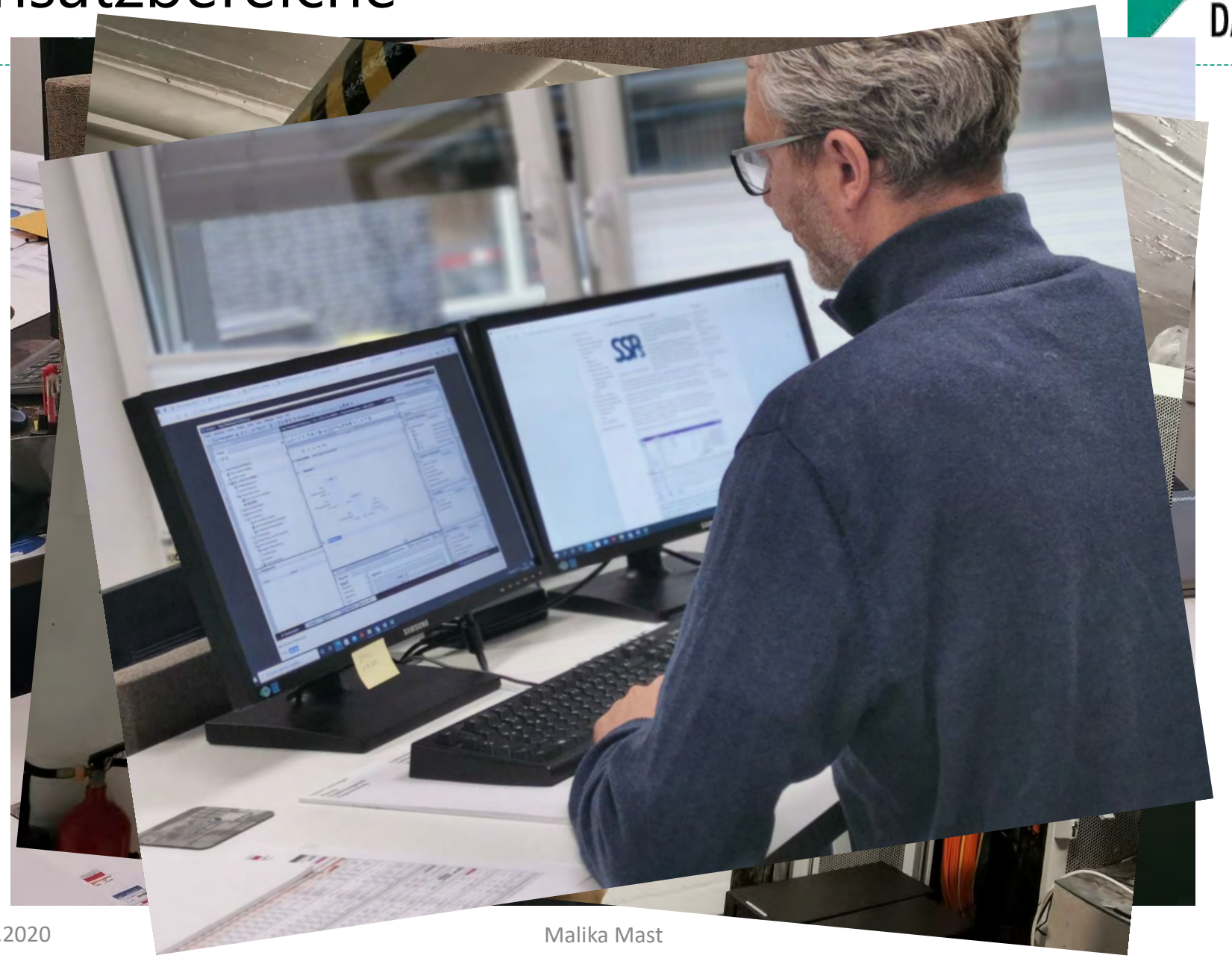
RAMSYS
DAS machen Ingenieure

Stetige Weiterentwicklung

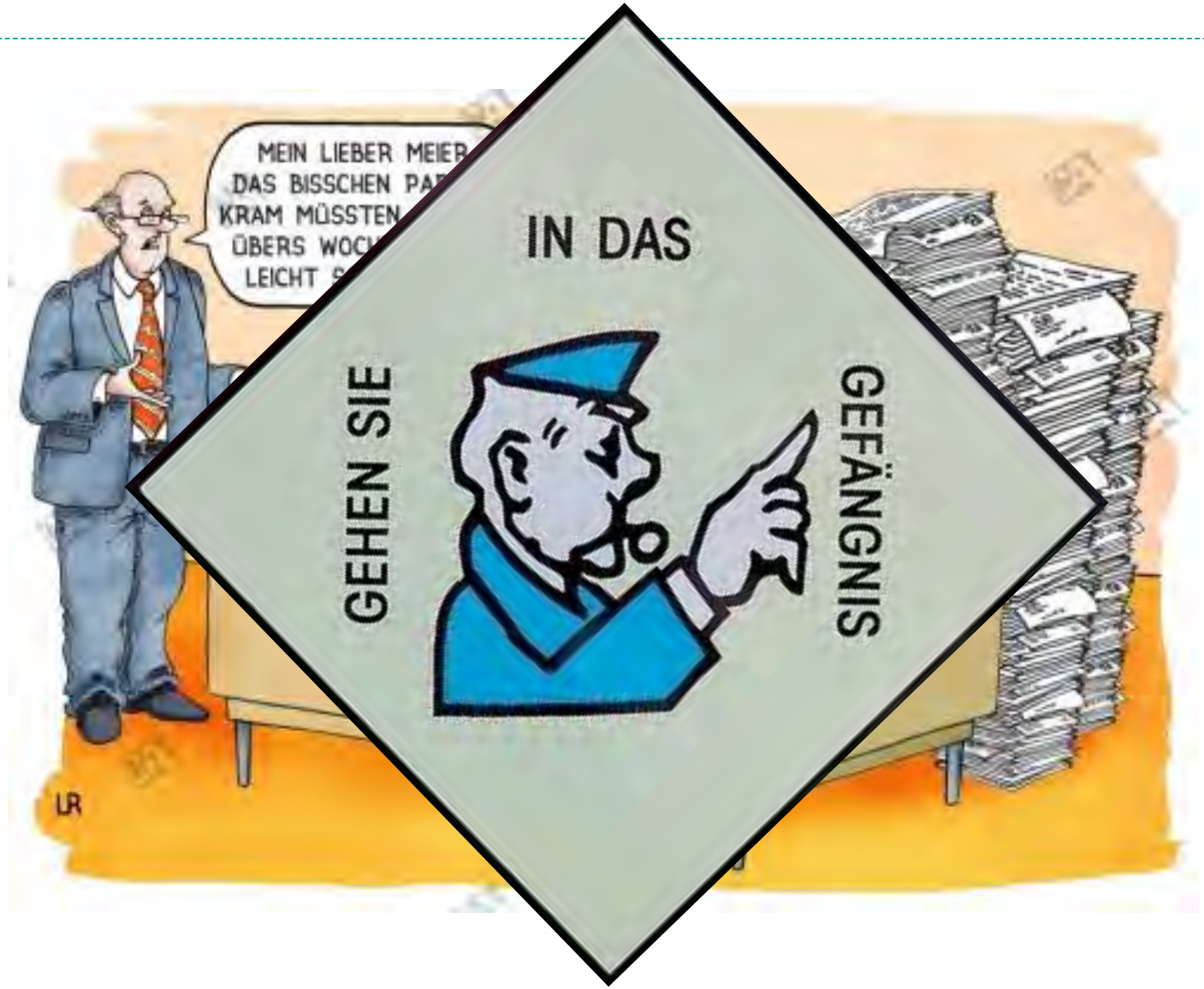


Einsatzbereiche

RAMSYS
DAS machen Ingenieure



Dokumentation



Sicherheitslebenszyklus

Für Ingenieurbüros im Normalfall

Management und Beurteilung der

Aufbau und Planung des Sicherheits-lebenszyklus

Gefährdungs- und Risikobeurteilung

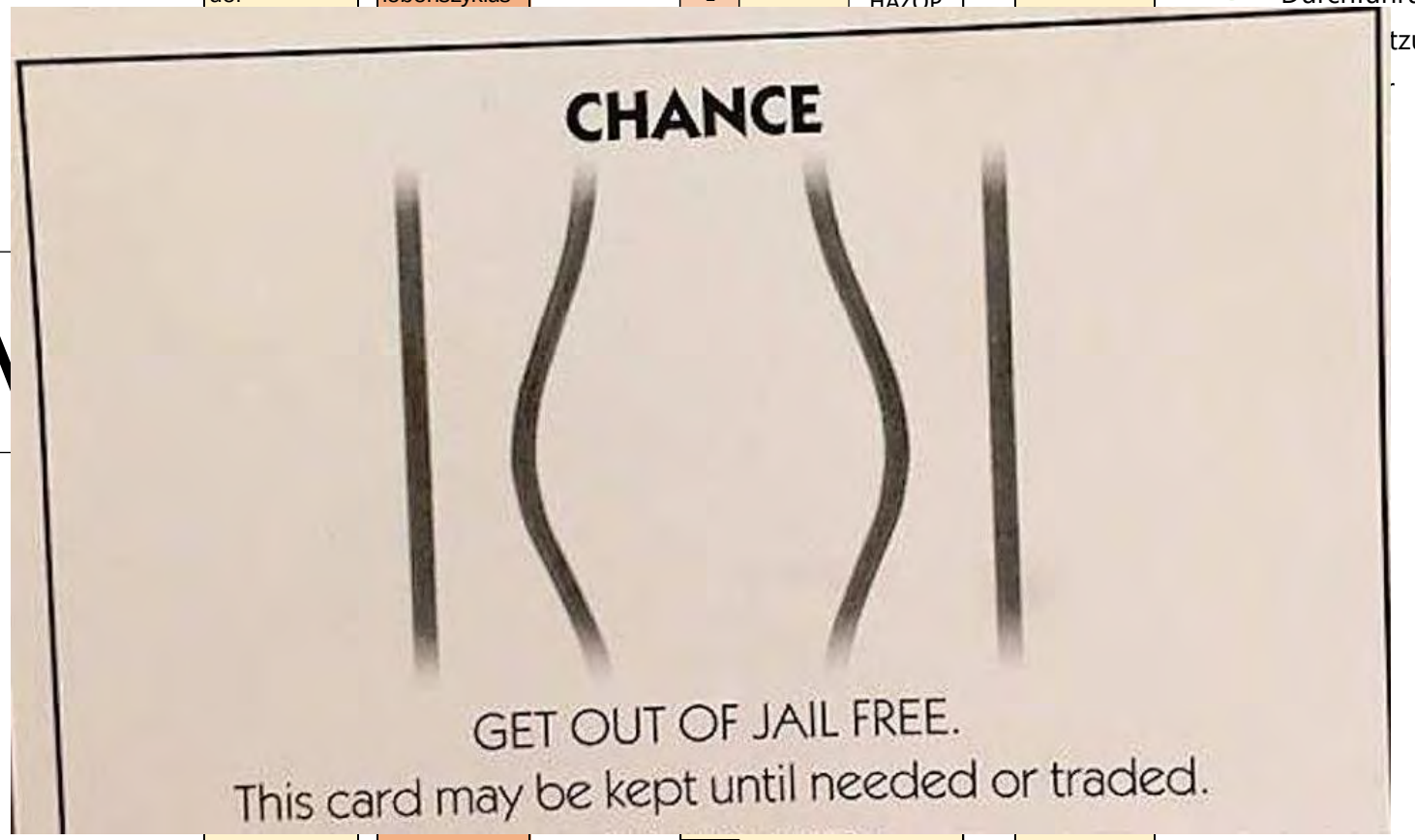
1

HAZOP

Verifikation

- Durchführung
- tzung
-

FSM



7

Zeitpunkt 5

Außerbetriebnahme

8

10

11

12

IEC61511 Teil 1

Kontaktdaten Malika Mast

Persönliche Vorstellung:

Malika Mast

Geschäftsführerin

- FSCEA (Functional Safety Certified Engineer Application)
  A031_01255/18 (TÜV Nord)
- FS Eng für Maschinen
  # 14527/17 (TÜV Rheinland)

Kontaktdaten:

Hervester Straße 36

46286 Dorsten

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

m.mast@ramsys.org

www.ramsys.org

Reduzierungsstufe

versus

Safety Integrity Level (SIL)

SIL-Slam, Online Seminar

Martin Herrmann,
Evonik Operations GmbH

EVONIK
KRAFT FÜR NEUES

Explosionsschutz und Funktionale Sicherheit

Technische Regeln für Gefahrstoffe TRGS 725

Technische Regeln für Gefahrstoffe	Gefährliche explosionsfähige Atmosphäre – Mess-, Steuer- und Regeleinrichtungen im Rahmen von Explosionsschutzmaßnahmen	TRGS 725

Reduzierungsstufen

DIN EN 50495 (VDE 0170-18)

	DIN EN 50495 (VDE 0170-18)	DIN
	Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation" bekannt gegeben worden.	VDE

Safety Integrity Level (SIL)

VDI/VDE 2180 Blatt 6

ICS 25.040.40, 35.240.50	VDI/VDE-RICHTLINIEN	Juni 2013 / June 2013
VEREIN DEUTSCHER INGENIEURE VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK	Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) Anwendung der funktionalen Sicherheit im Rahmen von Explosionsschutzmaßnahmen Safeguarding of industrial process plants by means of process control engineering (PCE) Application of functional safety in the context of explosion protection	VDI/VDE 2180 Blatt 6 Ausg. deutsch/englisch Issue German/English

Safety Integrity Level (SIL)

IEC TS 60079-42

Risk Reduction Factor (RRF)

Explosionsschutz und Funktionale Sicherheit

Lösung ???

Explosionsschutz und Funktionale Sicherheit

Wir brauchen eine Norm

IEC-DIN-EN-VDE-VDI/VDE 615110079-725-2180

Teil 1 (informativ)

… gibt es aber leider nicht …

Gefährdungsbeurteilung nach GefStoffV[1)]

Explosionsschutz

TRGS 720 [2006, z. Zt. Beschlussvorlage beim AGS]
Gefährliche explosionsfähige Atmosphäre -Allgemeines

TRGS 721 [ENTWURF 2019]
Gefährliche explosionsfähige Atmosphäre - Beurteilung der Explosionsgefährdung

TRGS 722 [2012]
Vermeidung oder Einschränkung gefährlicher explosionsfähiger Gemische

TRGS 723 [2019]
Vermeidung der Entzündung gefährlicher explosionsfähiger Gemische

TRGS 724 [2019]
Maßnahmen des konstruktiven Explosionsschutzes, welche die Auswirkung einer Explosion auf ein unbedenkliches Maß beschränken

TRGS 725 [2018]
Mess-, Steuer- und Regeleinrichtungen im Rahmen von Explosionsschutzmaßnahmen

Kann die Bildung gefährlicher explosionsfähiger Gemische nicht sicher verhindert werden, hat der Arbeitgeber zu beurteilen und zu dokumentieren:

1. die Wahrscheinlichkeit und Dauer des Auftretens gefährlicher explosionsfähiger Gemische (siehe hierzu TRGS 722),

2. die Wahrscheinlichkeit des Vorhandenseins oder der Entstehung und des Wirksamwerdens von Zündquellen einschließlich elektrostatischer Entladungen (siehe hierzu TRGS 723 und TRGS 727) und

3. das Ausmaß der zu erwartenden Auswirkungen von Explosionen (siehe hierzu TRGS 724).

1) Aufzählung nicht vollständig

Gefährdungsbeurteilung nach GefStoffV

Explosionsschutz

TRGS 720 [2006]
Gefährliche explosionsfähige Atmosphäre -Allgemeines

TRGS 721 [ENTWURF 2019]
Gefährliche explosionsfähige Atmosphäre - Beurteilung der Explosionsgefährdung

TRGS 722 [2012]
Vermeidung oder Einschränkung gefährlicher explosionsfähiger Gemische

TRGS 723 [2019]
Vermeidung der Entzündung gefährlicher explosionsfähiger Gemische

TRGS 724 [2019]
Maßnahmen des konstruktiven Explosionsschutzes, welche die Auswirkung einer Explosion auf ein unbedenkliches Maß beschränken

TRGS 725 [2018]
Mess-, Steuer- und Regeleinrichtungen im Rahmen von Explosionsschutzmaßnahmen

Kann die Bildung gefährlicher explosionsfähiger Gemische nicht sicher verhindert werden, hat der Arbeitgeber zu beurteilen und zu dokumentieren:

1. die Wahrscheinlichkeit und Dauer des Auftretens gefährlicher explosionsfähiger Gemische (siehe hierzu TRGS 722),

2. die Wahrscheinlichkeit des Vorhandenseins oder der Entstehung und des Wirksamwerdens von Zündquellen einschließlich elektrostatischer Entladungen (siehe hierzu TRGS 723 und TRGS 727) und

3. das Ausmaß der zu erwartenden Auswirkungen von Explosionen (siehe hierzu TRGS 724).

Gefährdungsbeurteilung nach GefStoffV

Explosionsschutz	Bezug zur Funktionalen Sicherheit
TRGS 720 [2006] Gefährliche explosionsfähige Atmosphäre -Allgemeines	
TRGS 721 [ENTWURF 2019] Gefährliche explosionsfähige Atmosphäre - Beurteilung der Explosionsgefährdung	
TRGS 722 [2012] Vermeidung oder Einschränkung g.e.A.	
TRGS 723 [2019] Vermeidung der Entzündung gefährlicher explosionsfähiger Gemische	
TRGS 724 [2019] Maßnahmen des konstruktiven Explosionsschutzes, welche die Auswirkung einer Explosion auf ein unbedenkliches Maß beschränken	
TRGS 725 [2018] Mess-, Steuer- und Regeleinrichtungen im Rahmen von Explosionsschutzmaßnahmen	**Anwendungsbereich:** • Diese TRGS konkretisiert die Anforderungen an die Zuverlässigkeit von Mess-, Steuer-, und Regelungseinrichtungen • Die Bewertung der Wirksamkeit von Maßnahmen nach TRGS 722, TRGS 723 und TRGS 724 **ist nicht Bestandteil der TRGS 725**

Funktionale Sicherheit TRGS 725

Lassen sich die Anforderungen der TRGS 725 für MSR-Einrichtungen im Explosionsschutz

mit den Anforderungen an PLT-Sicherheitseinrichtungen (z. B. VDI/ VDE 2180) direkt vergleichen?

Beispiel für die Umsetzung der Reduzierungsstufe 1 nach TRGS 725

Gefährdungsbeurteilung nach GefStoffV

Startpunkt für MSR-Einrichtungen

TRGS 725 — **oder** — **VDI/ VDE 2180 bzw. DIN EN 61511**

Betriebskonzept	Variante 1 **Ex-Vorrichtung K1** (Reduzierungsstufe 1)	Variante 2 **PLT- Betriebseinrichtung mit Sicherheitsfunktion** (PLT-BS)	Variante 3 **PLT-Sicherheitseinrichtung** (SIL 1)
– Erforderliche Schutzmaß-nahmen basieren auf dem Betriebskonzept – PLT-Betriebseinrichtungen **können** Bestandteil des Betriebskonzepts sein – MSR-Einrichtungen für die Anwendung der TRGS 725 festlegen	– Bewertung „mechanischer“ Komponenten der MSR-Einrichtung (ohne PLT) – Anhang 1 der TRGS 725 ist zu beachten – Keine Anforderungen an die Unabhängigkeit zwischen betrieblichen Einrichtungen und Ex-Einrichtungen im PLS => für die Überwachung – Änderungsmanagement (TRGS 725)	– Anforderungen an die Unabhängigkeit gemeinsam genutzter Komponenten (PLS) – Anwendung NA 165 – Änderungsmanagement (FuSi) – Anforderungen aus dem Anhang 1 Absatz 9 der TRGS 725 erfüllt !?	– PLT-SE ist in einer zertifizierten Steuerung realisiert (SSPS) – Risikoreduzierung größer als für eine K1-Maßnahme erforderlich (SIL 1 => 10 …100) – Alle Anforderungen der Funktionalen Sicherheit (SIL-Welt) werden eingehalten – ….

Zusammenfassung

- Die Bewertung der Wirksamkeit von Maßnahmen nach TRGS 722, TRGS 723 und TRGS 724 sind nicht Bestandteil der TRGS 725 aber wichtige Voraussetzung für die Festlegung von Anforderungen an MSR-Einrichtungen im Explosionsschutz

- Die Anforderungen der TRGS 725 lassen sich **[leider]** nicht direkt mit den Anforderungen der Funktionalen Sicherheit - z. B. der VDI/ VDE 2180 - vergleichen

- Die Überarbeitung der TRGS 725 beginnt noch in 2020


EVONIK
KRAFT FÜR NEUES

1. SIL – SLAM

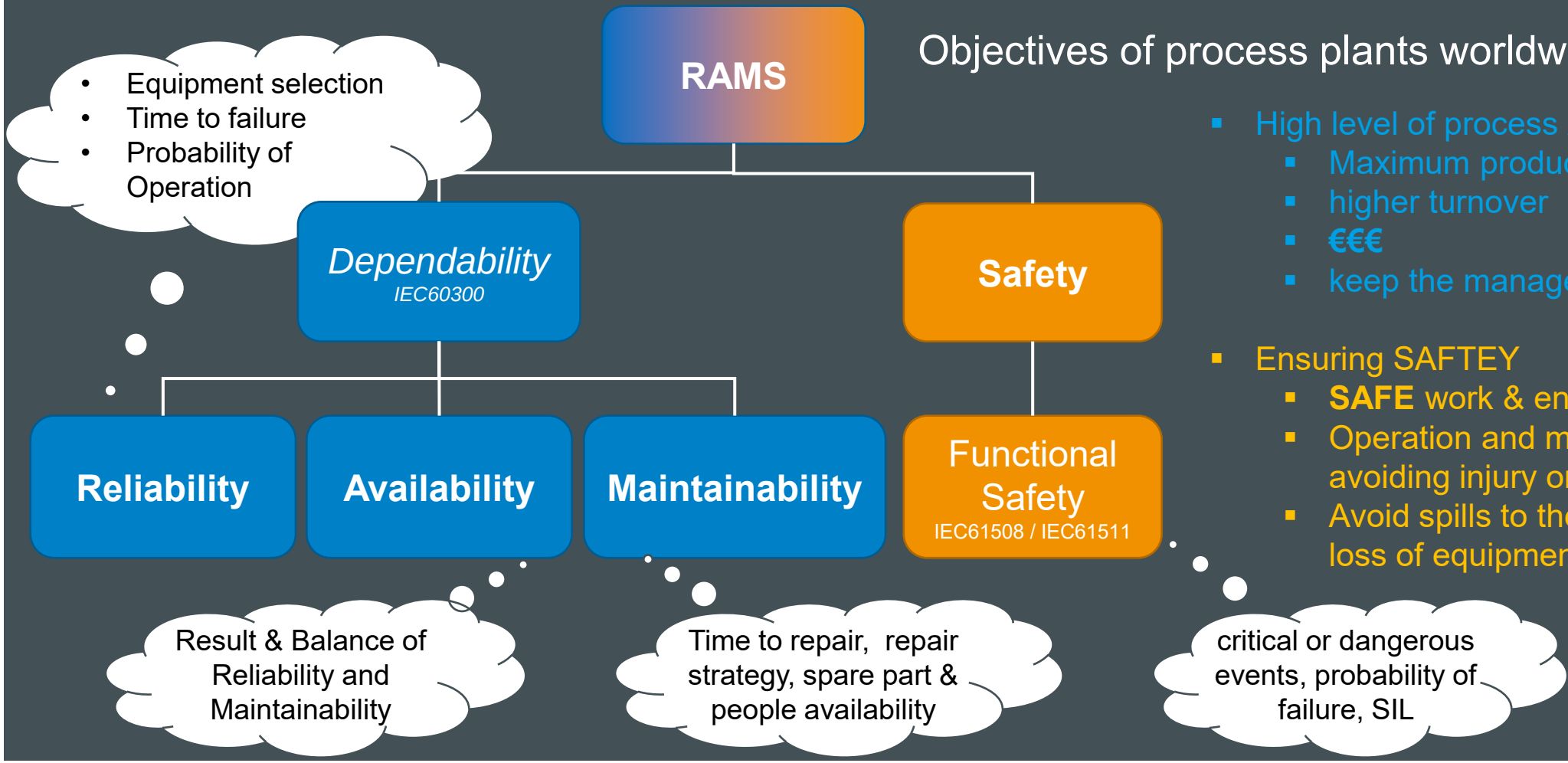
Verfügbarkeit von Sicherheitssystemen

30.09.2020

Ivo Hanspach - Director Product Management

HIMA SMART SAFETY.

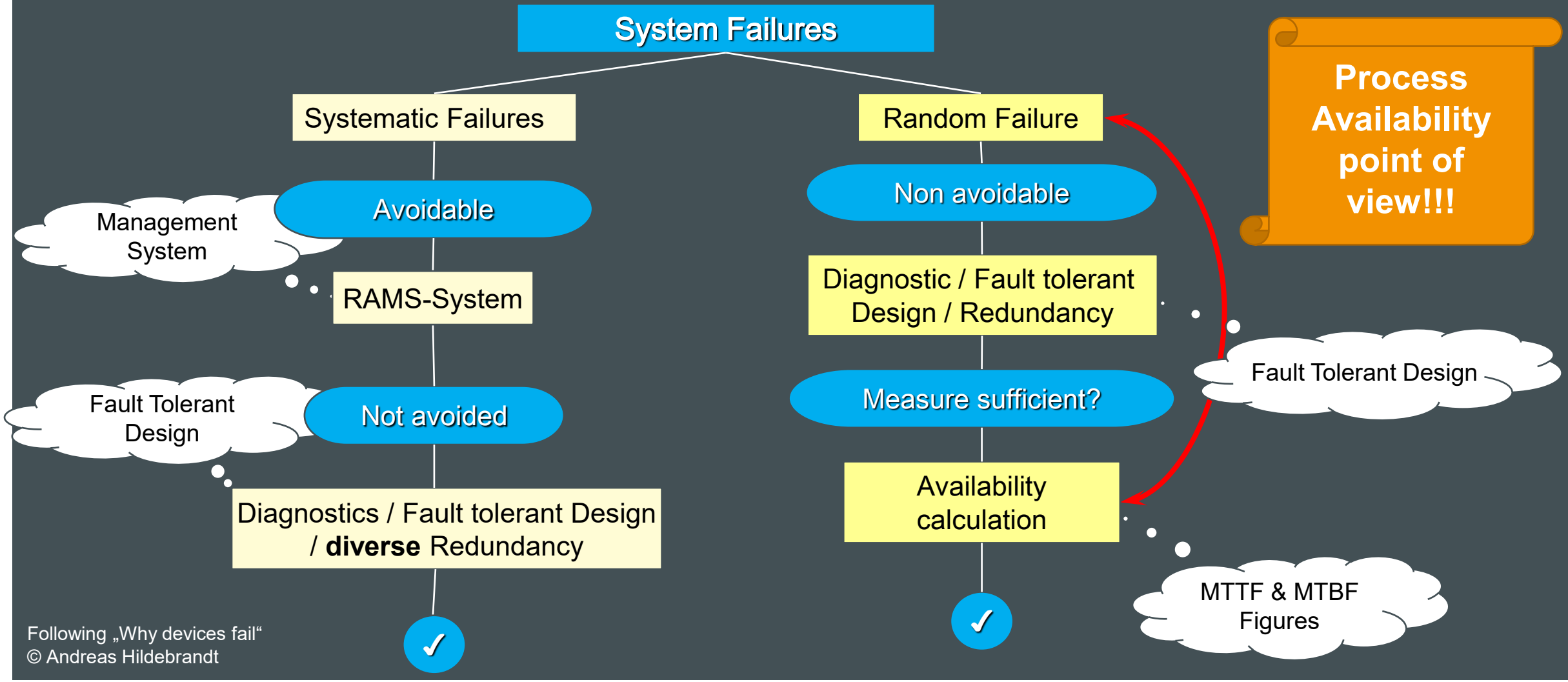
Objectives of process plants



Objectives of process plants worldwide are two-fold:

- High level of process **AVAILABILITY**
  - Maximum production
  - higher turnover
  - **€€€**
  - keep the management happy
- Ensuring SAFTEY
  - **SAFE** work & environment
  - Operation and maintaining and avoiding injury or death of humans
  - Avoid spills to the environment and loss of equipment or production

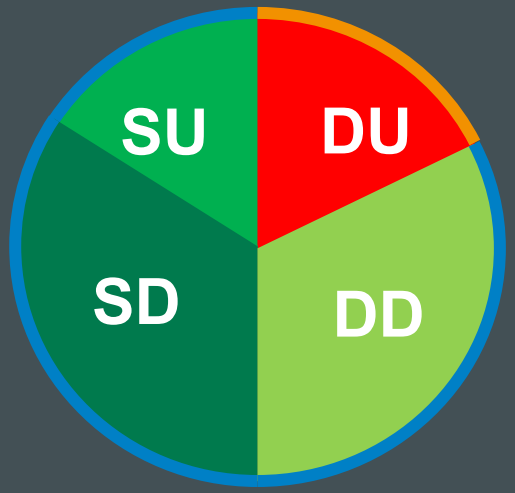
How devices can fail and how to control it



Failures (λ) - How devices can fail

- Safe Failures
  - Safe detected
  - Safe undetected

=> potential to cause loss of production (spurious trips)



- Dangerous Failures
  - Dangerous detected
  - Dangerous undetected

=> Potential to cause damage

Dependability
IEC60300

Safety

Equations for spurious trip rate calculation => ISA TR84.0.02

How Systems operate - MTTF & MTTR & MTBF

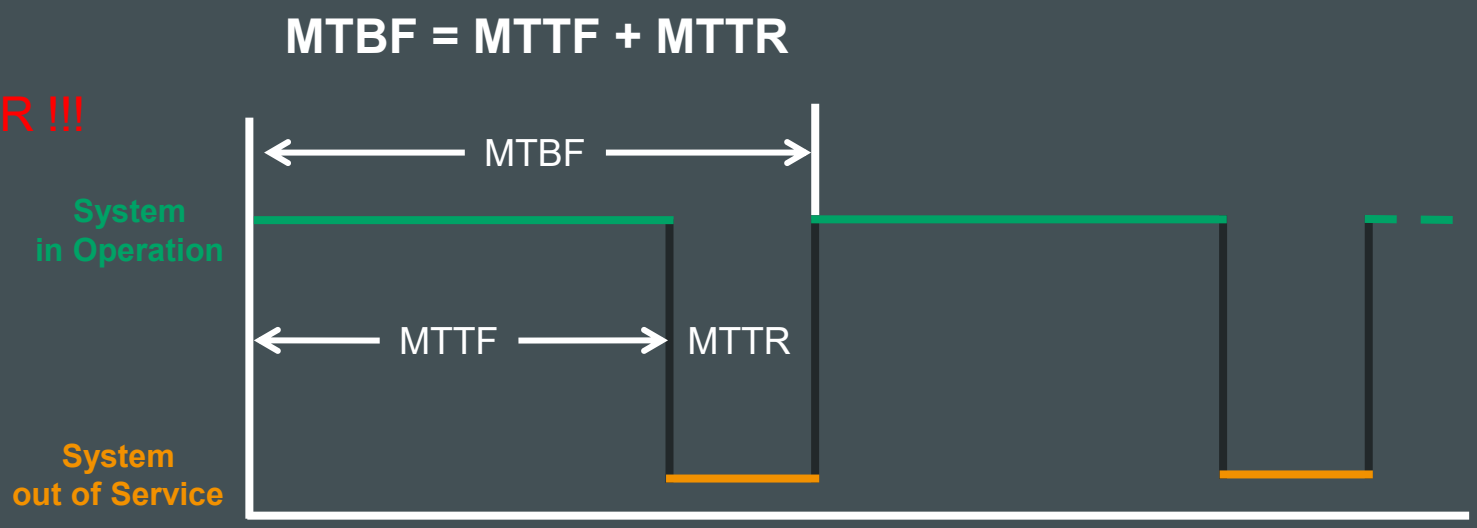
MTTF = Mean Time To Failure

MTTR = Mean Time To Restoration (Detect+Repair)

MTBF = Mean Time between failures
(is the abbreviation for the mean (average) operating time between failures of repairable systems)

Very often assumed and stated:

MTBF = MTTF: only if MTTF>>MTTR !!!



From failure rate (λ) to MTTF

λ (failure rate) vs. MTFF

For components/devices with constant failure rate (general prerequisite):

$$MTTF = 1 / \lambda$$

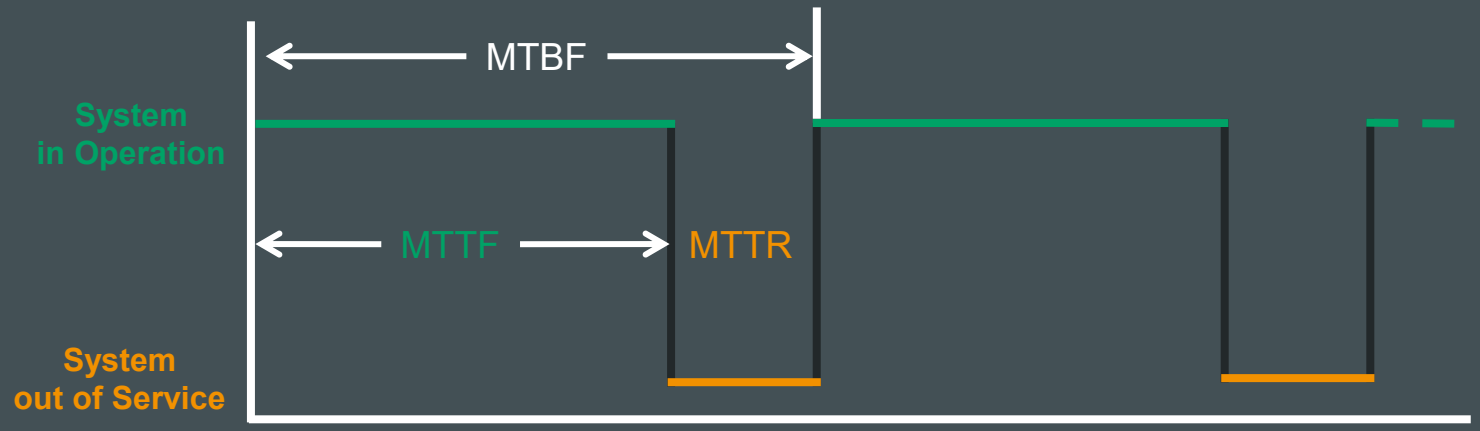
gem. IEC 61508 Teil 7 D.2.3.2

λ (failure rate) = number of failures / number of operating hours

How about the Availability of Systems

The availability of a system is determined by the following equation:

$$\text{Availability [\%]} = \frac{MTTF}{MTTF + MTTR}$$



Just a simple price query?

1th Choice and recommendation of the purchase department

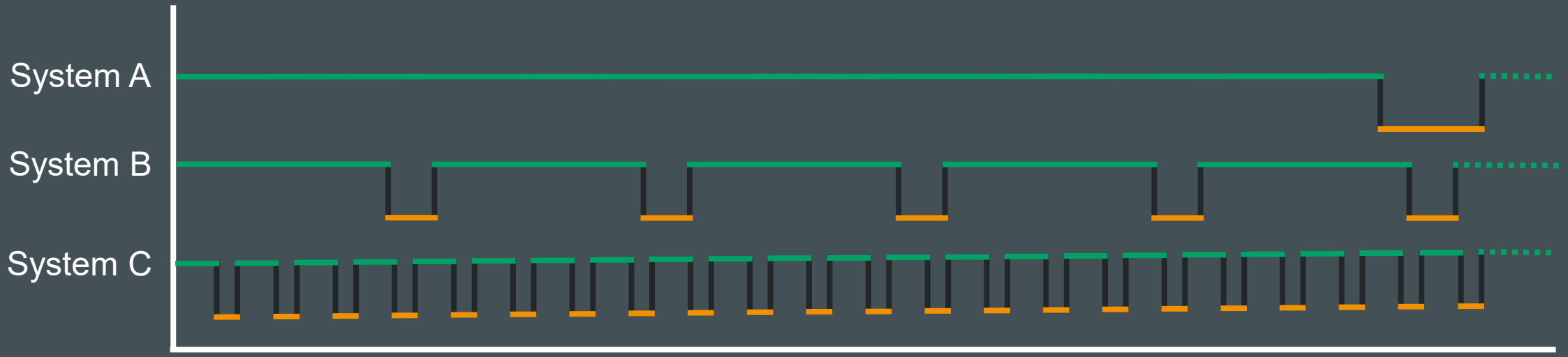
System	Availability [%]	Price
A	99,9965755%	65.000 €
B	99,9976852%	55.000€
C	99,9988426%	45.000€

This system has the lowest price and best availability!!!

Which System will you choose for a process application with the necessity for continuous operation?

Just a simple price query? What about Figures?

System	Availability [%]	Price	MTTF	MTTR
A	99,9965755%	65.000 €	10 years	3 hours
B	99,9976852%	55.000€	1 Month	1 minute
C	99,9988426%	45.000€	1 Day	1 second



System C is the best available one but not really reliable for “process or continues” applications

Further on – Don’t Compare Appels and Oranges

$MTTF_{module}$ >> $MTTF_{system}$ >> $MTTF_{comprehensive\ system}$

That‘s simply mathematics

$$MTBF_{seriell} = \frac{1}{\frac{1}{MTBF_a} + \frac{1}{MTBF_b} + \frac{MTTR}{MTBF_a \cdot MTBF_b}}$$

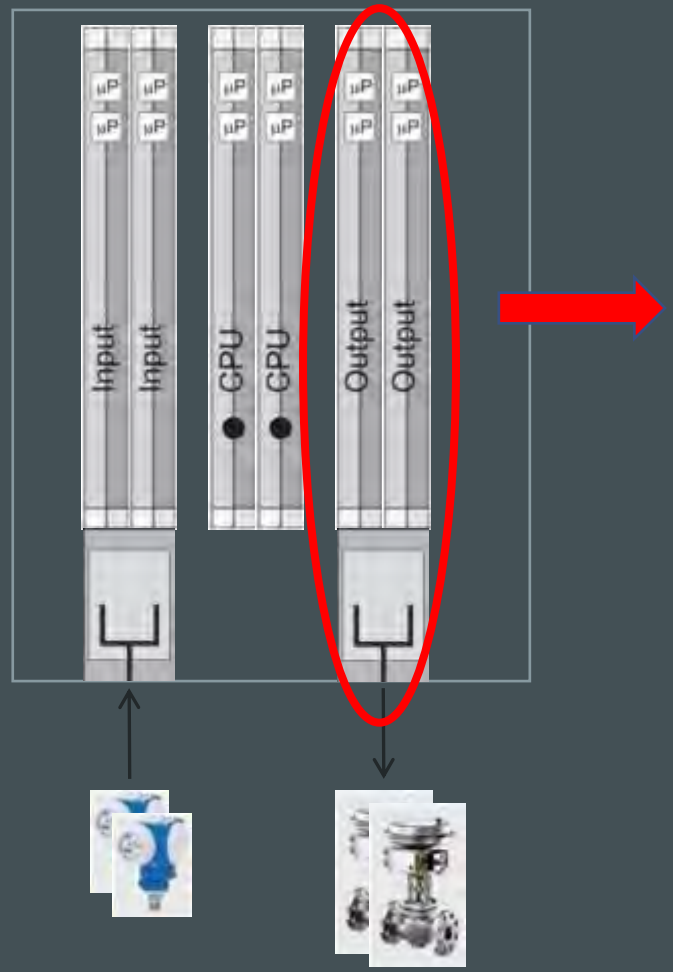
Further on – Don’t Compare Appels and Oranges

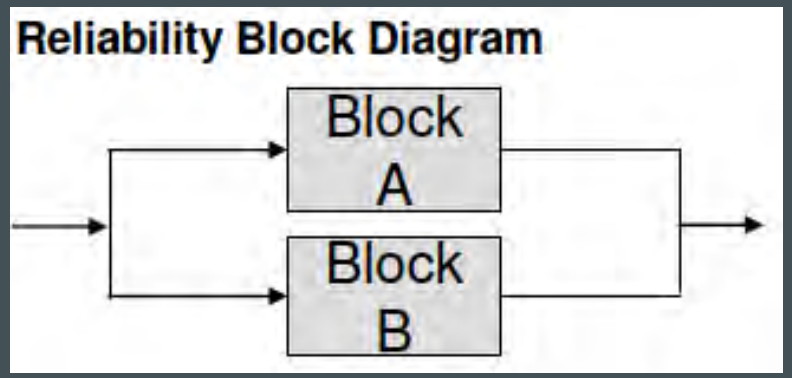
$MTTF_{module}$ >> $MTTF_{system}$ >> $MTTF_{comprehensive\ system}$

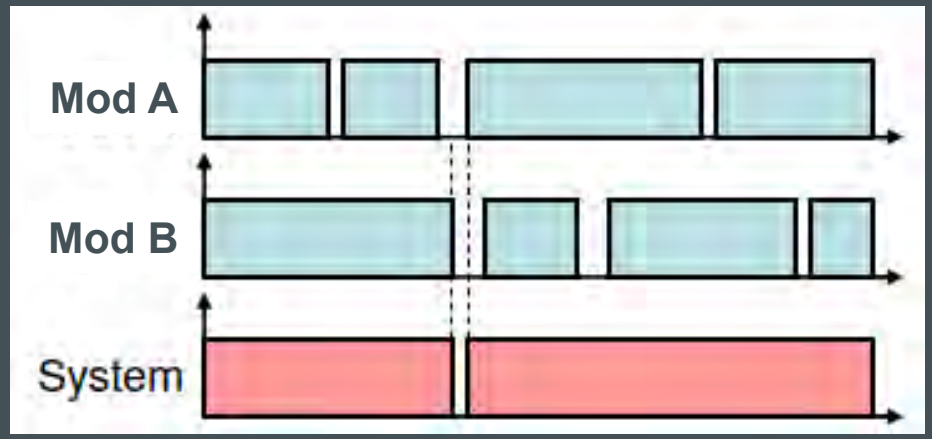
Is a system less reliable just because it has more modules?
Is a system less available just because it has more modules?
Is a system less safe just because it has more modules?

Don’t rely just on numbers!

and why redundancy is the most effective measure to achieve a highly reliable and available system







Effect of faults in a redundant-parallel configuration

MTBF figures - What are you really looking for?

- MTBF numbers are very much influenced by environmental conditions (temp., vibration, aggressive air, voltage bursts, etc.)
- Simplified MTBF formulas often do not consider common cause or common mode factors
- MTBF just represents the effects of random failures, MTBF based on data books never consider systematic failures, human factor or security issues
- Define meaningful and coherent process units or SIFs before starting a calculating
- *The MTBF calculation for a complete system cabinet or network of systems usually makes no sense*

- To benchmark the systems:
  - define the number of devices, I/O points, SIFs and a fixed MTTR
  - the SIF architecture (1oo2, 2oo3...)
  - the function (energized or de-energized to trip),
  - additional equipment like isolators or relays, power supplies
  - environmental conditions (e.g. temperature)
    otherwise you compare apples and oranges

Questions?

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
Website: www.hima.com

1. SIL – SLAM

Verfügbarkeit von Sicherheitssystemen

30.09.2020

Ivo Hanspach - Director Product Management

HIMA SMART SAFETY.

Funktionale Sicherheit im Maschinenbau – Verifizieren & Validieren

SIL SLAM

30.09.2020

Einführung

“Verifizieren” bedeutet: Baue ich das Haus richtig,
“Validierung”, ob ich das richtige Haus baue.

Verifizieren: Nachweis der Übereinstimmung mit den Vorgaben.

Verifizieren oder Validieren?

Oder beides?

Verifizierung: Überprüfung der Einzelentwicklungen/ Dinge/ Vorgänge/ Prozesse… mit anderen Methoden.

Validierung: Feststellen des Wertes für den Kunden (Schlußprüfung)

Einführung

Verifizieren

- Herkunft
  mittellateinisch verificare, zu lateinisch verus = wahr, richtig und facere = machen

- Bedeutung (lt. Duden)
  durch Überprüfen die Richtigkeit einer Sache bestätigen

- Beispiel
  Eine Hypothese verifizieren

Einführung

Validieren

- Herkunft
  Von lateinisch *validus* ‚kräftig', ‚wirksam', ‚fest'

- Bedeutung (lt. Duden)
  die Wichtigkeit, die Gültigkeit, den Wert von etwas feststellen, bestimmen

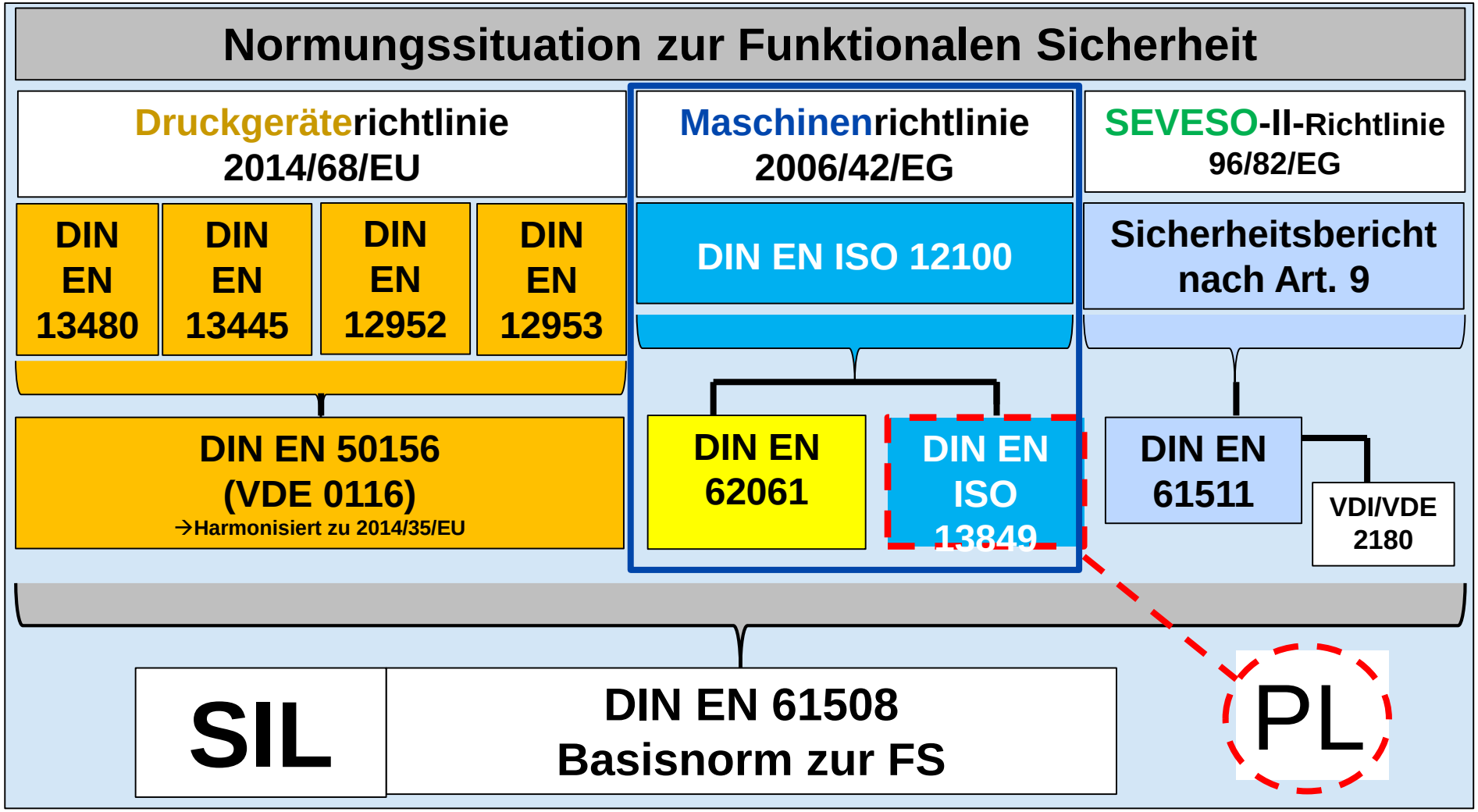
- Beispiel
  Ein Produkt validieren

Einführung

- Beispiel 1
  Bei einem Defibrillator sollen 3000 Volt über 3 Millisekunden anliegen, um ein Herz wieder in den normalen Rhythmus zu bringen. Wenn nun die 3000 Volt über 3 Millisekunden anliegen, das Herz aber nach erfolgter Defibrillation nicht wieder im richtigen Takt schlägt, ist die Verifizierung erfolgreich, aber die Validierung gescheitert. Im umgekehrten Fall würden nur 2000 Volt über 3 Millisekunden anliegen und das Herz trotz der zu geringen Spannung wieder im richtigen Takt schlagen. Somit ist die Verifizierung gescheitert und die Validierung erfolgreich.

- Beispiel 2
  Ein Rettungsring auf Booten soll in reflektierendem Orange gefertigt sein und die Maße eines durchschnittlichen Menschen aufweisen, um einen Schiffbrüchigen in Not helfen zu können. Wenn nun bestätigt wird, dass der Rettungsring reflektierend Orange leuchtet, das Material des Rettungsrings allerdings aus Beton ist und somit zum Untergehen neigt, dann war die Verifizierung erfolgreich, aber die Validierung ist gescheitert. Wenn der Rettungsring allerdings blau wäre und aus einem im Wasser tragfähigem Material besteht, ist die Verifizierung gescheitert aber die Validierung war erfolgreich.

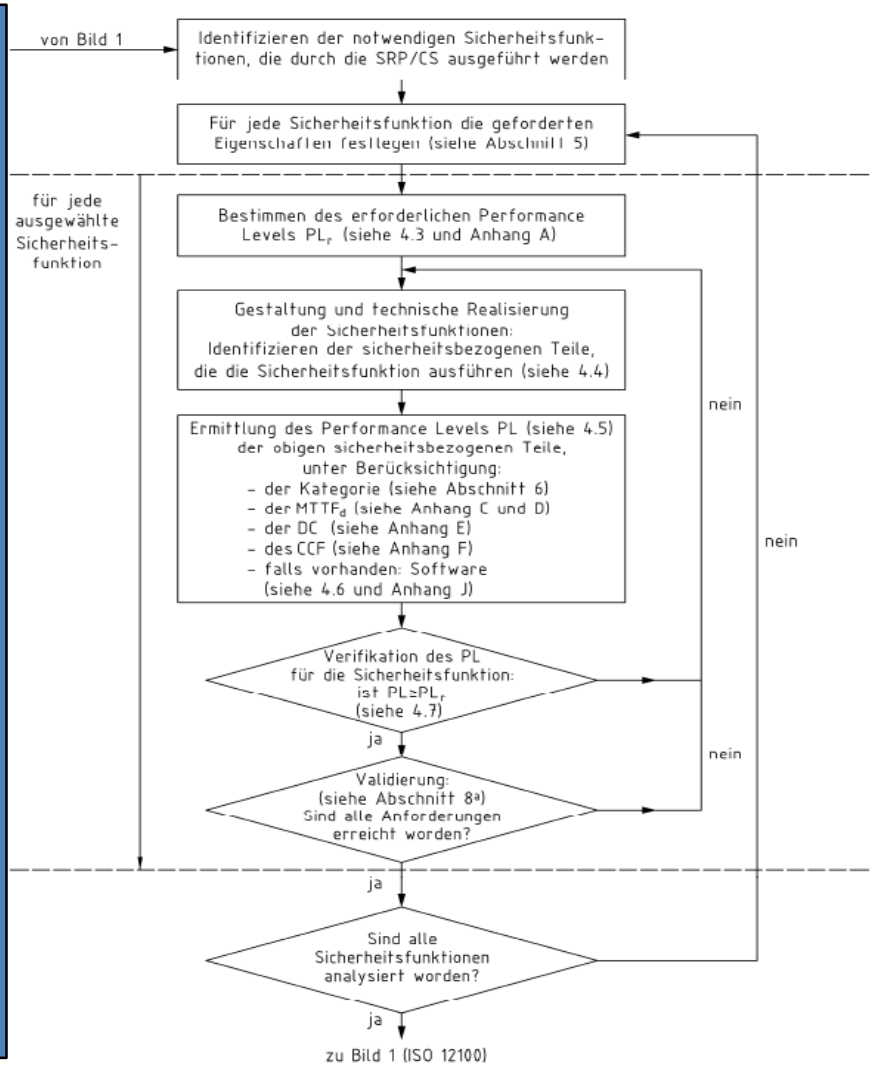
Rechtliche Grundlagen



V&V nach DIN EN ISO 13849-1 / -2

Risiko-beurteilung nach

DIN EN ISO 12100



Identifizierung der SF

Festlegung der Eigenschaften

Ermittlung des PLr (Risikograf)

Spezifikation

Strukturelle Auslegung der Sicherheitsfunktion

Verifikation

Validierung

Gesamtvalidierung

Entwurfsprozess der DIN EN 13849

V&V nach DIN EN ISO 13849-1 / -2

→ Verifikation, dass der erreichte PL den PLr erfüllt

Rechnerischer Nachweis

- Für jede einzelne Sicherheitsfunktion muss der PL des zugehörigen SRP/CS dem bestimmten erforderlichen Performance Level (PLr) entsprechen. Wenn das nicht der Fall ist, wird eine Wiederholung des Prozesses, notwendig.

- Die PL verschiedener SRP/CS, die Teil einer Sicherheitsfunktion sind, müssen größer oder gleich dem erforderlichen Performance Level (PLr) dieser Sicherheitsfunktion sein.

→ Validierung

- Die Gestaltung eines SRP/CS muss validiert werden. Die Validierung muss zeigen, dass die Kombination für jede Sicherheitsfunktion des SRP/CS die entsprechenden Anforderungen dieses Teils der ISO 13849 erfüllen.

- Für Einzelheiten zur Validierung, siehe ISO 13849-2.

DIN EN ISO 13849-2

V&V nach DIN EN ISO 13849-1 / -2

Validieren nach DIN EN ISO 13849-2

- Der Zweck des Validierungsverfahrens ist es, zu bestätigen, dass die Gestaltung der sicherheitsbezogenen Teile der Steuerung (SRP/CS) die Spezifikation der Sicherheitsanforderungen der Maschinen unterstützt.

- Die Validierung muss aufzeigen, dass jedes SRP/CS die Anforderungen von ISO 13849-1 erfüllt, insbesondere bei

a) den festgelegten Sicherheitseigenschaften der Sicherheitsfunktionen, wie diese bei der sinnvollen Gestaltung vorgesehen wurde;
b) den Anforderungen für den festgelegte Performance Level
   – den Anforderungen für die festgelegte Kategorie
   - den Maßnahmen zur Beherrschung und zur Vermeidung systematischer Ausfälle
   - den Anforderungen an die Software, falls vorhanden und
   – der Fähigkeit, eine Sicherheitsfunktion unter den erwarteten Umgebungsbedingungen zu leisten
c) der ergonomischen Gestaltung der Benutzerschnittstelle, z. B. damit der Benutzer nicht verleitet wird, in einer gefährlichen Weise zu handeln, indem er z. B. die SRP/CS umgeht

V&V nach DIN EN 62061

Risiko-beurteilung nach

DIN EN ISO 12100

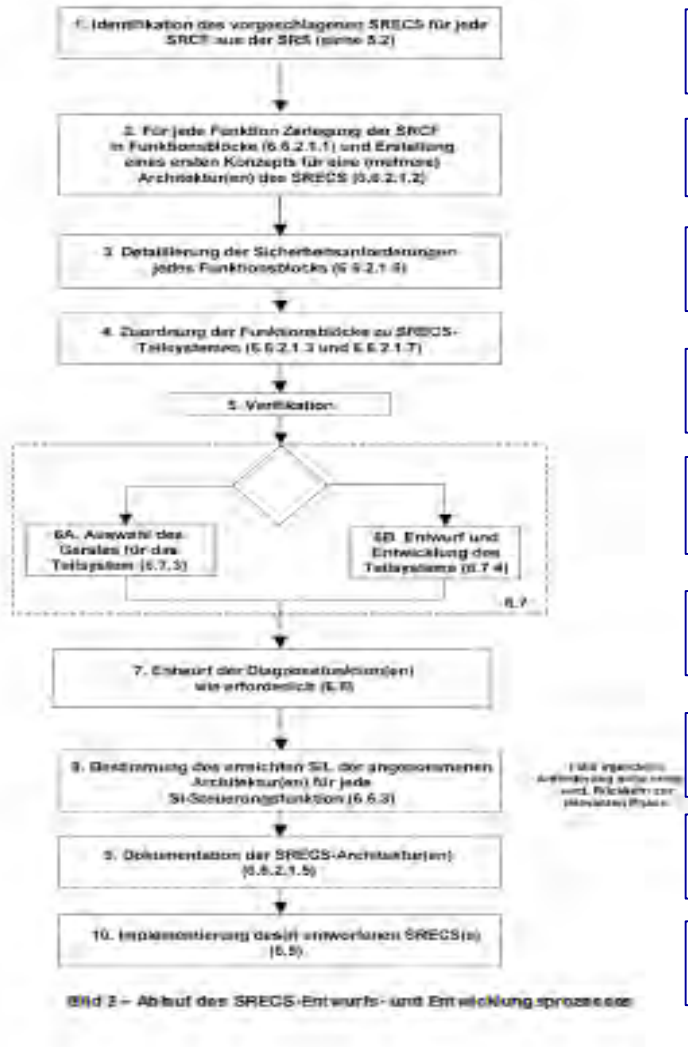


Bild 2 – Ablauf des SRECS-Entwurfs- und Entwicklungsprozesses

- **Identifizierung der SF**
- **Zerlegung in Funktionsblöcke**
- **Detaillierung der Funktionsblöcke**
- **Zuordnung zu Teilsystemen**
- **Verifikation**
- **Strukturelle Auslegung**
- **Diagnose**
- **Rechnerischer Nachweis**
- **Dokumentation**
- **Implementierung**

Entwurfsprozess der DIN EN 62061

V&V nach DIN EN 62061

Verifizieren nach DIN EN 62061

→ Verifikation

- Bestätigung durch Unterstützung (z.B. Tests, Analysen) dass das SRECS, seine Teilsysteme oder Teilsystem-Elemente die durch die zugehörige Spezifikation gestellten Anforderungen erfüllt.

Validieren nach DIN EN 62061

→ Validierung

- Bestätigung durch Unterstützung (z.B. Tests, Analysen) dass das SRECS die Anforderungen zur funktionalen Sicherheit der spezifischen Anwendung erfüllt.

Ihre Meinung

Verifizieren und
Validieren!

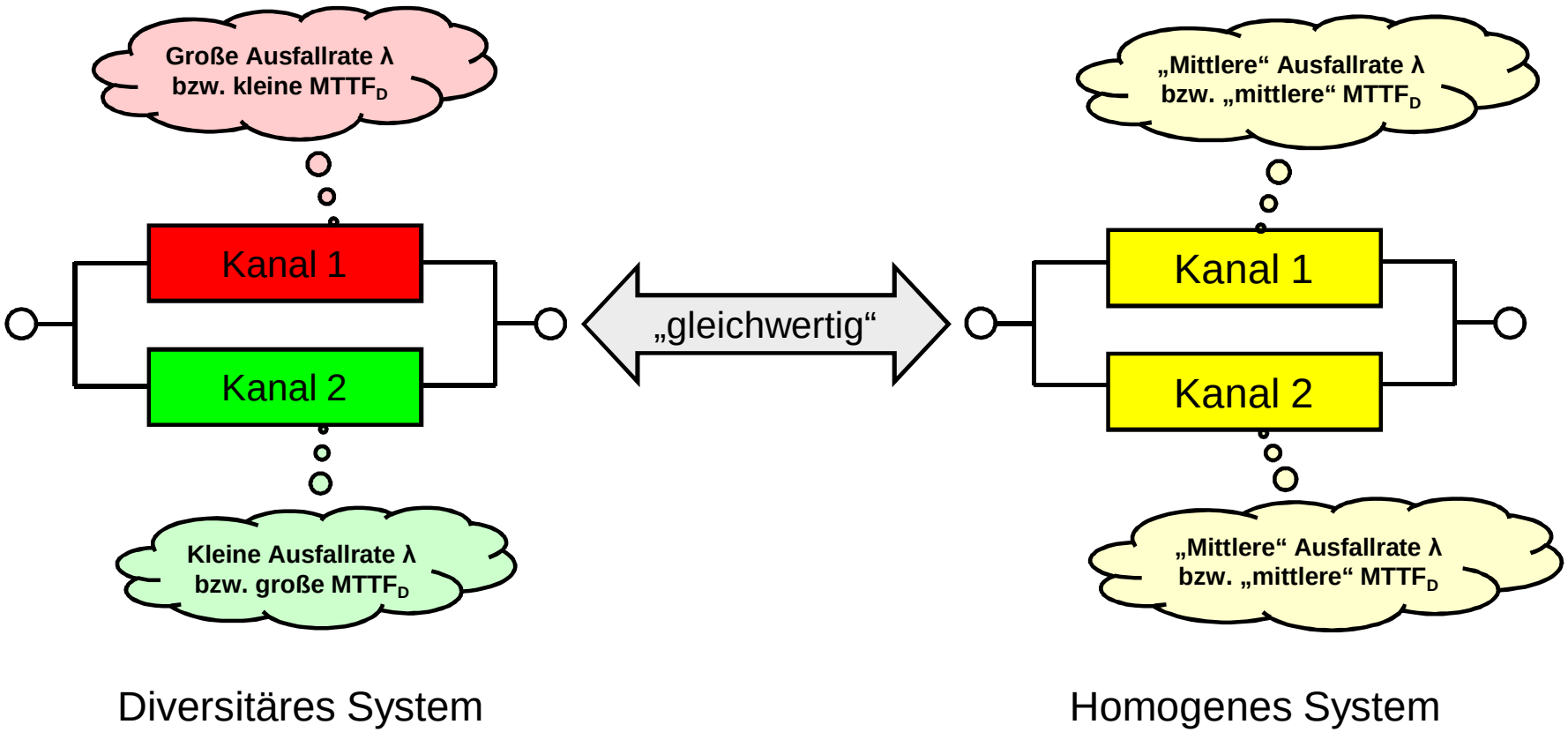
Aber wie?

Your automation, our passion.

PEPPERL+FUCHS

Falsche Formel – was soll‘s

Das Problem



Falsche Formel – was soll‘s

Symmetrisierung nach ISO 13849 Anhang D

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right]$$

„Das bedeutet, dass ein redundantes System mit einer $MTTF_D$ von 100 Jahren in einem Kanal und einer $MTTF_D$ von 3 Jahren im anderen Kanal **gleichwertig** ist zu einem System mit einer $MTTF_D$ von 66 Jahren in jedem Kanal.“

Falsche Formel – was soll‘s

Der Fehler

Mittlere Lebensdauer eines diversitären Systems (beide Kanäle haben eine unterschiedliche konstante Ausfallrate):

$$MTTF_{diversitär} = MTTF_1 + MTTF_2 - \frac{MTTF_1 \cdot MTTF_2}{MTTF_1 + MTTF_2}$$

Mittlere Lebensdauer eines homogenen Systems (beide Kanäle haben die gleiche konstante Ausfallrate):

$$MTTF_{homogen} = 1{,}5 \cdot MTTF_{Kanal}$$

$$MTTF_{diversitär} = MTTF_{homogen}$$

$$MTTF_1 + MTTF_2 - \frac{MTTF_1 \cdot MTTF_2}{MTTF_1 + MTTF_2} = \frac{3}{2} \cdot MTTF_{Kanal}$$

$$\mathrm{MTTF_D} = \frac{2}{3}\left[\mathrm{MTTF_{DC1}} + \mathrm{MTTF_{DC2}} - \frac{1}{\frac{1}{\mathrm{MTTF_{DC1}}} + \frac{1}{\mathrm{MTTF_{DC2}}}}\right]$$

Die MTTF des diversitären Systems ist genauso groß wie die MTTF des homogenen Systems

Falsche Formel – was soll‘s

Der Fehler

$$\boldsymbol{Versagenswahrscheinlichkeit = f(\lambda)}$$

$$MTTF = \frac{1}{\lambda}$$

„gleichwertig“ ???

Falsche Formel – was soll‘s

Die Ursache

Der Begriff MTTF ist de facto ein Homonym!

Genauer: MTTF ist polysem (mehrdeutig)

„Offizielle“ Bedeutung (IEV 192-05-11):

MTTF = Mittlere Lebensdauer
(z. B. 80 Jahre bei Menschen)

Zweite Bedeutung (Elektrotechnik):

MTTF = Kehrwert der Ausfallrate λ im Bodenbereich der Badewannenkurve
(z. B. 1300 Jahre bei Menschen)

Pixabay

Pixabay

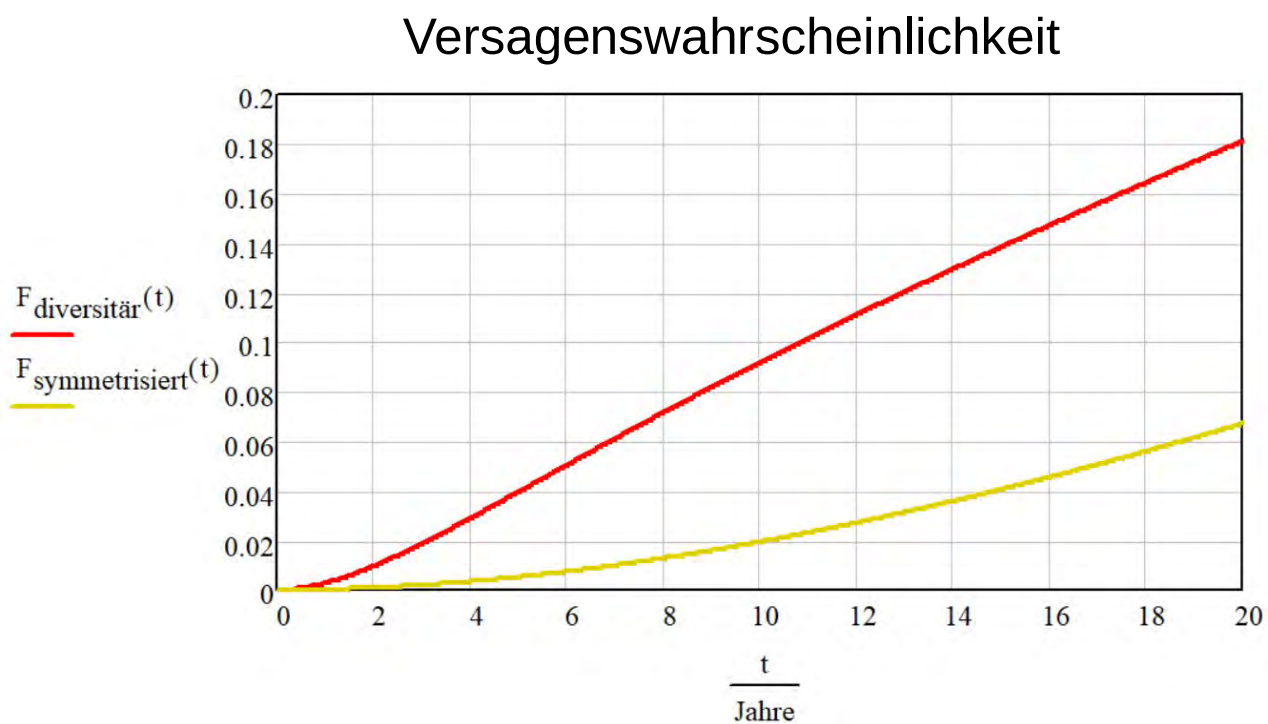
Falsche Formel – was soll‘s

Die Ursache

Bei der Herleitung der Symmetrisierungsformel wurde die MTTF als „mittlere Lebensdauer“ verstanden. D. h., die mittlere Lebensdauer des symmetrisierten (homogenen) Systems ist genauso groß wie die des diversitären Systems. Für die Versagenswahrscheinlichkeit ist jedoch nicht die mittlere Lebensdauer ausschlaggebend, sondern die Ausfallrate λ! Diese ist bei redundanten Systemen nicht ohne Weiteres aus der mittleren Lebensdauer abzuleiten!

Falsche Formel – was soll‘s

Das Ergebnis



Die Versagenswahrscheinlichkeit des diversitären Systems ist größer als die des (angeblich) „gleichwertigen“ homogenen Systems.

Falsche Formel – was soll‘s

Die Konsequenz

Keine!!!

Warum „keine“?

1. Eine Änderung würde unnötig „Staub aufwirbeln“
2. Die Rechnung ist vergleichsweise unwichtig
3. Der Fehler ist in der Praxis meist kleiner als die Unschärfe des Ergebnisses aufgrund der Streuung der Eingangsdaten
4. Fehler bei der Modellbildung und bei der Interpretation des Ergebnisses sind oft wesentlich gravierender (Was ist „Wahrscheinlichkeit“?)
5. Unsinnige Rechnungen an anderer Stelle stellen ein wesentlich größeres Problem dar (Stichwort: Mechanik)

iStockphoto

Falsche Formel – was soll‘s

Die „richtige“ Lösung

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right]$$

$$MTTF_D = \sqrt{MTTF_{DC1} \cdot MTTF_{DC2}}$$

Online-SIL-Slam am 30. September 2020

Falsche Formel – was soll‘s

Restrisiko