

Tag 1: Fachvorträge

2022
SIL Sprechstunde
PEPPERL+FUCHS



Expertenrunde

Dirk Hablawetz, BASF

Marco Knödler, Yncoris

Gregor Schmitt-Pauksztat, Bayer

Michael Moog, Pilz

Ingo Rolle, HS Harz + HS Darmstadt (DKE)

Christian Demski, Dow Chemical

Udo Menck, Dow Chemical

Stefan Aschenbrenner, Exida

Malika Mast, Ramsys

Holger Laible, Siemens

Peter Arnold, Eichler

Ivo Hanspach, HIMA

Peter Sieber, HIMA

Leonard Yousif, SAMSON

Johann Ströbl, TÜV-Süd

Karsten Klingler

Wolfgang Reinelt, Schneider Electric

Stefan Lauer, Endress+Hauser

Michael Kindermann, Pepperl+Fuchs

Hasan Sülük, Pepperl+Fuchs

Dieter Fiebig, Pepperl+Fuchs

Zeitplan erster Tag

Zeit	Vortragsthema	Referent
11:00 – 12:30 Uhr	Begrüßung, Vorstellung des Programms, Motivation „Gebrauchsdauer“	Hildebrandt
	VDI-Empfehlung zur Gebrauchsdauer	Moog
	Warum Angabe der Gebrauchsdauer und was ist danach?	Aschenbrenner
12:30 – 13:30 Uhr	Mittagspause	
13:30 – 15:00 Uhr	Was ist zu tun, wenn man Geräte austauscht und muss man sie noch testen, wenn man sie bald ersetzt?	Demski
	Retrofitting in der Funktionalen Sicherheit	Mast
	Ist Abschalten wirklich sicher?	Hanspach
15:00 – 15:30 Uhr	Kaffeepause	
15:30 – 17:00 Uhr	FIT4FUNctionalSafety - Wie mit “SIL-Mechanik” in Sicherheitsfunktionen umgehen? Und was wir heute für morgen lernen müssen, um FIT für die Zukunft der FuSi zu bleiben.	Knödler
	Künstliche Intelligenz	Laible
	Gebrauchsdauer	Kindermann
Ab 17:30 Uhr	Führung durch das Technikmuseum, anschließend Abendessen	

Zeitplan zweiter Tag

Zeit	Thema	Moderation
9:00 – 10:30 Uhr	Diskussion der Teilnehmerfragen	Hildebrandt
10:30 – 11:00 Uhr	Frühstückspause	
11:00 – 12:30 Uhr	Diskussion der Teilnehmerfragen	Hildebrandt
12:30 – 13:30 Uhr	Mittagspause	
13:30 – 15:00 Uhr	Diskussion der Teilnehmerfragen	Hildebrandt
Ab 15:00 Uhr	Ende der SIL-Sprechstunde	

Frage einreichen: <https://www.pepperl-fuchs.com/germany/de/37893.htm>

Auszug aus einem Sicherheitshandbuch

Gebrauchsdauer

„Jedoch sollte sich nach IEC/EN 61508-2 die Annahme einer Gebrauchsdauer an allgemeingültigen Erfahrungswerten orientieren. Die Erfahrung zeigt, dass die Gebrauchsdauer oft in einem Bereich zwischen 8 und 12 Jahren liegt. Nach DIN EN 61508-2:2011 Anmerkung N3 können geeignete Maßnahmen des Herstellers und des Anlagenbetreibers die Gebrauchsdauer verlängern. Unserer Erfahrung nach kann die Gebrauchsdauer eines Produkts von Pepperl+Fuchs länger sein, wenn die Umgebungsbedingungen eine lange Gebrauchsdauer unterstützen, z. B. wenn die Umgebungstemperatur deutlich unter 60 °C liegt. Beachten Sie, dass sich die Gebrauchsdauer auf die (konstante) Ausfallrate des Geräts bezieht. Die tatsächliche Lebensdauer kann höher sein.“



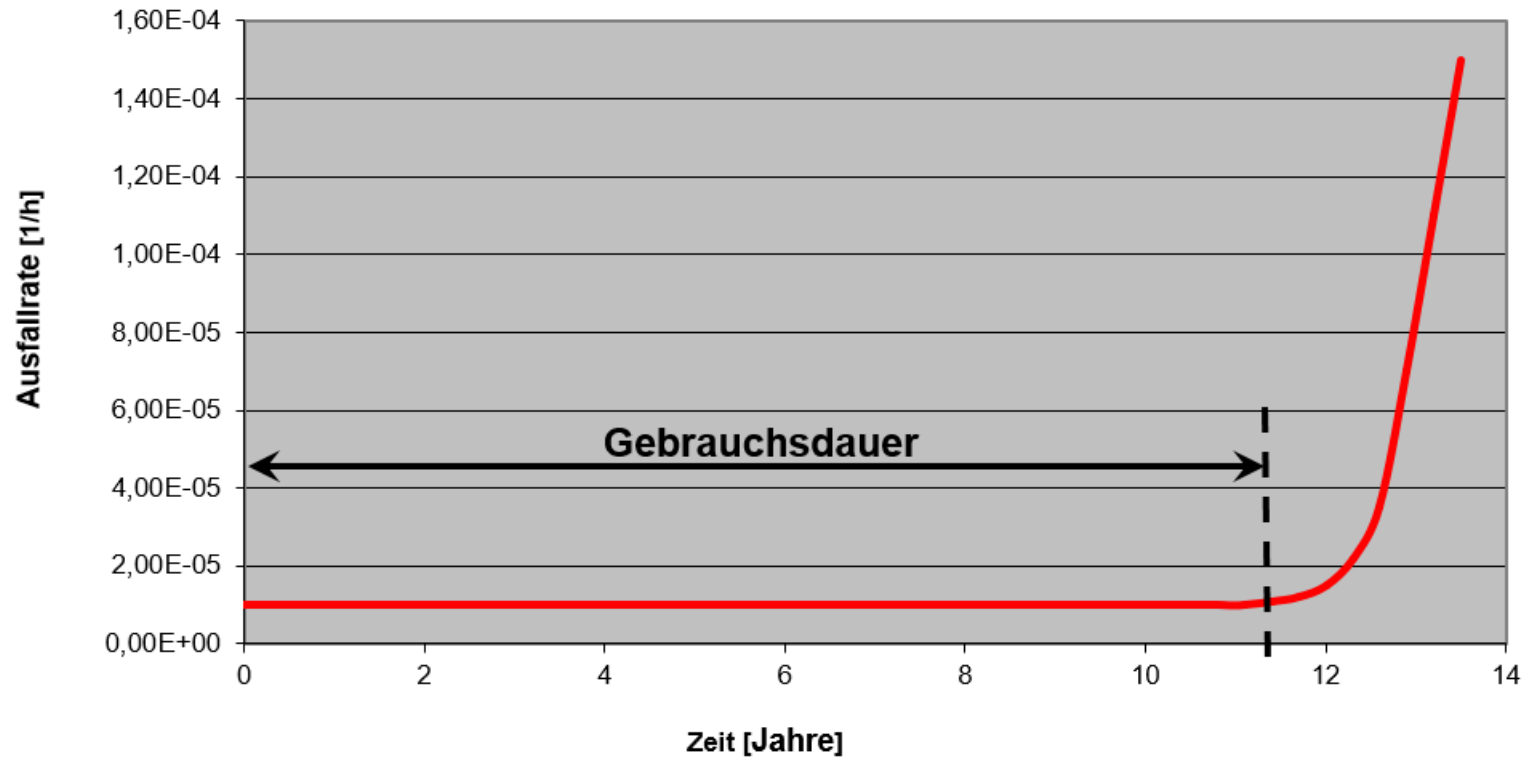
Sicherheitshandbuch

EN 61508 Teil 2, Kapitel 7.4.9.5, Anmerkung 3

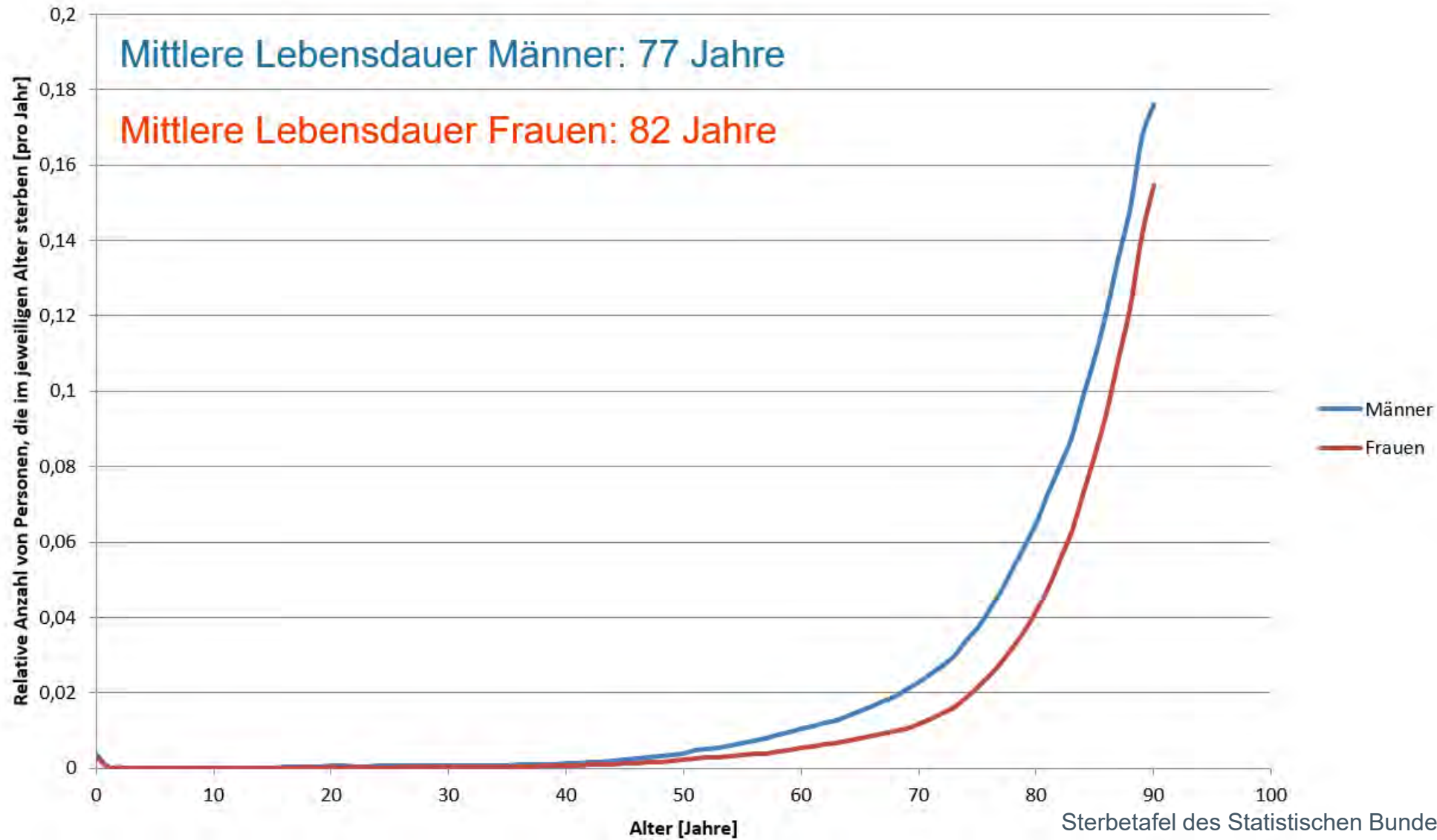
Obwohl für die meisten probabilistischen Abschätzungsmethoden eine **konstante Ausfallrate** angenommen wird, trifft diese nur unter der Voraussetzung zu, dass die **Gebrauchsdauer** von Elementen nicht überschritten wird. **Nach Ablauf ihrer Gebrauchsdauer (d. h. wenn die Ausfallwahrscheinlichkeit mit der Zeit bedeutend ansteigt)** sind die Ergebnisse der meisten probabilistischen Berechnungsmethoden daher wenig aussagekräftig. Daher sollte jede probabilistische Abschätzung eine **Festlegung der Gebrauchsdauer** der Elemente enthalten. Die **Gebrauchsdauer hängt stark vom Element selbst und seinen Betriebsbedingungen ab** – im Besonderen von der Temperatur (zum Beispiel können Elektrolytkondensatoren sehr empfindlich sein). Die Erfahrung hat gezeigt, dass die **Gebrauchsdauer oft innerhalb eines Bereiches von 8 bis 12 Jahren** liegt. Sie kann jedoch bedeutend geringer sein, wenn Elemente nahe an ihren Spezifikationsgrenzen betrieben werden.

Zeitabhängige Ausfallrate

„Badewannenkurve“



Badewannenkurve des Menschen



Sterbetafel des Statistischen Bundesamts, Wiesbaden

Zeitplan erster Tag

Zeit	Vortragsthema	Referent
11:00 – 12:30 Uhr	Begrüßung, Vorstellung des Programms, Motivation „Gebrauchsdauer“	Hildebrandt
	VDI-Empfehlung zur Gebrauchsdauer	Moog
	Warum Angabe der Gebrauchsdauer und was ist danach?	Aschenbrenner
12:30 – 13:30 Uhr	Mittagspause	
13:30 – 15:00 Uhr	Was ist zu tun, wenn man Geräte austauscht und muss man sie noch testen, wenn man sie bald ersetzt?	Demski
	Retrofitting in der Funktionalen Sicherheit	Mast
	Ist Abschalten wirklich sicher?	Hanspach
15:00 – 15:30 Uhr	Kaffeepause	
15:30 – 17:00 Uhr	FIT4FUNctionalSafety - Wie mit “SIL-Mechanik” in Sicherheitsfunktionen umgehen? Und was wir heute für morgen lernen müssen, um FIT für die Zukunft der FuSi zu bleiben.	Knödler
	Künstliche Intelligenz	Laible
	Gebrauchsdauer	Kindermann
Ab 17:30 Uhr	Führung durch das Technikmuseum, anschließend Abendessen	

VDI-Empfehlung zur Gebrauchsdauer Information zum Status Quo



Arbeitstitel: Funktionseinheiten in Sicherheitssteuerungen
Was tun am Ende der Gebrauchsdauer?

SIL-Sprechstunde Pepperl + Fuchs
Michael Moog
Fachreferent Funktionale Sicherheit Maschinen
Sinsheim, 28-09-2022

▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Wo stehen wir aktuell beim Thema Gebrauchsdauer?
DIN EN ISO 13849-1:2015 – Gebrauchsdauer

...

3.1.28 Gebrauchsdauer TM (Mission Time)

Zeitraum, der die vorgegebene Verwendung der SRP/CS abdeckt.

...

4.5.4 Vereinfachtes Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL

Dieser Abschnitt beschreibt ein vereinfachtes Verfahren, um die quantifizierbaren Aspekte des PL eines SRP/CS auf der Basis vorgesehener Architekturen abzuschätzen.

...

Für vorgesehene Architekturen werden folgende typische Annahmen getroffen:

- **Gebrauchsdauer, 20 Jahre** (siehe Abschnitt 10);
- **konstante Ausfallraten innerhalb der Gebrauchsdauer;**

...

▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Wo stehen wir aktuell beim Thema Gebrauchsdauer?
DIN EN ISO 13849-1:2015 – Gebrauchsdauer

10 Technische Dokumentation

Bei der Gestaltung eines SRP/CS muss deren Konstrukteur mindestens folgende Informationen über das sicherheitsbezogene Teil dokumentieren:

...

- die auf die Zuverlässigkeit bezogenen Parameter (MTTFD, DC, CCF und Gebrauchsdauer);

...

▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Wo stehen wir aktuell beim Thema Gebrauchsdauer?
ISO FDIS 13849-1:2022 – Mission Time

3.1.36 mission time TM

Period of time covering the intended use of a safety-related part of a control system (SRP/CS)

...

6.1.8 Simplified procedure for estimating the performance level for subsystems

This subclause describes a simplified procedure for estimating the PL of a subsystem based on designated architectures. ...

...

The simplified approach is based on:

- a) mission time (TM), 20 years (see 3.1.35)
- b) constant failure rates within the mission time;

...

NOTE 1 The mission time (TM) is assumed to be 20 years, within which the component reliability by constant failure rates can be described or approximated. This is generally accomplished in electronic subsystems

The SRP/CS is replaced when the mission time is reached or equivalent measures are performed to ensure that the estimated PL is still valid.

▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Wo stehen wir aktuell beim Thema Gebrauchsdauer?
ISO FDIS 13849-1:2022 – Mission Time

12 Technical documentation

When designing an SRP/CS according to this document at least the following information relevant to the safety-related part shall be documented for internal purposes:

...

g) parameters relevant to the reliability (MTTFD, DC, CCF and T10D) and the mission time;

...

▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Wo stehen wir aktuell beim Thema Gebrauchsdauer?
EN IEC 62061 – 3.2 Terms and definitions

...

3.2.42

Useful lifetime minimum elapsed time between the installation of the SCS or subsystem or subsystem element and the point in time when component failure rates of the SCS or subsystem or subsystem element can no longer be predicted, with any accuracy

Note 1 to entry:

Typically, it will be **20 years or less** unless the **manufacturers** of the SCS and its subsystems can **justify a longer lifetime** by providing evidence, based on calculations, showing that **reliability data is valid for the longer life time**.

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Wo stehen wir aktuell beim Thema Gebrauchsdauer?
IFA Report 2/2017 Anwendung der DIN EN ISO 13849 Anhang G



<https://publikationen.dguv.de/forschung/ifa/ifa-report/3145/ifa-report-2/2017-funktionale-sicherheit-von-maschinensteuerungen-anwendung-der-din-en-iso-13849>

Download

IFA Report 2/2017 (PDF, 5,2 MB)
Onlinefassung 2021 aktualisiert

Download

IFA Report 2/2017e (PDF, 18.8 MB)

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Wo stehen wir aktuell beim Thema Gebrauchsdauer?
IFA Report 2/2017 Anwendung der DIN EN ISO 13849 Anhang G

Anhang G: Was steckt hinter dem Säulendiagramm in Bild 5 der DIN EN ISO 13849-1?

...

Soll die **Gebrauchsdauer** eines SRP/CS **20 Jahre überschreiten**, so **verlieren** die **nach dem vereinfachten Verfahren** (Anhang K der Norm) **ermittelten PFHD-Werte** in den meisten Fällen ihre **Grundlage**.

Unter Umständen kann diese Situation **mit wenigen Nachbesserungen trotzdem im Rahmen des vereinfachten Verfahrens behandelt werden**. Dabei sind **zwei Fälle** zu unterscheiden.

...

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Wo stehen wir aktuell beim Thema Gebrauchsdauer? IFA Report 2/2017 Anwendung der DIN EN ISO 13849 Anhang G

Auszüge Anhang G

- Im ersten Fall ist das SRP/CS von vornherein für eine Gebrauchsdauer größer als 20 Jahre spezifiziert. Dann kann der Einfluss der höheren Gebrauchsdauer aus den Markov-Modellen, die Anhang K der Norm zugrunde liegen, zur sicheren Seite hin folgendermaßen abgeschätzt werden: Pro fünf Jahre längere Gebrauchsdauer als 20 Jahre wird bei den Kategorien 2, 3 und 4 ein prozentualer PFH_D-Zuschlag von 15 % eingerechnet (Kategorie B oder 1 erfordern keine PFH_D-Anpassung). Es ist nicht sinnvoll, die Gebrauchsdauer über 30 Jahre hinaus zu vergrößern. Das vereinfachte Verfahren und SISTEMA sind also trotzdem nutzbar. Voraussetzung sind konstante Ausfallraten unabhängig von der Gebrauchsdauer. Für Verschleißbauteile bedeutet dies, dass diese für die spezifizizierte höhere Gebrauchsdauer T_M ausgelegt werden müssen (T_{10D} ≥ T_M) oder nach Ablauf von T_{10D} jeweils vorsorglich ausgetauscht werden müssen.

- Im zweiten Fall war das SRP/CS ausgelegt für 20 Jahre Gebrauchsdauer, soll aber nun darüber hinaus weiterverwendet werden. Dann kann die aus der Markov-Modellierung zu erwartende PFH_D-Verschlechterung mit einem wie im ersten Fall beschriebenen Zuschlag abgeschätzt werden. Kritisch wird es bei enthaltenen Verschleißbauteilen oder sich durch Alterung verschlechternden Bauteilen, zu denen typischerweise „chemische“ Bauteile (z. B. „nasse“ Elektrolytkondensatoren, Batterien, elektrochemische Sensoren), mechanische Bauteile (z. B. Bremse, Kupplung), elektromechanische Bauteile (z. B. Schalter, Relais, Schütze), fluidtechnische Bauteile (z. B. Ventile) und manche optische Bauteile (z. B. Optokoppler) gehören. Hier kann der Betreiber der Maschine in der Regel nicht selbst beurteilen, ob alle enthaltenen Bauteile auch für eine verlängerte Gebrauchsdauer ausgelegt sind oder welche Maßnahmen, z. B. vorsorglicher Austausch einzelner Bauteile, Proof-Test usw., in diesem Fall durchzuführen sind. Eine Verlängerung der Gebrauchsdauer – bei o. g. PFH_D-Zuschlag – kann dann nur erfolgen, wenn Herstellerangaben darüber vorliegen, was bei einer Verlängerung der Gebrauchsdauer zu tun ist, und wenn diese Maßnahmen vom Betreiber umgesetzt werden.

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Inhaltsübersicht der noch in der Bearbeitung befindlichen VDI-Dokuments

VDI-Gebrauchsdauer („Blaues Papier“)	1
Anwendungsbereich	2
Kapitel 1 – Informationen für den Betreiber	4
1.1 → Begriffe	4
1.2 → Funktionseinheiten mit unterschiedlicher Begrenzung der Gebrauchsdauer	7
1.3 → Gebrauchsdauer => die Herstellerseite ist entscheidend	8
1.4 → Start der Gebrauchsdauer	9
1.4.1 → von Funktionseinheiten	9
1.4.2 → von Sicherheitssteuerungen	9
1.5 → Gebrauchsdauer der Sicherheitssteuerung vs. Nutzungsdauer der Maschine	10
1.6 → Vorgehensweise bei Ablauf der Gebrauchsdauer	12
1.6.1 → Austausch einzelner Funktionseinheiten	12
1.6.2 → Ertüchtigung (Umbau) der Sicherheitssteuerung	14
1.6.3 → „weiterführende Maßnahmen“ => Erläuterungen / Hinweise	15
Kapitel 2 – Weiterführende Informationen und Erläuterungen	19
2.1 → Begriffe	21
2.2 → Zusammenhänge verschiedener Parameter zur Ausfallwahrscheinlichkeit	26
2.3 → Gebrauchsdauer	30
2.3.1 → Beginn der Gebrauchsdauer	30
2.3.2 → Bedingungen und Einflussfaktoren auf die Gebrauchsdauer	31
2.3.3 → Gebrauchsdauer Funktionseinheit ermitteln	33
2.3.4 → Gebrauchsdauer der Sicherheitssteuerung ermitteln	33
2.3.5 → Überholen der betroffenen Funktionseinheit/en	35
2.3.6 → Was tun, wenn die definierte Gebrauchsdauer endet?	36
Kapitel 3 – Fazit und Ausblick	37
Anhang	38

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Gliederung des noch in der Bearbeitung befindlichen VDI-Dokuments

Das Dokument ist in zwei Kapitel aufgeteilt:

Im Kapitel 1 werden Maßnahmen beschrieben, die ein Betreiber von Maschinen bzw. Anlagen ergreifen kann, wenn Sicherheitssteuerungen oder Funktionseinheiten das Ende ihrer Gebrauchsdauer erreichen. Zur besseren Lesbarkeit sind im Kapitel 1 die Zusammenhänge etwas vereinfachter dargestellt, damit der Betreiber sich leichter in der Thematik zurechtfindet.

Detaillierte Herleitungen und Zusammenhänge zum Thema „Gebrauchsdauer“ – insbesondere aus Sicht der „Funktionalen Sicherheit“ – sind in Kapitel 2 zu finden.

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Anwendungsbereich des noch in der Bearbeitung befindlichen Dokuments

Anwendungsbereich

In Maschinen/Anlagen werden erforderliche Maßnahmen zur Risikominderung oft durch Sicherheitsfunktionen realisiert.

Hierfür werden mechanische, fluidtechnische und elektrische/elektronische Geräte, Komponenten, Baugruppen, etc. (als Sensoren, Logikeinheiten und Aktoren) verwendet.

Dabei spielt das Thema „Wahrscheinlichkeit eines gefahrbringenden Ausfalls“ eine wichtige Rolle, um die Zuverlässigkeit der realisierten Sicherheitsfunktionen zu bewerten.

Zur Vereinfachung wird in diesem Dokument für Geräte, Komponenten, Baugruppen, etc., die üblicherweise als Ganzes vom Betreiber selbst ausgetauscht werden dürfen, stellvertretend der Begriff „Funktionseinheiten“ verwendet

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Anwendungsbereich des noch in der Bearbeitung befindlichen Dokuments

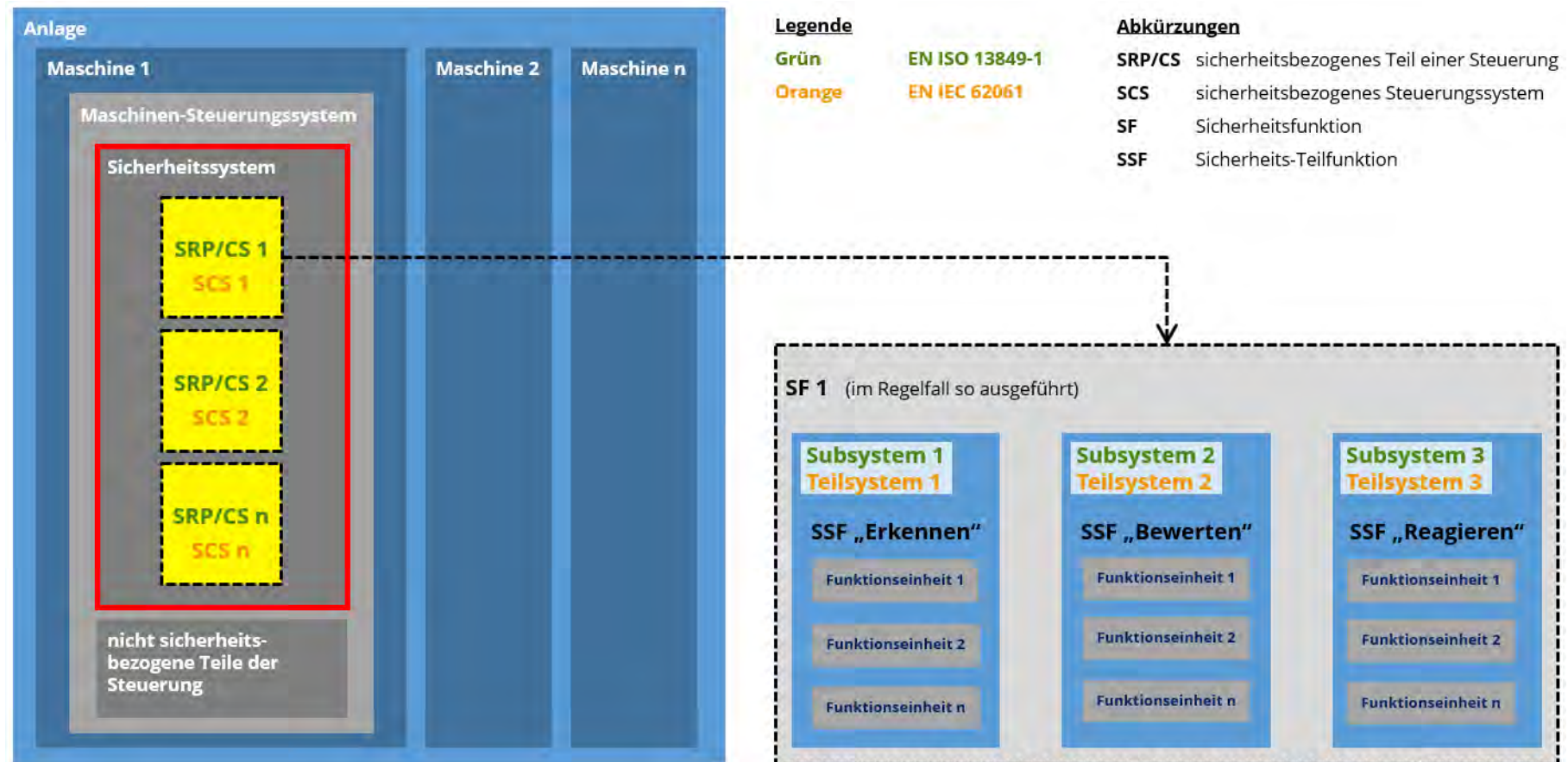
Dieses Dokument fasst zum Thema „Gebrauchsdauer“ die aktuellen Regelwerke zusammen.

Die Bewertung und Umsetzung der Maßnahmen liegen in der Verantwortung des Betreibers.

Der Fokus liegt dabei auf „Maschinen“ im Sinne der Maschinenrichtlinie – also Einzelmaschinen, Kombination von Einzelmaschinen zu einer (Produktions-)Anlage, Gesamtheit von Maschinen, usw. Im weiteren Verlauf des Dokuments wird hierfür stellvertretend der Begriff „Maschine“ verwendet!

▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

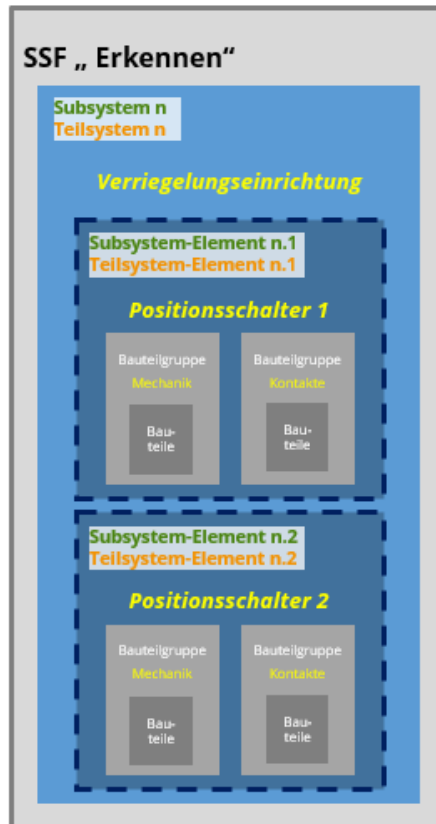
Blockdiagramm sicherheitstechnischer Aufbau einer typischen Maschine



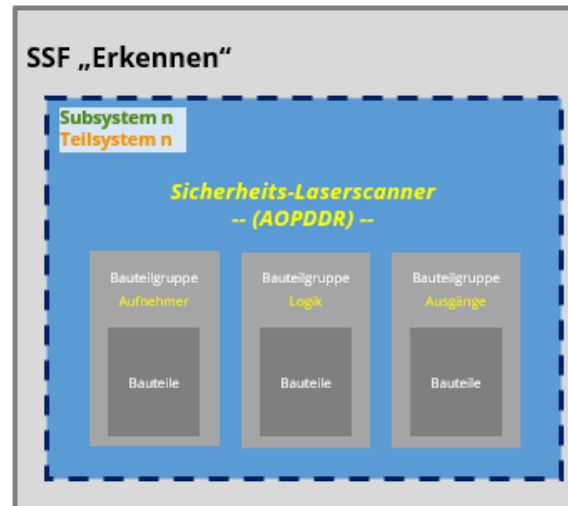
▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Blockdiagramm sicherheitstechnischer Aufbau einer typischen Maschine Beispiele Blockdiagramm „Erkennen“ (Eingang / Input)

Beispiel 1




Beispiel 2



Legende

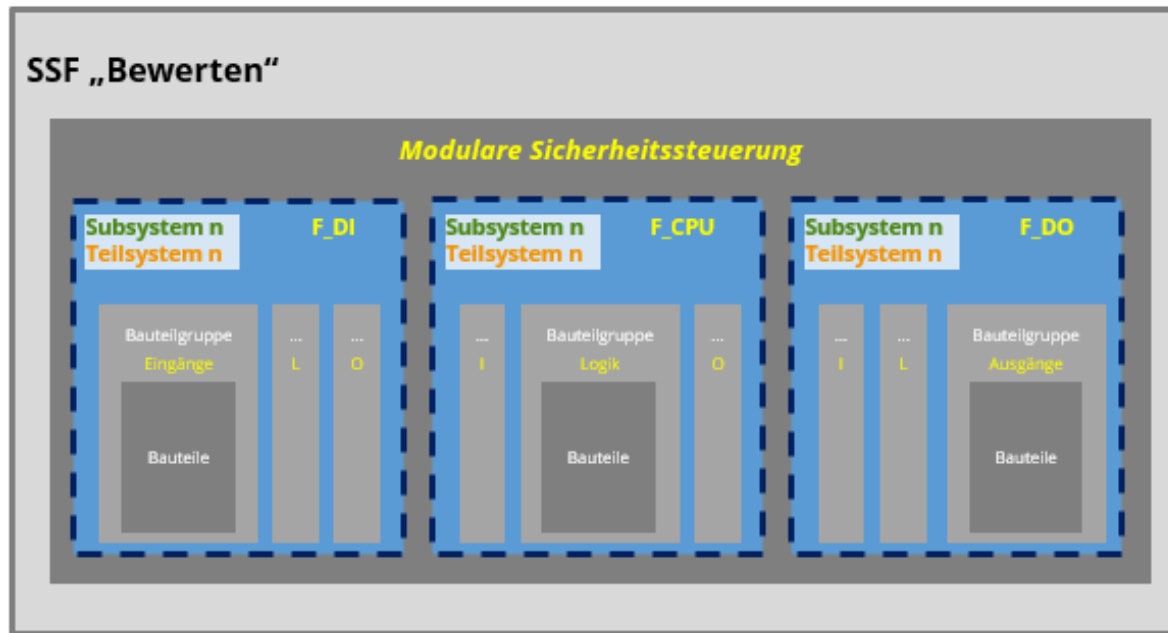
- Grün EN ISO 13849-1
- Orange EN IEC 62061

 = Funktionseinheit

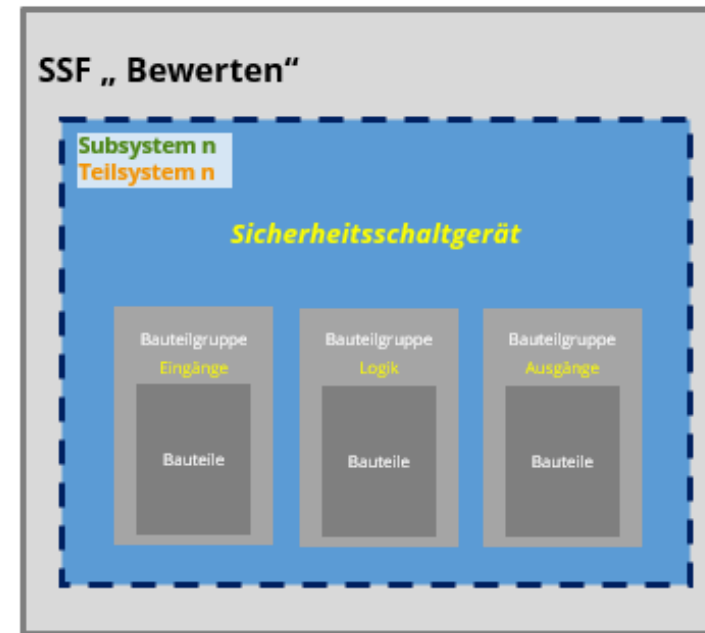
▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Blockdiagramm sicherheitstechnischer Aufbau einer typischen Maschine Beispiele Blockdiagramm „Bewerten“ (Logik)

Beispiel 1



Beispiel 2



Legende

Grün EN ISO 13849-1

Orange EN IEC 62061

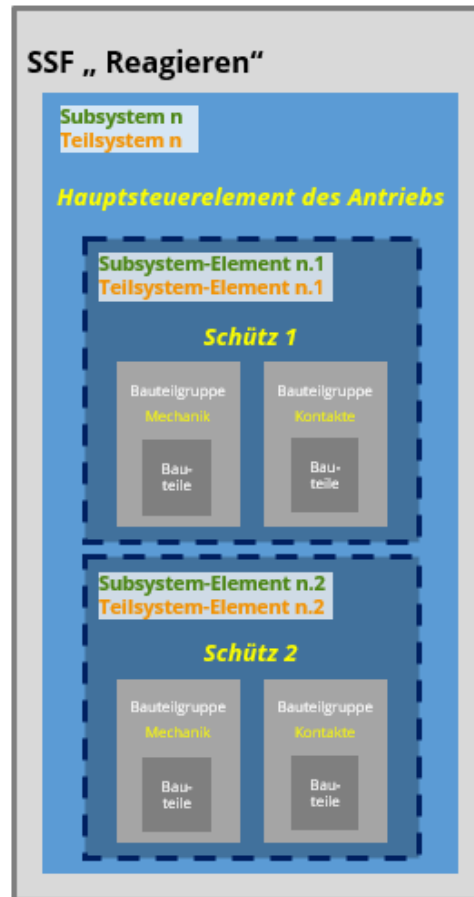


= Funktionseinheit

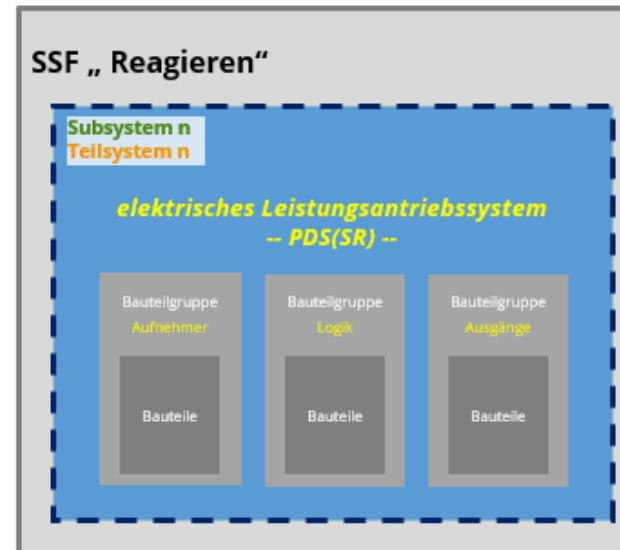
▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Blockdiagramm sicherheitstechnischer Aufbau einer typischen Maschine Beispiele Blockdiagramm „Reagieren“ (Ausgang/Output)

Beispiel 1




Beispiel 2



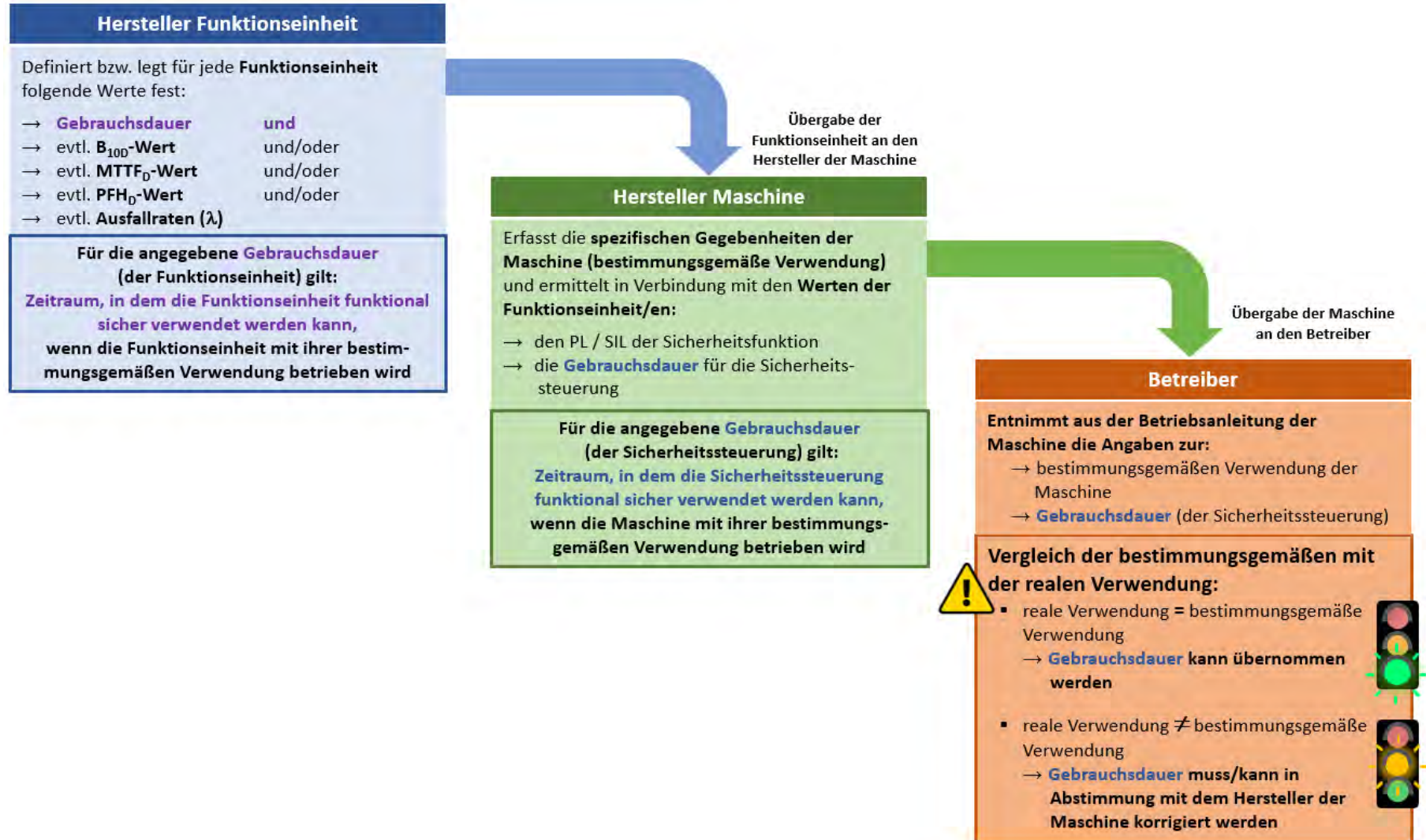
Legende

- Grün EN ISO 13849-1
- Orange EN IEC 62061

 = Funktionseinheit

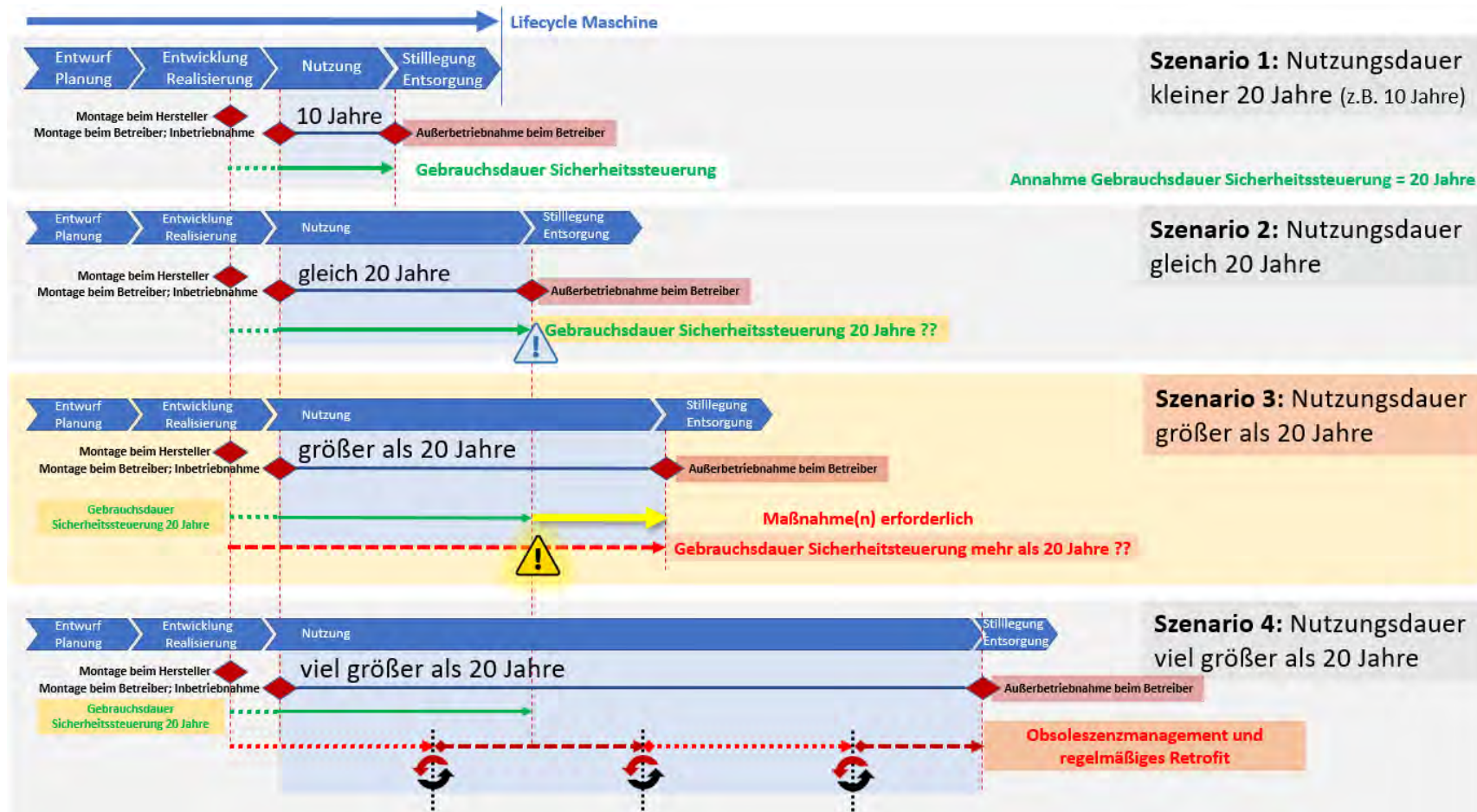
▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Wer muss was beitragen?



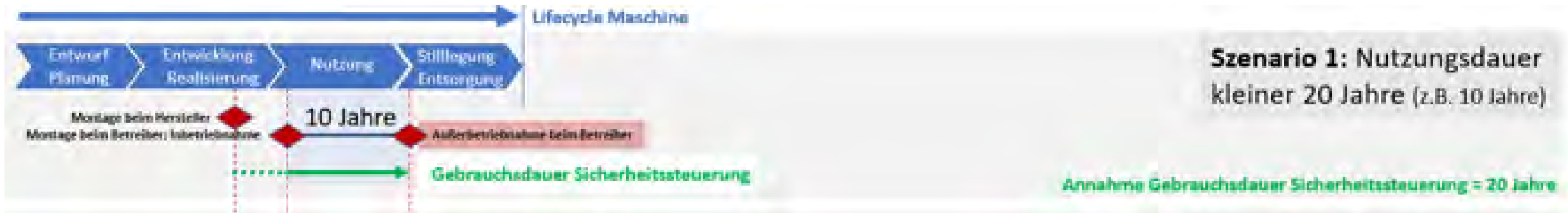
► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Schaubild mit 4 Szenarien der möglichen Maschinen-Nutzungsdauer



► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

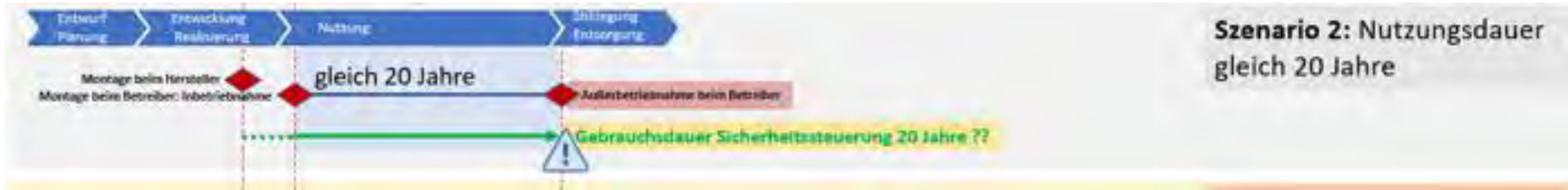
Szenario 1: Die Maschine wird deutlich kürzer als die Gebrauchsdauer betrieben



Wenn die Maschine geplant **deutlich kürzer als die Gebrauchsdauer der Sicherheitssteuerung betrieben** wird (im Beispiel wird sie nach Ablauf der Abschreibung von 10 Jahren stillgelegt oder gegen eine neuere Maschine ausgetauscht), sind **keine Maßnahmen erforderlich**. Die Gebrauchsdauer beginnt mit Einbau der Sicherheitssteuerung im Lieferwerk in die Maschine, die Maschine geht nach Lieferung und Montage beim Kunden/Betreiber in Betrieb. Damit ist die Zeitspanne der Gebrauchsdauer nur unwesentlich länger als die Nutzung durch den Betreiber.

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Szenario 2: Die Maschine wird mit Ablauf der Gebrauchsdauer außer Betrieb genommen



Wenn die Maschine (ggfs. sogar geplant) quasi gleichzeitig mit Ablauf der Gebrauchsdauer der Sicherheitssteuerung stillgelegt wird, sind ebenso keine Maßnahmen erforderlich. Denn bevor die Wahrscheinlichkeit kritischer Ausfälle der Sicherheitssteuerung zunimmt, wird die Maschine außer Betrieb genommen.

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Szenario 3: Die Maschine wird länger als die Gebrauchsdauer betrieben



Sollte die Maschine deutlich über das Ende der Gebrauchsdauer hinaus betrieben werden (geplant oder z.B. durch eine Entscheidung, den Betrieb der Maschine zu verlängern, anstatt neu zu investieren) so ist mit dem Zeitpunkt des Ablaufs der Gebrauchsdauer (hier im Beispiel nach 20 Jahren) sehr intensiv zu prüfen, welche Maßnahmen ergriffen werden müssen, um den Betrieb gefahrlos weiter aufrecht erhalten zu können. Entweder wurde die Maschine schon so ausgelegt, dass ein Retrofit durchgeführt werden kann, oder man prüft entsprechend, welche Maßnahmen umsetzbar sind.

Das Ergebnis kann in diesem Zusammenhang auch sein, dass Umbau und Ertüchtigung der Maschine z.B. den finanziellen Rahmen sprengen und die Maschine doch stillgelegt und ggfs. ausgetauscht werden muss.

► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

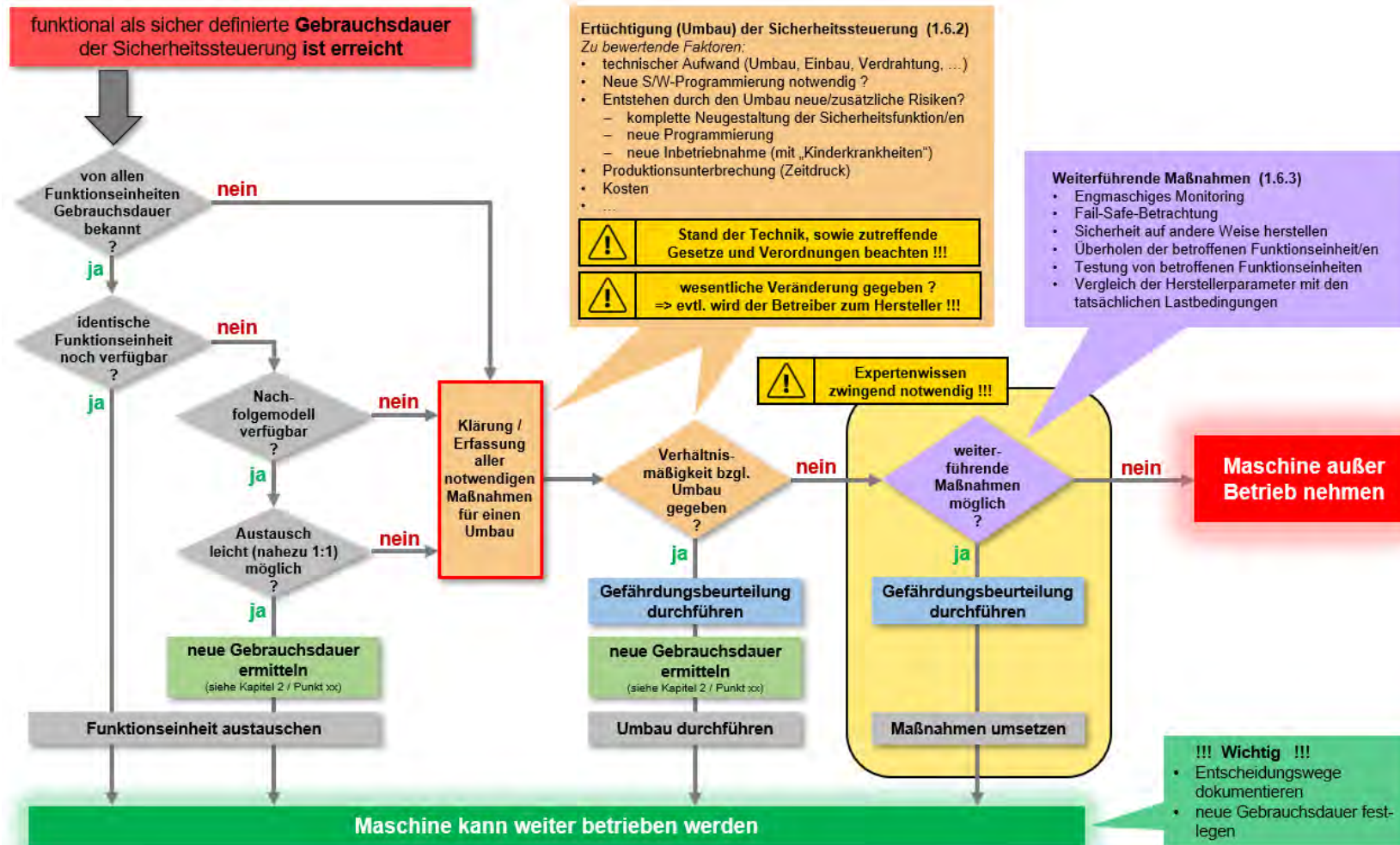
Szenario 4: Die Maschine wird von Beginn an so ausgelegt, dass in mehreren Zyklen ein sehr langer Lifecycle mit einer oder sogar mehreren Retrofit-Maßnahmen geplant wird.



In Ergänzung zum vorherigen Szenario gibt es Maschinen, die von Beginn an so ausgelegt und geplant werden, dass der **Lebenszyklus ein Mehrfaches der Gebrauchsdauer der Sicherheitssteuerung beträgt**. Diese Maschinen durchlaufen **mehrfache Retrofits**, in denen die **gesamte Sicherheitssteuerung ausgetauscht wird**, während die **mechanischen Komponenten der Maschine im Originalzustand bleiben bzw. teilweise auch angepasst oder erneuert werden**. Man folgt also im Lebenszyklus der Maschine dem sog. **Obsoleszenzmanagement**: Man berücksichtigt bei der Planung der Maschine, dass ihre Steuerung und Sicherheitstechnik nach vielen Jahren (beispielsweise 10 Jahren) gegen eine moderne Ausführung ausgetauscht werden können, da die bisher verwendeten Funktionseinheiten vom Lieferanten abgekündigt wurden.

▶ VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Ablaufdiagramm bei Erreichen der funktional sicheren Gebrauchsdauer aus Betreibersicht



► VDI-Empfehlung zur Gebrauchsdauer Funktionseinheiten in Sicherheitssteuerungen

Dokumentenstatus: Finale Bearbeitungsphase

Dokumentumfang: derzeit 40 Seiten

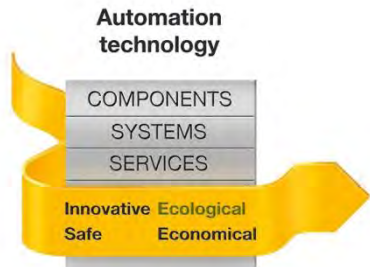
Geplante Veröffentlichung: Voraussichtlich Ende 2022

Veröffentlichungsort: <https://www.vdi.de/ueber-uns/presse/publikationen>

Publikationen

Ob Agenda, Statusreport oder Positionspapier: In unserer Datenbank finden Sie alle Arten von Publikationen des VDI, die unser großes Themenspektrum widerspiegeln.

Als VDI-Mitglied finden Sie alle VDI-Publikationen auch im geschlossenen Mitgliederbereich „Mein VDI“.



Vielen Dank für ihre Aufmerksamkeit!

Michael Moog
 Pilz GmbH & Co KG
m.moog@pilz.de
 Mobil 0160-94709487



PILZ
 THE SPIRIT OF SAFETY

CMSE®, InduraNET® p®, PAS4000®, PAScal®, PASconfig®, Pilz®, PIT®, PLID®, PMCPrimo®, PMCProtego®, PMClendo®, PMD®, PMP®, PNOZ®, Primo®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, THE SPIRIT OF SAFETY® are registered and protected trademarks of Pilz GmbH & Co. KG in some countries. We would point out that product features may vary from the details stated in this document, depending on the status at the time of publication and the scope of the equipment. We accept no responsibility for the validity, accuracy and entirety of the text and graphics presented in this information. Please contact our Technical Support if you have any questions.

▶ **VDI-Empfehlung zur Gebrauchsdauer
Funktionseinheiten in Sicherheitssteuerungen**

▶ **VDI-Empfehlung zur Gebrauchsdauer
Funktionseinheiten in Sicherheitssteuerungen**



SIL Sprechstunde
Pepperl+Fuchs SE
2022

28. – 29.09.2022

Stephan Aschenbrenner

Warum Angabe der Gebrauchsdauer und was ist
nach 10-12 Jahren?

◆ Stephan H. Aschenbrenner, CFSE

- Dipl. Ing. (Univ) for Electrical Engineering and Automation of the Technical University of Munich (TUM)
- Start as a software and hardware developer of programmable electronic systems
- At TÜV Product Service GmbH responsible for machinery safety components later at TÜV Product Service Inc. in the USA responsible for setting up a functional safety department for the Americas
- Business Unit Manager at TÜV Product Service
- Since 2001 at *exida.com* GmbH involved in both product analysis and design process improvements in the process industry, the machinery industry, as well as in the automotive and semiconductor industry
- Responsible for *exida's* FMEDA tool SILcal
- Since 2007 Certified Functional Safety Expert (CFSE)
- Since 2013 Managing Partner at *exida.com* GmbH
- Since 2017 Head of AK 914.0.4 (German IEC 61508-1/-2 committee)
- Since 2017 Active member of MT 61508-1/-2
- Since 2020 CEO at *exida.com* GmbH
- Over 27 years of experience and extensive knowledge in the safety and reliability field



◆ IEC 61508-2 § 7.4.9.5

NOTE 3 Although a constant failure rate is assumed by most probabilistic estimation methods this only applies provided that the useful lifetime of elements is not exceeded. Beyond their useful lifetime (i.e. as the probability of failure significantly increases with time) the results of most probabilistic calculation methods are therefore meaningless. Thus any probabilistic estimation should include a specification of the elements' useful lifetimes. The useful lifetime is highly dependent on the element itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive). Experience has shown that the useful lifetime often lies within a range of 8 to 12 years. It can, however, be significantly less if elements are operated near to their specification limits.

- ◆ Die Gebrauchsdauer hängt stark von der Komponente selbst und seinen Betriebsbedingungen ab, insbesondere von der Temperatur (Elektrolytkondensatoren können beispielsweise sehr empfindlich sein).

NOTE 3 Although a constant failure rate is assumed by most probabilistic estimation methods this only applies provided that the useful lifetime of elements is not exceeded. Beyond their useful lifetime (i.e. as the probability of failure significantly increases with time) the results of most probabilistic calculation methods are therefore meaningless. Thus any probabilistic estimation should include a specification of the elements' useful lifetimes. The useful lifetime is highly dependent on the element itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive). Experience has shown that the useful lifetime often lies within a range of 8 to 12 years. It can, however, be significantly less if elements are operated near to their specification limits.

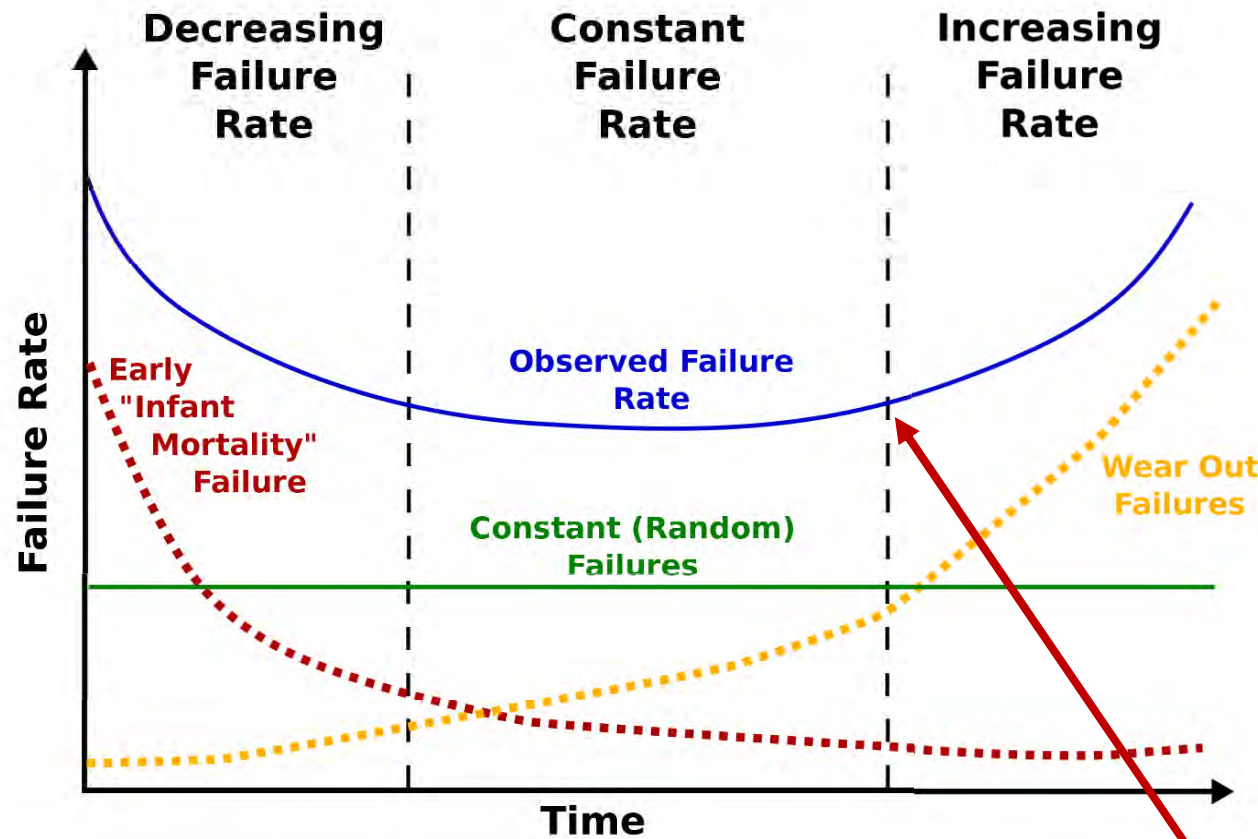
h) Calculate safe failure fraction of the element as:

$$SFF = (\sum \lambda_S + \sum \lambda_{Dd}) / (\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du})$$

NOTE 4 The above equation is applicable when the failure rates are based on constant failure rates (see 3.6.15 of IEC 61508-4 for the definitive formula).

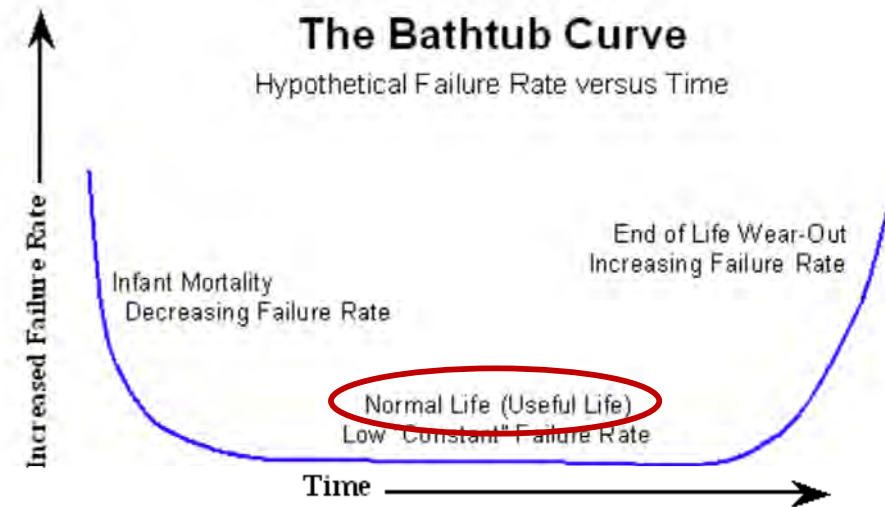
$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

NOTE 2 This definition is applicable providing the individual components have constant failure rates.



https://en.wikipedia.org/wiki/Bathtub_curve

- Failure rates are only valid within the useful life. Infant mortality and wear-out are not part of the useful life.



<https://www.weibull.com/hotwire/issue22/hottopics22.htm>

Useful lifetime of components with reduced useful lifetime **contributing to λ_{du}**

Type	Useful life
Microcontroller	About 20 years
Opto-coupler	About 20 years
Capacitor (electrolytic) – Aluminum	About 90 000 hours
Capacitor (electrolytic) – Tantalum	About 500 000 hours
Relay	10^7 mechanical operations at nominal load conditions 10^5 electrical operations at rated resistive load

- ◆ Die Gebrauchsdauer hängt stark von der Komponente selbst und seinen Betriebsbedingungen ab.
 - ◆ Elektrolytkondensator - Aluminium: Die Betriebstemperatur hat einen direkten Einfluss auf diese Zeit. Daher verringert bereits eine kleine Abweichung von der Betriebsumgebungstemperatur die Nutzungsdauer drastisch. Die Lebensdauer von Kondensatoren bei niedrigeren Temperaturen folgt der "**10°C-Verdoppelungsregel**", wonach sich die **Lebensdauer verdoppelt für jede Verringerung der Betriebstemperatur um 10°C**.
 - ◆ Ein Leistungshalbleiter kann bei einer konstant hohen Temperatur extrem lange problemlos arbeiten. Dasselbe Bauteil kann jedoch **innerhalb kurzer Zeit ausfallen, wenn die Temperatur ständig um einen hohen Betrag schwankt**.

- ◆ Proposal received for 7.4.9.5 of IEC 61508-2. Add following Note.

Note:

However, by suitable design and/or implementation of diagnostics dangerous failures can be transferred into the safe failures. Hence only dangerous *undetected* failures contribute to the PFDavg, the useful lifetime for safety purposes of the complete device can therefore be extended to 25 to 30 years.

Why do I not accept it?

◆ IEC 61508-2 Annex C, C.1 d)

d) From an estimate of the failure rate of each component or group of components, (λ), (see Note 4) and the results of the failure mode and effect analysis, for each component or group of components, calculate the safe failure rate (λ_S), and the dangerous failure rate (λ_D). When one of these failure rates is not constant, its average over the period shall be estimated and used in DC and SFF calculations.

◆ IEC 61508-4, 3.6.15 and 3.6.16

SFF

property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$$\text{SFF} = (\Sigma\lambda_{S \text{ avg}} + \Sigma\lambda_{Dd \text{ avg}}) / (\Sigma\lambda_{S \text{ avg}} + \Sigma\lambda_{Dd \text{ avg}} + \Sigma\lambda_{Du \text{ avg}})$$

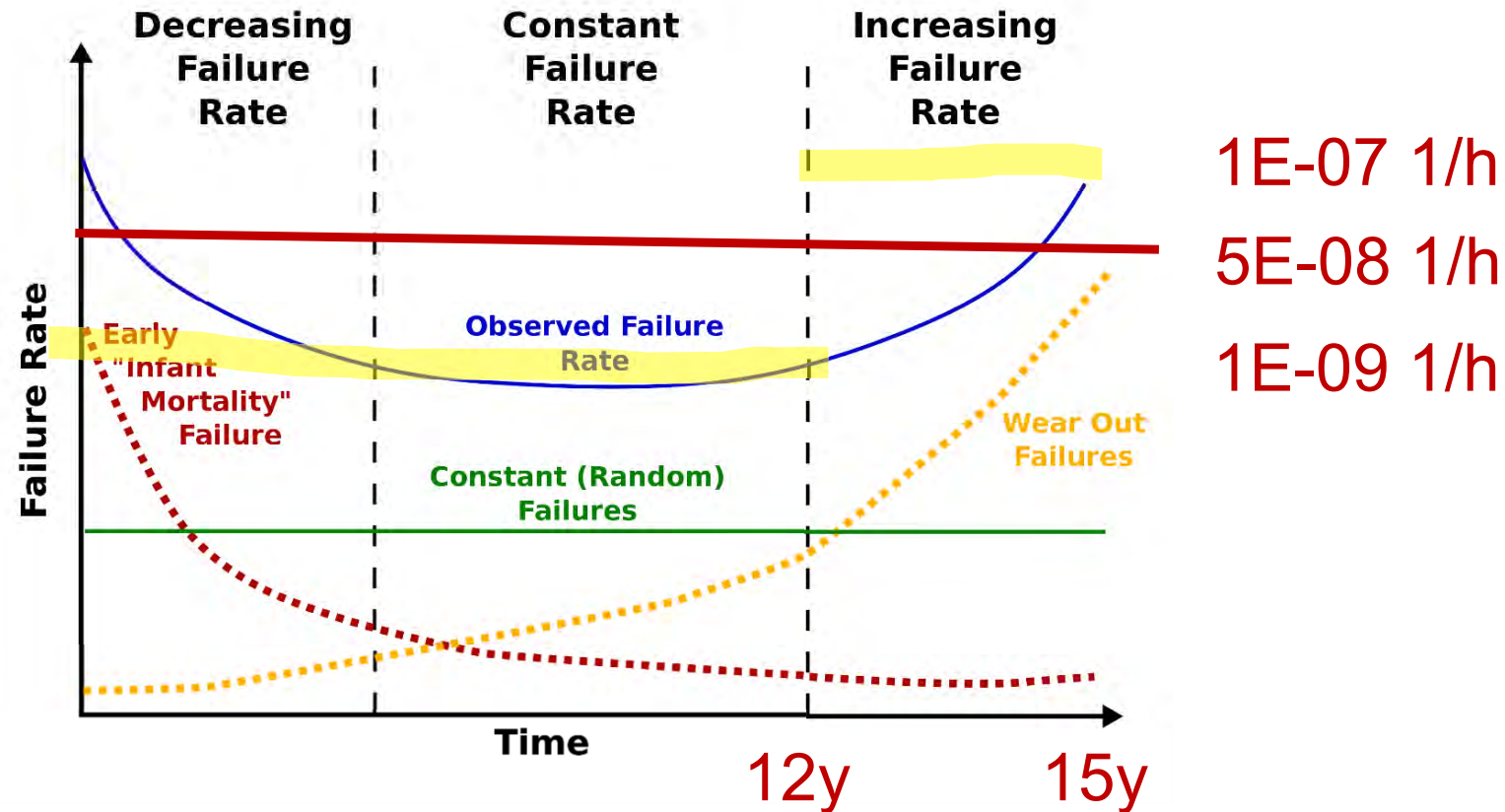
when the failure rates are based on constant failure rates the equation can be simplified to:

$$\text{SFF} = (\Sigma\lambda_S + \Sigma\lambda_{Dd}) / (\Sigma\lambda_S + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$$

NOTE 5 The failure rate of redundant systems is generally non constant. Nevertheless when all failures are quickly revealed, independent and quickly repaired, $\lambda(t)$ converges quickly to an asymptotic value λ_{as} which is the *equivalent failure rate* of the systems. It should not be confused with the average failure rate described in Note 3 which doesn't necessarily converge to an asymptotic value.

Was ist nach 10-12 Jahren?

- IEC 61508-2 Annex C, C.1 d) "... When one of these failure rates is not constant, its **average over the period shall be estimated ...**"



- ◆ Der Schlüssel zur Beantwortung der Frage nach der Gebrauchsdauer liegt im Lastprofil der Anwendung. Im Prinzip gibt es für jede Anwendung ein solches Lastprofil.
- ◆ Es muss weiter diskutiert werden, ob eine Mittelung der Ausfallrate möglich ist und wie weit die Gebrauchsdauer damit verlängert werden kann.





excellence in dependable automation

Many Thanks for your Attention

stephan.aschenbrenner@exida.com

+49/8362-507274



**Functional
Safety
Discipline**

Was prüfen wir, wenn Ventile getauscht werden.....

Impulsvortrag



Christian Demski

Technical Expertise and Support
Leverage Globally, Act Regionally, Execute Locally – *Faster and Smarter*



IEC Anforderungen an Prüfungen

16.3.3 Documentation of proof tests and inspection

The user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

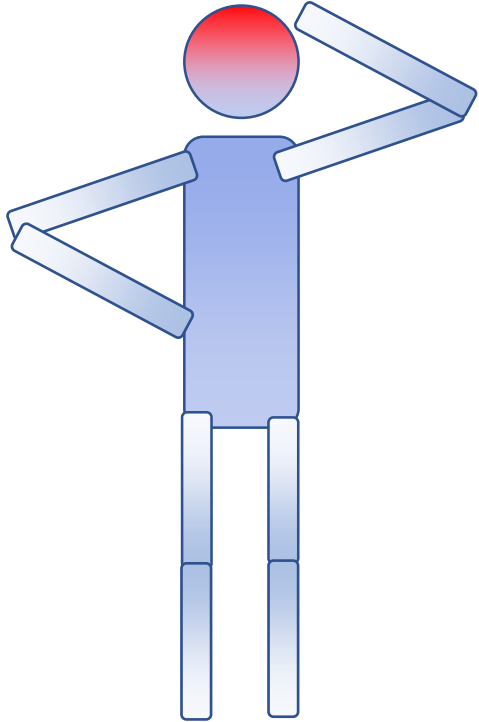
- a) description of the tests and inspections performed including identification of the test procedure used;
- b) dates of the tests and inspections;
- c) name of the person(s) who performed the tests and inspections;
- d) serial number or other unique identifier of the system tested (e.g., loop number, tag number, equipment number, and SIF number);
- e) results of the tests and inspection including the "as-found" condition, all faults found (including the failure mode) and the "as-left" condition.

Quelle: IEC 61511 (2016)

Aber was prüfen wir wenn Geräte geplant getauscht werden?



Beispiel an einem Ventil.....



- Neben den bekannten und verwendeten Prüfkriterien stellt sich bei Ventilen oft eine weitere Frage:

„Wie dicht muss das Ventil sein, um das Szenario zu verhindern?“

Wie komme ich an diese Daten, bzw. welche Daten benötige ich?



- In der praktischen Umsetzung stellen sich für die Instandhaltung dann folgende Fragen:
 - Bis zu welcher Dichtigkeit darf ich ein Ventil wiederverwenden?
 - Bei welcher vorgefundenen Dichtigkeit habe ich ein Safety Problem?
 - Nur... Wenn ich das Ventil morgen wegschmeiße und es gegen ein neues austausche... Welchen Grund habe ich es heute noch zu prüfen?



Wann fallen Ventile durch die Prüfungen?

- Prüfung gegen den definierten Grenzwert?
- Prüfung gegen 50% von dem Grenzwert (Wir nehmen z.B. 45%)?
- Wann ist das Ergebnis ein Maintenance Problem, wann ein Process Safety Problem?

	Reliability Problem (Das Ventil kann ohne eine Aufarbeitung oder einen Austausch nicht mehr eingebaut werden)	Safety Problem (Sicherheitsfunktion hätte nicht mehr funktioniert, wird voraussichtlich nicht funktionieren.)
Gerät soll wiederbenutzt werden		
Geräte wird geplant ausgetauscht		
Gerät sollte wiedebenutzt werden wird aber getauscht		

Wenn ich ein Gerät Morgen wegschmeiße, was prüfe ich heute?

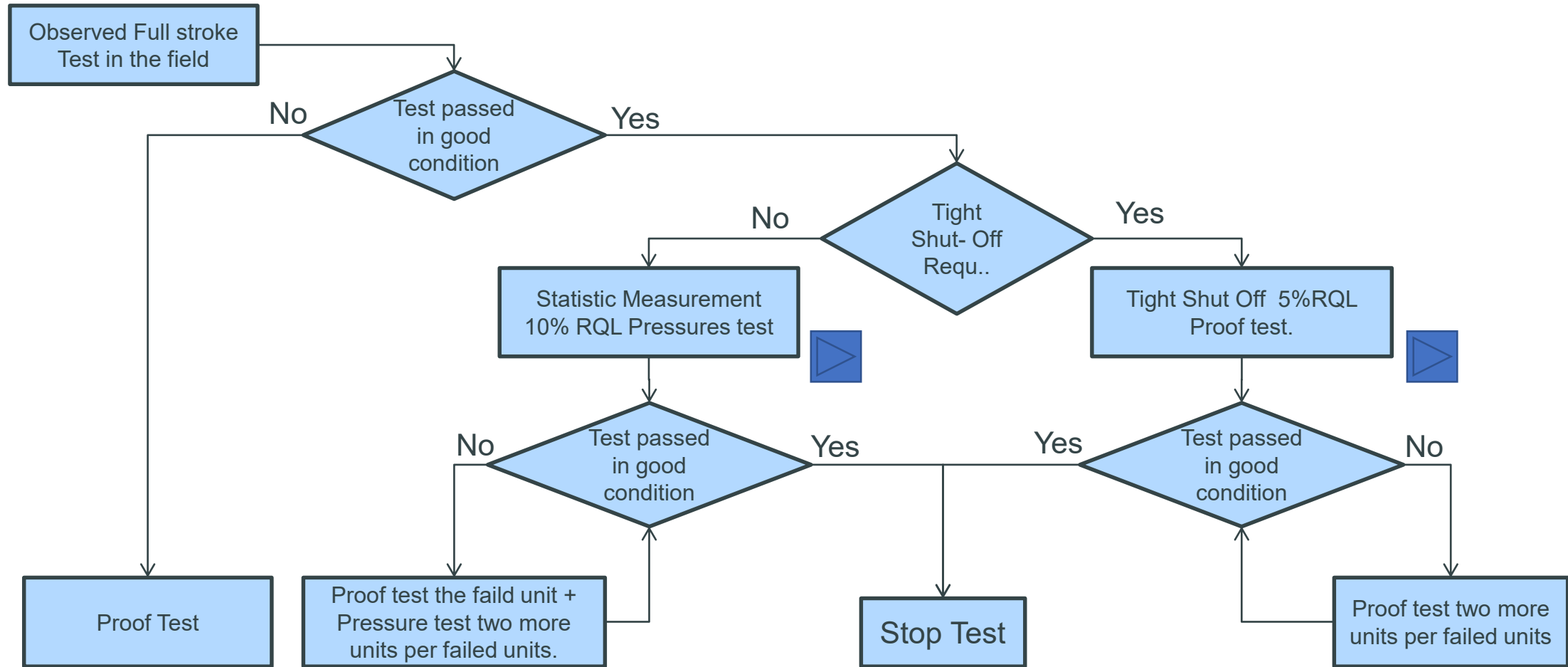


- Prüfung, ob das Ventil die Sicherheitsanforderung noch erfüllt hätte...
- Warum will ich das wissen?
 - Ist das Instandhaltungskonzept richtig gewählt?
 - Wurde die Mission Time richtig gewählt?
 - Hätte mich die SIF die letzten Jahre noch sicher geschützt?
 - Muss das Design verändert werden?
 - Wenn eine Prüfung verschoben werden muss, haben wir Daten die eine solche Verschiebung zulassen?
 - Wenn Mission Time oder Prüfintervalle verändert werden, muss dies durch Daten unterstützt werden.
 -





Nur um mal eine Idee zu geben wie so eine Entscheidung getroffen werden könnte...





Vielen Dank für die Aufmerksamkeit.

Über eine rege Diskussion würde ich mich sehr freuen!

Wenn sie später noch Fragen, Anregungen und Anmerkungen haben, kontaktieren sie mich bitte:

E-Mail: cdemski@dow.com



Christian Demski
Dow Deutschland Anlagenge...
Discipline Activity Leader
Technical Expertise & Support
+49 41469 13814 Work
+49 1523 8255298 Other
CDemski@dow.com
Postfach 1120
Stade, ND 21677





Kleiner Exkurs zur Dichtheit: Erlaubte Leckrate

Welche Daten benötige ich:

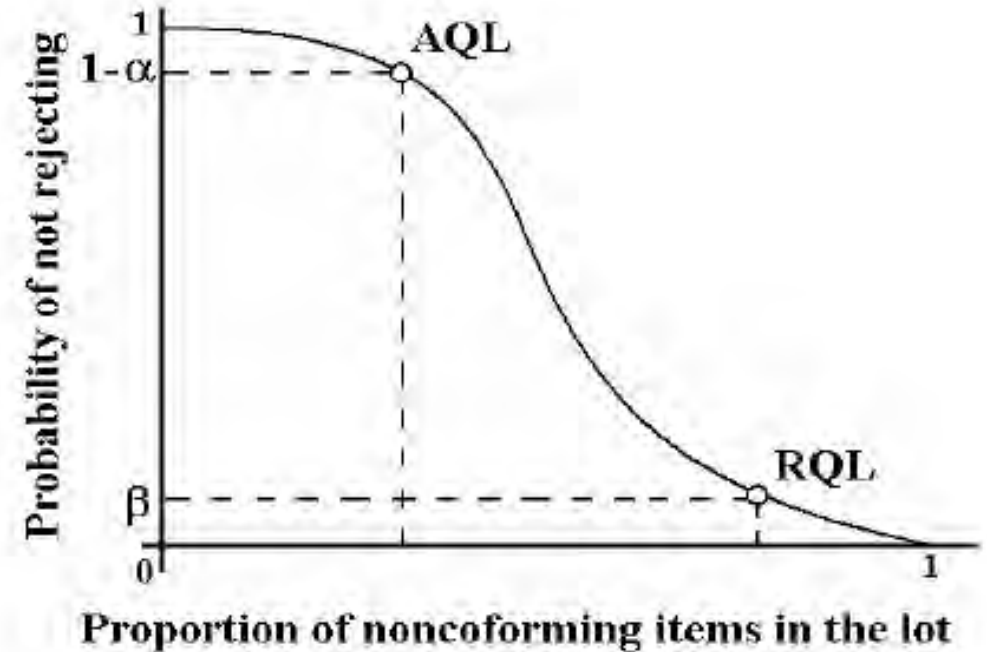
- 30 Kg/h.....
- 30 kg/h bei einem Differenzdruck von 8 bar über dem Ventil
- 30 kg / h bei einem Differenzdruck von 8 bar über dem Ventil bei einem Nachdruck von 1 bara
- 30 kg/h bei einem Differenzdruck von Propylen von 8 bar über dem Ventil bei einem Nachdruck von 1 bara
- Jetzt kann Maintenance auch prüfen.... Nur nicht mit Propylen.





Wer noch nicht genug Statistik hatte....

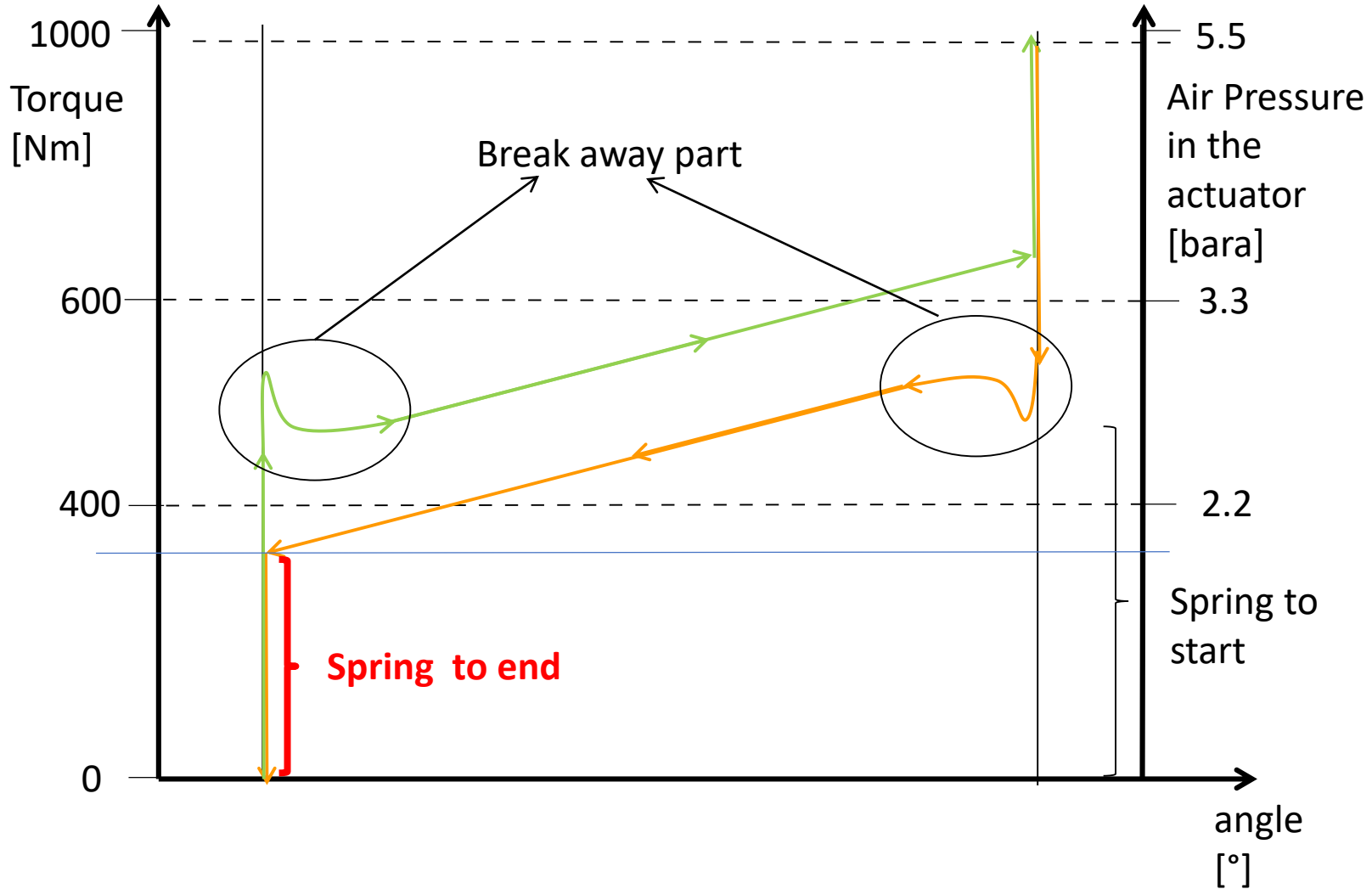
- To determine the amount for the sample testing some parameters have to be set. Two parameters define the shape of the distribution.
- One is the AQL (Acceptance Quality Level):
 - This is a value representing the probability of which a lot that has the quality is rejected by mistake. *Risk of the manufacturer.*
- The other one is the RQL (Reject Quality Level):
 - This is a value representing the probability that a lot with too many failures is accepted by mistake. *Consumer risk.*
- **In this case the consumer risk is chosen, because we have to make sure that the quality meets at least a minimum standard.**



Proportion of nonconforming items in the lot

Fig. 1: Operating characteristic curve

Exkurs zum Drucktest





Retrofitting in der Prozessindustrie

Funktionale Sicherheit

Persönliche Vorstellung

Persönliche Vorstellung:

Malika Mast

Geschäftsführerin RAMSYS GmbH

- FSCEA (Functional Safety Certified Engineer Application)
A031_01255/18 (TÜV Nord)
- FS Eng für Maschinen
14527/17 (TÜV Rheinland)
- FS Eng im Arbeitsgebiet Explosion Protection
Id.-Nr.: 0328/2019 (TÜV Süd)

Kontaktdaten:

Hervester Straße 36

46286 Dorsten

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

m.mast@ramsys.org

www.ramsys.org



Agenda

I. Retrofitting

- (1) Was bedeutet „Retroffiting“?
- (2) Sicherheitslebenszyklus

II. Änderungsmanagement

- (1) Was sollte ich in der FuSi tun?
- (2) Gefährdungsbeurteilung

III. Welche Dokumentation benötige ich am Ende eines Retrofittings?

- (1) Engineering-Doku und FuSi-Dokumentation
- (2) Lebenszyklusakte

IV. Gebrauchsdauer

- (1) Herstellerangaben
- (2) Gebrauchsdauer nach VDI / VDE 2180
- (3) Fazit: Gebrauchsdauer

I. Retrofitting

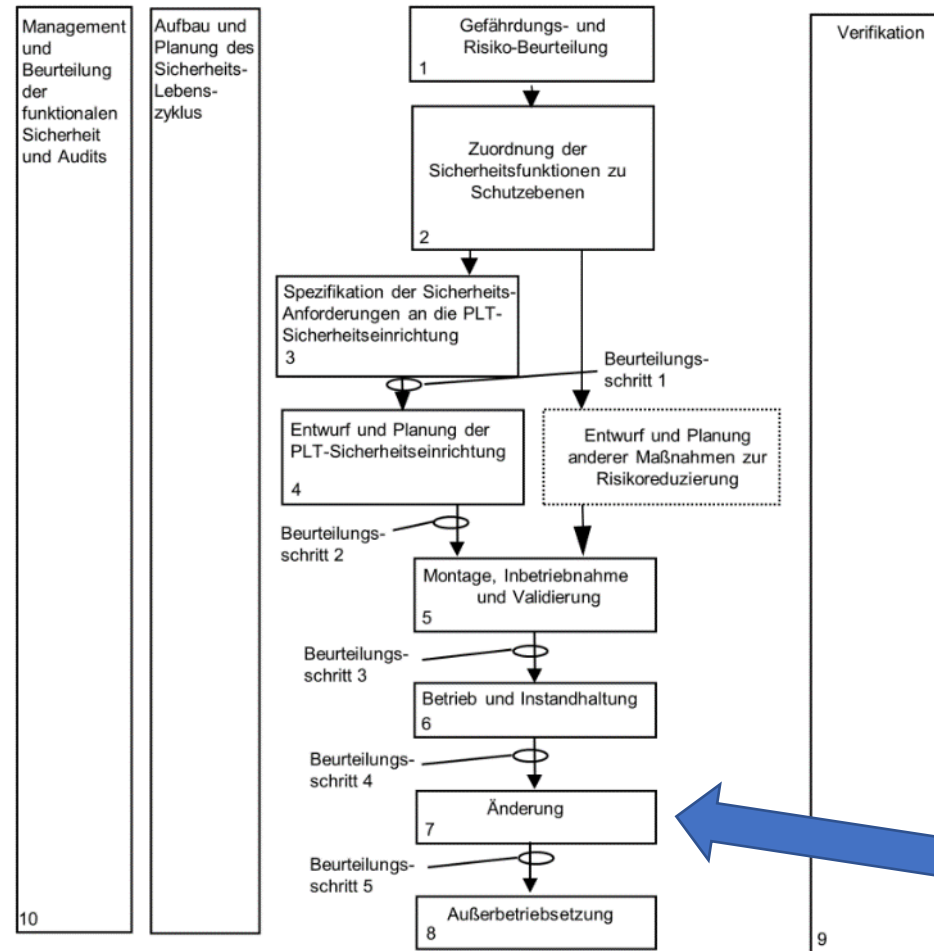
- (1) Was bedeutet „Retrofitting“?
- (2) Stichwort: Funktionale Sicherheit

(1) Was bedeutet Retrofitting?

- ◆ Unter Retrofit (engl. für nachrüsten, umrüsten, Nachrüstung) wird die Modernisierung oder der Ausbau bestehender (meist älterer) Anlagen und Betriebsmittel verstanden
- ◆ In der Regel spricht man hier von Anlagen die weit älter als 15 oder sogar 20 Jahre sind
- ◆ Es ist keine Visualisierung, automatische Auswertung, etc. vorhanden
- ◆ Vor einem „Retrofitting“ wird geprüft ob das „Retrofitting“ oder eine Neuanlage günstiger ist

(2) Sicherheitslebenszyklus

- Ein Umbau, eine Nachrüstung oder eine Modernisierung wird in Phase 7 des Sicherheitslebenszyklus beschrieben



M. Mast

II. Änderungsmanagement

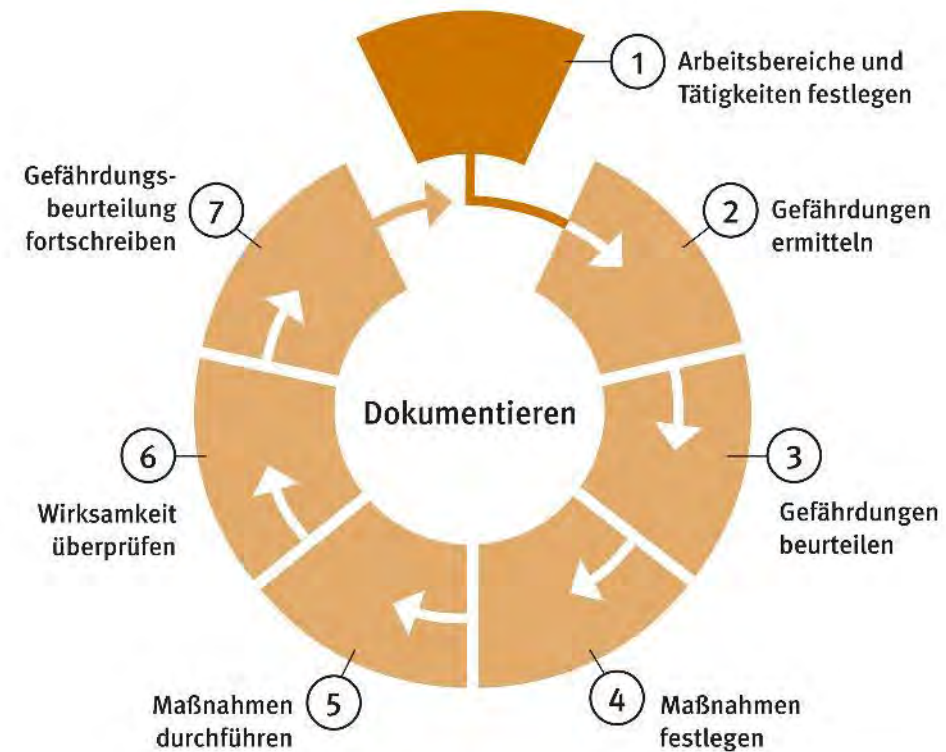
- (1) Was sollte ich in der FuSi tun?
- (2) Gefährdungsbeurteilung

(1) Was sollte ich in der FuSi tun?

- Vor einer Änderung einer PLT-Betriebseinrichtung mit Sicherheitsfunktion oder einer PLT-Sicherheitseinrichtung wird analysiert wie umfangreich die geplante Änderung und deren Auswirkungen auf die Sicherheitsfunktion sind
- Bewegen wir uns im Umfeld des Themas: „Retrofitting“, ist eine solche Analyse eigentlich nicht notwendig
- Wir befinden uns immer in dem Bereich einer Änderung, an dem ein „erneuter“ durchlauf des Sicherheitslebenszyklus zwingend notwendig ist

(2) Gefährdungsbeurteilung

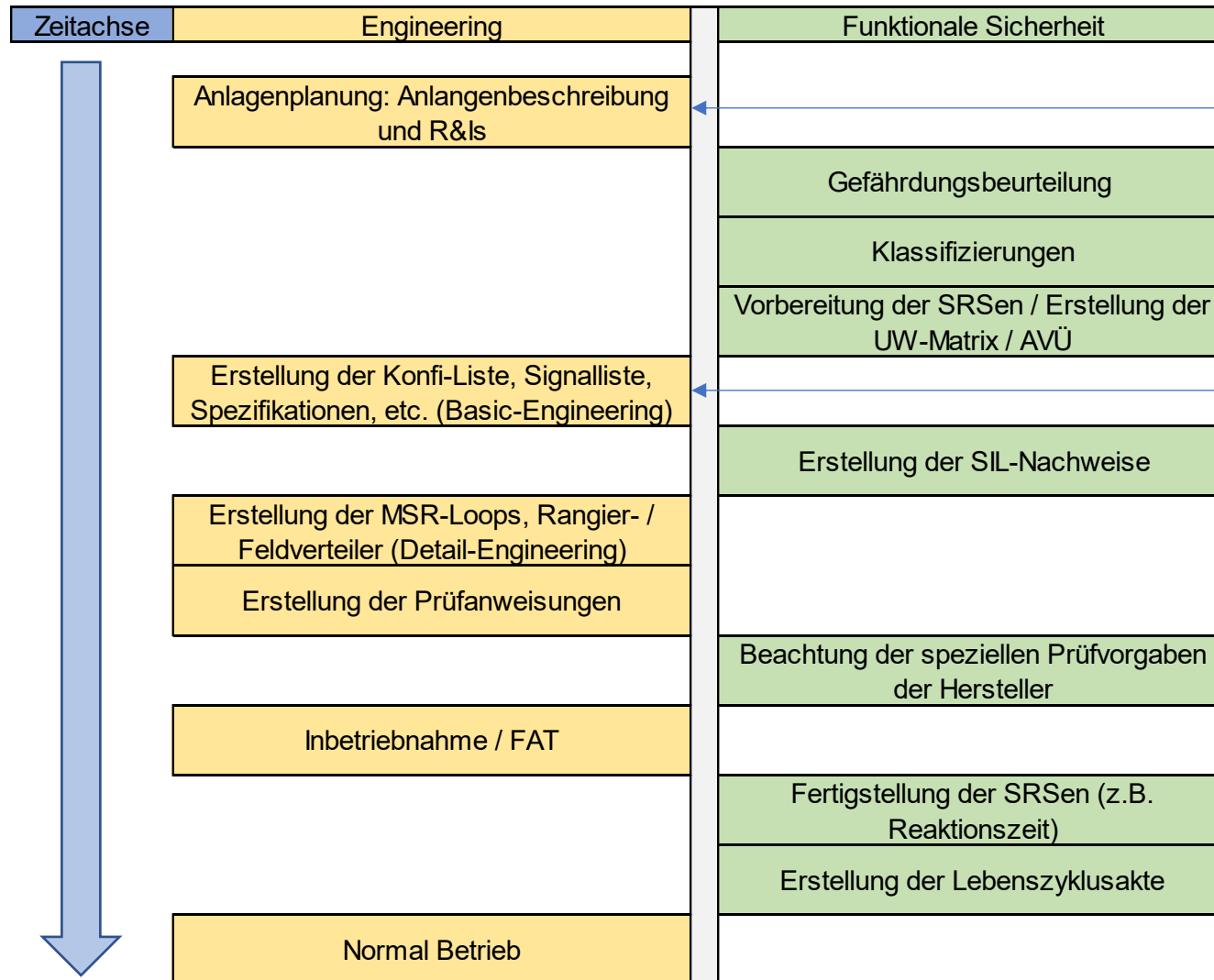
- Wie bei jeder Neuplanung / jedem Umbau oder ähnlichen wird eine Gefährdungsbeurteilung benötigt



III. Welche Dokumentation benötige ich am Ende eines Retrofittings?

- (1) Engineering-Doku und FuSi-Dokumentation
- (2) Lebenszyklusakte

(1) Engineering-Doku und FuSi-Dokumentation



Ablauf kann je nach Firma / Projekt variieren

- Funktionale Sicherheit
- Engineering

(2) Lebenszyklusakte

- ◆ Es gibt keine 100% genaue Festlegung welche Dokumentation in der Lebenszyklusakte enthalten sein sollte
- ◆ Generell kann man folgende Punkte festhalten:
 - ◆ Die Dokumentation die im Laufe des Sicherheitslebenszyklus erstellt wird
 - ◆ Die Dokumente die für die Erstellung dieser Dokumentation benötigt werden (z.B. Fließbilder, Funktionspläne, etc.)
 - ◆ Herstellerdokumentation (z.B. Sicherheitshandbücher, Datenblätter, etc.)

(2) Lebenszyklusakte

- ▣ Beispiel für einen Auszug, der Anforderungen eines Betriebes, einer Lebenszykluskate
- ▣ Variiert nach den eigenen Werksinternen Standards (FSM)

	<i>Kapitel</i>	<i>Unterkapitel</i>	<i>Erklärung /Beschreibung der Dokumente</i>
01.00	Spezifikation& Entwurf		
01.01		Klassifizierung	Risikobeurteilung inkl. Randbedingungen / HAZOP Klassifizierung Protokollierung
01.02		Absicherungskonzept	PID Sicherheitstechnischer Auslegungsbericht / Sicherheitsbetrachtung Funktionspläne Alarm und Verriegelungsübersicht

IV. Gebrauchsdauer

- (1) Herstellerangaben
- (2) Gebrauchsdauer nach VDI / VDE 2180
- (3) Fazit: Gebrauchsdauer

(1) Herstellerangaben

- Viele Hersteller machen eigene Angaben zur Gebrauchsdauer seiner Geräte oder beziehen sich direkt auf die DIN EN 61508 und die Aussage 8-12 Jahre. Gleichzeitig findet man in der Regel den Hinweis auf die Möglichkeit zur Verlängerung
- Damit liegt die Verantwortung eindeutig beim Betreiber

However, according to IEC 61508-2, a useful life time, based on experience, should be assumed. Experience has shown that the useful life time often lies within a range period of about 8 ... 12 **years**.

As noted in DIN EN 61508-2:2011 note NA4, appropriate measures taken by the manufacturer and operator can extend the useful lifetime.



2014-05

Liquiphant FailSafe mit Nivotester FailSafe

Gefährliche unerkannte Fehler in dieser Betrachtung:

Als gefährlicher unerkannter Fehler wird ein falsches Ausgangssignal betrachtet, bei dem eine Anforderung als Gut-Zustand gemeldet wird. (Erklärung der Begriffe "Gut-Zustand" und "Anforderung" → 8).

Lebensdauer elektrischer Bauteile:

Die zugrunde gelegten Ausfallraten elektrischer Bauteile gelten innerhalb der nutzbaren Lebensdauer gemäß IEC 61508-2:2010 Abschnitt 7.4.9.5 Hinweis 3.



Nach DIN EN 61508-2:2011 Hinweis NA4 sind durch entsprechende Maßnahmen des Herstellers und des Betreibers längere Gebrauchsdauern zu erreichen.

(2) Gebrauchsdauer nach VDI / VDE 2180

- ◆ „Die Gebrauchsdauer einer Komponente beschreibt diejenige Zeit, während eine Komponente eine näherungsweise konstante Ausfallrate aufweist.“ (VDI / VDE 2180-Blatt 2; 9.5)
- ◆ Die DIN EN 61508-2, Abschnitt 7.4.9.5 Anmerkung 3 spricht von einem Erfahrungswert für die Gebrauchsdauer von 8-12 Jahren, die jedoch durch entsprechende Maßnahmen des Herstellers und des Betreibers auch deutlich verlängert werden kann (siehe auch NE131: NAMUR Standardgerät, Feldgeräte für Standardanwendungen) (VDI / VDE 2180-Blatt 2; 9.5)

(2) Gebrauchsdauer nach VDI / VDE 2180

- Maßnahmen um die Gebrauchsdauer zu verlängern nach VDI / VDE 2180 Blatt-2; 9.5

Verlängernde Maßnahme	Betreiber	Hersteller
Erstens	Reduzierung kritischer Applikationsbedingungen (z.B. Umwelteinflüsse)	Gerätedesign (z.B. Vermeidung alterungskritischer Bauteile)
Zweitens	Auslegung der PLT-Sicherheitseinrichtung, dass diese im Fehlerfall den sicheren Zustand erreichen	Aktives Fehlverhalten (Fehler sollen erkannt werden oder den sicheren Zustand auslösen)
Drittens	Applikationsspezifische Instandhaltungsmaßnahmen	Gerätespezifische Instandhaltungsempfehlungen
Viertens	Verifizierung durch Stördatenerfassung	

(3) Fazit: Gebrauchsdauer

1

- Herstellerangaben
- Angabe der DIN EN 61508 (8-12Jahre)

2

- Berücksichtigung der Maßnahmen der VDI / VDE 2180
- Aufbau einer Störfalldatenbank mit Hilfe der NE 131 und NE 93

3

- Eigene Verantwortung der Betreiber auf Grund von Erfahrungswerten
- Absprache mit einer ZÜS

Vielen Dank für Ihre Aufmerksamkeit

Malika Mast Dipl. Ing / Geschäftsführerin

E-Mail: M.Mast@ramsys.org

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

Mobil: 0171 / 3037392

Ist Abschalten sicher und wenn ja wie?

HIMA

SMART
SAFETY.

29.09.2022 / 13. SIL – Sprechstunde

Ivo Hanspach – Director Product Management

Agenda

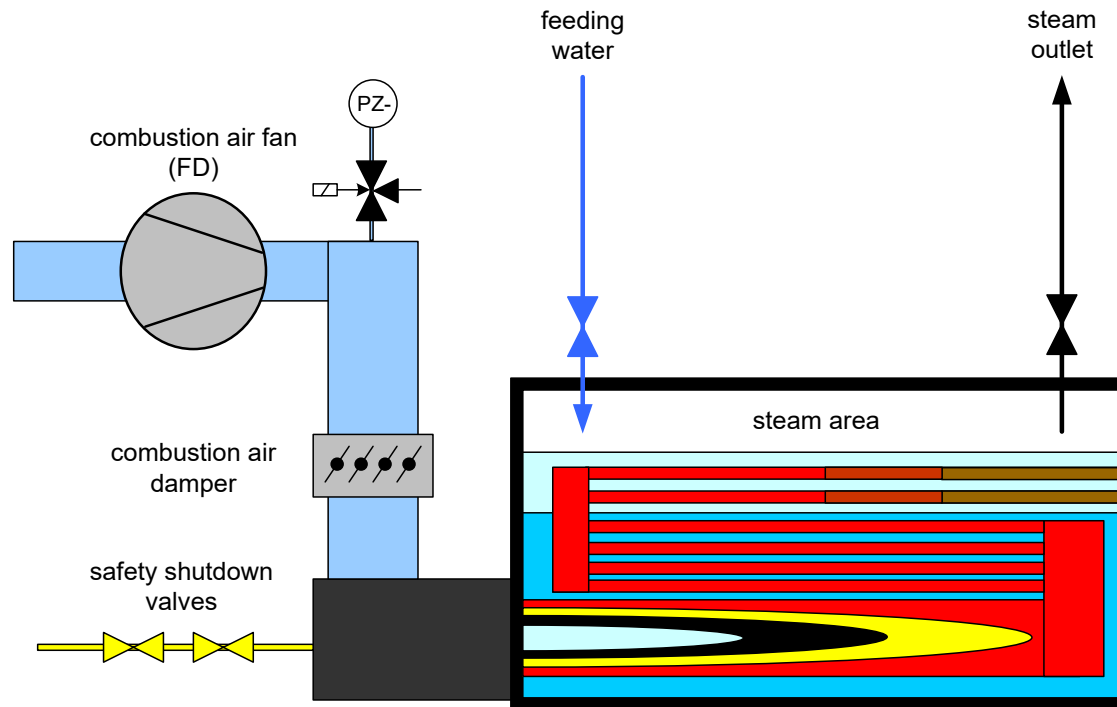


1. Introduction - Which state is really safe?
2. Safe States, Safety Standards & possible Technical Principles
3. Technical & Probabilistic considerations

Which state is safe?

- Burner

=> Flame out



- Close fuel supply

=> Switch Off
„De-Energize To Trip“

Which state is safe?

- Turbine
=> Overspeed detected



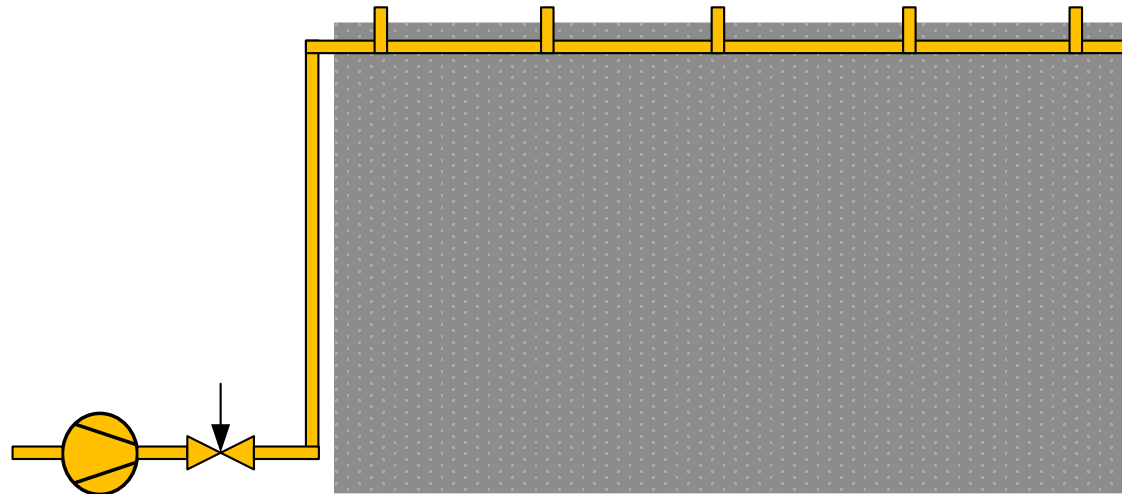
- Switch off motor / switch off steam supply

=> Switch Off
„De-Energize To Trip“

Which state is safe?



- Tank with level monitoring
=> Fill level to high (LZHH)



- Close valves / switch off pump

=> Switch Off
„De-Energize To Trip“

Which state is safe?



- Fire extinguishing system
=> Fire detected



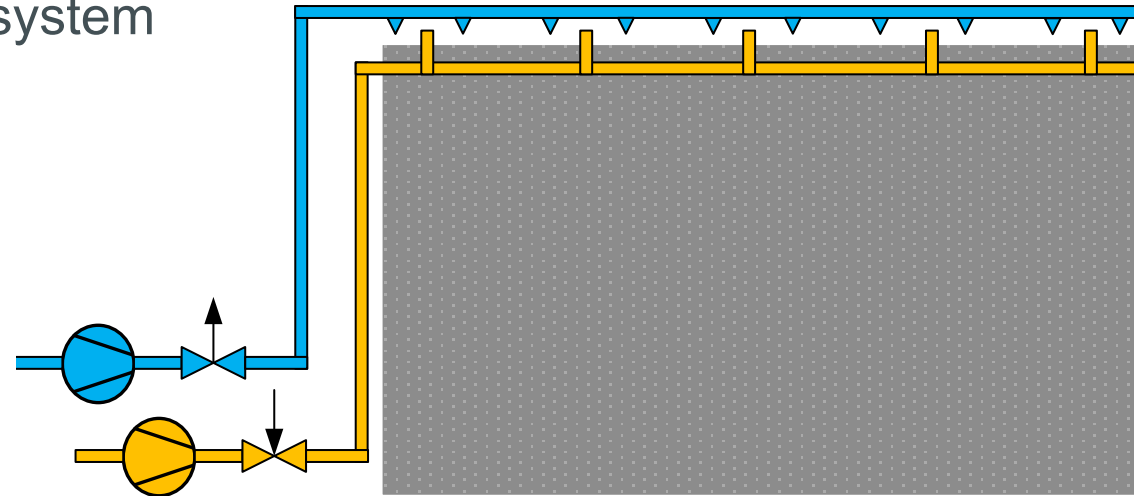
- Open extinguishing valves & switch on pumps

=> Switch On
„Energize To Trip“?!?



Which state is safe?

- Tank with level monitoring
=> Overfilled => Fire
- Fire extinguishing system
=> Fire detected



- Close valves / switch off pump
- Switch on extinguishing pump, open valves

=> Switch Off & Switch On
„De-Energize To Trip“ & „Energize To Trip“

Which state is safe?

- CO2 - Fire extinguishing system
=> Fire detected



- Open extinguishing valves & switch on pumps
(If no people are inside)



=> Switch Off & Switch On
„De-Energize To Trip“ & „Energize To Trip“

Which state is safe?

- Acryl Acid Storage
 - => Storage below 25°C
 - => no undercutting of 15°C => exotherm reaction
 - => no overcutting of 50°C => exotherm reaction



=> Switch Off & Switch On
„De-Energize To Trip“ & „Energize To Trip“

Which state is safe?



- Airport => Overall Power failure



- Switch on emergency power generators, switch on emergency/escape route lighting
- Switch off unnecessary power consumers
- Targeted power & load control

=> Switch Off & Switch On
„De-Energize To Trip“ & „Energize To Trip“

Safe States

DET (De-Energized To Trip)

ETT (Energized To Trip)

SDS (State Dependent Safety)



Statements IEC 61511

10.3 SIS safety requirements

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

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

- requirements relating to manual shutdown for each SIF;
- requirements relating to energize or de-energize to trip for each SIF;
- requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semi-

11.6.2 Energize to trip circuits shall apply means to ensure circuit and power supply integrity.

NOTE 1 An example of such means is an end-of-line monitor, where a pilot current is continuously monitored to detect circuit continuity and where the pilot current is not of sufficient magnitude to affect proper I/O operation.

NOTE 2 Additional requirements for loss of power can be found in 11.2.11.

11.2.11 For any SIS device that on loss of utility (e.g., electrical power, air, hydraulics or pneumatic supply) does not fail to the safe state, loss of utility and SIS circuit integrity shall be detected and alarmed (e.g., end-of-line monitoring, supply pressure measurement, hydraulic or pneumatic pressure monitoring) and action taken according to 11.3.

Different concepts for safety

Probabilistic Approach

Tabelle 2 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ A-Element oder Teilsystem ausgeführt wird

Anteil sicherer Ausfälle eines Elements	Hardwarefehlertoleranz		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3

Tabelle 3 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ B-Element oder Teilsystem ausgeführt wird

Anteil sicherer Ausfälle eines Elements	Hardwarefehlertoleranz		
	0	1	2
< 60 %	nicht erlaubt	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

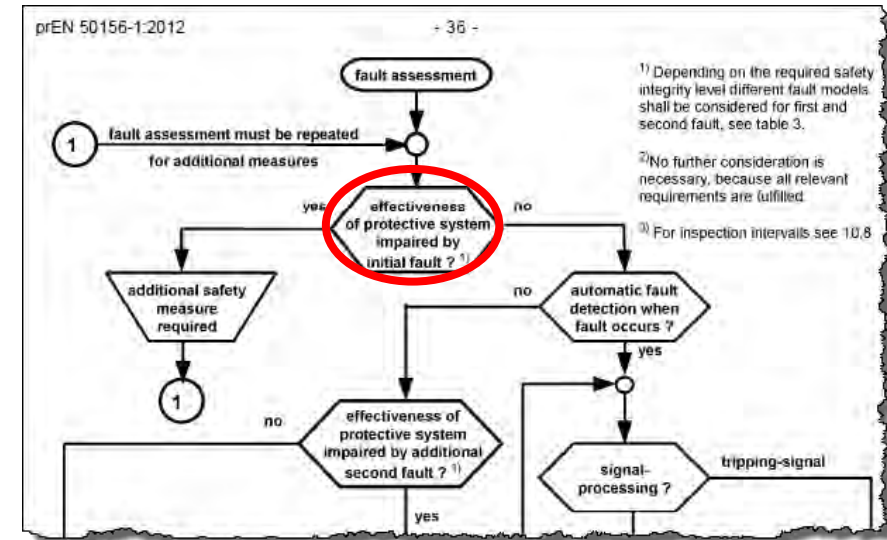
Safety integrity level	Average probability of dangerous failure on demand of the safety function
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Safety integrity level	Average frequency of dangerous failure of the safety function (hr ⁻¹)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

NOTE See Notes 2 to 6 below for details on interpreting this table.

NOTE See Notes 2 to 6 below for details on interpreting this table.

Deterministic Approach (EN 50156)



$$PF_{DG} = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE}t_{GE} + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

Different concepts for safety

Probabilistic Approach

Safe failure fraction an element	Hardware fault tolerance		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

NOTE: This table is for information only.

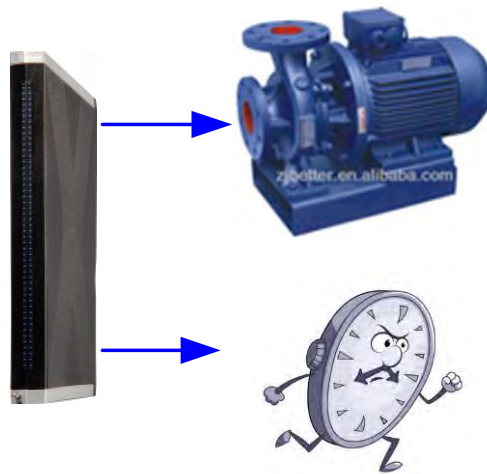
Safety integrity level	Average probability of dangerous failure on demand of the safety function
4	≥ 10 ⁻⁵ to < 10 ⁻⁴

Safety integrity level	Average frequency of dangerous failure of the safety function (hr ⁻¹)
4	≥ 10 ⁻⁹ to < 10 ⁻⁸
3	≥ 10 ⁻⁸ to < 10 ⁻⁷
2	≥ 10 ⁻⁷ to < 10 ⁻⁶
1	≥ 10 ⁻⁶ to < 10 ⁻⁵

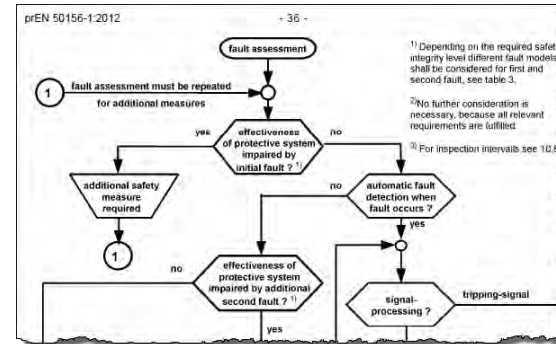
NOTE: See Notes 2 to 6 below for details on interpreting this table.

$$PFD_G = 2(1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU}^2 t_{CAE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left(\frac{T_i}{2} + MRT \right)$$

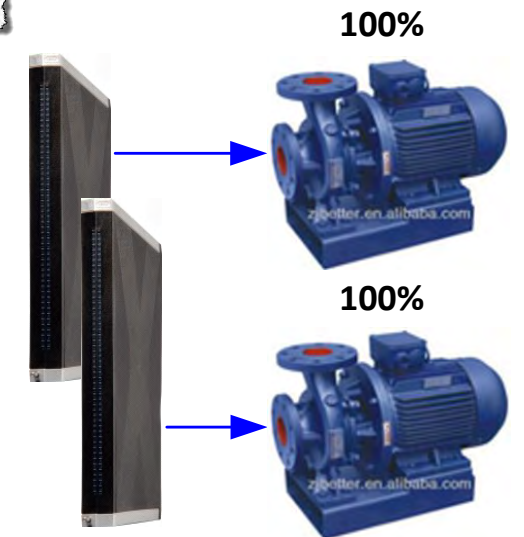
Safety with
HFT = 0
is possible



Deterministic Approach


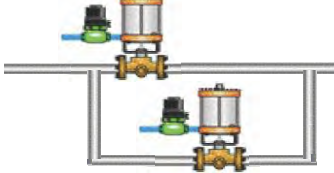
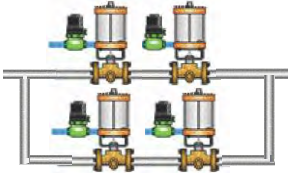


Safety with
HFT = 0
is not possible



Fault Tolerant SIF & Operating principles



<p style="text-align: center;">DET (De-energized To Trip)</p> 	<p style="text-align: center;">ETT (Energized To Trip)</p> 	<p style="text-align: center;">SDS (State Dependent Safety)</p> 
<p>Clearly Defined Safe State:</p> <ul style="list-style-type: none"> • e.g. Closing fuel line <ul style="list-style-type: none"> ▪ Increased Safety ▪ Reduced Availability ▪ Closed circuit principle 	<p>Clearly Defined Safe State:</p> <ul style="list-style-type: none"> • e.g. Opening emergency reactant (stop reaction) <ul style="list-style-type: none"> ▪ Increased Safety ▪ Reduced Availability ▪ Open circuit principle 	<p>Safe reaction (Energize or De-Energize) depends on the State of the process:</p> <ul style="list-style-type: none"> • (e.g. Pipeline Safety, chemical reactors) <ul style="list-style-type: none"> ▪ Increased Safety ▪ Increased Availability ▪ “Depends”

For open circuit current principle – check for needs or additional measures (monitoring, redundancy, ...) for: Sensors / Actors; Signal cables; Interface technology; Safety systems; Power Supplies; Pressure vessels; ...

Technical & probabilistic consideration

DET (De-Energized To Trip)

ETT (Energized To Trip)

SDS (State Dependent Safety)



And What about calculations?



Safety Data to be evaluated



HIMax

Functional Safety Data

i The operating requirements provided in the safety manual and in the module-specific manuals must be observed for all modules.

1.1.1

Functional Safety Data

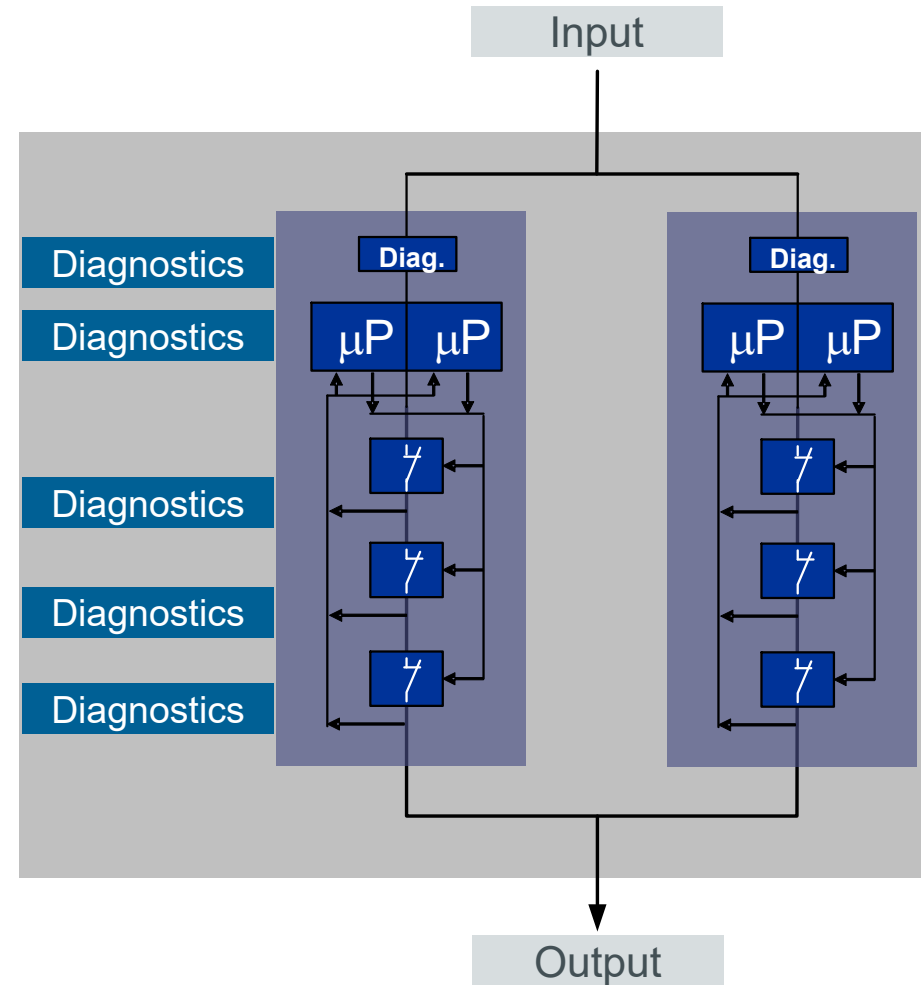
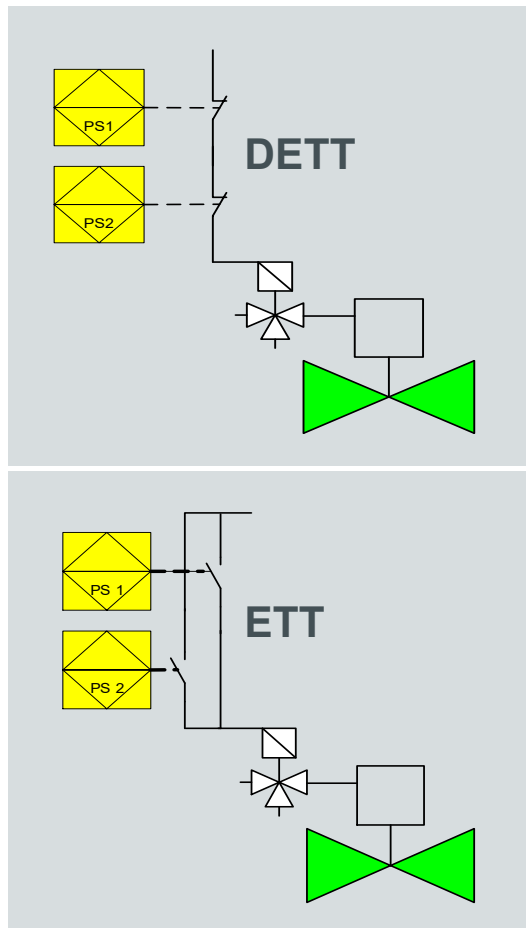
HIMax

1.1.2 Energize to Trip Principle

The proof test interval T_1 indicated for the HIMax modules is 5 years.

Module	Module	MTTF in years	λ_S / h^{-1}	λ_{DD} / h^{-1}	λ_{DU} / h^{-1}	PFD	PFH / h^{-1}	SFF	SIL
X-DI 16 01	X-DI 16 01	29.46	1.26E-06	1.25E-06	1.07E-08	1.25E-04	5.37E-09	99.57 %	3
X-DI 32 01	X-DI 32 01	35.55	1.09E-06	1.08E-06	9.06E-09	1.24E-04	5.33E-09	99.59 %	3
X-DI 32 01 A	X-DI 32 01 A	31.72	1.30E-06	1.24E-06	7.82E-09	1.39E-04	5.53E-09	99.69 %	3
X-DI 32 02	X-DI 32 02	34.20	1.08E-06	1.07E-06	8.97E-09	1.06E-04	4.55E-09	99.59 %	3
X-DI 32 05	X-DI 32 05								
X-DI 32 02 A	X-DI 32 02 A	30.72	1.28E-06	1.22E-06	7.69E-09	1.20E-04	4.70E-09	99.69 %	3
X-DI 32 03	X-DI 32 03	39.45	9.65E-07	9.57E-07	7.78E-09	1.02E-04	4.37E-09	99.60 %	3
X-DI 32 04	X-DI 32 04	39.38	9.66E-07	9.58E-07	7.79E-09	1.02E-04	4.36E-09	99.60 %	3

Design principles for DET, ETT, SDS



From failure rate (λ) to MTTF



λ (failure rate) vs. MTTF

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

$$\text{MTTF} = 1 / \lambda$$

According to. IEC 61508 Part 7 D.2.3.2

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

How systems operate – MTTF, MTTR, MTBF



MTTF = Mean Time To Failure

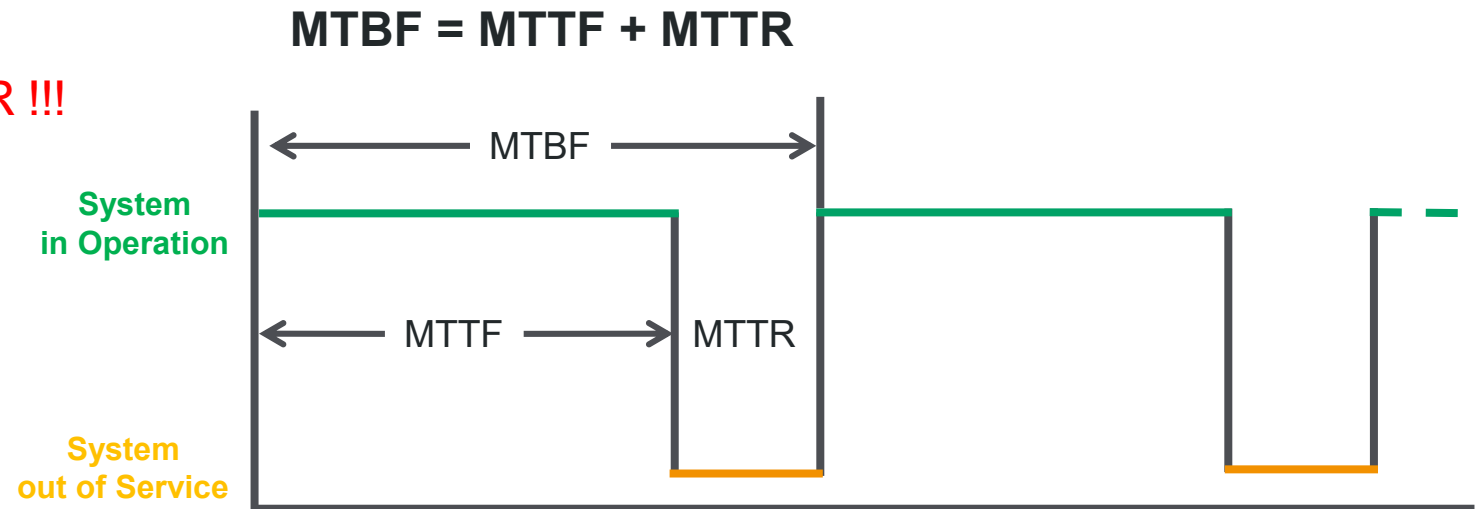
MTTR = Mean Time To Restoration (Detect+Repair)

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 $MTTF \gg MTTR$!!!

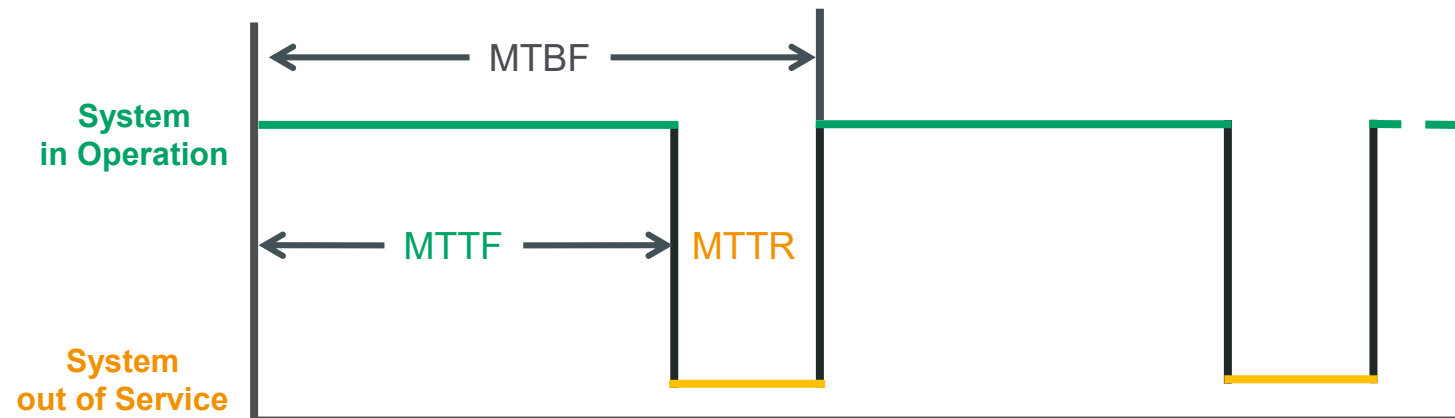


How about the availability of systems



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

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



How about the availability of systems



1st 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€

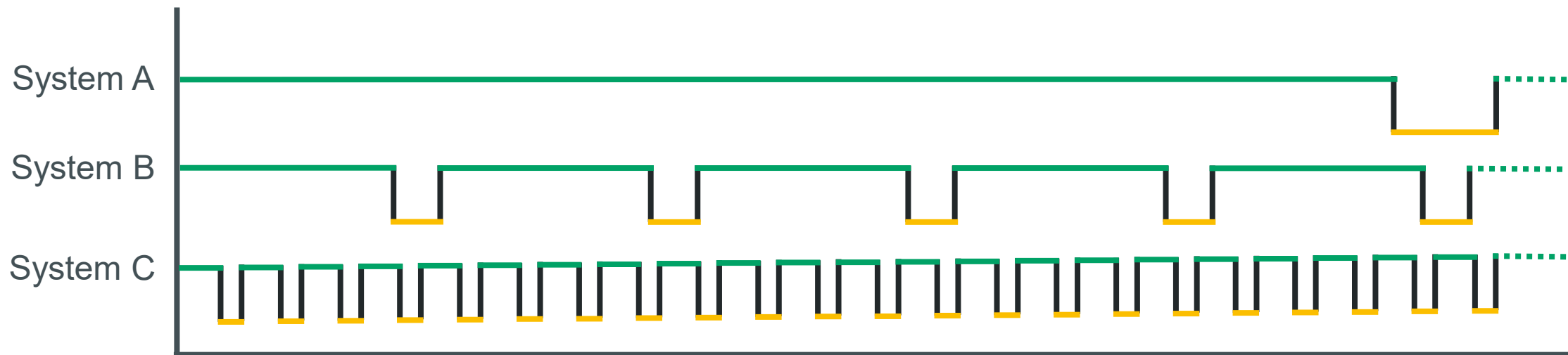
This system has the lowest price and best availability!!!

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

How about the availability of systems



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 continuous” applications

MTBF figures – What are you really looking for?

- MTBF numbers are very much influenced by environmental conditions (temp., vibration, aggressive air, salt fog, voltage bursts, etc.)
- Simplified MTBF formulas 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 build fault tolerant subsystems or systems:
 - define the number of devices, I/O points, SIFs and a fixed MTTR
 - the SIF architecture (1oo2, 2oo3...)
 - the function (energize or de-energize to trip, state depended safety function),
 - additional equipment like isolators or relays, power supplies
 - environmental conditions (e.g. temperature)

=> *otherwise you compare apples and oranges*

Do you have questions?



Simple things can be difficult!



Thank you for your attention!



Ivo Hanspach

Director Product Management – Safety Systems

HIMA Paul Hildebrandt GmbH

Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone: +49 (0) 6202 / 709-0

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

Email: info@hima.com

Website: www.hima.com

#FIT4FUNctionalsafety

WIE MIT "SIL-MECHANIK" IN SICHERHEITSFUNKTIONEN UMGEHEN?
UND WAS WIR HEUTE FÜR MORGEN LERNEN MÜSSEN, UM FIT FÜR DIE ZUKUNFT DER
FUSI ZU BLEIBEN – GEDANKEN ZUR GEBRAUCHSDAUER VON METHODEN...



Marco Knödler

Team Lead I&C (Yncoris) + Associate Lecturer Functional Safety (German universities of applied sciences)

- NAMUR WG 4.5 – VDI/VDE-GMA FA 6.13
- DIN NA 003-01-01 AA - CEN/TC 69/WG 1 -
- DKE STD_1941.0.8 - SCI 4.0 Expert Panel AI in Industrial Applications



Einen Experten zu Rate ziehen? (FITness-) Alter?

Kann ich den Zahlen trauen?

FIT?

Fit für meinen Zweck?

Risiko reduzieren ?

Regelmäßiger Check?



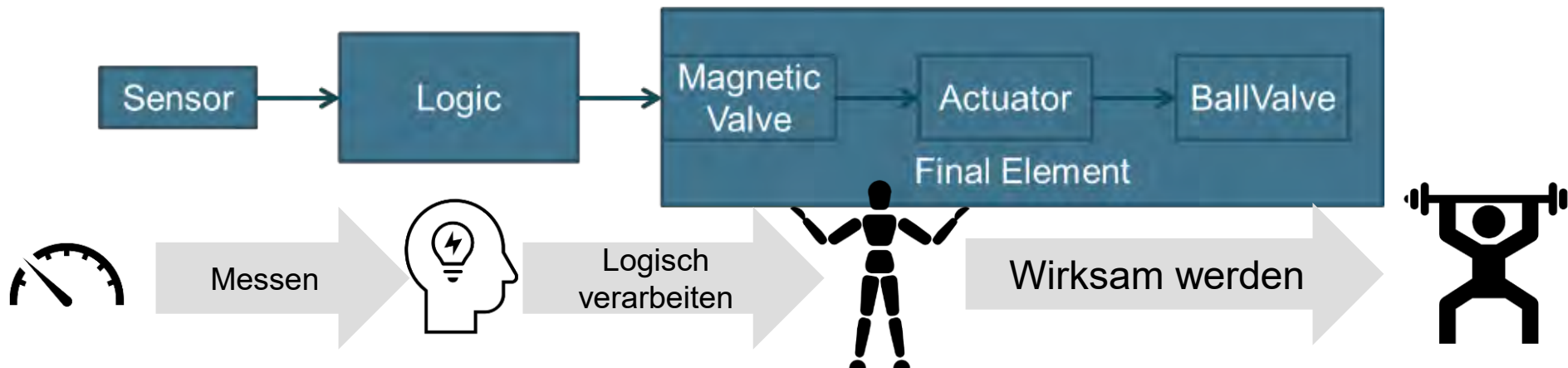
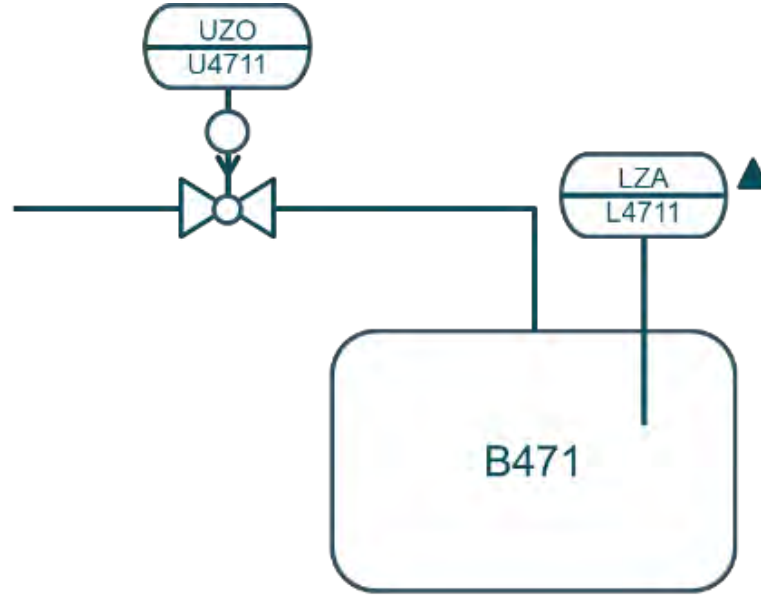


Entsprechend dem festgelegten Zweck

<https://www.mayoclinic.org/healthy-lifestyle/fitness/in-depth/fitness/art-20046433>



SAFETY INTEGRITY LEVEL (SIL) & FITNESS AM BEISPIEL EINER ÜBERFÜLLSICHERUNG



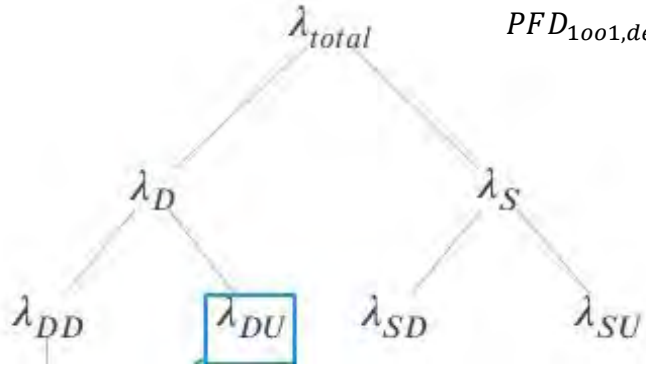
- In most situations, safety is achieved by a number of protective systems which rely on many technologies (for example **mechanical**, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and **actuators**) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this International Standard is concerned with electrical/electronic/programmable electronic (E/E/PE) safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

IEC 61508-1 : 1998 - INTRODUCTION

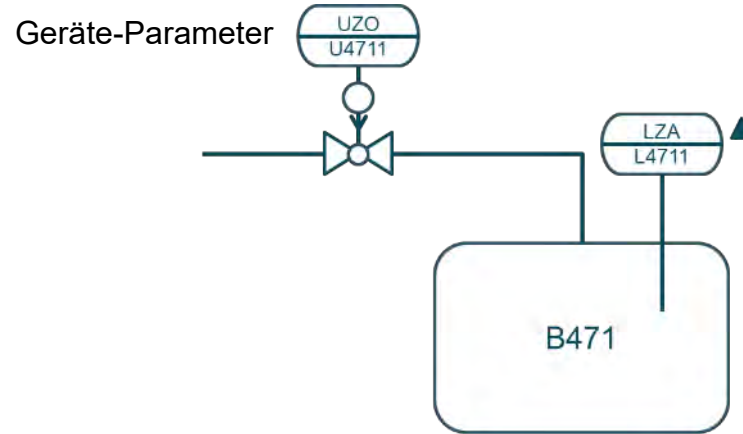
AN E/E/PE SAFETY-RELATED SYSTEM COVERS ALL PARTS OF THE SYSTEM THAT ARE NECESSARY TO CARRY OUT THE SAFETY FUNCTION (I.E . FROM SENSOR, THROUGH CONTROL LOGIC AND COMMUNICATION SYSTEMS , TO FINAL ACTUATOR, [...]).

IEC 61508-0 : 2005 - Objective

PFD BERECHNUNG



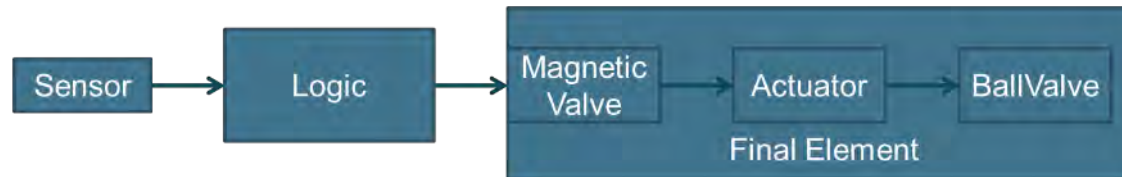
$$PFD_{1001,device} = PTC_0 \lambda_{DU} \frac{T_0}{2} + (PTC_1 - PTC_0) \lambda_{DU} \frac{T_1}{2} + (1 - PTC_1) \lambda_{DU} \frac{T_2}{2}$$



SIL Safety Integrity Level	RRFmin (Minimum Probability Reduction Factor)	PFDmax (maximum of Probability on Demand)	HFT Hardware Fault Tolerance
SIL 1	10	0,1	0
SIL 2	100	0,01	0
SIL 3	1000	0,001	1
SIL 4	10000	0,0001	3

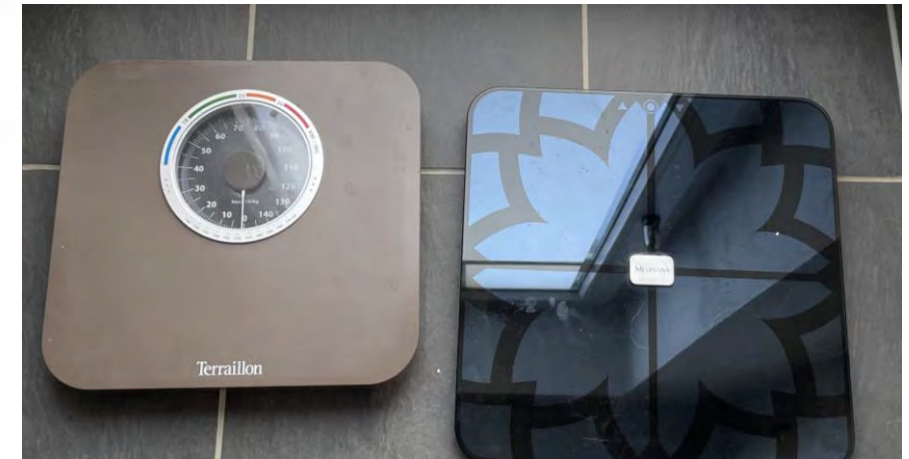
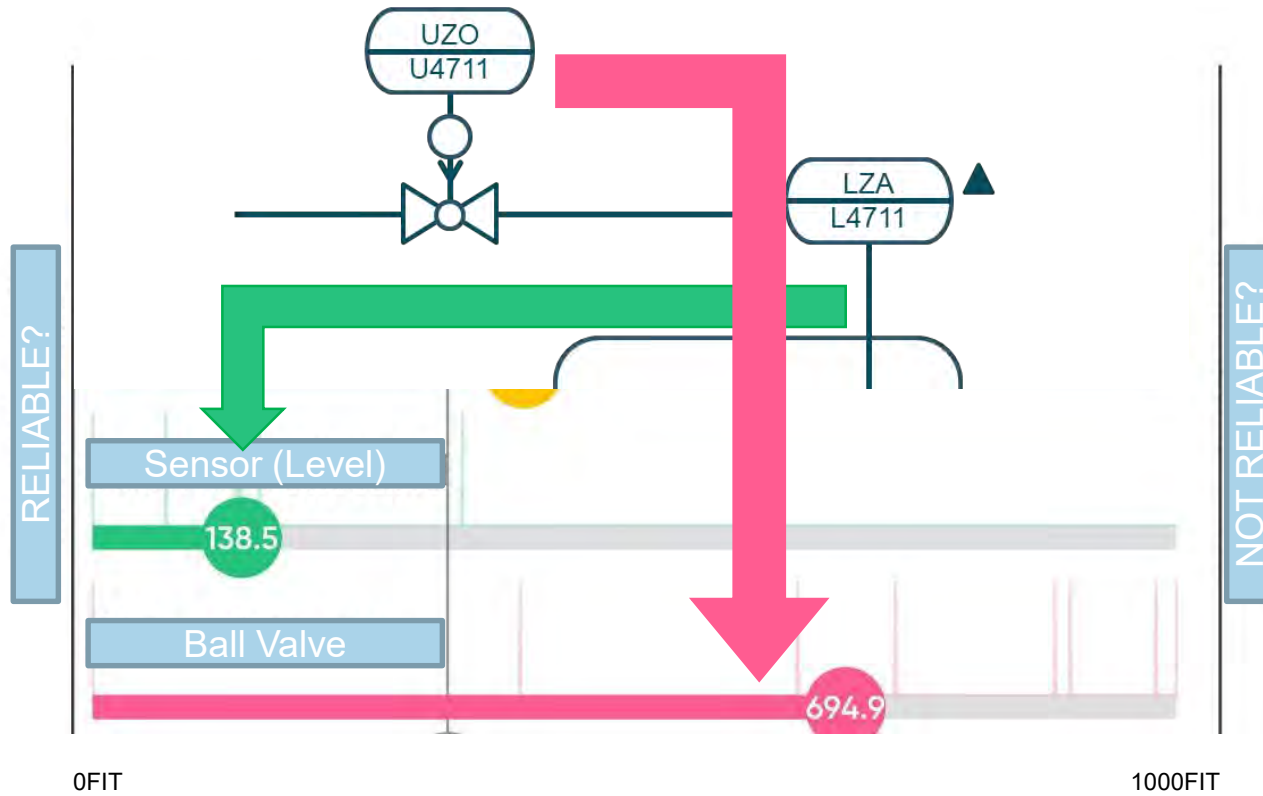
= Rate gefährlicher und unentdeckter Ausfälle, Failures In Time [FIT] = failures per 10⁹ hours

(1 Jahr = 8760 Stunden,
10⁹ Stunden = 114.155,25 Jahre)



$$PFD_{avg\ total} = PFD_{Sensor} + PFD_{Logic\ processing} + PFD_{final_element}$$

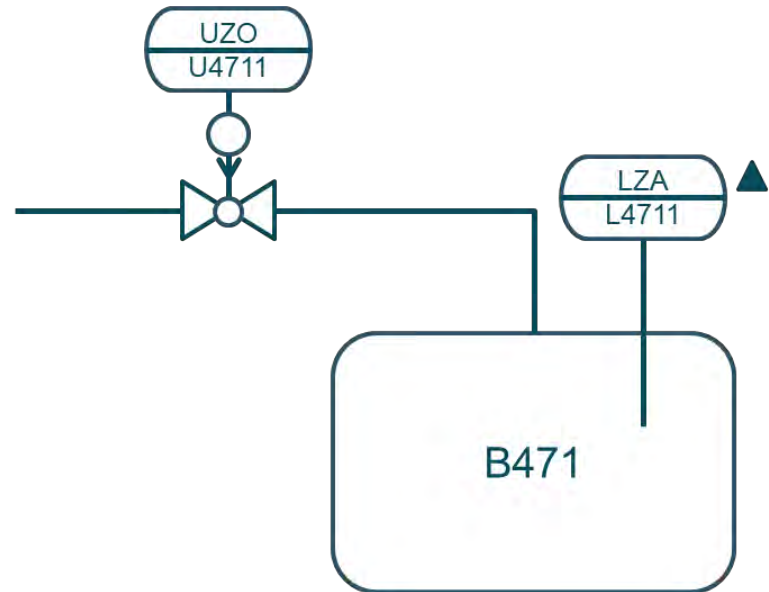
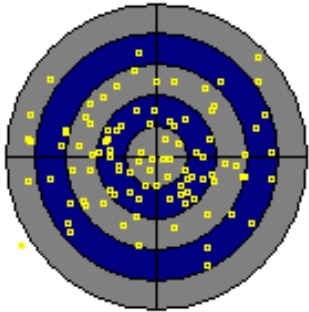
RECHERCHE VON AUSFALLRATEN (LAMBDA_DU [FIT])



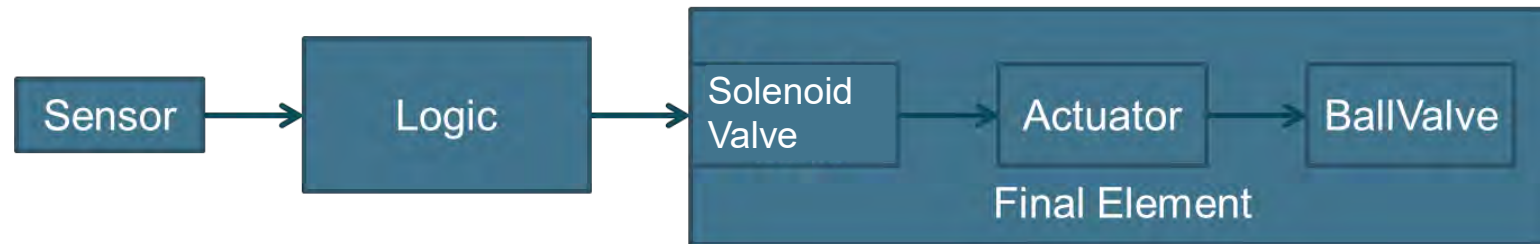
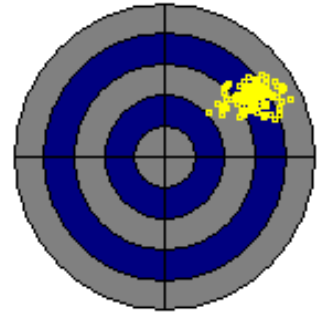
Wenn ich erwarte, dass die Mechanik grundsätzlich zuverlässiger ist...



MIT WELCHER ART VON AUSFÄLLEN HABEN WIR ES ZU TUN?



FITness-Indikatoren haben (unterschiedliche) Auswirkungen auf (eine Wahrscheinlichkeit des) Ausfalls... die meisten sind nicht „zufällig“ – sind sie geeignet für die Probabilistik?

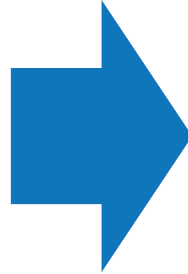


Functional safety of safety-related automated industrial valves – a Manufacturer oriented standard

CEN/TC 69/WG 1/AHG 3 WI 00069217

History

- 2016 – 2018 national Meetings
- Since 2019 CEN Work Item 00069217
 - TC 69 Industrial Valves
 - WG 1 Basic standards
 - AHG 3 Functional Safety
- Participants
 - Manufacturers of valves and actuators
 - End users and system integrators
 - Third Parties



Timeline

- Enquiry Draft is on it's way
- Rework will be done 2023
- **Publication in 2024**



Klassifizierung von Edelstahl, z.B. A2-70 (Standard-Edelstahl)

A
2

Kennzeichen Werkstoffgruppe
A = Austenitischer Edelstahl (Chrom-Nickel-Stahl)

Kennzeichen Stahlgruppe
1 = Automatenstahl
2 = Kalttauchstahl legiert mit Chrom und Nickel (klassisch)
3 = Kalttauchstahl mit Chrom und Nickel legiert und stabilisiert
4 = Kalttauchstahl mit Chrom, Nickel und Molybdän
5 = Kalttauchstahl mit Chrom, Nickel und Molybdän (stabilisiert) mit Titan, Niob und Tantal

-70

Festigkeitsangabe: Zugfestigkeit
50 = 1/10 der Zugfestigkeit (mindestens 500 N/mm²)
70 = 1/10 der Zugfestigkeit (mindestens 700 N/mm²)
80 = 1/10 der Zugfestigkeit (mindestens 800 N/mm²)



Startpunkt der Diskussion im CEN: Basis-Ausfallraten für Schrauben =5 FIT für FMEDA -> Gesamt FIT für Armatur -> PFD

Reales Thema: Welche Schrauben nutze ich? -> max. Drehmoment unterschiedlich um Faktor 1,5

DN	Flanschtyp nach EN 5211	Zulässiges Drehmoment am Flanschbild 1) nach ISO 5211 [Nm]	Zulässiges Drehmoment für A4-70 Schrauben am Flanschbild 2) [Nm]	Zulässiges Drehmoment für A4-70 Schrauben auf Abscheren am Flanschbild 2) [Nm]	M _{ref} LoseiB/Grundmoment [Nm]	mit Sicherheitsfaktor 1,5 = M _{dref}
15	F04	63	89	546	22	33
25	F05	125	151	1092	43	65
40	F07	250	302	2348	66	99
50	F07	250	384	2348	106	159
80	F10	500	887	5420	140	210
100	F10	500	1177	5420	200	300
150	F12	1000	2354	9652	434	651
200	F14	2000	4709	20099	534	801
250	F14	2000	6278	20099	800	1200
300	F16	4000	12556	37013	1066	1599
400	F25	8000	25112	72931	2120	3180

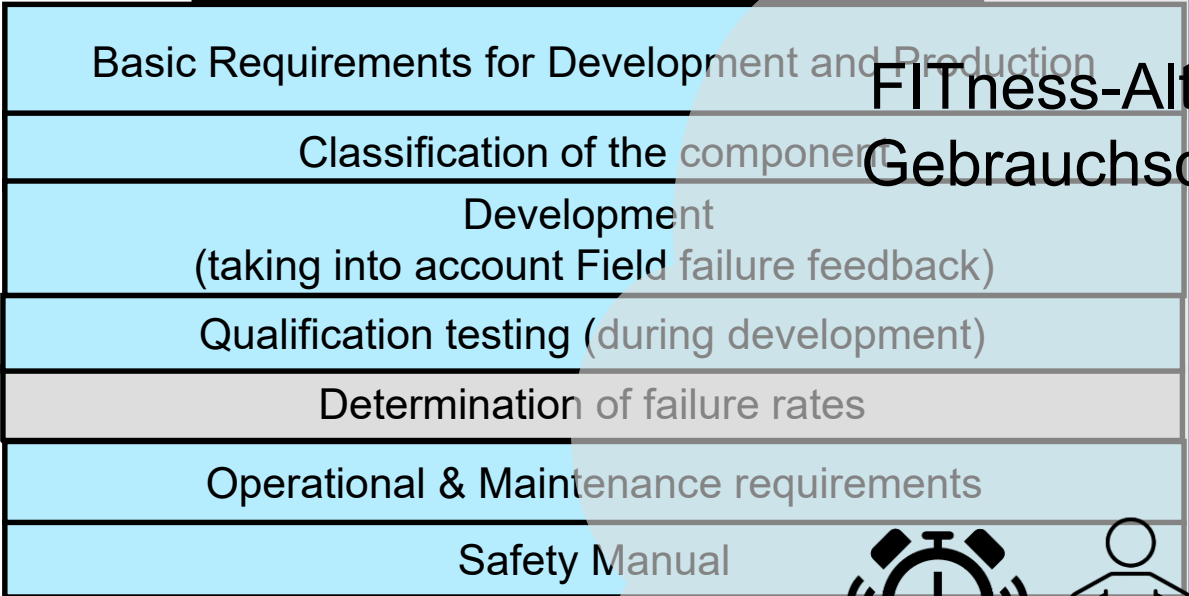
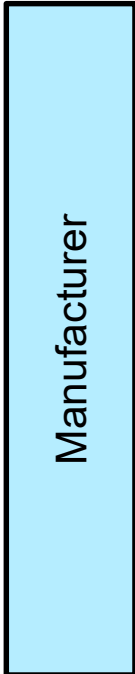
*1,5

Verbindung zu schwach / Drehmoment zu hoch

1) Die Berechnungen der zulässigen Momente basiert auf den Festigkeitswerten von Schrauben mit einer Zugbeanspruchung > 290 MPa z.B. A2-70

Functional Safety of safety-related automated industrial valves

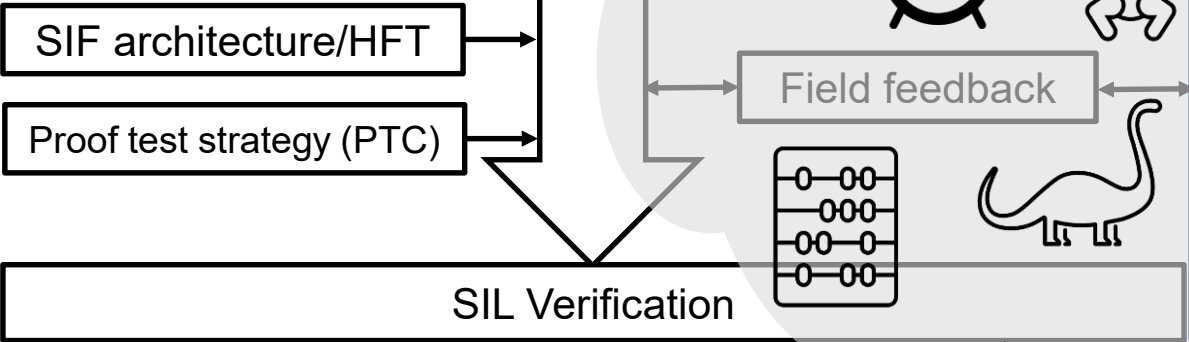
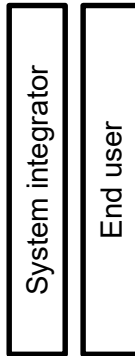
As per Manufacturer standard currently developed in CEN/TC 69, prEN 00069217



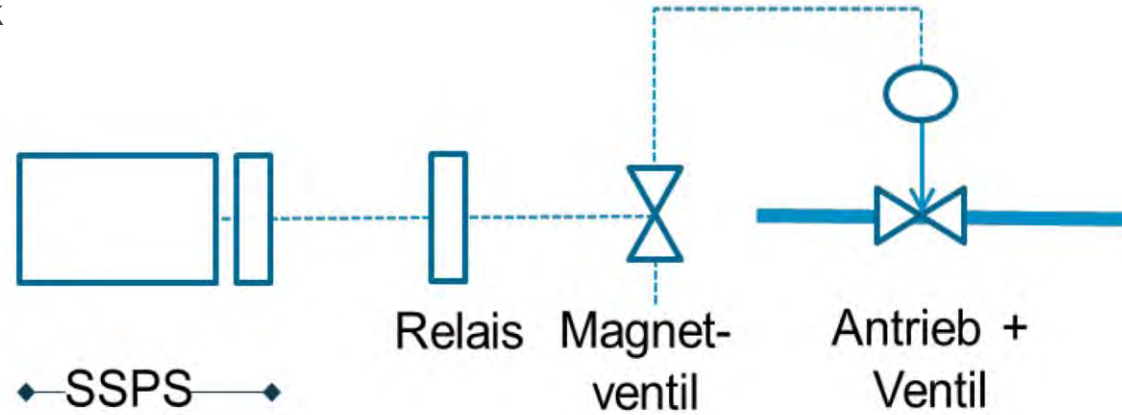
Fitness-Alder -> Gebrauchsdauer

F I T F O R E P U R P O S E

Daily end user business as per IEC61511



- VDI/VDE2180-4 sieht 2 Möglichkeiten vor, Mechanik im Sinne von Ausfallraten (zufällige Fehler) zu berücksichtigen (ohne den Fokus auf systematisch richtiges Vorgehen zu verlieren)
- Anwenderdaten verwenden
- Wenn Hersteller-Daten verwendet werden, muss ebenfalls sichergestellt sein, dass Systematische Fehler
 - soweit wie möglich (durch ein geeignetes Management -System) ausgeschlossen
 - und nicht in der Ausfallrate berücksichtigt sind



PFD von Hersteller

λ_{DU} von Hersteller

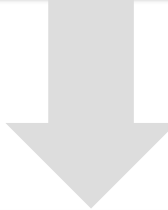
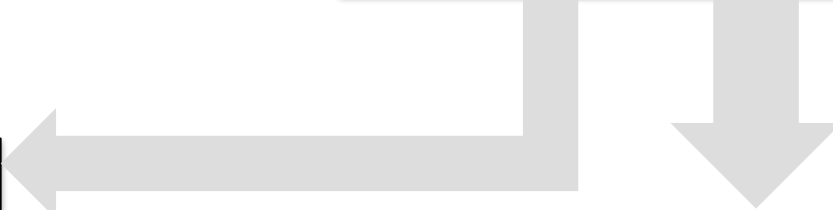
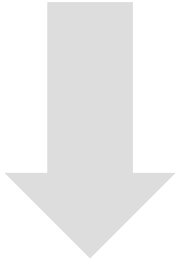
λ_{DU} von Hersteller

Die PFD Betrachtung der IEC 61508 (und abgeleiteter Normen & Richtlinien) gilt für den konstanten Bereich der Badewannekurve.

CEN-Normungsvorhaben

Anwender-Erfahrung und realer Bedarf

Anwenderdaten



IEC DTR 61511-4 2018:

„Ed. 2 ... needed to address the common misinterpretations of the Ed. 1 requirements that became evident ... over the intervening years.

For example, Ed. 2 reinforced the necessity to **design for functional safety management rather than a narrow focus on a calculation and to manage the actual performance of the SIS over time.** “

Systematische
Fehler vermeiden

Zufällige Ausfälle
beherrschen



IEC 61511-1

Edition 2.0 2016-02

**INTERNATIONAL
STANDARD**

**NORME
INTERNATIONALE**

Functional safety – Safety instrumented systems for the process industry sector –
Part 1: Framework, definitions, system, hardware and application programming requirements

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation –
Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

DIE MORAL VON DER GESCHICHT... WIE SIEHT DIE FUSI DER ZUKUNFT AUS?

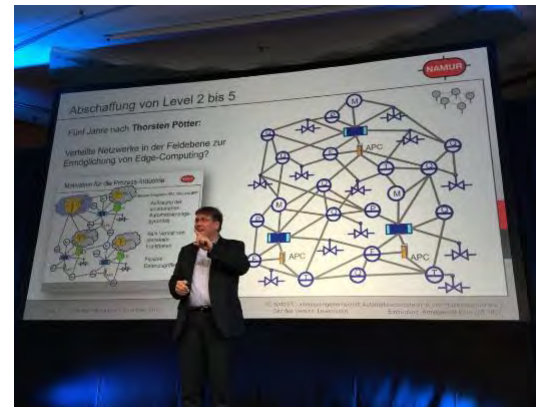
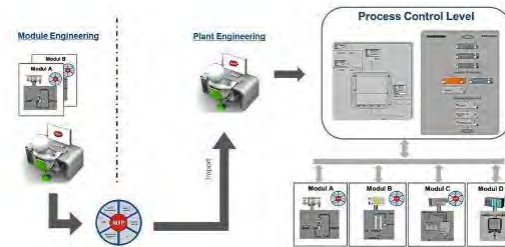
„Der Versuch, mangelhafte Systematik oder Gewissheit durch die Nutzung probabilistischer Methoden auszugleichen, kann nur scheitern. Sicherheit kann man nicht durch „blindes Rechnen“ erreichen, sondern nur mit ingenieurtechnischem Sachverstand. Was wie die Besinnung auf alte Tugenden klingt, ist auch im Ausblick auf die mögliche funktionale Sicherheit der Zukunft sinnvoll. Die funktionale Sicherheit steht vor einem Paradigmenwechsel, der in den nächsten Jahren vor allem software-unterstützte Methoden als Innovationselement in der Sicherheitstechnik in den Vordergrund rücken wird, beispielsweise auch aus dem Bereich der Künstlichen Intelligenz. Was die Zukunft der funktionalen Sicherheit auch bringt: Besser systematisch richtig als zufällig falsch.“

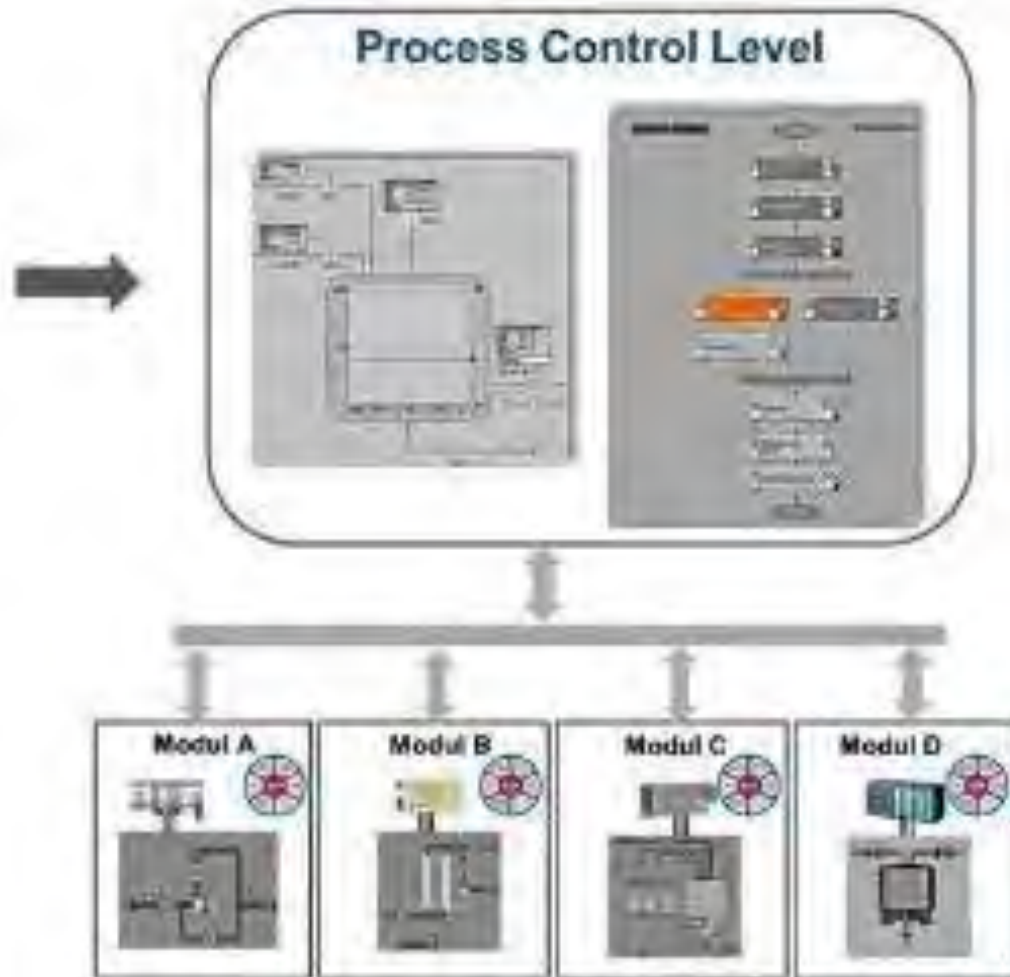
atp edition 2021 , Hauptbeitrag – Hablawetz/Matalla/Knödler/Schmitt-Pauksztat

#Systematisch Richtig statt Zufällig Falsch

- Steigende Vernetzung
- Umfassendere Daten
- Weniger (einfache) Hardware
- Mehr Software-Anteil
- Steigende Komplexität
- Beispiele:
 - APL4Safety
 - MTP-Safety
 - NOAmeets/needsSecurity (4Safety)

■ Eindrücke NAMUR Hauptsitzungen





- Die Flexibilisierung modularer Anlagen stellt die Vorgehensweisen zur Risikoreduktion mit PLT-Sicherheitseinrichtungen vor neue Herausforderungen.
- Um Flexibilitätseinbußen zu verringern, muss der gesamte Sicherheitslebenszyklus sowie die darin enthaltenen Tätigkeiten für die Anforderungen der modularen Automation angepasst werden.
- ***#Funktionale Sicherheit #Functional Safety Orchestration #modulare Anlagen #modulare Prozessautomation #modularerSIS-Sicherheitslebenszyklus #Safety-MTP***

<https://www.process-worldwide.com/ai-autonomously-runs-chemical-plant-for-35-days-a-1105250/?cmp=nl-317&uuid=916df1653133e864a95560eb0a0782fc>

Next-Gen Control Technology

AI Autonomously Runs Chemical Plant for 35 Days

24.03.2022 | Source: Press release

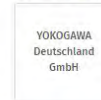
In a field test, a chemical plant in Japan ran autonomously for 35 days with the assistance of an artificial intelligence (AI) solution developed by Yokogawa and the Nara Institute of Science and Technology. The next-generation control technology is capable of taking into account numerous factors such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



(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 „gefühl-nicht-deterministisch“ (Dr. Henrik Putzer) bezeichnet werden kann: Nicht immer liefert eine Systemkomponente auf Basis von maschinellem Lernen die erwarteten Ergebnisse. Diese Fehlermöglichkeit kann mit einer Unsicherheit (uncertainty) beschrieben werden. In der Hardware wird dies durch die Ausfallrate oder das LAMBDA bezeichnet. Im Gegensatz zu dieser aleatorischen Unsicherheit in der Hardware (kann irgendwann zufällig z. B. durch Alterung ausfallen) muss dem Neuronalen Netz eine epistemische Unsicherheit zugeordnet werden (eine Fehlererkennung 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 ein neuer Kennwert, das LAMBDA-AI, vorgeschlagen (Dr. Henrik Putzer). Doch die Methoden zur Ermittlung des LAMBDA-AI sind noch in der Erforschung. Klar ist, dass der Entwicklungsprozess, die Metriken und ggfs. auch die Analyse des vom Neuronalen Netz gelernten Wissens eine Rolle spielen werden.

Probabilistik?



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

<https://www.dke.de/de/news/2019/vde-dke-kongress-funktionale-sicherheit-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“.

282

Sensorik

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.

248

Probabilistik

Quelle: Stördaten-
Auswertung
NAMUR.smart

Probabilistik?

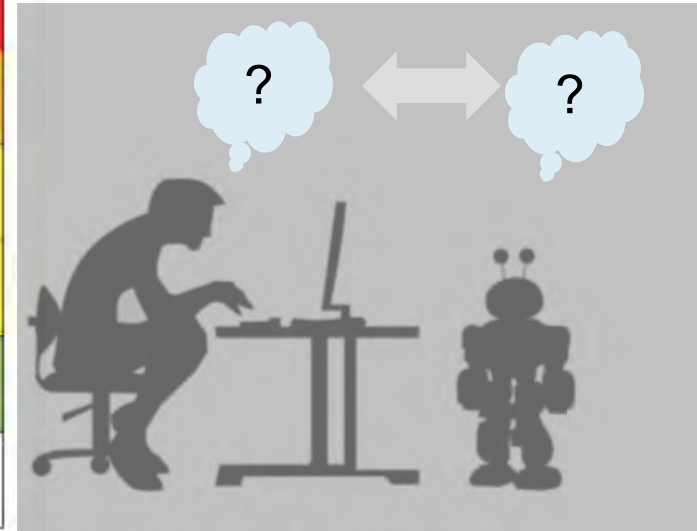
Zufällige Fehler
Systematische Fehler

AI 4 (FUNCTIONAL) SAFETY

Usage Level (property of application)

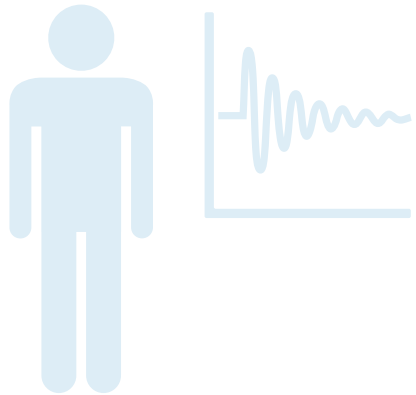
AI Technology Class =>	Class I (1)	Class II (1)	Class III (1)
Technique Usage Level	can be systematically reviewed, as the used methods are fully transparent and understood, and the AI can be unambiguously mapped to the final application.	can be partly reviewed, verified and validated, but the AI is not completely transparent or understood, and/or the AI cannot be unambiguously mapped to the final application.	cannot, or only to a small extent, 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 „a0“	not recommended for broader 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 „a0“	
Usage Level B1 used during development of a safety relevant E/E/PE system (offline support tool) and automated decision making possible.		See clause „e1“	See clause „a0“
Usage Level B2 used during development of a safety relevant E/E/PE system (offline support tool) and no automated decision making.		See clause „e1“	See clause „c0“
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 „g1“	See clause „a1“
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



current state of exchange and discussion based on the development of ISO/IEC DTR 5469 "Artificial intelligence - Functional safety and AI systems"

Verstanden?
gleichwertig?
Akzeptiert?



Code + Code > Code?

Systematisch richtige Abbildung der Realität



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



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

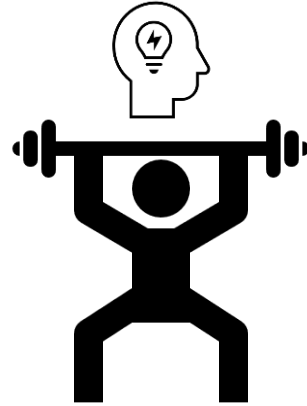
Systematisch richtiger Einfluss auf die Realität

IEC DTR 61511-4 2018:
 „Ed. 2 ... needed to address the common misinterpretations of the Ed. 1 requirements that became evident ... over the intervening years.

For example, Ed. 2 reinforced the necessity to

design for functional safety management rather than a narrow focus on a calculation

and to manage the actual performance of the SIS over time. “



FUNCTIONAL FIT-NESS

„functional FITness is about preparing you for life”

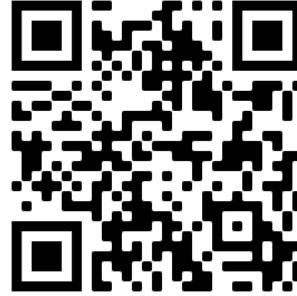


- Design für
- Systemat
- Klar formulie
- Verlässlich in
- einfach a
- v
- Sicherheits
- festgelegte
- beherrschen

Kompetenz



NAMUR@
LinkedIn



NAMUR
Homepage

DANKE FÜR DIE AUFMERKSAMKEIT!

Marco Knödler

Team Lead I&C (Yncoris) + Associate Lecturer Functional Safety (German universities of applied sciences)

- NAMUR WG 4.5 – VDI/VDE-GMA FA 6.13
- DIN NA 003-01-01 AA - CEN/TC 69/WG 1 -
- DKE STD_1941.0.8 - SCI 4.0 Expert Panel AI in Industrial Applications
FS Eng (TÜV Rheinland, # 5762/12, SIS - # 5716/12, Machinery)





Künstliche Intelligenz und Regulierung

“We are convinced that AI technologies can help in meeting the great societal challenges we face such as man-made global warming, social injustices, and dangerous diseases.

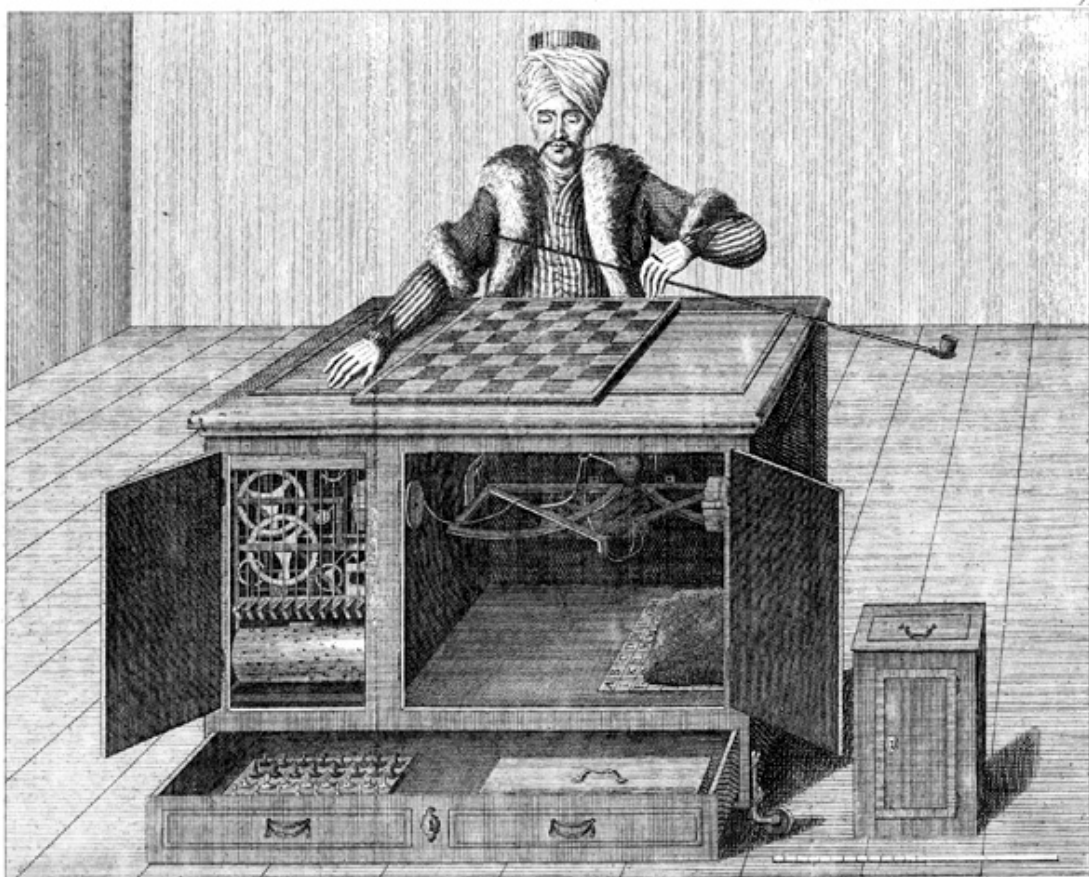
We dedicate ourselves with great energy to work on AI solutions to these tasks.”

(Zitat der Internetseite des DFKI)

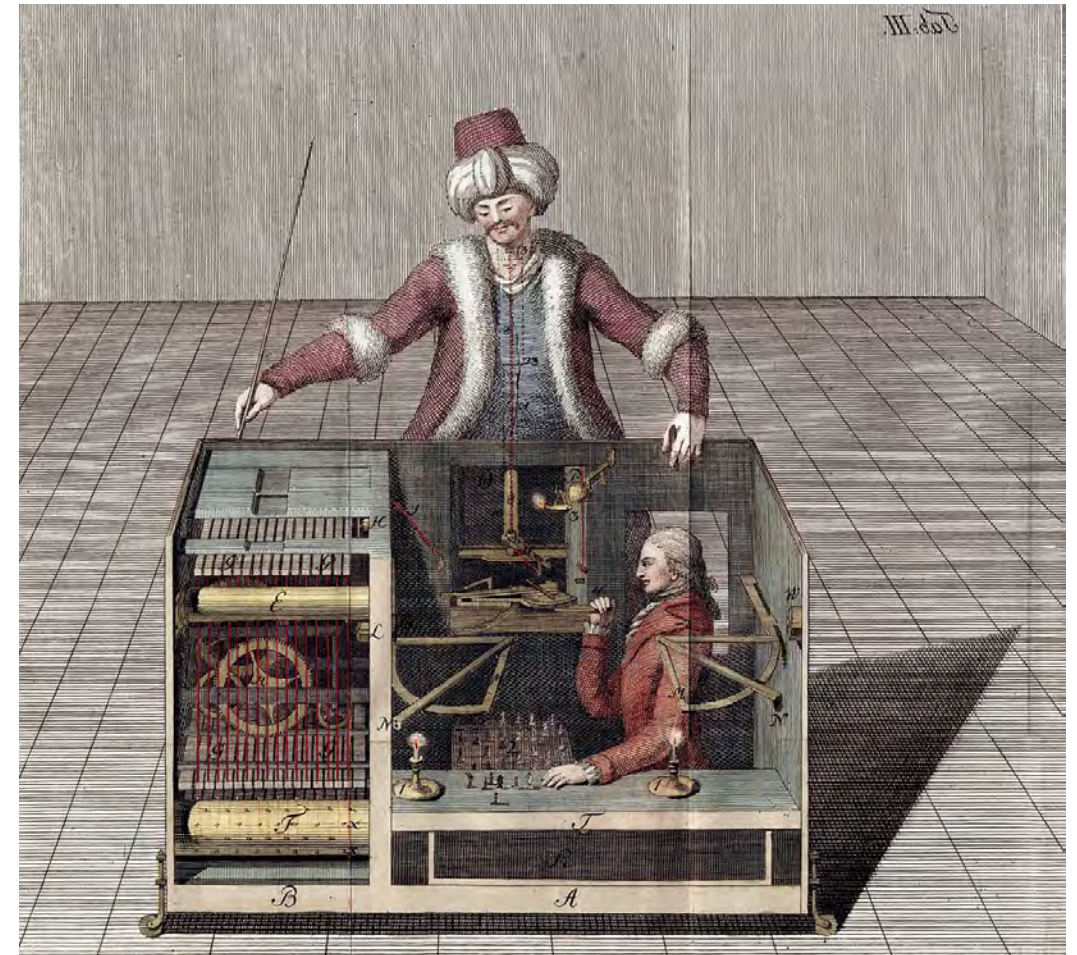


International
Electrotechnical
Commission

Der Schachtürke von 1770 (Implikation von Intelligenz)

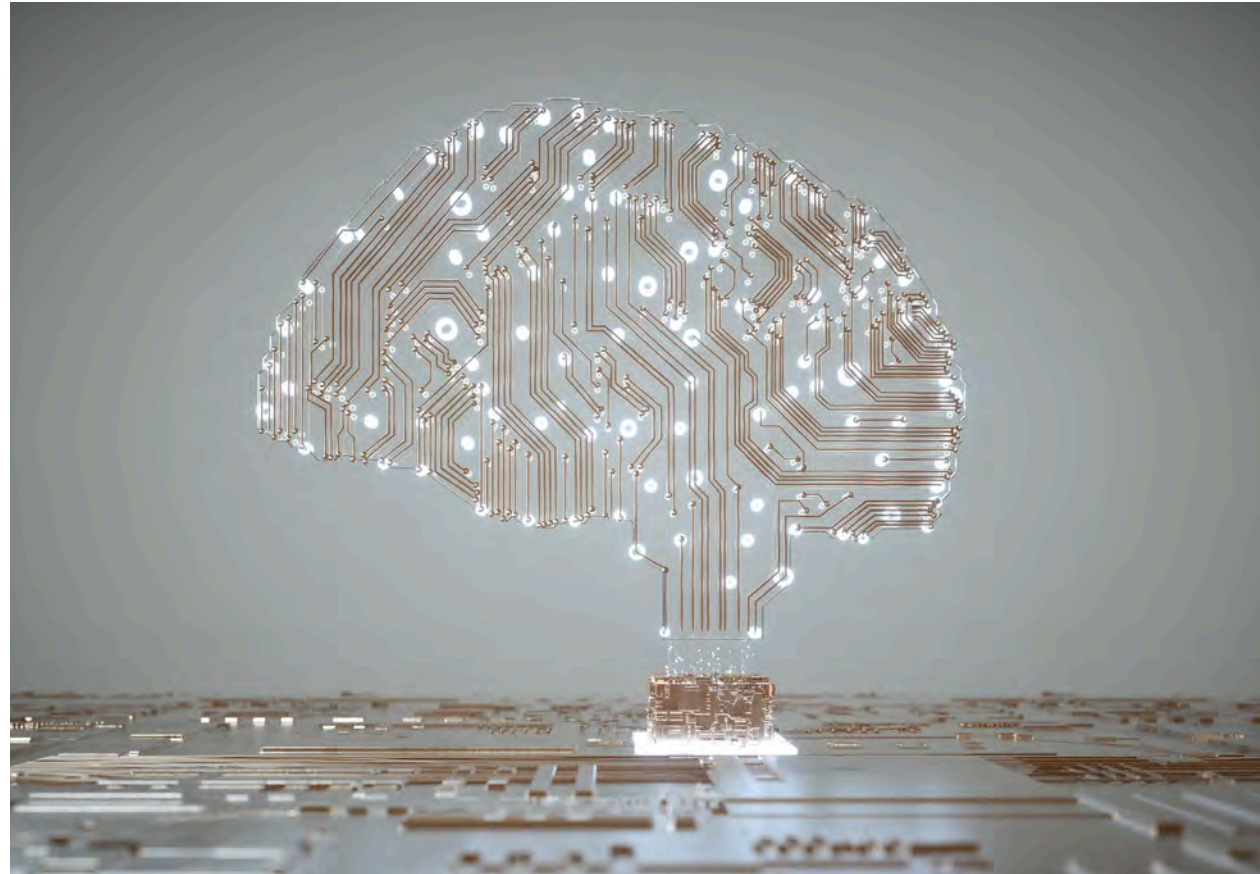


W. de Kempelen del. Ch. à Mechel exaud. Basilea. P. G. Patz, fecit.
Der Schach-Spieler, wie er vor dem Spiel gezeigt wird, von vorne. Le Joueur d'Échecs, tel qu'on le montre avant le jeu, par devant.

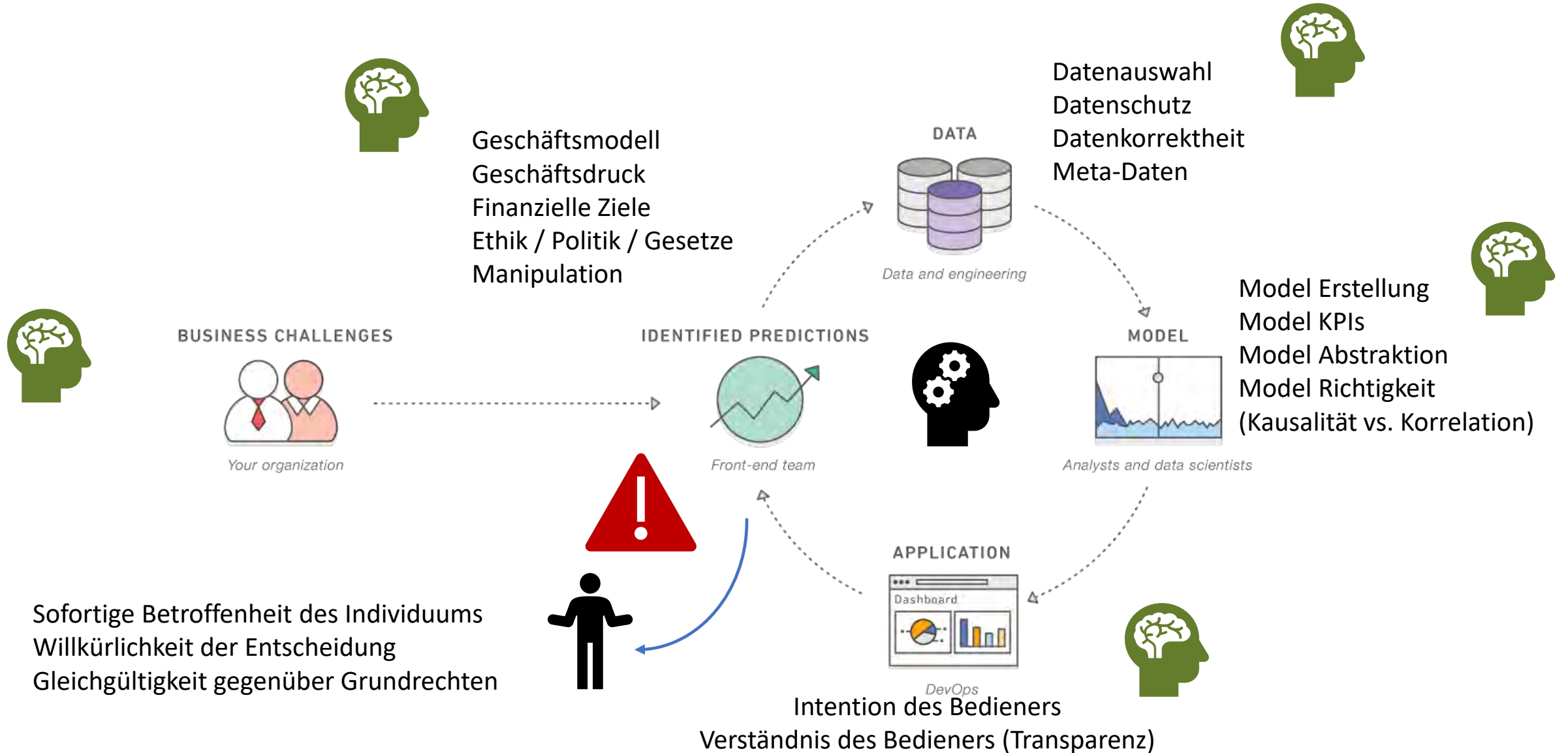


III. do C

KI Systeme und deren “Probleme” (Randbedingungen)



Generelles Konzept eines KI Systems



Gefahr von KI Systemen - Skalierbarkeit



Grundlagen von Ethik und Recht

(wurden im Detail letztes Jahr besprochen)



Der Schutz der Rechte des Einzelnen und die Zustimmung ist der Schlüssel zu einer freien Gesellschaft!



- Das Prinzip des Nutzens: **“The greatest happiness of the greatest number is the foundatioun of morals and legislation.”** Mit Freude (Happiness) verstand er die Summe des Wohlergehens und die Abwesenheit von Schmerz und Leid.
- Scharfe Kritik wurde von Bentham’s Student John Stuart Mill formuliert, da beim **Utilitarismus** die Motivation des menschlichen Gewissens unberücksichtigt bleibt.
 - a. **Berücksichtigt nicht die individuellen Rechte**
 - b. **Es ist nicht möglich alle Vorlieben und Werte zu erfassen.**



John Locke erweiterte die Idee des Sozialvertrags von Thomas Hobbes’s und entwickelte das **Konzept der natürlichen Rechte, das Recht auf Privatbesitz und das Prinzip der Zustimmung der Regierten**. Seine Ideen formen die ideologische Basis heutiger “freier demokratischer” Gesellschaften.



Zur Erinnerung Auszüge der Menschenrechte...

Article 1: **All human beings** are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

Article 6: **Everyone** has the right to recognition everywhere as a person before the law.

Article 9: **No one** shall be subjected to arbitrary arrest, detention or exile.

Article 10: **Everyone** is entitled in full equality to a fair and public hearing by an independent and impartial tribunal...

Article 11-1: **Everyone** charged ... has the right to be presumed innocent until proved guilty...

Article 13-2: **Everyone** has the right to leave any country, including his own, and to return to his country.

Article 21-2: **Everyone** has the right of equal access to public service in his country.

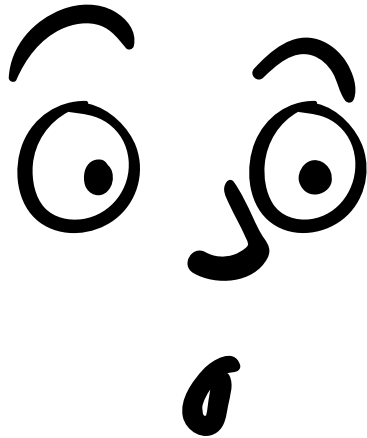
Article 26-3: Parents have a prior right to choose the kind of education that shall be given to their children.

Article 27-1: **Everyone** has the right freely to participate in the cultural life of the community, ...and its benefits.

Universal Declaration of Human Rights

<https://www.un.org/en/about-us/universal-declaration-of-human-rights>

Nun zur geplanten Regulierung...



Brussels, 21.4.2021
COM(2021) 206 final
2021/0106 (COD)

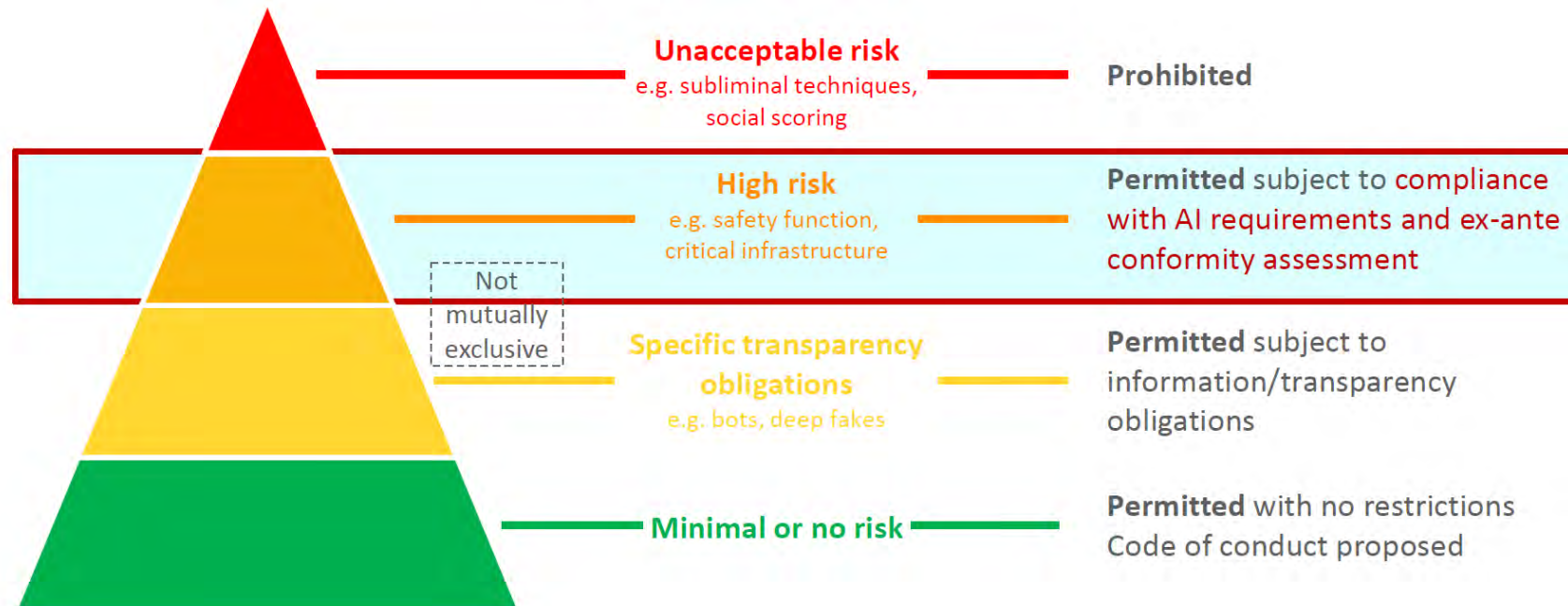
Proposal for a

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?

Risk-based approach of AI regulation



“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?

1) Biometric identification and categorisation of natural persons

(a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;



2) Management and operation of critical infrastructure

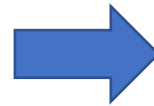
(a) AI systems intended to be used as **safety components in the management and operation** of road traffic and the supply of water, gas, heating and electricity.



3) Education and vocational training

(a) AI systems intended to be used for the purpose of determining access or **assigning natural persons** to educational and vocational training institutions;

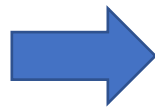
(b) AI systems intended to be used for the purpose of **assessing students** in educational and vocational training institutions and for **assessing participants** in tests commonly required for admission to educational institutions.



4) Employment, workers management and access to self-employment

(a) AI systems intended to be **used for recruitment or selection of natural persons**, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;

(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for **task allocation and for monitoring and evaluating performance and behavior of persons** in such relationships.



5) Access to and enjoyment of essential private services and public services and benefits

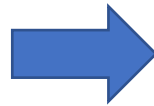
- (a) AI systems intended to be used by public authorities or on behalf of public authorities **to evaluate the eligibility of natural persons** for public assistance benefits and services, as well as to **grant, reduce, revoke, or reclaim such benefits and services;**
- (b) AI systems intended to be used **to evaluate the creditworthiness of natural persons or establish their credit score,** with the exception of AI systems put into service by small scale providers for their own use;
- (c) AI systems intended to be used **to dispatch, or to establish priority** in the dispatching of **emergency first response services, including by firefighters and medical aid.**



6) Law enforcement

a) AI systems intended to be used by **law enforcement authorities** for making individual risk assessments of natural persons in order **to assess the risk of a natural person** for offending or reoffending or the risk for potential victims of criminal offences;

(b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or **to detect the emotional state of a natural person**;



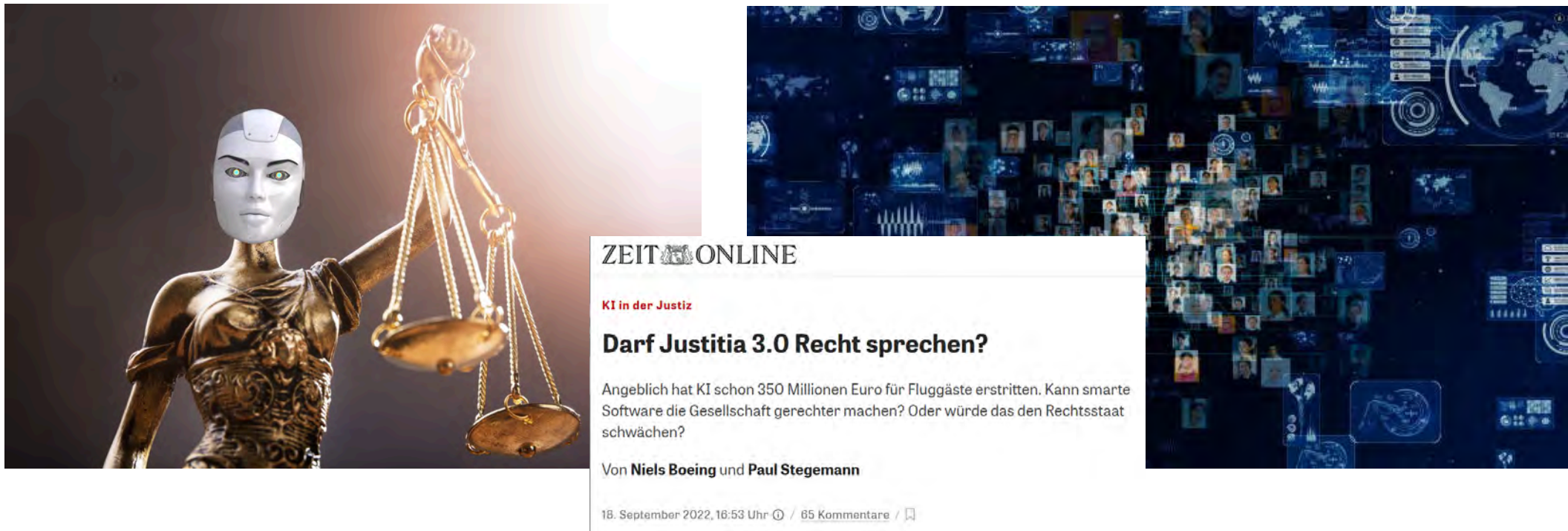
7) Migration, asylum and border control management

- (a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or **to detect the emotional state** of a natural person;
- (b) AI systems intended to be used by competent public authorities to assess a risk, including a **security risk, a risk of irregular immigration, or a health risk, posed by a natural person** who intends to enter or has entered into the territory of a Member State;
- (c) AI systems intended to be used by competent public authorities for the **verification of the authenticity of travel documents** and supporting documentation of natural persons and **detect non-authentic documents** by checking their security features;
- (d) AI systems intended to assist competent public authorities for the **examination of applications for asylum, visa and residence permits** and associated complaints with regard to the **eligibility of the natural persons** applying for a status.



8) Administration of justice and democratic processes

(a) AI systems intended to assist a judicial authority in **researching and interpreting facts** and the law and in **applying the law** to a concrete set of facts.




ZEIT ONLINE

KI in der Justiz

Darf Justitia 3.0 Recht sprechen?

Angeblich hat KI schon 350 Millionen Euro für Fluggäste erstritten. Kann smarte Software die Gesellschaft gerechter machen? Oder würde das den Rechtsstaat schwächen?

Von **Niels Boeing** und **Paul Stegemann**

18. September 2022, 16:53 Uhr / 65 Kommentare / 

Konflikte und ungleiche Macht

Begrenzte Transparenz der Algorithmen

Begrenztes Wissen

Wenig Kontrolle über Daten

Sofortige Betroffenheit

Wenig Wahlfreiheit

Limitierte Rechtsmittel



Untransparent / Patente

Business Case

Expertenwissen

Kontrolle über Daten
und Algorithmen

Politische Unterstützung

Globale Aufstellung

CAUTION

Hat diese
Automatisierung mit
Softwarealgorithmen
ein hohes
Missbrauchspotential?



The Pepperl+Fuchs Corporate Group

Gebrauchsdauer

Useful Lifetime?

Useful Life?

Mission Time?

Was jetzt?

Und wieso?



Your automation, our passion.

 **PEPPERL+FUCHS**

Agenda

- Woher kommt's?
- Fundstellen Normung
- Fundstellen in anderer Form
- Fazit

Über mich

Dipl. Ing. Michael Kindermann

- Dipl. Ing. Elektrotechnik (Automatisierung)
@ Universität Kaiserslautern
- 10 Jahre EW-Ingenieur @ Pepperl + Fuchs
- **Betreuung funktional sicherer Geräte seit 2001** (EN 954-1 EN 61508)
- 3 Jahre Zertifizierung Explosionsschutz @ UL International
- Certified **FS**-Engineer in HW/SW design
- Seit 2011 **Head of Functional Safety Management @ Pepperl+Fuchs**
 - Überwachung der Arbeit der Normenexperten für funktionale Sicherheit
 - Verantwortlich für Prozesse mit Bezug zu funktionaler Sicherheit
 - **Functional Safety Manager** für Geräteentwicklung
 - **Gremienarbeit** GK 914 (**FS** – IEC 61508), AK 225.1 (Maschinen und **FS**), K132.0.1 (FMEA), K241 (Ex und **FS**)
 - **Moderation GAK 914.0.3** (**FS** Software), **AK 914.0.9** (Statistische Evaluierung von **FS** Software) und **AK 914.0.11** (AI und **FS**)



Quelle: P+F

Woher kommt's?

Mission Time – **Gebrauchsdauer** in ISO 13849-1

3.1.28

Gebrauchsdauer

T_M

Zeitraum, der die vorgegebene Verwendung der SRP/CS abdeckt

In Kap. 4.5.4 erklärt - nicht auf kritische Ausfälle begrenzt

Für vorgesehene Architekturen werden folgende typische Annahmen getroffen:

- **Gebrauchsdauer**, 20 Jahre (siehe Abschnitt 10);
- konstante Ausfallraten innerhalb der **Gebrauchsdauer**;

10 Technische Dokumentation

Bei der Gestaltung eines SRP/CS muss deren Konstrukteur mindestens folgende Informationen über das sicherheitsbezogene Teil dokumentieren:

- die auf die Zuverlässigkeit bezogenen Parameter ($MTTF_d$, DC, CCF und **Einsatzdauer**);

Woher kommt's?

Mission Time – Gebrauchsdauer in ISO 13849-1

Die Verfahren der Zuverlässigkeit in diesem Teil der ISO 13849 setzen voraus, dass die Ausfälle von Bauteilen exponentiell über der Zeit verteilt sind: $F(t) = 1 - \exp(-\lambda dt)$. Bei pneumatischen und elektro-mechanischen Bauteilen ist eine Weibull-Verteilung wahrscheinlicher. Wenn aber die Betriebszeit der Bauteile auf die mittlere Zeit bis 10 % der Bauteile gefährlich ausfallen (T_{10d}) begrenzt wird, kann eine konstante gefahrbringende Ausfallrate (λ_d) während dieser Gebrauchsdauer wie folgt abgeschätzt werden:

$$\lambda_d \approx \frac{0,1}{T_{10d}} = \frac{0,1 \times n_{op}}{B_{10d}} \quad (C.5)$$

Quelle: DIN EN ISO 13849-1 Kap. 3 und Anhang C

weibull distribution is more likely. But if the operation time until 10 % of the components fail dangerously over this operation time can be estimated as

$$0,1 \quad 0,1 \times n_{op}$$

Also: Ende der Badewanne – bezogen nur auf kritische Ausfälle?

Woher kommt's?

Mission Time – **Gebrauchsdauer** in ISO 13849-1

3.1.28

Gebrauchsdauer

T_M

Zeitraum, der die vorgegebene Verwendung der SRP/CS abdeckt



Problem mit dem Begriff:

- Bezug hier auf **Maschinenbau**
- Begriff auch bei den **Automobilisten**
- Begriff auch in der **Avionik**

Kleine Anmerkung: in der IEC 62061 heißt es “useful lifetime”.
Meistens mit “lifetime” zusammengesrieben.



Quelle: Pixabay

Woher kommt's

Gebrauchsdauer in der IEC 61508

Bei den Begriffen in Teil 4 nur hier:

3.6.16

Ausfallrate (en: failure rate)

Zuverlässigkeitsparameter ($\lambda(t)$) einer Einheit (einzelne Bauteile oder Systeme) derart, dass $\lambda(t) \cdot dt$ die Ausfallwahrscheinlichkeit dieser Einheit innerhalb $[t, t+dt]$ ist, vorausgesetzt, dass sie während $[0, t]$ nicht ausgefallen ist

ANMERKUNG 1 Mathematisch ist $\lambda(t)$ die bedingte Ausfallwahrscheinlichkeit pro Zeiteinheit über $[t, t+dt]$. Sie steht in starker Beziehung mit der Zuverlässigkeitsfunktion (d. h. Wahrscheinlichkeit keines Ausfalls von 0 bis t) durch die allgemeine Formel:

$$R(t) = \exp\left(-\int_0^t \lambda(\tau) d\tau\right). \text{ Umgekehrt wird sie durch die Zuverlässigkeitsfunktion definiert mit: } \lambda(t) = -\frac{dR(t)}{dt} \frac{1}{R(t)}.$$

ANMERKUNG 2 Ausfallraten und ihre Unsicherheiten können aus Rückläufern aus dem Feld unter Anwendung herkömmlicher Statistiken abgeschätzt werden. Während der „Gebrauchsdauer“ (d.h. nach den Früh- und vor den Spätausfällen) ist die Ausfallrate eines einfachen Objekts mehr oder weniger konstant: $\lambda(t) \equiv \lambda$.

Quelle: DIN EN IEC 61508-4

Achtung: hier nicht auf kritische Ausfälle begrenzt

Dann ist doch alles klar...

Auf Englisch in IEC 61508-4: useful life per Fußnote

NOTE 2 Failure rates and their uncertainties can be estimated from field feedback by using conventional statistics. During the "useful life" (i.e. after burn-in and before wear-out), the failure rate of a simple item is more or less constant, $\lambda(t) \equiv \lambda$.

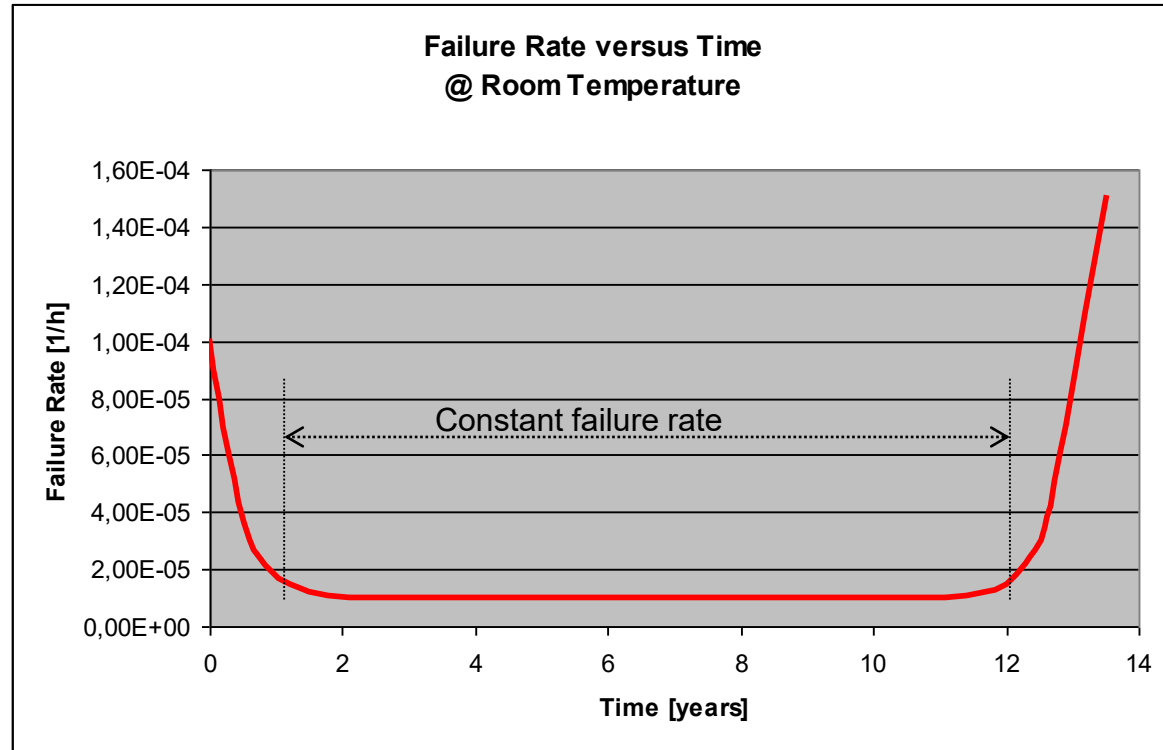
In IEC 61508-2: useful lifetime praktisch als Definition

NOTE 3 Although a constant failure rate is assumed by most probabilistic estimation methods this only applies provided that the useful lifetime of elements is not exceeded. Beyond their useful lifetime (i.e. as the probability of failure significantly increases with time) the results of most probabilistic calculation methods are therefore meaningless. Thus any probabilistic estimation should include a specification of the elements' useful lifetimes. The useful lifetime is highly dependent on the element itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive). Experience has shown that the useful lifetime often lies within a range of 8 to 12 years. It can, however, be significantly less if elements are operated near to their specification limits.

Quelle: IEC 61508-2 Kap. 7.4.9.5

Fundstellen Normung: Dann ist doch alles klar...

Egal wie: Ende der Badewanne. In beiden Fällen.



Quelle: P+F

Achtung Umkehrschluss:
Ende muss mit
systematischer Eignung
zusammenhängen

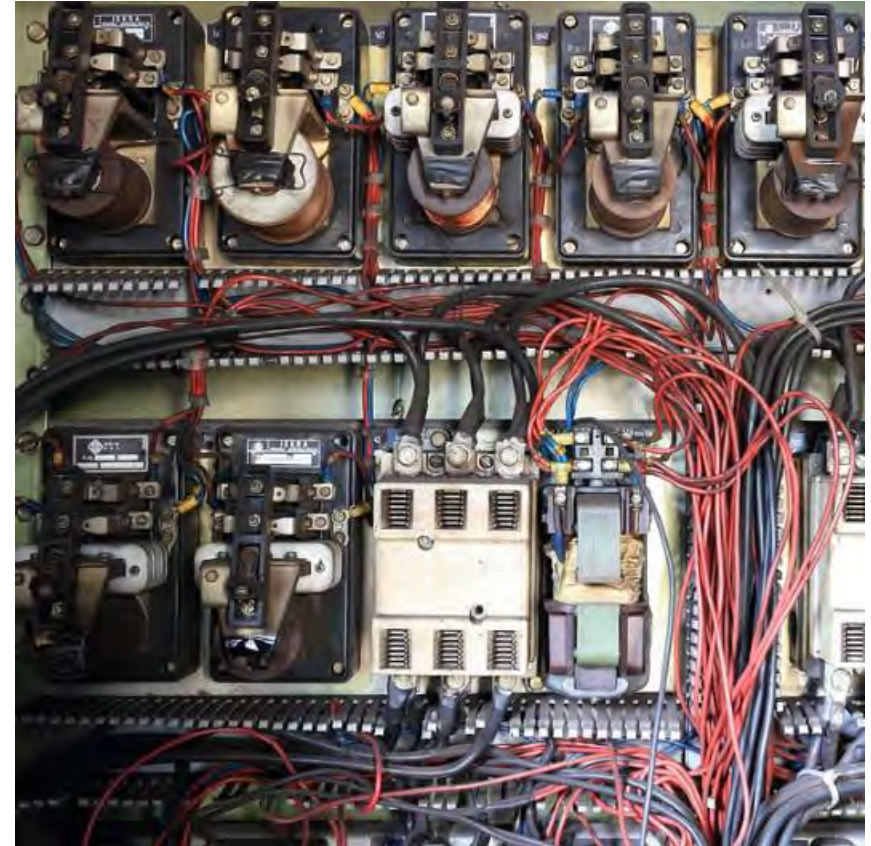
Bestätigt in:
EN 61709:2019+AC:2019
Anhang E: useful life
(DE: Brauchbarkeitszeit)

Fundstellen Begleitliteratur: IFA Report 2/2017

Anhang G

- Erläuterungen zur Verlängerung der Gebrauchsdauer über 20 Jahre hinaus eingefügt

Pro fünf Jahre längere Gebrauchsdauer als 20 Jahre wird bei den Kategorien 2, 3 und 4 ein prozentualer PFH_D -Zuschlag von 15% eingerechnet (Kategorie B oder 1 erfordern keine PFH_D -Anpassung). Das vereinfachte Verfahren und SISTEMA sind also trotzdem nutzbar. Voraussetzung sind konstante Ausfallraten unabhängig von der Gebrauchsdauer. Für Verschleißbauteile bedeutet dies, dass diese für die spezifizierte höhere Gebrauchsdauer T_M ausgelegt werden müssen ($T_{10D} \geq T_M$) oder nach Ablauf von T_{10D} jeweils vorsorglich ausgetauscht werden müssen.



Quelle: Pixabay

Doch Probabilistik???

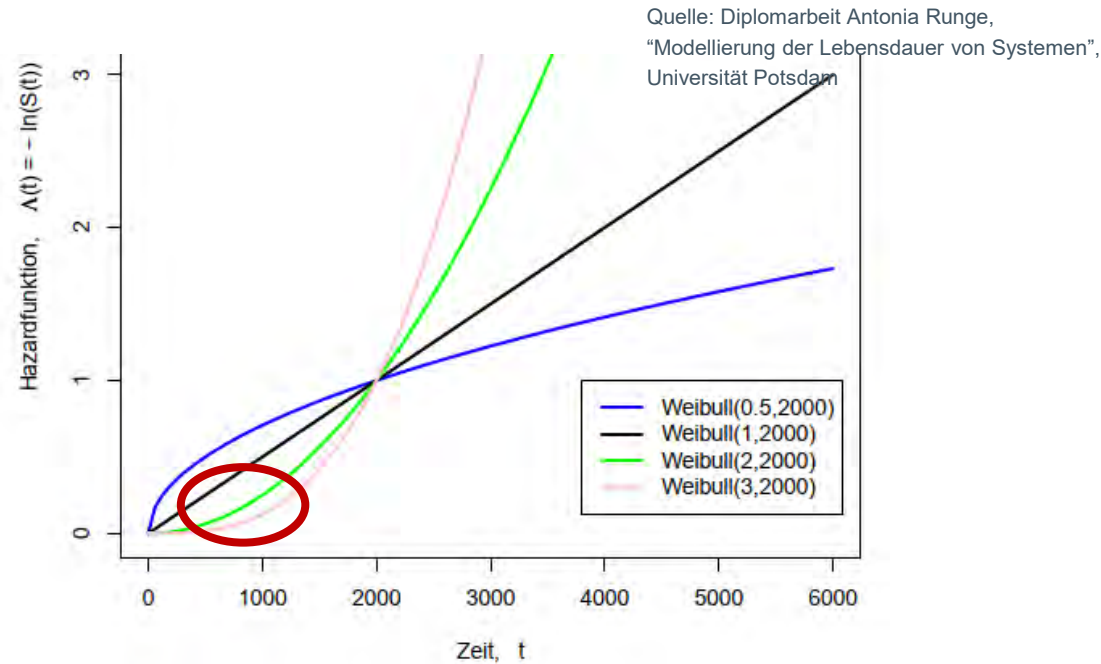
Beruhigend: Verschleißbauteile – Ende der Badewanne – thematisiert.

Fundstellen Begleitliteratur: IFA Report 2/2017

Auflösung:

Zusammenhang ist empirisch aus Erfahrungswerten ermittelt

Interpretation: doch etwas Weibull-Anteil?



Vielleicht deshalb der Vorschlag, in der IEC 61508 auch **nicht konstante Fehlermodelle** zu erwähnen / einzuführen?

Fundstellen: praktische Anwendung zu Hause

20 Jahre? 30 Jahre???

Außerhalb Safety macht niemand solche Aussagen...



Quelle: Pixabay

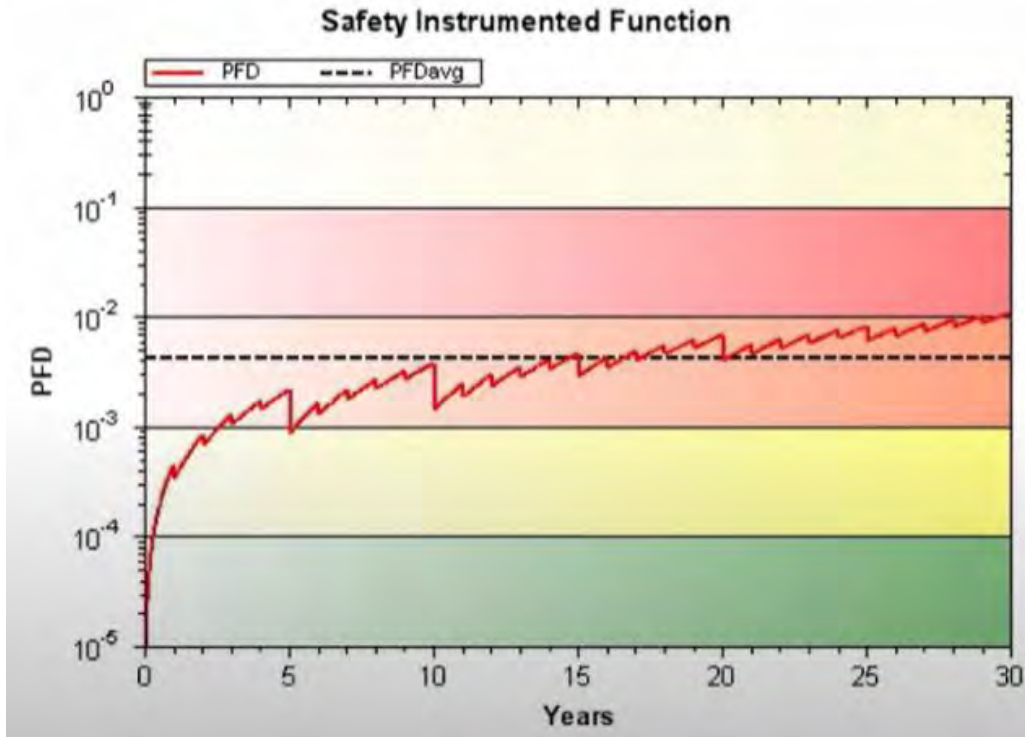
Fundstellen: Vortrag der ISA

- Mission time is the operational period of the SIF, after which failures undetectable by proof test return to zero, and the SIF is in an “as new” condition.
- Comparison
 - Mission Time is about undetected random failures. Useful Life is about wear-out failures
 - Mission time is a chosen design parameter. Useful life is a property of a device.
 - Mission time affects PFD_{avg} calculations. Useful Life is a pre-requisite for calculations

Quelle: “Useful Life of Safety Instrumented Systems”
by Stephen Thomas, NVIDIA, for ISA, 2019

- **Bezug zu Proof Test ist neu in Bezug auf Mission Time (ISO 13849 beschreibt High-Demand Anwendungen).**
- **“Design Parameter” ist tatsächlich in ISO 13849 zu finden.**
- **Weiterer Gedanke: Link zu PFD_{avg} und damit einer SIL-Stufe!**

Fundstellen: Video Tutorial von exida



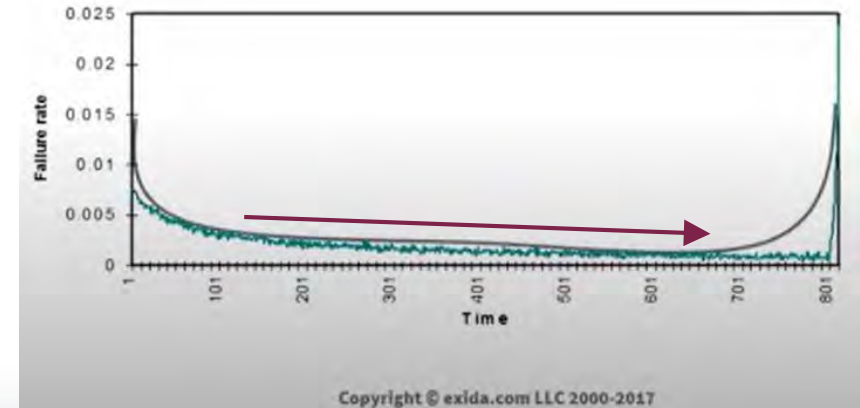
Quelle: exida



It's Time!! Useful Life, MTTF, and Mission Time
<https://www.youtube.com/watch?v=CVTwXEuQgQc&t=1017s>

Bei nicht perfektem Proof Test könnte eine “Mission Time” auch bedeuten dass ausgetauscht werden muss wenn die PFDavg bei Weiterbenutzung nicht im nötigen Rahmen bleibt.

Weitere Grafik spricht aber gegen Weibull...



Copyright © exida.com LLC 2000-2017

Mission Time und Useful Lifetime nebeneinander?

Es gibt einen Normen-Arbeitskreis der überlegt, beide Begriffe zu verwenden -

- ⇔ **mit** Bezug auf Gefahr (Mission Time)
⇔ **ohne** Bezug auf Gefahr (Useful Lifetime)

Überlegung: was passiert wenn nicht gefahrbringende Fehler für einen Ausfall sorgen?

Beispiel:

- **Elektrolyt - Stützkondensator** verliert Kapazität
- Spannungsregler außerhalb seiner Spezifikation
- Schaltung läuft weiter – **Ausfälle nur sicher**



Quelle: Pixabay

Resultat: klar geht es in die sichere Richtung. **Austausch trotzdem naheliegend.**

Fazit

- **Es ist allgemein sinnvoll, eine **Gebrauchsdauer** zu planen.**

*ANMERKUNG 3 NA4) Obwohl für die meisten probabilistischen Abschätzungsmethoden eine konstante Ausfallrate angenommen wird, trifft diese nur unter der Voraussetzung zu, dass die Gebrauchsdauer von Elementen nicht überschritten wird. Nach Ablauf ihrer Gebrauchsdauer (d. h. wenn die Ausfallwahrscheinlichkeit mit der Zeit bedeutend ansteigt) sind die **Ergebnisse der meisten probabilistischen Berechnungsmethoden daher wenig aussagekräftig.***

Quelle: DIN EN IEC 61508-2 Kap. 7.4.9.5

*(in der Englischen Version „**meaningless**“ - klingt irgendwie überzeugender)*

- **Bekannt: in der deutschen Ausgabe der IEC 61508-2:2010 auch über **Stördatenerfassung** festzulegen**
- **Meine Meinung: nur als **allgemeine Gebrauchsdauer** – nicht nur bei Gefahr**
- **Ausblick: IEC 61511 legt auch Wert auf Bewährung in Anwendung, Thema **“Mission Profiles”** auch in der Normung zu Zuverlässigkeitstechniken (DKE K132). Prüfung für Applikation nach In-Haus-Standards**

Fazit



Quelle: funny-jokes.com

Pepperl+Fuchs at a Glance



One Company | Unlimited Solutions

6,600
EMPLOYEES



around the world
to assist with all
your needs

6



MANUFACTURING
LOCATIONS

Unlimited
POSSIBLE SOLUTIONS



offered by our experts around the world

80
LOCAL OFFICES



on six continents

50,000
PRODUCTS



available to solve
all your application
needs

3
HEADQUARTERS



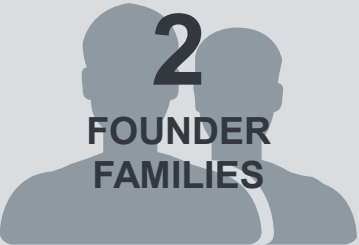
in Europe,
the USA, and Asia

790
MILLION €



Revenue

2
FOUNDER
FAMILIES



privately own 100 %
of the company

1
COMPANY



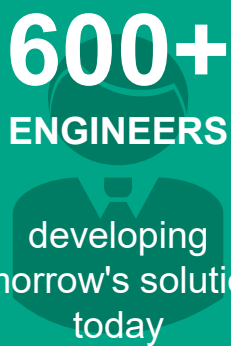
that solves every
challenge

77
YEARS



since the company
was founded in
Mannheim, Germany

600+
ENGINEERS



developing
tomorrow's solutions
today

Pepperl+Fuchs SE

Lilienthalstraße 200
68307 Mannheim
Germany

www.pepperl-fuchs.com

Tel: +49 621 776-0

mkindermann@de.pepperl-fuchs.com



Your automation, our passion.

 **PEPPERL+FUCHS**

SIL-Sprechstunde 2022

Tag 2: Fragen und Antworten

13. SIL-Sprechstunde 2022

1. Warum benötigt man die Angabe der Gebrauchsdauer und was passiert nach 10-12 Jahren?

Siehe 5.

2. Wie sind Sicherheitsfunktionen im Fall von „Energized to Safe & State dependent Safety“ zu behandeln?

Besondere Vorsichtsmaßnahmen wegen der möglichen Ausfallrichtung erforderlich. Beispiel redundante Verdrahtung, redundante oder ausfallsichere Versorgung über Batterien, besondere Absicherung des Prozesses zum Wechseln des „Safe State“.

3. Was ist beim Austausch von „SIL-Geräten“ zu beachten?

Siehe 5.

4. Wie geht man beim SIL-Nachweis mit Mechanik um?

Hier entstehen Regelwerke. Übliches Vorgehen ist aber eventuell deterministisch, z.B. berücksichtigt bei EN 50156 über Redundanz - oder per Überdimensionierung und Fehlerausschluss. Wenn die Auslegung gut genug ist wird nicht von probabilistischem Ausfallverhalten ausgegangen. Mechanik-Norm z.B. bei Drehgebern: manchmal 20-fache Sicherheit (keine Diskussion mit dem Assessor) oder 4-fache Überdimensionierung (Nachweis mit Tests). Bei geringerer Sicherheit höhere Ansprüche an Tests, wird aber auch hin und wieder genutzt. Wird aber rein als systematischer Ausfall berücksichtigt.

5. IEC 61508, Nationale Fußnote N3, Maßnahmen des Herstellers zur Nutzung von PLT-SE über das Gebrauchsdauerende hinaus:

- Kann eine Hersteller die Aussagen über die in der Norm unter N3 -->1) aufgeführten Punkte machen?

- Wie sieht ein gerätespezifisches Instandhaltungsmanagement bei Sensoren aus? - Sind alle drei Punkte unter N3 --> 1) nicht Totschlagargumente um sich grade nicht mit dem Thema zu befassen?

Deutsche nationale Fußnote in der IEC 61508 die besagt: längere Gebrauchsdauern sind durch Maßnahmen des Herstellers und Anwenders zu erreichen. In der Frage ging es um die Maßnahmen des Herstellers - mögliche Maßnahmen können sein: Entsprechendes Herstellerdesign, z.B. Vermeidung alterungskritischer Bauteile, und/oder aktives Fehlerverhalten (Fehler sollten erkennbar sein, oder das Gerät sollte sicherheitsgerichtet ausfallen), und/oder Überdimensionierung, und/oder Gerätespezifische Instandhaltungsempfehlungen.

Hersteller von SSPSen: Der Hersteller wird sich an die genannten Punkte halten (alterungskritischer Bauteile), er wird Diagnose verwenden um Fehler zu erkennen, er wird 20 Jahre Mission Time angeben, fertig.

Fragesteller: Es gibt Hersteller die nur 8-12 Jahre angeben, mit der Begründung dass sie nicht wissen können wie die Geräte vor Ort installiert sind (Umgebungsbedingungen, z.B. klimatisiert oder im Feld bei 60-70°C oder bei schwankenden Temperaturen betrieben)

Dass eine Elektronik die klimatisiert betrieben wird länger hält als 8-12 Jahre wird akzeptiert, aber kann man auch im Feld betriebene Geräte (z.B Sensoren oder Stellglieder) länger als 8-12 Jahre sicherheitsgerichtet betreiben?

Assessor: Wenn der Hersteller keine kritischen Bauteile verwendet, Diagnosen verwendet und Tipps für Instandhaltungsmaßnahmen gibt, kann der Hersteller dennoch äußerst schwierig Angaben zum weiteren Betrieb machen. Z.B. 15, 20, 30 Jahre.

Hersteller: SFF sagt aus, wie gut das Gerät entwickelt wurde und wie wahrscheinlich werden auch unentdeckte systematische Fehler erkannt. Wieviel Diagnose ist enthalten, wie fällt das Gerät aus. Auch die absolute Ausfallrate gibt Aufschluss darüber.

Anderer Anwender: Die meisten Hersteller schreiben 8-12 Jahre in die Safety Manuals, ggf. wird in manchen Fällen die Ausfallrate für längere Laufzeiten (Gebrauchsdauern) erhöht.

Hersteller: Bei Sensoren sind Temperaturzyklen im Betrieb üblich, Aussage schwierig - Temperatur ist erfahrungsgemäß ein entscheidender Faktor. Weniger für Standardbauteile aber integrierte Schaltkreise. SSPS wird fast immer klimatisiert betrieben – gefahrbringende Ausfallrate entscheidend.

Weiterer Anwender: Die SFF ist kein guter Orientierungspunkt.

Weiterer Anwender: gut wenn die Hersteller genannte Maßnahmen anwenden. 8-12 Jahre sind ok da Anwender verlängernde Maßnahmen anwenden kann wie in der Norm beschrieben. Absolute Länge aber nicht ersichtlich.

Assessor: bekanntes Problem, aber es traut sich niemand, etwas anderes anzugeben da Wirksamkeit der Maßnahmen schwer einschätzbar. Angabe von Lebensdauer von 50 Jahren wäre unseriös - wer übernimmt diese Verantwortung? Die Norm sagt 8-12 Jahre - wer traut sich etwas stark Abweichendes anzugeben? Idee: Aufnahme im IFA-Bericht, konkreter Vorschlag für z.B. 15% höhere Angaben.

Normung: wer weiß worauf die Aussage in der Norm beruht? Relevant sind nur Angaben der Hersteller und die Einschätzung der eigenen Anwendung. Daraus wird das eigene „Handeln“ abgeleitet.

Assessor: Wenn ein Hersteller 12 Jahre angibt wird der Mitbewerber 13 Jahre angeben, der nächste 14 Jahre. Genau festlegen kann es niemand.

Anwender aus der Großchemie: Uns reichen 8-12 Jahre aus. Auch wenn keine Angaben gegeben sind, ziehen wir unsere eigenen Schlüsse.

Hersteller: könnte es vielleicht auch Gründe geben die Zeiten zu verkürzen? Wie sieht es mit der derzeitigen Chipentwicklung bezüglich Miniaturisierung und immer höheren Packungsdichten in IC's aus? Haben neue und sehr kleine Bauformen mit immer geringeren Abständen im IC nicht höhere Ausfallraten?

Die oft als Grundlage verwendete SN29500 gibt einen Anhaltspunkt, berücksichtigt aber nicht die aktuellen Miniaturisierungen.

Man bedenke neue Regularien wie den Cyber Resilience Act. Wenn alles secure sein muss, steht dann nicht öfter eine Revision an? Daher ist vielleicht auch der Stand der Technik nicht spezifiziert oder gar im Wandel. Dementsprechend kann man aus verlängernden Maßnahmen im Feld alleine nicht unbedingt auf längere Gebrauchsdauern schließen.

Assessor: Ja, die Miniaturisierung sollte auch berücksichtigt werden, und diese kann bestimmt auch zur Verringerung der Gebrauchsdauer beitragen.

Weiterer Referent: mit Miniaturisierung, smarten Anwendungen und Security sollte man sich immer fragen, ob Geräte mit diesen Eigenschaften richtig für die SIF sind. Man sollte hier das Marketing von dem realen Bedarf unterscheiden. Bei bisherigen traditionellen Geräten kann man gerne über die Verlängerung der Gebrauchsdauer diskutieren um sich dennoch sicher in SIF zu bewegen, aber bei Geräten mit Smart-Phone Funktionalität und look-and-feel ist das nicht richtig. Letzteres überhaupt in der SIF. Wenn ein Smart Transmitter z.B. mit WLAN für die Funktion wünschenswert ist, ist er vermutlich nicht geeignet für die SIF. Hier muss man sich wieder um Security kümmern, was nicht förderlich für die SFF oder die Diskussion der Verlängerung der Gebrauchsdauer ist.

Assessor: Aspekt Bestandsschutz - es geht um die Sicherheit. Dort gibt es nicht immer Bestandsschutz, siehe Betriebssicherheitsverordnung. Endlose Gebrauchsdauer ist nicht unbedingt vorauszusetzen.

6. IEC 61508, Nationale Fußnote N3, Maßnahmen des Betreibers zur Nutzung von PLT-SE über das Gebrauchsdauerende hinaus:

- Erreichen des sicheren Anlagenzustandes --> reicht es nicht aus das die Fehlfunktion erkannt wird und entsprechende Instandhaltungsmaßnahmen vorliegen anstelle vom Abschalten der Anlage?

- Stördatenerfassung: Wie ist die Erfahrung aus dem Plenum als Maßnahme über das Gebrauchsdauerende die PLT-SE zu betreiben? - -> müssen die Punkte der Norm im Bereich der N3 zu 1 und 2) vollständig erfüllt werden oder kann der Betreiber wenn er Maßnahmen zu 2) erfüllt auf Punkte zu 1) verzichten?

Assessor: hängt davon ab ob die Anlage voll automatisiert gefahren wird. Bei manueller Bedienung kann eine Gegenmaßnahme getroffen werden. Wie ist die Fehlerreaktionszeit – ist der Operator schnell genug? Bei automatisierter Fahrweise kann die Sicherheit evtl. nicht mehr gegeben werden. MTTR beachten. Es ist hilfreich, vorher zu definieren was wie gemacht wird und dies bei Eintritt zu dokumentieren.

Anlagenbetreiber zur Stördatenerfassung: ein ausgefallenes Gerät wird immer analysiert und der Ausfall bewertet.

Fragesteller: Erfahrung ist, dass die Stördatenerfassung bei Kunden sehr „rudimentär“ ist mit wenigen Rückmeldungen. Daher wird die Gebrauchsdauer nach Herstellerangaben benutzt.

Weiterer Anlagenbetreiber: Wenn wir Stördaten bekommen und haben abweichende Informationen (mehr Störfälle) werden diese benutzt. Stördatenerfassung ist notwendig und sollte auf jeden Fall erfolgen. Tool – NAMUR-Smart erfasst diese.

7. Häufig werden Sicherheitsfunktionen bei Batch-Anlagen durch prozessbedingte Fahrweisen (Behälter A/B) durch Signale wie Rückmeldungen, Schlüsselschalter überbrückt. Meine Fragen dazu lauten:

- Inwiefern sind diese Überbrückungssignale (keine temporären Wartungseingriffe, sondern kontinuierlicher Art) in der SIL Nachweisführung der Sicherheitsfunktion zu betrachten?
- Müssen diese Überbrückungssignale die gleiche Anforderung der Sicherheitsfunktion entsprechen (eine Fehlfunktion der Überbrückung, lässt die SIF versagen.)

Fragesteller: bei früheren Sicherheitsbetrachtungen wurden solche Überbrückungen z.B im Batch-Betrieb nicht in der SIL-Nachweisführung betrachtet. NAMUR NE154 gibt das eigentlich vor.

Wenn Sensoren zum Aktivieren und Reaktivieren der SIF enthalten sind ist das genauso zu bewerten wie der Sensor der den SIL überwacht.

Beide Sensoren müssen funktionieren. 2 aus 2 - Berechnung muss erfolgen. Für SIL 3 ist die SIF redundant aufzubauen. Dieser „Störeingriff“ ist zu berücksichtigen.

Operator-Eingriff (Bedienungseingriff) zum Aktivieren oder Deaktivieren ist möglich für SIL3 – allerdings sind 2 Leute nötig.

Bei Arbeit mit verschiedenen Rezepten in einer Anlage und Änderung der Rezeptur über die Leitstelle muss die Sicherheitssteuerung ggf. angepasst werden (ebenso ändern). Deshalb ist die geschickteste Variante, einen zusätzlichen Sensor für aktivieren und deaktivieren der SIF zu nutzen. Dann entfällt die manuelle Änderung bei Änderung des Rezeptes.

Das Rezept vom Leitsystem auf die Sicherheitssteuerung laden ist möglich, aber dann ändert das unsichere Leitsystem die SIF in der der Sicherheitssteuerung.

VDE 2180: Überbrückungen müssen berücksichtigt werden. Sensor für Aktivierung der Überbrückung installieren bei Rezeptänderung.

Antwort eines Assessors: Es ist auch eine Frage des Gesamtkonzepts: z.B. benötigen manche Trockener rezepturabhängig unterschiedliche Luftmengen um unterschiedliche Grenzwerte nicht zu überschreiten. Diese Abschaltwerte sind rezepturabhängig und können von dem Leitsystem gesteuert werden. Mit einem Konzept, mit dem diese Rezeptur vom Bediener ins Leitsystem eingegeben wird, können die Werte an die SSPS-Steuerung weitergegeben werden. Diese kann den Wert über einen anderen Weg zurückspiegeln, und diesen Rückgabewert kann wiederum der Bediener bestätigen (freigeben). Einfach um zu verifizieren, dass der Wert auch wirklich richtig angekommen ist. Einfach einen Wert übermitteln und zu hoffen dass dieser richtig ankommt geht natürlich nicht. Des Weiteren kann man damit nicht verhindern, dass der Bediener ohne prüfen des Rückgabewertes einfach bestätigt, aber dafür muss das Bedienpersonal extra geschult werden. Der Knackpunkt des menschlichen Versagens ist daher dennoch vorhanden. Eventuell mit 4-Augen-Prinzip

Weiterer Experte: Stichwort NE154: Natürlich muss bei einer Auswahl an Rezepten auch sichergestellt werden, dass das richtige Rezept ausgewählt wurde. Sonst hilft die sicherste Steuerung nichts. Also muss man sich auch um die Rezept-Verwaltung Gedanken machen.

Fragesteller: Kunde hat eine Batchanlage mit 18 Rezepten. Idee war ein Schlüsselschalter zur Auswahl der Rezepte, bei 18 Möglichkeiten wurde dies aber verworfen. Baustein, mit dem er seine Werte vom PLS übermittelt bekommt funktioniert seit 20 Jahren und ist von Prüfstelle akzeptiert.

Jetzt stellt sich aber die Frage nach der Informationssicherheit (Cybersecurity). Ist ein Profibus-Befehl mit Handshake und Bestätigung durch den Bediener ausreichend? Was kann man dem Kunden anbieten? Ein neuer Baustein? Eine neue SPS aber an gleicher Schnittstelle? Wie kann die Sicherheit zu gewährleistet werden? 1:1 Austausch?

Experten: Die Informationssicherheit muss neu überprüft werden. Ein Assessment mit dieser Zielsetzung durchführen unabhängig von der Safety Betrachtung.

Fragsteller: um die Schnittstelle nicht zu ändern: geht auch Profibus DP (kein Profisafe)?

Experten: Ja, wenn die Werte über einen anderen Kanal zurückgespiegelt werden und dadurch verifiziert werden können, evtl. mit 4 Augenprinzip und die Freigabe über einen HW-Schalter.

8. Wie gehe ich mit Sicherheitsfunktionen um, die ihre Sicherheitsgerichteten Grenzwerte von einem PLS übertragen bekommen? Wie kann hier der SIL-Nachweis erbracht werden, dass die spezifizierte SIL Anforderung erreicht worden ist (SIL1,2,3 konform?). Wie ist hier das Thema Information Sicherheit zu bewerten?

Siehe Frage zuvor oben

9. Wie ist mit Sicherheitsfunktionen mit einkanaligen binären Eingangssignalen (bspw. Überfüllsicherung, Not-AUS) umzugehen, die einen Kurzschluss zwischen Feldgerät und EA-Karte nicht erkennen?....Nicht alle binären Eingangsmodule erkennen den Kurzschlussfall.--> im Kurzschluss-Fall würde die Sicherheitsfunktion nicht auslösen. Ist der Verzicht auf eine Kurzschluss-Überwachung (Drahtbruch führt zur Auslösung SIF) für eine bestimmte SIL Einstufung akzeptabel?

Rein formal für SIL1 ausreichend, wenn aber mehr Diagnose benötigt würde, z.B. ab SIL2, dann müsste ein Gerät verwendet werden der Kurzschluss und Drahtbruch erkennt.

Experten: keine einfache Möglichkeit, weitere Fehler in der Sicherheitsanwendung zu erkennen die sich durch Kurzschluss zeigen. Der Anwender kann diesen Fehler selten durch andere Maßnahmen ausschließen. Kein Gerät hat keine Ausfallrate, die Nutzung einer Kurzschlussüberwachung ist anzuraten. Kalkulatorisch kann das ok sein aber das Konzept (Sicherheitsdesign) ist nicht geeignet.

Wenn die Eingangskarte einer SPS den Kurzschluss und die Unterbrechung nicht erkennen kann, sollte man sich fragen, ob es für eine Sicherheitsanwendung eine geeignete Karte ist.

In der DIN EN ISO 13850 (Sicherheit von Maschinen - Not-Halt-Funktion – Gestaltungsleitsätze) ist für einen Notaus auch die Kurzschlussüberwachung vorgeschrieben.

10. Ist für ein mechanisches Sicherheitsventil eines Druckbehälters, eine Beurteilung (z.B. LOPA, ...) erforderlich, dass alleinig dieses Sicherheitsventil den sicherheitstechnischen Anforderungen genügt? Was fordern die Regelwerke?

Assessor: Ein mechanisches Ventil unterliegt der Druckgeräteverordnung DGVO und muss als Sicherheitsbauteil zertifiziert sein. Wenn es für die maximale Menge des Anwendungsfalls ausgelegt ist, dann muss man nur noch auf ein Bauteilkennzeichen achten und dann ist keine Lopa nötig. Wenn das Sicherheitsventil nur für Teilmengen ausgelegt ist, dann muss das ganze Konzept betrachtet werden.

Anderer Experte: In diesem Zusammenhang ist noch wichtig darauf zu achten, ob es ein einfacher oder zweifacher Stopp ist. Das Sicherheitsventil muss natürlich immer für die Sicherheitsfunktion bewertet werden. z.B. ob es Fälle gibt die zu Verstopfung führen können. Aber prinzipiell ist es nach der DGVO ausreichend, ein Bauteil mit geprüfter Sicherheit zu verwenden und das gesamte System mit Druckbehälter und Sicherheitssystem in der Konformitätsbewertung zu dokumentieren.

Gleicher Assessor: Wenn ein Druckgerät mit Sicherheitsventil bestückt wurde, geht von dem Druckgerät kein Risiko mehr aus. Das Risiko besteht beim Bersten des Druckbehälters. Um dem entgegenzuwirken verwendet man das Ventil. Wenn ein Ventil verwendet wird das die nötige Menge abgeben kann, dann ist das ausreichend und es muss kein weiteres Sicherheitsventil verwendet werden.

Die Versagenswahrscheinlichkeit eines mechanischen Sicherheitsventils: Wenn es nach der DIN EN ISO 4126 hergestellt wurde, Bauteilgeprüft ist und zyklisch überwacht wird, hat es theoretisch keine Ausfälle.

Weiterer Experte: Elektrische Sicherheit wird auch nicht in Frage gestellt. Es wird zwar oft eine Isolationsmessung gemacht, aber die Isolation hat ja auch eine Versagenswahrscheinlichkeit. Aber diese interessiert niemanden. Es wird geprüft und fertig. Hinweis: Systematik betrachten, Rechnen wird überbewertet.

11. Thema: Überdimensionierung von Schützen.

Nach welcher Norm sollte man das begründen und welche Werte sind relevant ?

Betrachtung Überlast NE 142 und damit die DIN ISO 13849-2 „Der Strom der durch die Schaltkontakte geleitet wird, sollte weniger als die Hälfte des Stromnennwertes“ d.h.

Nennstrom Motor / Nennstrom Schütz * 0,5 Betrachtung Kurzschlusschutz DIN EN 50156-

1; 10.5.5.3.5 „Bei der Bemessung der Überstromschutzeinrichtung ist der vom Gerätehersteller angegebene Nennstrom mit einem Sicherheitsfaktor von 0,6 zu

multiplizieren“ d.h. Absicherung Stromkreis / Angabe des Schütz Hersteller über max.

Ausführung des Kurzschlusschutzes * 0,6

Feststellung: DIN EN 50156 erlaubt den Ausschluss des Fehlerbildes „Kontakt öffnet nicht“. DIN ISO 13849-2 sagt dass das Fehlerbild nicht ausgeschlossen werden darf.

Experte: Geltungsbereich der Norm beachten und gewichten - beides hier nicht zutreffend, da eine „normale“ verfahrenstechnische Anlage zugrunde liegt.

Frage nach Schalten des Nennstroms oder im Kurzschlussfall. -> Überlast mit 0,5 abgedeckt, Kurzschluss durch die Sicherung mit 0,6.

Weitere Kommentare: Klassisches Verfahren in der Verfahrenstechnik über NE142 ist üblich (mindestens 2-facher Nennstrom) Bei Sicherheitsrelais wird oft auch vor und hinter dem Relay abgeschaltet. Das Schütz wird überdimensioniert und Steuerstromkreis wird auch abgeschaltet.

Es muss nicht immer der schlechteste Fall angenommen werden. Es kann auch für jede Anwendung speziell begründet werden.

12. Wer ist Hersteller / Inverkehrbringer von Niederspannungsschaltgerätekombinationen (ugs. Schaltschrank nach DIN EN 61439) mit Sicherheitssteuerungen in verfahrenstechnischen Anlagen und damit auch für die EG-Konformitätserklärung dieser verantwortlich? - Stichwort der Schaltschrankbauer als verlängerte Werkbank



Adobe Acrobat Document

Experte: Dies ist Verhandlungssache und sollte schriftlich vereinbart und festgehalten werden. Wenn ein Anlagenverantwortlicher Komponenten bestellt, wie z.B. einen Schaltschrank, dann wird üblicherweise festgehalten, dass dieser nach den Regeln der Technik aufgebaut werden muss. Dann trägt der Besteller nicht die Verantwortung für das was der Monteur montiert hat, er wird den Schaltschrank mit Konformitätsbewertung bestellen und in Auftrag geben. Dann wird natürlich der Schaltschrankverantwortliche (also der Hersteller des Schaltschranks) zu irgendeiner Maßnahme greifen, um letztendlich nachzuweisen, dass er sich an die Regeln der Technik gehalten hat, und das ist normalerweise die Konformitätsbewertung. Es ist aber auch möglich, dass die Beiden sich untereinander einigen und beschließen, der Schaltschrank wird Teil einer Gesamtanlage die nicht diesem CE unterliegt, und sich auf eine Herstellererklärung einigen. Entscheidend ist, unter welchen Regelungsrahmen es fällt, und was letztendlich zwischen den Beiden vereinbart ist.

Teilnehmers: Bei einer verlängerten Werkbank sieht das anders aus. Wenn der Monteur (Schaltschrankbauer) genaue Vorgaben für die Komponenten bekommt, dann kann er die Konformitätserklärung nicht ausstellen. Dann sollte der Planer die Konformitätserklärung erstellen und unterschreiben.

Antwort darauf: Es kommt auf das Vertragsverhältnis an. Wenn man den Schaltschrank mit CE-Zeichen bestellt, dann kann der „Monteur“ die Aufgabe übernehmen und die Konformitätsbewertung durchführen oder er nimmt den Auftrag nicht an. Stichwort Vertragsfreiheit: hier kann festgelegt werden, ob ein CE-Kennzeichen ausreicht, oder ob ein TÜV den „Schaltschrank“ bewerten soll. Dies liegt im Ermessen der Vertragspartner.

Feststellung erste Seite links: Konformitätsbewertung und CE gibt es für die Anlage nicht – es ist keine Maschine. Daher ist der Betreiber verantwortlich.

Erste Seite Mitte: Schaltschrank - EMV oder Niederspannungsrichtlinie NSR sind evtl. ausgenommen - abhängig davon ob Sicherheitstechnik verbaut ist oder nicht. Wenn ein Betreiber einen Schaltschrank bestellt, dann wird der Hersteller des Schaltschranks dokumentieren dass er sich an die geltenden Regeln gehalten hat. Das kann auch eine Herstellererklärung sein. Das ist Vertragsrecht. Bei verlängerter Werkbank mit klaren Vorgaben hat der Betreiber des Schaltschranks ggf. die Haftung.

Frage ist wer am Markt bereitstellt. Und: findet mit einer Auslieferung in eine Prozessanlage eine Bereitstellung am Markt im Sinne der NSR oder MRL statt, oder wird nur etwas ausgeliefert was im Gesamtkontext der Prozessanlage betrieben wird – das legt fest ob eine RL anwendbar ist oder nicht. Aber: es gibt in der MRL die unvollständige Maschine – auch dort gibt es Regeln zur Dokumentation. Auch wichtig: die Mitarbeiter die an den Geräten arbeiten haben ein Recht auf geeignete Bewertung ihrer Arbeitsumgebung – auch bei Wechsel des Betreibers.

Zweite Seite Mitte: woran ist zu erkennen wer hier verantwortlich ist?

Beispiel: wenn man außerhalb der EU ein Gerät kauft, neu benennt (neuen Namen drauf schreibt) und in der EU verkauft, dann muss derjenige die Konformitätsbeschreibung erstellen, der dieses „neue Gerät“ in Verkehr bringt. Es ist hier ein rein formaler Akt - egal auf welcher Grundlage das geschieht. Wenn dieses Gerät abbrennt, kommt die Behörde erst zu dem, der auf dem Typenschild seinen Namen geschrieben hat, da dieser die Konformitätsbewertung durchgeführt hat. Dann ist es eine vertragliche Sache, ob etwaige Ansprüche am Originalhersteller geltend gemacht werden können. Hier geht es um eine rein vertragliche Vereinbarung.

13. Wie unterscheiden sich die Anforderungen an ein SIS bei steigender SIL-Anforderung (z.B. SIL1 im Vergleich zu SIL3) bezüglich Vermeidung systematischer Fehler? Gibt es neben der Mehrkanaligkeit des SIS und dem Unabhängigkeitsgrad der Personen für Validierung u. Verifikation (4-Augen-Prinzip) weitere Unterschiede?

Assessor: Es gibt Unterschiede in der EN 61508 in den Tabellen zwischen SIL2 und SIL3 was die Verifikation angeht, also die tiefe von Tests, z.B. SW-Tests (Unit-Tests, Integrationstests), ob man einen reinen Funktionstest macht oder einen white box Test. Das ist abhängig vom SIL.

Kommt die Frage aus Herstellersicht oder Anwendersicht? -> Beides

Experte: Bisher wurde nach der 61508 argumentiert - Herstellersicht. In der 61511 gilt die systematische Betrachtungsweise, dort wäre alles als SIL3 zu bewerten. Es sind die gleichen Maßnahmen vorzusehen. Der einzige Unterschied des SIL in der 61511 sind die Anforderungen an PFD und HFT.

Fragesteller: Wie ist das dann mit dem Unabhängigkeitsgrad der Person?

Antwort: Die 61511 sagt nur, es muss eine unabhängige Person sein, die mit dieser speziellen Phase des Lebenszyklus nichts zu tun hatte.

Fragesteller: Was ist ausreichend unabhängig?

Antwort: Hier ist eine eigene Entscheidung nötig – festlegen und dokumentieren.

Nicht nur das Schadensausmaß bedenken, sondern ob es systematische Fehler sind die betrachtet werden müssen. Wie wird eine redundante Schaltung für SIL3 aufgebaut: sind gemeinsame Ausfälle zu betrachten bei gemeinsamer Nutzung eines Kabels, oder trennt man die Kabel in separaten Kabelkanälen. Gibt es spezielle Notfallszenarien die betrachtet werden müssen? Gib es überhaupt die Möglichkeiten?

Antwort: Bei SIL1 sicher keine Trennung - aber bei SIL3 ist das Gefährdungsrisiko sehr groß und man muss auch solche Maßnahmen erwägen. Geräte müssen aber auch dafür geeignet sein (mehrere Klemmen für redundante Verdrahtung).

Schadensausmaß ist nicht alles: SIL sagt ja nicht welche Art der Gefährdung abgefangen wird, sondern welche Risikominderung (Faktor 10, 100, 1000) festgelegt wurde. Und es wäre fatal,

Vermeidung systematischer Fehler zu ignorieren. Eine Organisation muss die möglichen systematischen Fehler evaluieren und etwas tun – ggf. auch im Betrieb beobachtete Dinge nachträglich berücksichtigen.

Frage: haben Assessor und Hersteller nach der 61508 gemeinsam die Verantwortung?

Assessor: 61508-1 Kapitel 8 zu Assessments. Unabhängige Organisation, Abteilung oder Person, als Empfehlung. Für den Hersteller gilt Fehlervermeidung nach 61508, manchmal Unterscheidung nach SIL1, SIL2 oder SIL3. Evtl. sagt eine Firma, sie stellt überwiegend SIL2 Produkte her und verwendet den Prozess generell. Aber es gibt auch Firmen die bei SIL1 etwas weniger machen als wenn sie SIL3 entwickeln.

Dienstleister: es sind auch Betreiber bekannt, eher kleinere Firmen, die bei SIL1 und 2 selbst prüfen, und ab SIL3 den TÜV beauftragen, einfach um bei SIL1 und 2 Kosten zu sparen.

Nächste SIL-Sprechstunde -19-20 Sep 2023 in Mannheim, Thema: SIL versus Performance Level (61508 versus 13849)

Umfeld vor Ort ist entscheidender als die Berechnung für die Intervallfestlegung. Zeitliche Abhängigkeiten bestimmen die Faktoren vor Ort nicht in der Mathe.