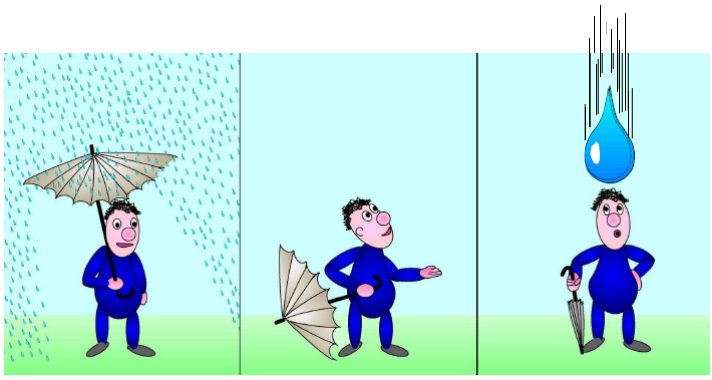
Inhalt

1. Einführung

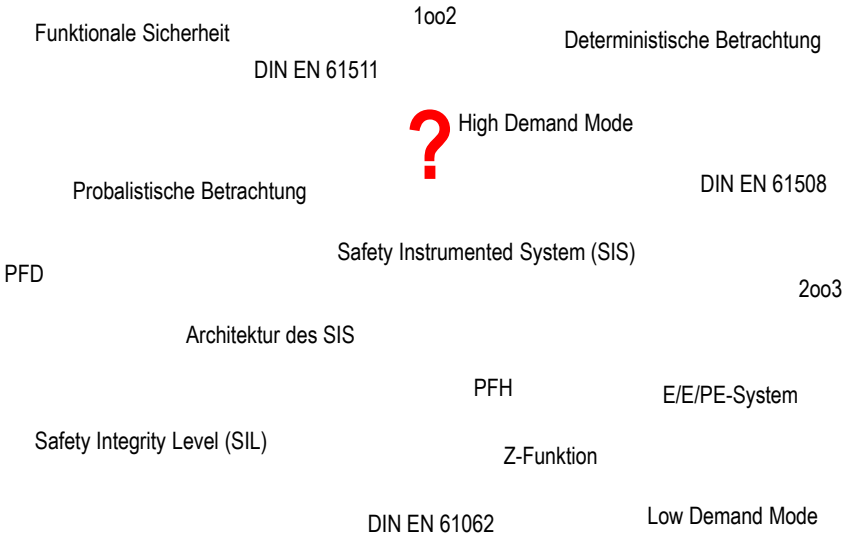
Referent : Hans-Dieter Schwender
TÜV-SÜD Industrieservice

Wie passieren Unfälle



G.C. Eltenton: Wenn ein unerwartetes Ereignis auf eine unvorbereitete Person trifft

Begriffe in der Funktionale Sicherheit



Was ist Sicherheit

Zitat Wikipedia:

„In komplexen Systemen ist es unmöglich, Risiken völlig auszuschließen. Das vertretbare Risiko für jede mögliche Art der Beeinträchtigung hängt von vielen Faktoren ab und wird zudem subjektiv und kulturell verschieden bewertet. Im Allgemeinen werden höhere Wahrscheinlichkeiten für Beeinträchtigungen mit steigendem Nutzen (beispielsweise Aktien-Spekulation, Teilnahme am Straßenverkehr) als vertretbar angesehen.

Um den Zustand von Sicherheit zu erreichen, werden Sicherheitskonzepte erstellt und umgesetzt. Sicherheitsmaßnahmen sind erfolgreich, wenn sie dazu führen, dass mit ihnen sowohl erwartete als auch nicht erwartete Beeinträchtigungen abgewehrt bzw. hinreichend unwahrscheinlich gemacht werden.“

Wen betrifft die funktionale Sicherheit?

Betreiber	Stellt die Anforderung der sicherheitstechn. Komponenten Muss einen Nachweis über das verbleibende Risikopotential erbringen
Anlagenbauer	Auslegung der Anlage
Gerätelieferant	Bestätigung der Klassifizierung sowie die Ermittlung der Gerätespezifischen Daten (λ, SFF HFT…)
Behörde und Versicherung	Nachweisforderung für eine ausreichende Reduzierung des Restrisikos der Anlage

Definition von Risiko

Risiko = Wahrscheinlichkeit des Eintritts eines gefährlichen Ereignisses * Konsequenzen (Kosten) eines gefährlichen Ereignisses

Akzeptiertes Restrisiko muss individuell eingeschätzt werden. Was für den Einen akzeptabel ist, kann für den Anderen bereits inakzeptabel sein!

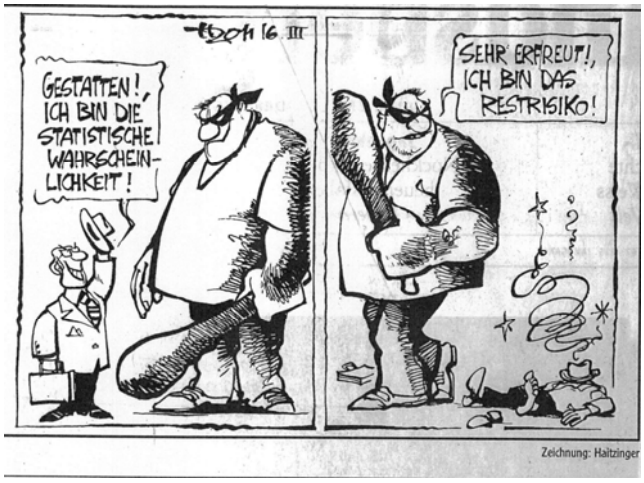
Das Restrisiko ist abhängig von:

- Land / Region
- Jeweiligen Gesellschaft
- Gesetze
- Kosten

Risikoauslegung mal anders

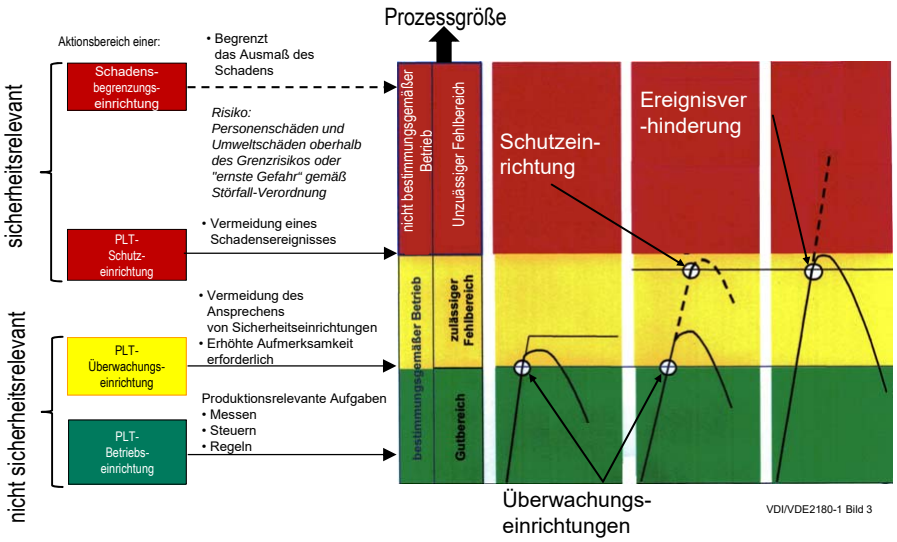
Andere Länder, andere Einschätzung des Risikos Quelle Youtube

So bitte nicht!



Quelle: Landsberger Tagblatt 16.03.2011

Darstellung der Wirkungsweise von PLT-Einrichtungen

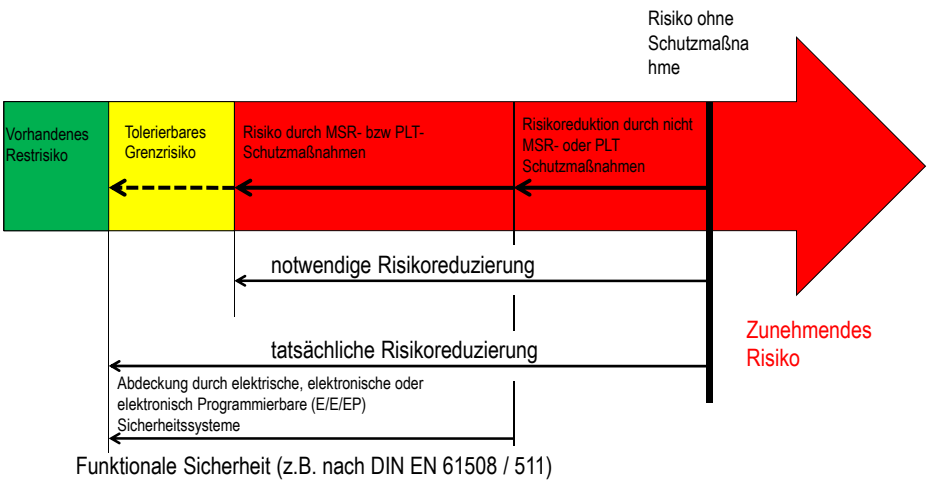


Möglichkeiten der Risikominderung

Möglichkeiten der Risikominderung

Die Schutzebenen sind in ihrer Funktion voneinander unabhängig. In der Regel dürfen Geräte der Steuerungs- und Regelungsebene **nicht** gleichzeitig für die Realisierung einer Schutzmaßnahme verwendet werden!

Risikoreduzierung



Unterscheidung von *"Sicherheit"*

Man kann verschieden Arten von Sicherheit durch Angabe der jeweiligen Ursache der möglichen Gefährdung unterscheiden:

- Elektrische Sicherheit: Bringt den Schutz vor Gefährdungen durch den elektrischen Strom zum Ausdruck.
  - DIN EN 50156-1 (VDE0116)
  - VDE 0100

- Sicherheit vor Zündung einer explosionsfähigen Atmosphäre, eines explosionsfähigen Gemisches
  - (z. B.: 1999/92/EG (ATEX 137),
  - ProdSG, BetrSichV, TRGS 725, VDE, etc.)

- Funktionale Sicherheit: Die Sicherheit hängt von der korrekten Funktion ab:
  - (z. B.: 2014/68/EU → DGRL,
  - ProdSG, BetrSichV, TRBS 1201 Teil 2,
  - EN 61508, EN 61511, EN 50156, VDI/VDE 2180, etc.)

Festlegung der funktionalen Sicherheit

Die Normen zur funktionalen Sicherheit befassen sich mit der funktionalen Sicherheit sicherheitsbezogener

- Elektrischer Systeme
- Elektronischer Systeme
- Programmierbarer elektronischer Systeme

Also demnach gilt:

Es geht **nicht** um mechanische Systeme!

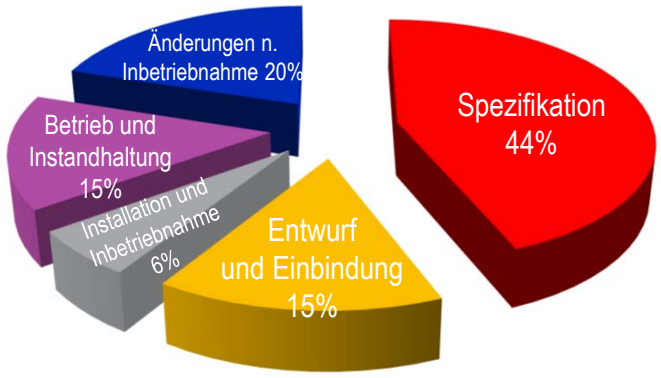
Warum versagen Schutzfunktionen?

Systematische Fehler	Zufällige Fehler
Entwicklungsfehler Planungsfehler Verdrahtungsfehler	Ergeben sich aus Fehlern der Hardware und treten zufällig auf (z.B. Kurzschluss)
Qualitätssichernde Maßnahmen (Management der funktionalen Sicherheit)	Ermittlung der Versagenswahrscheinlichkeit (Probabilistik)

Fehleraufteilung

Studie der HSE (Health and safety enviroment)

Hauptursache in den Phasen



Basis der funktionalen Sicherheit

- Das Vermeiden systematischer Fehler bei Entwicklung, Fertigung und Betrieb des sicherheitskritischen Systems

- Das Beherrschen von systematischen Fehlern während des Betriebes

- Das Beherrschen von zufälligen Fehlern während des Betriebes

Anforderung an die funktionale Sicherheit

Korrekte Funktion sicherheitsbezogener Teile von Schutzsystemen

Ziel:

Das überwachte System muß bei Auftritt von Fehlern oder Ausfällen:

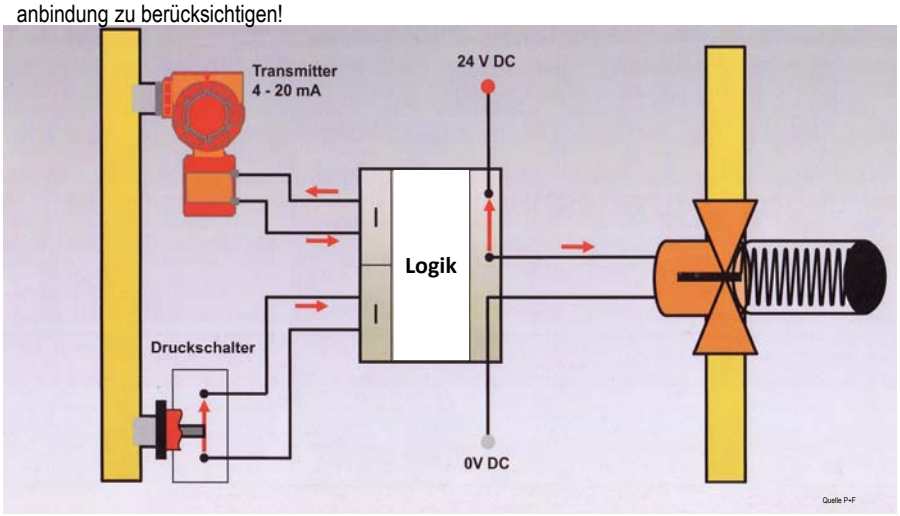
- In einem sicheren Zustand verbleiben

oder

- In einen sicheren Zustand gebracht werden

SIS-Kreis

Bei der Betrachtung des Sicherheitsgerichteten Kreises ist auch die Prozess-anbindung zu berücksichtigen!



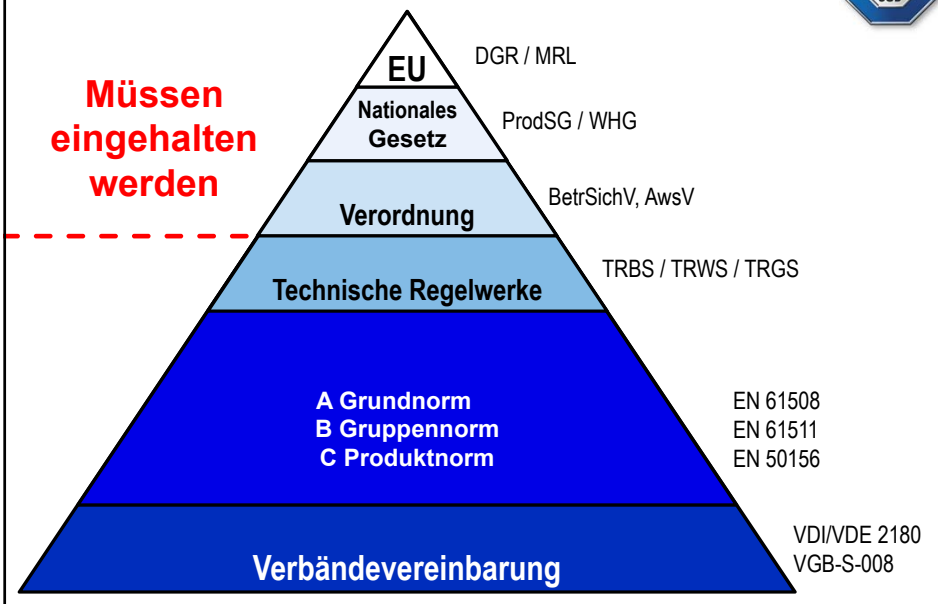
Zusammenfassung

- Funktionale Sicherheit betrifft uns alle
- Mittels einer Risikoreduzierung muss das vorhandene Risiko auf ein tolerierbares Risiko reduziert werden
- Funktionale Sicherheit im Sinne der DIN EN 61508 umfasst alle sicherheitsbezogene E, E, EP–Systeme
- Man unterscheidet zwischen systematischen und zufälligen Fehlern
- Durch die funktionale Sicherheit muss das System bei Fehlern im sicheren Zustand verbleiben, oder in den sicheren Zustand gebracht werden
- Bei der funktionalen Sicherheit ist der gesamte Kreis von Sensor bis Aktor inkl. der Prozessanbindung zu betrachten

2. Regelwerke

Referent : Hans-Dieter Schwender
TÜV-SÜD Industrieservice

Risikominderung durch Normen und Richtlinien



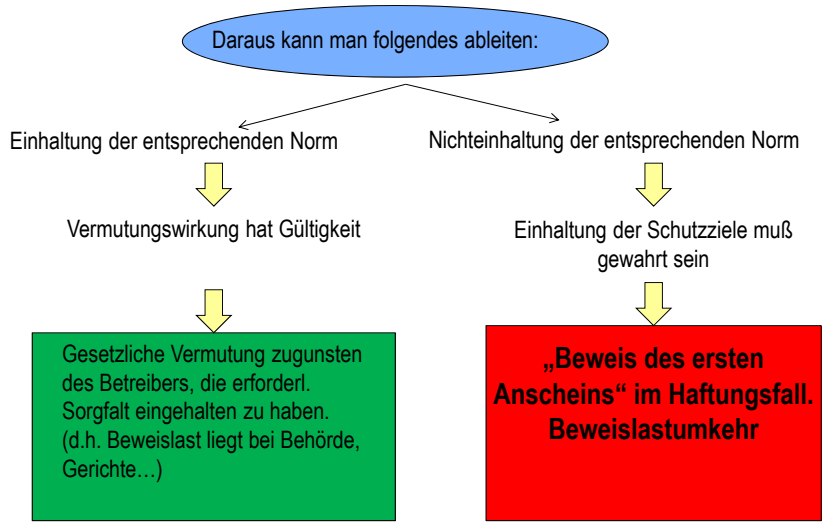
Rechtliche Einordnung von DIN-Normen

Urteil des BGH vom 14.05.1998 im Bezug zwischen Technik in Normen und dem Recht:

„Die DIN-Normen sind keine Rechtsnormen, sondern private technische Regelungen mit Empfehlungscharakter. Sie könne die anerkannten Regeln der Technik wiedergeben oder hinter diesen zurückbleiben."

Damit ergibt sich die widerlegbare gesetzliche Vermutung, dass bei Einhaltung der techn. Regeln der genannten Verbände auch die „allgemein anerkannten Regeln der Technik" eingehalten sind (Vermutungswirkung)

Rechtliche Einordnung von DIN-Normen



Gegenüberstellung alt zu neu

Nach der Übernahme der IEC 61508 ins nationale Regelwerk wurde die Betrachtungsweise gravierend geändert

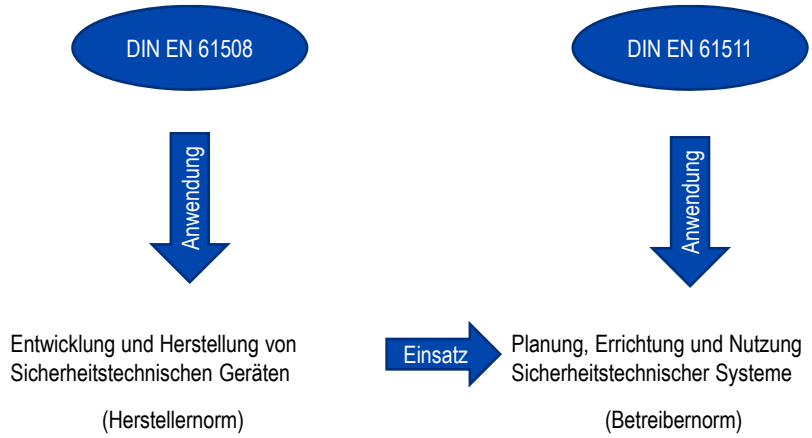
Was war:	Betrachtung von einzelnen Komponenten (Sensor, Signalverarbeitung, Aktor einzeln betrachtet!)
Heute:	Betrachtung der gesamten Sicherheitsgerichteten Funktion (gesamter Kreis von Sensor bis zum Aktor inkl. deren Anbindung!)

Ansätze zur funktionalen Sicherheit

Bisher: Qualitativer Ansatz
d.h. Sicherheit durch z.B.
- Redundanz („Einfehler-sicher“, „Zweifehler-sicher“…)
- selbstüberwachend
- Diversitär
- „bewährte Technik bzw. Betriebsmittel“
- Bauteilprüfung z.B. gem. VdTÜV-Merkblatt

Jetzt: Quantitativer Ansatz
d.h. Sicherheit durch probabilistische Betrachtungsweise
(pobability = Wahrscheinlichkeit)

Beziehung zwischen DIN EN61508 und DIN EN 61511



Gegenüberstellung der Ansätze

Probabilistik
(quantitativer Ansatz)

Wahrscheinlichkeit

Analyse der Fehler-wahrscheinlichkeit z.B. FMEDA (Failure Modes Effects and Diagnositc Analysis)

Rechnerischer Nachweis zur Erfüllung der Anforderung

Normen :

- EN 61508
- EN 61511

Deterministik
(qualitativer Ansatz)

Fehlerausschluss

Einsatz von bauteilgeprüften Geräten besonderer Bauart.

Bauteilgeprüfte Geräte besonderer Bauart gelten als fehlersichere Funktionseinheiten / Redundanzen

Normen :

- EN 50156-1

Zusammenfassung

- Bei Einhaltung der Normen tritt die Vermutungswirkung in Kraft
- Basisnorm der funktionalen Sicherheit ist die DIN EN 61508
- Das Maß der funktionalen Sicherheit ist „SIL“
- Der Ansatz der funktionalen Sicherheit ist die Probabilistik

3. Management der funktionalen Sicherheit

Referent : Hans-Dieter Schwender
TÜV-SÜD Industrieservice

Management der funktionalen Sicherheit

Auszug aus der DIN EN 61511-1:

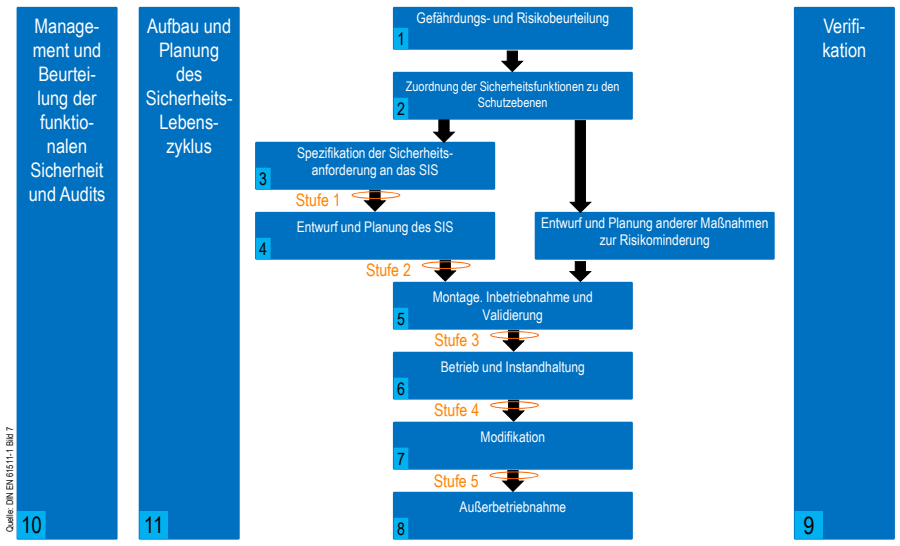
5 Management der funktionalen Sicherheit

5.1 Ziel

Das Ziel der Anforderungen des Abschnitt 5 ist es, die erforderlichen Managementtätigkeiten festzulegen, mit denen sichergestellt wird, dass die Ziele der funktionalen Sicherheit erreicht werden..

ANMERKUNG 1 In Abschnitt 5 werden nur die Maßnahmen betrachtet, die zur Erreichung und Aufrechterhaltung der funktionalen Sicherheit einer PLT-Sicherheitseinrichtung notwendig sind, ohne jedoch andere allgemeine Maßnahmen zur Gesundheit und Sicherheit am Arbeitsplatz zu berühren.

Phasen des SIS Sicherheitslebenszyklus



Verifikation / Validierung

➢ Definition Verifikation:

- Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, dass die Anforderungen erfüllt worden sind → d. b.

  erfüllt das System die im Pflichtenheft gestellten Anforderungen z.B. rechn, Nachweis
  Beispiel Rettungsring → sieht er so aus

➢ Definition Validierung:

- Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines objektiven Nachweises, dass die besonderen Anforderungen für eine spezielle beabsichtigte Verwendung erfüllt worden sind → d.B.

  Ist es das richtig System mit dem wir uns beschäftigen-Tauglichkeit?
  Beispiel Rettungsring → schwimmt er

Ziel des Managements der Funktionalen Sicherheit

Das FSM stellt den organisatorischen Rahmen zur

- Einführung,
- Aufrechterhaltung und
- Sicherstellung

aller prozesstechnischen und technischen Methoden und Maßnahmen dar, welche zur Erreichung der geforderten Funktionalen Sicherheit von sicherheitstechnischen Funktionen benötigt werden.

Qualifikation Sicherheitsmanagement

Personen, Abteilungen oder Organisationen, die an der Durchführung von Maßnahmen im Sicherheitslebenszyklus beteiligt sind, müssen kompetent für die von ihnen verantworteten Tätigkeiten sein.

Die Beurteilung der Kompetenz erfolgt unter Beachtung der folgenden Merkmale:

a) techn. Wissen, Ausbildung und Erfahrung bezogen auf die prozesstechn. Anwendung

b) techn. Wissen, Ausbildung und Erfahrung bezogen auf die eingesetzte Technologie (z. B. elektrische, elektronische oder programmierbare elektronische Technologie)

c) technisches Wissen, Ausbildung und Erfahrung bezogen auf die Sensoren und Aktoren

d) sicherheitstechnisches Wissen (z. B. über Sicherheitsanalysen)

Qualifikation Sicherheitsmanagement

e) Kenntnis der gesetzlichen und behördlichen Anforderungen

f) ausreichende Management- und Führungsqualitäten für die jeweilige Aufgabe im Sicherheitslebenszyklus

g) das Verständnis für die möglichen Folgen eines Ereignisses

h) den Sicherheits-Integritätslevel der sicherheitstechnischen Funktionen

i) die Neuartigkeit und Komplexität einer Anwendung beziehungsweise einer Technologie.

Spezifikation der Sicherheitsanforderungen - Funktion

- Beschreibung der sicherheitstechnischen Funktion(en)
  → z.B. verbale Beschreibung, Fließbild, …
- Definition des „Sicheren Zustandes“
- Erforderliche Reaktionszeit zur Erreichung des sicheren Zustandes
- Beschreibung der Messsignale und Grenzwerte
- Erforderliche Kriterien zur Erfüllung der sicherheitstechnischen Funktion
  → z. B. Dichtes Schließen
- Betriebliche Anforderungen → z. B. An- und Abfahren im Handbetrieb, Zurücksetzen nach Abschaltung, Maßnahmen im Falle eines entdeckten Fehlers, etc.
- Schnittstellen zu anderen betrieblichen Einrichtungen → z. B. Protokollierung
- Mögliche gefahrbringende Kombination von Ausgangszuständen
- Extremwerte aller Umweltbedingungen → z. B. Temperaturauslegung, Ex-Bereich, Schutzart

Spezifikation der Sicherheitsanforderungen - Integrität

Anforderungen an die Sicherheitsintegrität :

- Sicherheitsintegritätslevel (SIL) je sicherheitstechnischer Funktion
- Geschätzte Rate der Anforderungen an die sicherheitstechnischen Funktionen und deren Auslöser
- Anforderungen an das Intervall der Wiederholungsprüfungen (Proof Testintervall T1)
- Mittlere Reparaturzeit (MTTR = Mean Time To Reparation)

Beurteilung, Revision, Auditieren

Teammitglieder:

Mind. ein Mitglied des Teams muss erfahren und kompetent bei der funktionalen Sicherheit sein, darf aber nicht bei dem Entwurf des Projektes beteiligt gewesen sein!

Umfasst das Team einen größeren Kreis, sollten mehr als eine erfahrene Personen im Team sein.

Zeitpunkt und Ziel der Beurteilung

Die Zeitpunkte im Sicherheitslebenszyklus, zu denen eine Beurteilung erfolgt, müssen bereits bei der Sicherheitsplanung festgelegt werden.

Das Ziel der Verifikation ist es, durch Überprüfung, Analyse und/oder Test nachzuweisen, dass die Ergebnisse der jeweiligen Stufe des Sicherheitslebenszyklus den Anforderungen des Verifikationsplans entsprechen.

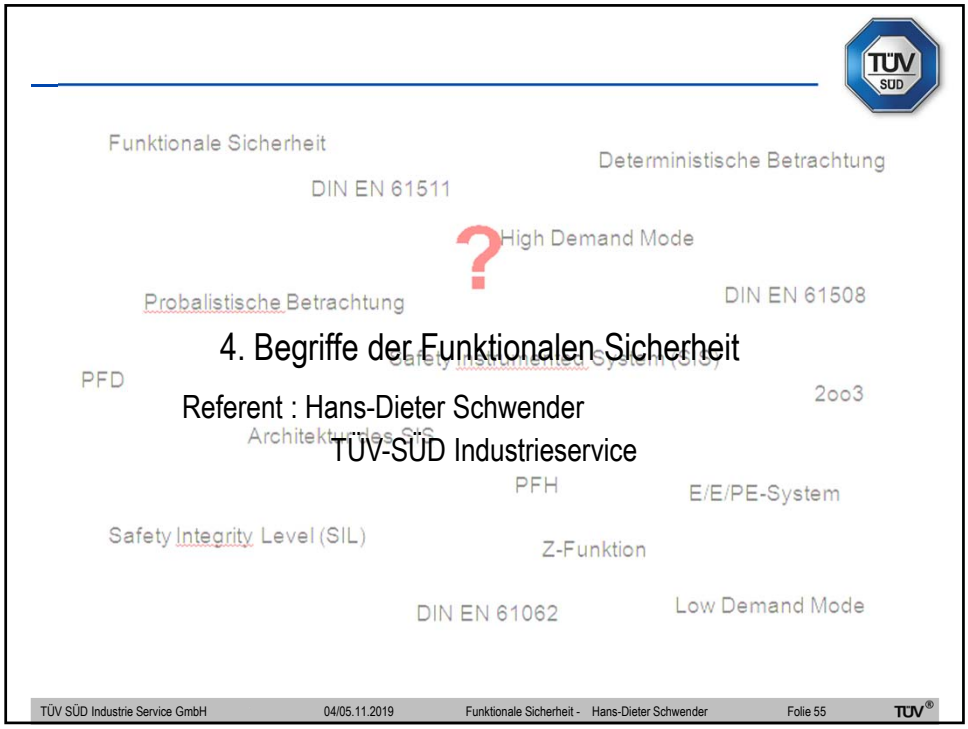
Wichtiges Erkenntnis

Die Normenreihen EN 61508 / 61511 fordern:

- **Lieferanten und Auftragnehmer müssen ein „funktionales Sicherheitsmanagement“ nachweisen…**
- …deshalb ist eine Bescheinigung des funktionalen Sicherheitsmanagements oder ein vergleichbarer Beleg das **ERSTE** wonach ein Käufer fragen sollte

Zusammenfassung

- Die Normreihe 61508 fordert, dass Lieferanten und Subunternehmer ein „funktionales Sicherheitsmanagement“ nachweisen
- Es wurde ein Sicherheitslebenszyklus entwickelt
- Dieser beschreibt den Weg von der Idee bis zur Stillsetzung
- Das FSM stellt den organisatorischen Rahmen zum Erreichen der funktionalen Sicherheit
- Innerhalb des FSM werden auch die Verifizierung und Validierung festgelegt



Low Demand

Low Demand System: Sicherheitsfunktion mit niedriger Anforderungsrate (z.B. Druckmessung oder Überfüllsicherung in der Prozessindustrie, Überdrehzahlschutz Not-Aus…)

Kennzeichnung: Das Sicherheitssystem darf nur einmal im Jahr angefordert werden

Kenngröße: PFD (Probability of Failure on Demand)

- ❖ Gefährliche Versagenswahrscheinlichkeit bei Anforderung
- ❖ Daten direkt über Hersteller
- ❖ durch Betreiber aus Betriebsbewährung
- ❖ FMEDA-Untersuchung nach DIN-EN 61508
- ❖ aus Datenbanken

PFD

Tabelle 2 – Sicherheits-Integritätslevel – Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit niedriger Anforderungsrate betrieben wird

Sicherheits-Integritätslevel (SIL)	Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion (PFD_{avg})
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$

High Demand

High Demand System: Sicherheitsfunktion mit hoher oder kontinuierlicher Anforderungsrate (z.B. Fertigungsindustrie wie Presse)

Kennzeichnung: Das Sicherheitssystem wird häufiger als einmal im Jahr angefordert oder arbeitet kontinuierlich.

Kenngröße: PFH (Probability of Failure per Hour)

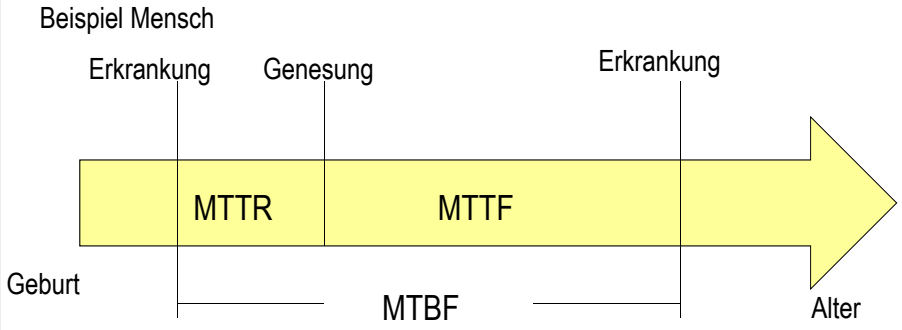
- Gefährliche Versagenswahrscheinlichkeit pro Stunde
- Daten direkt über Hersteller
- durch Betreiber aus Betriebsbewährung
- FMEDA-Untersuchung nach DIN-EN 61508
- aus Datenbanken

PFH

Tabelle 3 – Sicherheits-Integritätslevel – Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher Anforderungsrate oder in der Betriebsart mit kontinuierlicher Anforderung betrieben wird

Sicherheits-Integritätslevel (SIL)	Mittlere Häufigkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion [h^{-1}] (PFH)
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

MTTF, MTTR, MTBF



MTTR = Mean Time To Repair (mittlere Reparaturzeit)

MTTF = Mean Time To Failure (Mittelwert Ausfallfreier Zeit)

MTBF = Mean Time Between Failure(Zeit zwischen 2 Fehlern)

MTTF, MTTR, MTBF

Wichtig:

Reaktionszeit des SIS < Fehlertoleranzzeit des Prozesses

Ausfallrate λ

- gefährliche Fehler
- sicherheitsgerichtete Fehler
- unerkannte Fehler
- erkannte Fehler

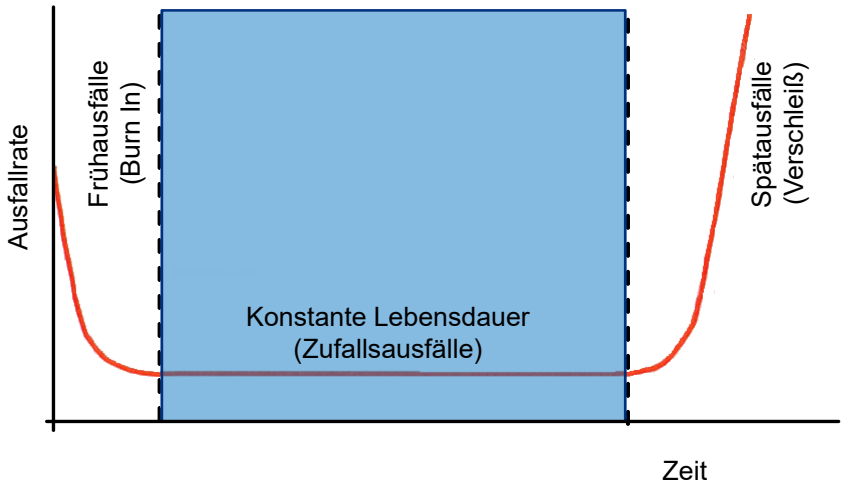
Fehlerarten	Erkennbare Fehler	Unerkannte Fehler
Sichere Fehler	λ_{SD}	λ_{SU}
Gefährliche Fehler	λ_{DD}	λ_{DU}

$$\lambda_{Total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$$

PFD

Bei λ = **konstant** ⇨ **MTBF = $1/\lambda_{Total}$**

Badewannenkurve



Diagnosedeckungsgrad DC

Anteil der gefahrbringenden Ausfälle, die durch automatische diagnostische Online-Prüfungen erkannt werden. Je höher der Deckungsgrad ist, desto wahrscheinlicher ist, dass ein gefährlicher Fehler erkannt wird.

$$DC = \frac{\Sigma \lambda_{SD} + \Sigma \lambda_{DD}}{\Sigma \lambda_{DTotal}}$$

Anteil sicherer Ausfälle SFF

Safe failure fraction SFF:

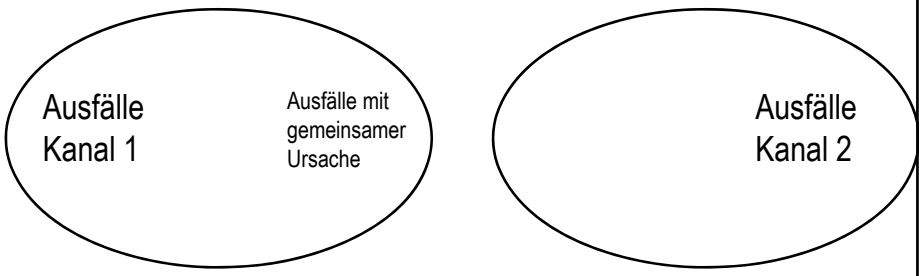
Anteil der sicheren Ausfälle. Je höher dieser Anteil ist, desto besser ist die Fehlerbeherrschung.

$$SFF = \frac{\Sigma \lambda_S + \Sigma \lambda_{DD}}{\Sigma \lambda_{DTotal}}$$

Common Cause Faktor β

Ausfälle infolge gemeinsamer Ursache

Es gibt eine endliche Wahrscheinlichkeit dafür, dass unabhängige zufällige Hardwareausfälle in allen Kanälen eines mehrkanaligen Systems so auftreten, dass alle Kanäle gleichzeitig ausfallen!



Eine Berücksichtigung bei der Berechnung wird mittels des β - Faktors realisiert

Abschätzung CommonCause Faktor β

- Methoden zur Ermittlung des Faktors werden in EN 61508-6 Anhang D dargestellt (β-Faktor Modell und Binomial-Ausfallraten-Modell)
- Alternativ bietet die EN 61508-6 auch die Abschätzung unter Verwendung von Tabellen (Anhang D.5)
- Nach VDI/VDE 2180 Blatt 1 Pkt. 2 liegt der Betafaktor in der Praxis zwischen 1 und 5 %
- Oftmals konservative Annahme von β = 10%

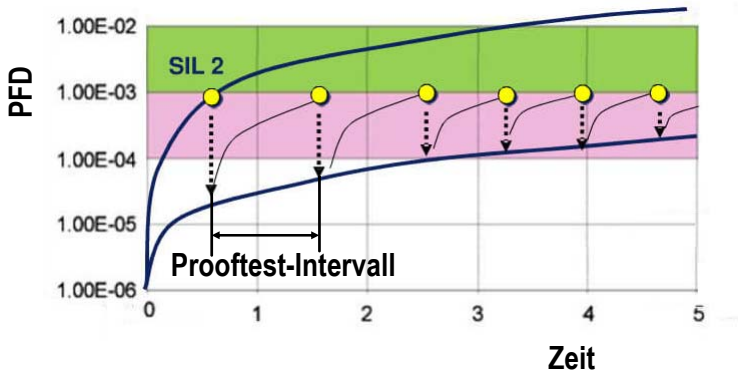
Proof-Test

Definition nach EN 61508:
„wiederkehrende Prüfung zur Aufdeckung von versteckten gefahrbringenden Ausfällen in einem sicherheitsbezogenen System, so dass nötigenfalls eine Reparatur das System in einen „Wie-Neu"-Zustand bringen oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand heranbringen kann

Dient also zur Aufdeckung gefährlicher Fehler

- Inhalte sind die Prüfung von:
  - Zustand der SIS
  - Funktionalität der SIS
  - Ordnungsprüfung (z.B. sind noch die korrekten Teile eingebaut, Lebensdauer…)
- Der Abstand zwischen den periodischen Prüfungen geht als Proof-Test-Intervall T_1 in den rechnerischen Nachweis mit ein

Proof-Test

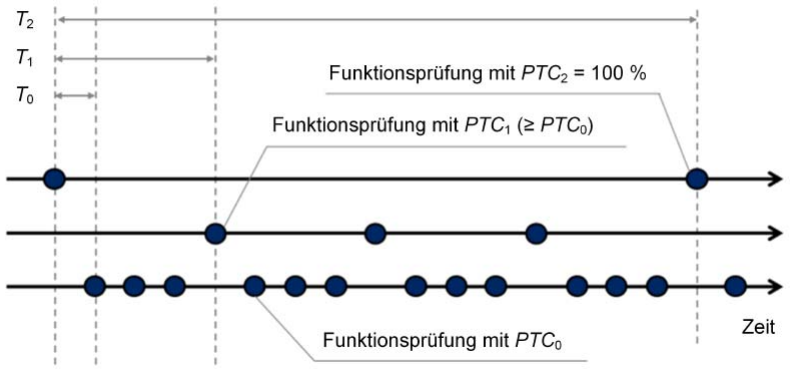


Deckungsgrad der Wiederholungsprüfung (PTC)

- Zeitpunkt T2: „klassischen“ Wiederholungsprüfung (stehender Anlage) mit 100% Prüftiefe
- Zeitpunkt T1: Zwischenprüfung Prüftiefe < 100%
- Zeitpunkt T0: Zwischenprüfung Prüftiefe < 100%

- Prüftiefe < 100%: z.B. Partial-Stroke-Test bei Ventilen oder Betätigen einer Prüftaste bei Sensoren
- 100%-Prüfung: kann in der Praxis häufig Generalüberholung der Aktorik oder Gerätetausch
- Für die Intervalle T0, T1 und T2 muss gelten:
  - $T0 \leq T1 \leq T2$ und
  - $T1 = j \cdot T0$, $T2 = k \cdot T1$
  - mit j, k ganze Zahlen

Gestaffeltes Prüfkonzept mit diversitärer Instrumentierung



NE 106_2018_09_06
Abschätzung PTC
BSP 1oo2

Quelle VDI/VDE 2180-1: 2019

Hardware-Fehler-Toleranz (HFT)

Definition:
Die Hardware-Fehlertoleranz ist die Fähigkeit einer Komponente oder eines Teilsystems, trotz des Vorliegens eines oder mehrerer gefahrbringender Hardwarefehler die geforderte sicherheitstechnische Funktion auszuführen.
Eine Hardware-Fehlertoleranz von 1 bedeutet, dass beispielsweise zwei Geräte vorhanden und so angeordnet
sind, dass ein gefahrbringender Ausfall nicht zum Verlust der Sicherheitsfunktion führen

Ermittlung des SIL

EN 61508-2 Tabelle 3 – Mindest-Hardware-Fehlertoleranz von Typ B-Elementen

SFF	Hardware-Fehlertoleranz		
	0	1	2
SFF < 60%	Nicht erlaubt	SIL 1	SIL 2
60% ≤ SFF < 90%	SIL 1	SIL 2	SIL 3
90% ≤ SFF < 99%	SIL 2	SIL 3	SIL 4
SFF ≥ 99%	SIL 3	SIL 4	SIL 4

EN 61508-2 Tabelle 2 – Mindest-Hardware-Fehlertoleranz von Typ A-Elementen

SFF	Hardware-Fehlertoleranz		
	0	1	2
SFF < 60%	SIL 1	SIL 2	SIL 3
60% ≤ SFF < 90%	SIL 2	SIL 3	SIL 4
90% ≤ SFF < 99%	SIL 3	SIL 4	SIL 4
SFF ≥ 99%	SIL 3	SIL 4	SIL 4

Ermittlung des SIL

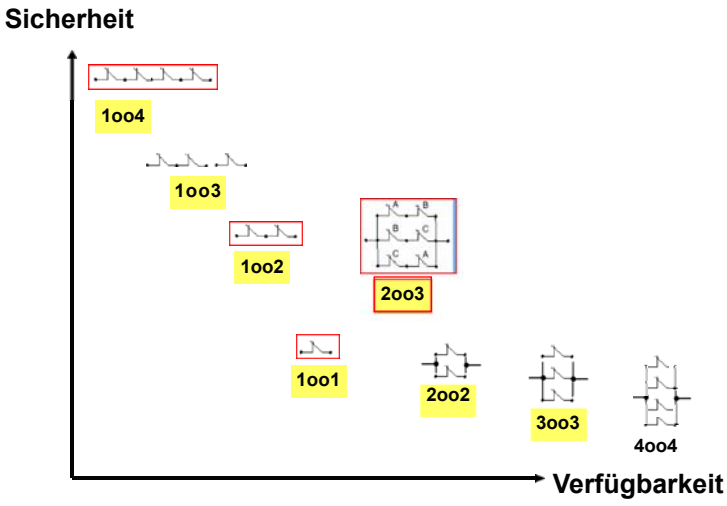
EN 61511-1 Tabelle 6 – Mindest-Hardware-Fehlertoleranz in Abhängigkeit des SIL

SIL	Hardware-Fehlertoleranz		
	0	1	2
1	X		
2 (Low Demand)	X		
2 (High Demand)		X	
3		X	
4			X

Ermittlung des SIL

- Hierbei muß der Diagnosedeckungsgrad bei Typ B-Geräten > 60% sein
- Bei Typ A Geräten kann die Mindest-HFT um eins reduziert werden (Begründung und Dokumentation erforderlich!)
- Hierbei muss die Begründung nachweisen, dass die gewählte Architektur geeignet ist und die Sicherheitsintegrität erfüllt.
- Ergibt diese Anwendung eine HFT von 0, muss die Begründung nachweisen, dass die entsprechenden gefahrbringenden Aufallarten ausgeschlossen werden können.

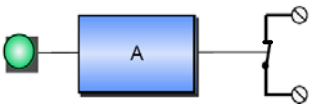
Auslegung mehrkanaliger Sicherheitseinrichtungen



Zusammenfassung

- Es wird in High und Low Demand Modus unterschieden
- MTBF ist die Zeit zwischen 2 Fehlern
- Die Ausfallwahrscheinlichkeit kann nur für konstante Bedingungen angegeben werden
- Common Cause Faktor ist ein Maß für Ausfälle infolge gemeinsamer Ursache
- HFT ist die Hardware Fehler Toleranz

Aufbau und Zuverlässigkeit → Architektur 1oo1



HFT = 0

1-kanaliger Aufbau

1 Fehler setzt die sicherheitstechnische Funktion außer Kraft

Aufbau und Zuverlässigkeit → Architektur 1oo1

Quelle DIN EN 61508

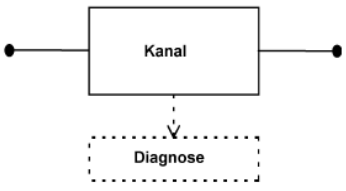
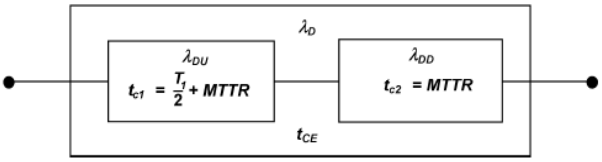
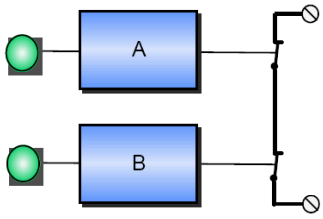


Bild B.4 – Blockschaltbild für 1oo1



Aufbau und Zuverlässigkeit → Architektur 1oo2



HFT = 1

2-kanaliger Aufbau – Die Kontakte sind hintereinander geschaltet

Das System benötigt nur einen Kanal um die sicherheits-technische Funktion auszuführen
→ Erhöhung der Sicherheitsfunktion.

Aufbau und Zuverlässigkeit → Architektur 1oo2

Quelle DIN EN 61508

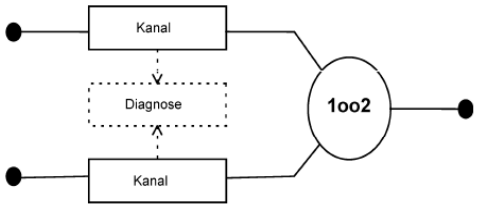
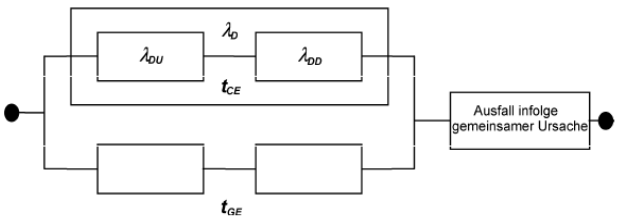
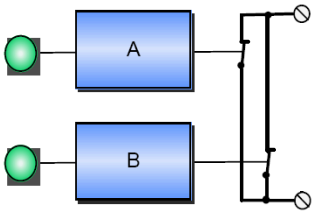


Bild B.6 – Blockschaltbild für 1oo2



Aufbau und Zuverlässigkeit → Architektur 2oo2



HFT = 0

2-kanaliger Aufbau – Die Kontakte sind parallel geschaltet

Beide Kanäle müssen zur Ausführung der sicherheitstechnischen Funktion schalten d. h. wenn ein Kanal defekt ist, wird die Sicherheitsfunktion außer Kraft gesetzt → Erhöhung der Betriebsverfügbarkeit

Aufbau und Zuverlässigkeit → Architektur 2oo2

Quelle DIN EN 61508

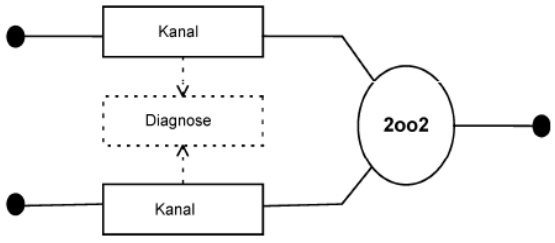
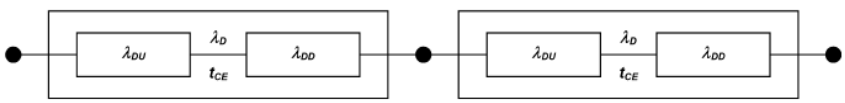
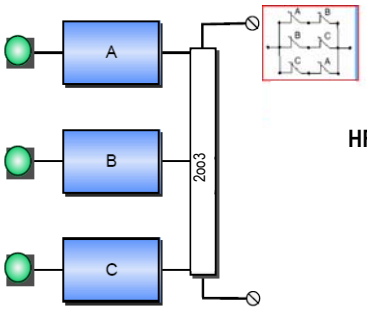


Bild B.8 – Blockschaltbild für 2oo2



Aufbau und Zuverlässigkeit → Architektur 2oo3



HFT = 1

3-kanaliger Aufbau

Mindestens 2 Kanäle müssen funktionstüchtig sein, damit die sicherheitstechnische funktioniert → Erhöhung der Betriebsverfügbarkeit

Der Ausfall eines Kanals hat keinen Einfluss auf die Sicherheitsfunktion→ Erhöhung der Sicherheit

Aufbau und Zuverlässigkeit → Architektur 2oo3

Quelle DIN EN 61508

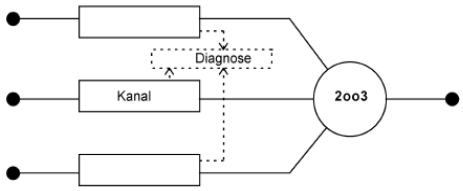
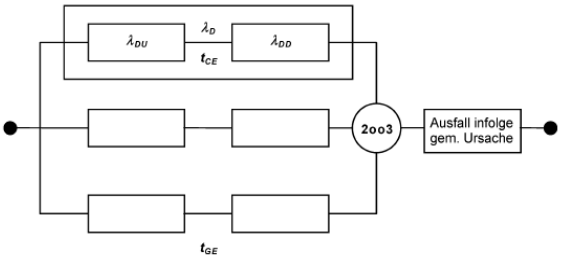


Bild B.12 – Blockschaltbild für 2oo3



Zusammenfassung

- Je nach Anforderung können unterschiedliche Architekturen realisiert werden
- Bei Anlagen, die Verfügbar sein müssen hat sich die 2oo3 Architektur durchgesetzt
- Zur Erhöhung der Sicherheit kann durch Einsatz von Gerätediversitären Komponenten der systematische Fehler reduziert werden

6. Rechnerischer Nachweis der funktionalen Sicherheit

Referent : Hans-Dieter Schwender
TÜV-SÜD Industrieservice

Safety Instrumented System (SIS)

- Es werden alle Komponenten, welche an der Sicherheits- oder Schutzfunktion beteiligt sind, hinsichtlich ihres Ausfallverhaltens betrachtet.

- Das gesamte sicherheitstechnisch System wird als **SIS** (**s**afety **i**ntegrated **s**ystem) bezeichnet

SIS

Was ist zu beachten

- Das SIS wird als Gesamtheit betrachtet
- Auch die Prozessanbindung ist zu betrachten
- Der „SIL-Level“ ist keine Geräteeigenschaft, sondern die Anforderung an das SIS
- Die Ausfallwahrscheinlichkeit und damit die erreichte „SIL-Stufe“ muss rechnerisch nachgewiesen werden
- Hierzu werden die einzelnen Ausfallwahrscheinlickkeiten miteinander verknüpft
- Das schwächste Glied der SIS-Kette bestimmt die Qualität des SIS

Bewertung der SIS-Kette

Um die Ausfallrate des Systems zu ermitteln müssen beachtet werden:

- HFT OK
- SFF OK
- Fehlerraten (PFD) OK

Wie erhalte ich die entsprechenden Werte:

HFT: Herstellerangabe bei einkanaligen Systemen

SFF: Herstellerangabe bzw. rechnerische Ermittlung aus den angegebenen λ-Werten:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_{Total}}$$

Mit $\lambda_{Total} = \lambda_S + \lambda_D$

Und $\lambda_D = \lambda_{DD} + \lambda_{DU}$; $\lambda_S = \lambda_{SD} + \lambda_{SU}$

PFD: Rechnerischer Nachweis mit Herstellerangaben λ_{DU} , β, DC, und der Festlegung des Prüfintervalls T_1

Das Prinzip der SIL (nach EN 61508)

HFT = Hardware Failure Tolerance (Hardwarefehlertoleranz)
SFF = Safe Failure Fraktion (Anteil sicherer ungefährlicher Ausfälle)
PFD = Probability of Failure on Demand (Ausfallwahrscheinlichkeit)

SFF \ HFT	0	1	2
< 60%	-----	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

Fehlerbeherrschung

Fehlererkennung

Tabelle für Gerätetyp B

PFD

10^{-2} ... 10^{-1}	SIL 1
10^{-3} ... 10^{-2}	SIL 2
10^{-4} ... 10^{-3}	SIL 3
10^{-5} ... 10^{-4}	SIL 4

Das Prinzip der SIL (nach EN 61511)

HFT = Hardware Failure Tolerance (Hardwarefehlertoleranz)

PFD = Probability of Failure on Demand (Ausfallwahrscheinlichkeit)

SIL	Hardware-Fehlertoleranz		
	0	1	2
1	X		
2 (Low Demand)	X		
2 (High Demand)		X	
3		X	
4			X

Fehlerbeherrschung

PFD

10^{-2} ... 10^{-1}	SIL 1
10^{-3} ... 10^{-2}	SIL 2
10^{-4} ... 10^{-3}	SIL 3
10^{-5} ... 10^{-4}	SIL 4

Ausfallwahrscheinlichkeit

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{ST}$$

Dabei gilt:

PFD_{SYS} die mittlere Ausfallwahrscheinlichkeit der Sicherheitsfunktion des E/E/EP-Systems

PFD_S die mittlere Ausfallwahrscheinlichkeit des Sensors

PFD_L die mittlere Ausfallwahrscheinlichkeit der Logik

PFD_{ST} die mittlere Ausfallwahrscheinlichkeit des Stellgliedes

Formeln nach EN 61508-6

da $\lambda_D t_{CE} << 1$

1oo1 $PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$ $\quad t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

1oo2 $PFD_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$

$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

2oo2 $PFD_G = 2\lambda_D t_{CE}$

2oo3 $PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$

$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

Formeln nach EN 61508-6 basierend auf PFD-Werte

1oo1

1oo2 $PFD \approx 4/3 * PFD_{1oo1}^2 + \beta * PFD_{1oo1}$

2oo2 $PFD \approx 2 * PFD_{1oo1}^3 + \beta * PFD_{1oo1}$

2oo3 $PFD \approx 4 * PFD_{1oo1}^2 + \beta * PFD_{1oo1}$

Formeln nach VDE 2180

1oo1 $PFD \approx ½ * \lambda_{DU} * T_1$

1oo2 $PFD \approx ⅓ * \lambda_{DU}^2 * T_1^2 + \beta * ½ * \lambda_{DU} * T_1$

2oo2 $PFD \approx \lambda_{DU} * T_1$

2oo3 $PFD \approx \lambda_{DU}^2 * T_1^2 + \beta * ½ * \lambda_{DU} * T_1$

Berechung weiterer Architekturen

MooN $PFD \approx (1+x)^n = 1 + \frac{nx}{1!} + \frac{N!}{(M-1)! * (N-M+2)!} * \lambda_{DU}^{N-M+1} * T_1^{N-M+1} + \beta \frac{\lambda_{DU}}{2} * T_1$

Bei M = N kann der β-Term auf 0 gesetzt werden

Ermittlung der effektiven Fehlerrate bei Gerätediversität

$$\lambda_{eff,1oo2} = \sqrt{\lambda_1 \lambda_2}$$

$$\lambda_{eff,1oo3} = \sqrt[3]{\lambda_1 \lambda_2 \lambda_3}$$

$$\lambda_{eff,2oo2} = \frac{1}{2} \cdot (\lambda_1 + \lambda_2)$$

$$\lambda_{eff,2oo3} = \sqrt{\frac{1}{3} \cdot (\lambda_1 \lambda_2 + \lambda_1 \lambda_3 + \lambda_2 \lambda_3)}$$

$$\lambda_{eff,2oo4} = \sqrt[3]{\frac{1}{4} \cdot (\lambda_1 \lambda_2 \lambda_3 + \lambda_1 \lambda_2 \lambda_4 + \lambda_1 \lambda_3 \lambda_4 + \lambda_2 \lambda_3 \lambda_4)}$$

Formeln mit der Berücksichtigung der Prüftiefe n. VDIVDE2180 1oo1

Kanal A:

$\lambda_{0,A} = PTC_{0,A} * \lambda_{DU,A}$

$\lambda_{1,A} = (PTC_{1,A} - PTC_{0,A}) * \lambda_{DU,A}$

$\lambda_{2,A} = (1 - PTC_{1,A}) * \lambda_{DU,A}$

Berechnung:

$PFD \approx \lambda_{0,A} * T_0/2 + \lambda_{1,A} * T_1/2 + \lambda_{2,A} * T_2/2$

Formeln mit der Berücksichtigung der Prüftiefe n. VDIVDE2180 1oo2

1oo2

Kanal A / channel A:

$$\lambda_{0,A} = PTC_{0,A} \cdot \lambda_{DU,A}$$
$$\lambda_{1,A} = \left(PTC_{1,A} - PTC_{0,A}\right)\lambda_{DU,A}$$
$$\lambda_{2,A} = \left(1 - PTC_{1,A}\right)\lambda_{DU,A}$$

Kanal B / channel B:

$$\lambda_{0,B} = PTC_{0,B} \cdot \lambda_{DU,B}$$
$$\lambda_{1,B} = \left(PTC_{1,B} - PTC_{0,B}\right)\lambda_{DU,B}$$
$$\lambda_{2,B} = \left(1 - PTC_{1,B}\right)\lambda_{DU,B}$$

Beitrag zum Ausfall mit gemeinsamer Ursache / common cause contribution:

$$PTC_{0,avg} = \frac{PTC_{0,A} + PTC_{0,B}}{2}$$
$$PTC_{1,avg} = \frac{PTC_{1,A} + PTC_{1,B}}{2}$$

$$\lambda_{0,avg} = PTC_{0,avg} \cdot \min\left\{\lambda_{DU,A}, \lambda_{DU,B}\right\}$$
$$\lambda_{1,avg} = \left(PTC_{1,avg} - PTC_{0,avg}\right) \cdot \min\left\{\lambda_{DU,A}, \lambda_{DU,B}\right\}$$
$$\lambda_{2,avg} = \left(1 - PTC_{1,avg}\right) \cdot \min\left\{\lambda_{DU,A}, \lambda_{DU,B}\right\}$$

Berechnung der *PFD* / calculation of *PFD*:

$$P_{K,A} = (1-\beta)\left[\lambda_{0,A}\frac{T_0}{2} + \lambda_{0,A}\frac{T_1}{2} + \lambda_{0,A}\frac{T_2}{2}\right]$$
$$P_{K,B} = (1-\beta)\left[\lambda_{0,B}\frac{T_0}{2} + \lambda_{0,B}\frac{T_1}{2} + \lambda_{0,B}\frac{T_2}{2}\right]$$
$$PFD_{1oo2} = (1-\beta)\left[\left(P_{K,A}\lambda_{0,B} + P_{K,B}\lambda_{0,A}\right)\frac{T_0}{3} + \left(P_{K,A}\lambda_{1,B} + P_{K,B}\lambda_{1,A}\right)\frac{T_1}{3} + \left(P_{K,A}\lambda_{2,B} + P_{K,B}\lambda_{2,A}\right)\frac{T_2}{3}\right]$$
$$+ \beta\left(\frac{T_0}{2}\lambda_{0,avg} + \frac{T_1}{2}\lambda_{1,avg} + \frac{T_2}{2}\lambda_{2,avg}\right)$$

Formeln mit der Berücksichtigung der Prüftiefe n. VDIVDE2180 1oo3

1oo3

Kanal A / channel A:

$$\lambda_{0,A} = PTC_{0,A} \cdot \lambda_{DU,A}$$
$$\lambda_{1,A} = \left(PTC_{1,A} - PTC_{0,A}\right)\lambda_{DU,A}$$
$$\lambda_{2,A} = \left(1 - PTC_{1,A}\right)\lambda_{DU,A}$$

Kanal B / channel B:

$$\lambda_{0,B} = PTC_{0,B} \cdot \lambda_{DU,B}$$
$$\lambda_{1,B} = \left(PTC_{1,B} - PTC_{0,B}\right)\lambda_{DU,B}$$
$$\lambda_{2,B} = \left(1 - PTC_{1,B}\right)\lambda_{DU,B}$$

Kanal C / channel C:

$$\lambda_{0,C} = PTC_{0,C} \cdot \lambda_{DU,C}$$
$$\lambda_{1,C} = \left(PTC_{1,C} - PTC_{0,C}\right)\lambda_{DU,C}$$
$$\lambda_{2,C} = \left(1 - PTC_{1,C}\right)\lambda_{DU,C}$$

Beitrag zum Ausfall mit gemeinsamer Ursache / common cause contribution:

$$PTC_{0,avg} = \frac{PTC_{0,A} + PTC_{0,B} + PTC_{0,C}}{3}$$

$$PTC_{1,avg} = \frac{PTC_{1,A} + PTC_{1,B} + PTC_{1,C}}{3}$$

$$\lambda_{0,avg} = PTC_{0,avg} \cdot \min\left\{\lambda_{DU,A}, \lambda_{DU,B}, \lambda_{DU,C}\right\}$$
$$\lambda_{1,avg} = \left(PTC_{1,avg} - PTC_{0,avg}\right) \cdot \min\left\{\lambda_{DU,A}, \lambda_{DU,B}, \lambda_{DU,C}\right\}$$
$$\lambda_{2,avg} = \left(1 - PTC_{1,avg}\right) \cdot \min\left\{\lambda_{DU,A}, \lambda_{DU,B}, \lambda_{DU,C}\right\}$$

Formeln mit der Berücksichtigung der Prüftiefe n. VDIVDE2180 1oo3

Berechnung der *PFD* / calculation of *PFD*:

$$P_{\mathrm{K.AB}} = \left(1-\frac{1}{2}\beta\right)\left[\left(P_{\mathrm{K.A}}\lambda_{0,\mathrm{B}} + P_{\mathrm{K.B}}\lambda_{0,\mathrm{A}}\right)\frac{T_0}{3} + \left(P_{\mathrm{K.A}}\lambda_{1,\mathrm{B}} + P_{\mathrm{K.B}}\lambda_{1,\mathrm{A}}\right)\frac{T_1}{3} + \left(P_{\mathrm{K.A}}\lambda_{2,\mathrm{B}} + P_{\mathrm{K.B}}\lambda_{2,\mathrm{A}}\right)\frac{T_2}{3}\right]$$

$$P_{\mathrm{K.BC}} = \left(1-\frac{1}{2}\beta\right)\left[\left(P_{\mathrm{K.B}}\lambda_{0,\mathrm{C}} + P_{\mathrm{K.C}}\lambda_{0,\mathrm{B}}\right)\frac{T_0}{3} + \left(P_{\mathrm{K.B}}\lambda_{1,\mathrm{C}} + P_{\mathrm{K.C}}\lambda_{1,\mathrm{B}}\right)\frac{T_1}{3} + \left(P_{\mathrm{K.B}}\lambda_{2,\mathrm{C}} + P_{\mathrm{K.C}}\lambda_{2,\mathrm{B}}\right)\frac{T_2}{3}\right]$$

$$P_{\mathrm{K.AC}} = \left(1-\frac{1}{2}\beta\right)\left[\left(P_{\mathrm{K.A}}\lambda_{0,\mathrm{C}} + P_{\mathrm{K.C}}\lambda_{0,\mathrm{A}}\right)\frac{T_0}{3} + \left(P_{\mathrm{K.A}}\lambda_{1,\mathrm{C}} + P_{\mathrm{K.C}}\lambda_{1,\mathrm{A}}\right)\frac{T_1}{3} + \left(P_{\mathrm{K.A}}\lambda_{2,\mathrm{C}} + P_{\mathrm{K.C}}\lambda_{2,\mathrm{A}}\right)\frac{T_2}{3}\right]$$

$$P_{\mathrm{K.A}} = \left(1-\frac{1}{2}\beta\right)\left(\lambda_{0,\mathrm{A}}\frac{T_0}{2} + \lambda_{1,\mathrm{A}}\frac{T_1}{2} + \lambda_{2,\mathrm{A}}\frac{T_2}{2}\right)$$

$$P_{\mathrm{K.B}} = \left(1-\frac{1}{2}\beta\right)\left(\lambda_{0,\mathrm{B}}\frac{T_0}{2} + \lambda_{1,\mathrm{B}}\frac{T_1}{2} + \lambda_{2,\mathrm{B}}\frac{T_2}{2}\right)$$

$$P_{\mathrm{K.C}} = \left(1-\frac{1}{2}\beta\right)\left(\lambda_{0,\mathrm{C}}\frac{T_0}{2} + \lambda_{1,\mathrm{C}}\frac{T_1}{2} + \lambda_{2,\mathrm{C}}\frac{T_2}{2}\right)$$

$$PFD_{1oo3} = \left(1-\frac{1}{2}\beta\right)\left[\begin{array}{l}\left(P_{\mathrm{K.BC}}\lambda_{0,\mathrm{A}} + P_{\mathrm{K.AC}}\lambda_{0,\mathrm{B}} + P_{\mathrm{K.AB}}\lambda_{0,\mathrm{C}}\right)\frac{T_0}{4} \\ + \left(P_{\mathrm{K.BC}}\lambda_{1,\mathrm{A}} + P_{\mathrm{K.AC}}\lambda_{1,\mathrm{B}} + P_{\mathrm{K.AB}}\lambda_{1,\mathrm{C}}\right)\frac{T_1}{4} + \left(P_{\mathrm{K.BC}}\lambda_{2,\mathrm{A}} + P_{\mathrm{K.AC}}\lambda_{2,\mathrm{B}} + P_{\mathrm{K.AB}}\lambda_{2,\mathrm{C}}\right)\frac{T_2}{4}\end{array}\right] + \frac{1}{2}\beta\left(\frac{T_0}{2}\lambda_{0,\mathrm{avg}} + \frac{T_1}{2}\lambda_{1,\mathrm{avg}} + \frac{T_2}{2}\lambda_{2,\mathrm{avg}}\right)$$

Formeln mit der Berücksichtigung der Prüftiefe n. VDIVDE2180 2oo2

2oo2

Kanal A / channel A:

$$\lambda_{0,\mathrm{A}} = PTC_{0,\mathrm{A}} \cdot \lambda_{\mathrm{DU,A}}$$

$$\lambda_{1,\mathrm{A}} = \left(PTC_{1,\mathrm{A}} - PTC_{0,\mathrm{A}}\right)\lambda_{\mathrm{DU,A}}$$

$$\lambda_{2,\mathrm{A}} = \left(1 - PTC_{1,\mathrm{A}}\right)\lambda_{\mathrm{DU,A}}$$

Kanal B / channel B:

$$\lambda_{0,\mathrm{B}} = PTC_{0,\mathrm{B}} \cdot \lambda_{\mathrm{DU,B}}$$

$$\lambda_{1,\mathrm{B}} = \left(PTC_{1,\mathrm{B}} - PTC_{0,\mathrm{B}}\right)\lambda_{\mathrm{DU,B}}$$

$$\lambda_{2,\mathrm{B}} = \left(1 - PTC_{1,\mathrm{B}}\right)\lambda_{\mathrm{DU,B}}$$

Berechnung der *PFD* / calculation of *PFD*:

$$PFD_{2oo2} \approx \left(\lambda_{0,\mathrm{A}}\frac{T_0}{2} + \lambda_{1,\mathrm{A}}\frac{T_1}{2} + \lambda_{2,\mathrm{A}}\frac{T_2}{2}\right) + \left(\lambda_{0,\mathrm{B}}\frac{T_0}{2} + \lambda_{1,\mathrm{B}}\frac{T_1}{2} + \lambda_{2,\mathrm{B}}\frac{T_2}{2}\right)$$

Formeln mit der Berücksichtigung der Prüftiefe n. VDIVDE2180 2oo3

2oo3

Kanal A / channel A:

$$\lambda_{0,A} = PTC_{0,A} \cdot \lambda_{DU,A}$$
$$\lambda_{1,A} = \left(PTC_{1,A} - PTC_{0,A}\right)\lambda_{DU,A}$$
$$\lambda_{2,A} = \left(1 - PTC_{1,A}\right)\lambda_{DU,A}$$

Kanal B / channel B:

$$\lambda_{0,B} = PTC_{0,B} \cdot \lambda_{DU,B}$$
$$\lambda_{1,B} = \left(PTC_{1,B} - PTC_{0,B}\right)\lambda_{DU,B}$$
$$\lambda_{2,B} = \left(1 - PTC_{1,B}\right)\lambda_{DU,B}$$

Kanal C / channel C:

$$\lambda_{0,C} = PTC_{0,C} \cdot \lambda_{DU,C}$$
$$\lambda_{1,C} = \left(PTC_{1,C} - PTC_{0,C}\right)\lambda_{DU,C}$$
$$\lambda_{2,C} = \left(1 - PTC_{1,C}\right)\lambda_{DU,C}$$

Beitrag zum Ausfall mit gemeinsamer Ursache / common cause contribution:

$$PTC_{0,avg} = \frac{PTC_{0,A} + PTC_{0,B} + PTC_{0,C}}{3} \qquad PTC_{1,avg} = \frac{PTC_{1,A} + PTC_{1,B} + PTC_{1,C}}{3}$$

$$\lambda_{0,avg} = PTC_{0,avg} \cdot \min\left\{\lambda_{DU,A}, \lambda_{DU,B}, \lambda_{DU,C}\right\}$$
$$\lambda_{1,avg} = \left(PTC_{1,avg} - PTC_{0,avg}\right) \cdot \min\left\{\lambda_{DU,A}, \lambda_{DU,B}, \lambda_{DU,C}\right\}$$
$$\lambda_{2,avg} = \left(1 - PTC_{1,avg}\right) \cdot \min\left\{\lambda_{DU,A}, \lambda_{DU,B}, \lambda_{DU,C}\right\}$$

Formeln mit der Berücksichtigung der Prüftiefe n. VDIVDE2180 2oo3

Berechnung der *PFD* / calculation of *PFD*:

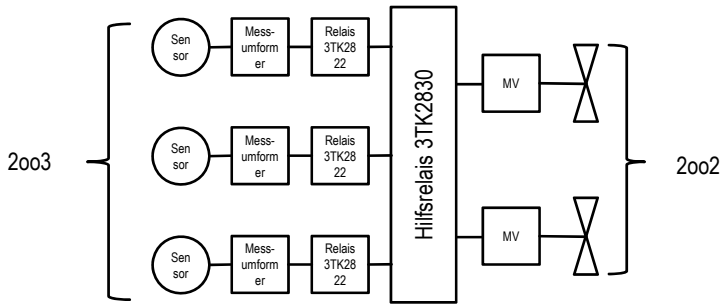
$$P_{K,AB} = \left(1 - \frac{3}{2}\beta\right)\left[\left(\lambda_{0,A}\frac{T_0}{2} + \lambda_{1,A}\frac{T_1}{2} + \lambda_{2,A}\frac{T_2}{2}\right) + \left(\lambda_{0,B}\frac{T_0}{2} + \lambda_{1,B}\frac{T_1}{2} + \lambda_{2,B}\frac{T_2}{2}\right)\right]$$
$$P_{K,BC} = \left(1 - \frac{3}{2}\beta\right)\left[\left(\lambda_{0,B}\frac{T_0}{2} + \lambda_{1,B}\frac{T_1}{2} + \lambda_{2,B}\frac{T_2}{2}\right) + \left(\lambda_{0,C}\frac{T_0}{2} + \lambda_{1,C}\frac{T_1}{2} + \lambda_{2,C}\frac{T_2}{2}\right)\right]$$
$$P_{K,AC} = \left(1 - \frac{3}{2}\beta\right)\left[\left(\lambda_{0,A}\frac{T_0}{2} + \lambda_{1,A}\frac{T_1}{2} + \lambda_{2,A}\frac{T_2}{2}\right) + \left(\lambda_{0,C}\frac{T_0}{2} + \lambda_{1,C}\frac{T_1}{2} + \lambda_{2,C}\frac{T_2}{2}\right)\right]$$

$$PFD_{2oo3} = \left(1 - \frac{3}{2}\beta\right)\left[\begin{array}{l}\left(P_{K,BC}\lambda_{0,A} + P_{K,AC}\lambda_{0,B} + P_{K,AB}\lambda_{0,C}\right)\frac{T_0}{3} \\ + \left(P_{K,BC}\lambda_{1,A} + P_{K,AC}\lambda_{1,B} + P_{K,AB}\lambda_{1,C}\right)\frac{T_1}{3} + \left(P_{K,BC}\lambda_{2,A} + P_{K,AC}\lambda_{2,B} + P_{K,AB}\lambda_{2,C}\right)\frac{T_2}{3}\end{array}\right] + \frac{3}{2}\beta\left(\frac{T_0}{2}\lambda_{0,avg} + \frac{T_1}{2}\lambda_{1,avg} + \frac{T_2}{2}\lambda_{2,avg}\right)$$

Einheiten

PFD	→ Dimensionslos
λ	→ 1/h oder
FIT	→ 10^{-9} 1/h
T1	→ h
t_{CE}, t_{GE}, T_{G2E}	→ h
MRT, MTTR	→ h
β	→ Dimensionslos

Blockschaltbild vereinfachen



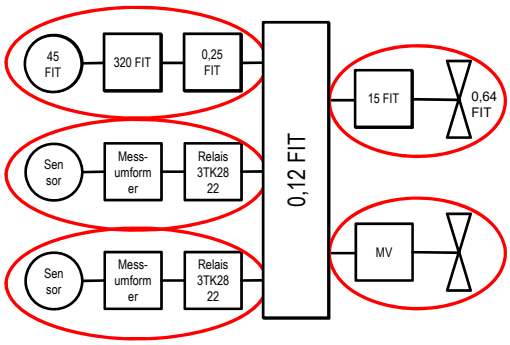
Blockschaltbild vereinfachen

Fiktiv angenommene Werte

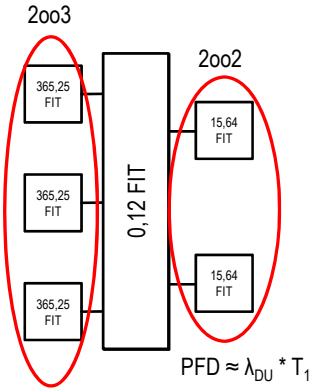
Gerät	λ_{DU}
Sensor	45 FIT
Messumformer	320 FIT
Sicherheitsrelais 3TK2822	0,25 FIT
Sicherheitsrelais 3TK2830	0,12 FIT
Magnetventil	15 FIT
Prozessventil	0,64 FIT

1 FIT ≙ 10^{-9}

Blockschaltbild vereinfachen



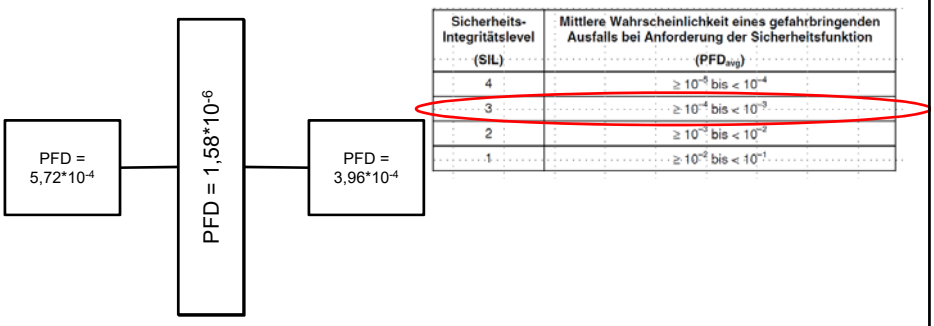
Blockschaltbild vereinfachen



$$PFD \approx \lambda_{DU}^2 * T_1^2 + \beta * ½ * \lambda_{DU} * T_1$$

Blockschaltbild vereinfachen

Mit T1 = 8760 h (1 Jahr), $\boldsymbol{\beta}$ = 10%, die Reparaturzeit ist vernachlässigbar kurz und die Ausfallraten sind konstant gilt:



Sicherheits-Integritätslevel (SIL)	Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion (PFD_{avg})
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$

$PFDges = \Sigma PFD = 0{,}97*10^{-3}$ ➡ **SIL 3**

Aber Achtung HFT der Aktoren beachten ➡ **SIL 2**

Zusammenfassung

- Betrachtung erfolgt für das gesamte SIS
- Das schwächste Glied der SIS-Kette bestimmt die Qualität des Kreises
- Bei der Bewertung des SIS müssen HFT, SFF und PFD die Anforderung erfüllen
- Bei der Berechnung sollten Blockschaltbilder erstellt und dann vereinfacht werden
- Vereinfachte Formeln sind in der VDI/VDE 2180 angegeben

7. Ermittlung der Kerndaten

Referent : Hans-Dieter Schwender
TÜV-SÜD Industrieservice

Nachweis der Zuverlässigkeit

- Die Normreihe 61508 fordert **KEINE** Zertifikate für Komponenten. Sie fordert den Nachweis der Zuverlässigkeit und Eignung für die Applikation
- Ein Zertifikat alleine ist **KEIN** ausreichender Nachweis für die Zuverlässigkeit und Eignung für eine Applikation
- Der zum Zertifikat gehörende Report gibt dem Designer eines Sicherheitskreise die notwendigen Zuverlässigkeitsdaten, um den Sicherheitskreis zu planen
- Der Report muss zeigen, wie die Daten ermittelt wurden
- Der Report muss die Grenzen der Anwendbarkeit der Daten aufzeigen
- Der Report muss Einschränkungen und Bedingungen darlegen

Kerndaten

- Sicherheitshandbuch der Hersteller
- Berichte der Prüforganisationen zu den Zertifikaten
- Eigen erstellte FMEDA-Untersuchungen nach EN 61508
- Der Betreiber über Betriebsbewährung (Bildung von Typicals)

Herstellererklärung 2

Kolbenschieberventil
Elektromagnetisch
betätigt

Herstellererklärung 3

3/2 Wege Sitzventil
Pneumatisch betätigt

Neue Bewertung 3/2, 5/2. 5/3 Kolbenschieberventil

- Anschluss: 1/4" oder 1/2" ISO G/NPT
- Für einfach- und doppeltwirkende Stellantriebe
- TÜV-Gutachten, basierend auf Baumusterprüfung nach DIN EN 161, DIN 3394 & IEC 61 508
- Verwendung von monostabilen Ventilen in sicherheitsgerichteten Systemen bis SIL 3
- Überschneidungsfreie Anschlüsse
- Handhilfsbetätigung nachrüstbar
- Für Freiluftmontage mit erschwerten Umgebungsbedingungen geeignet (Magnetsystem beachten)
- Die Ventile sind mit Magneten in den Zündschutzarten Ex e mb, Ex d mb, Ex mb, Ex ia in den Zonen 1 & 2 (Gase),), 21 & 22 (Stäube), ATEX cat. II 2GD
- Internationale Zulassungen: IEC Ex, FM, CSA weitere auf Anfrage

Technische Merkmale

Betriebsmedium:
Gefilterte, ölfreie und getrocknete Druckluft, Instrumentenluft, Stickstoff und andere neutrale, nicht brennbare trockene Fluide
Elektropneumatisch, indirekt gesteuert
Betriebsdruck:
2,5 ... 8 bar (36 ... 116 psi) bei interner Steuerluftversorgung
0 ... 8 bar (0 ... 116 psi) bei externer Steuerluftversorgung (G 1/2, 1/2 NPT oder bei Low-Power-Pilotsystem)

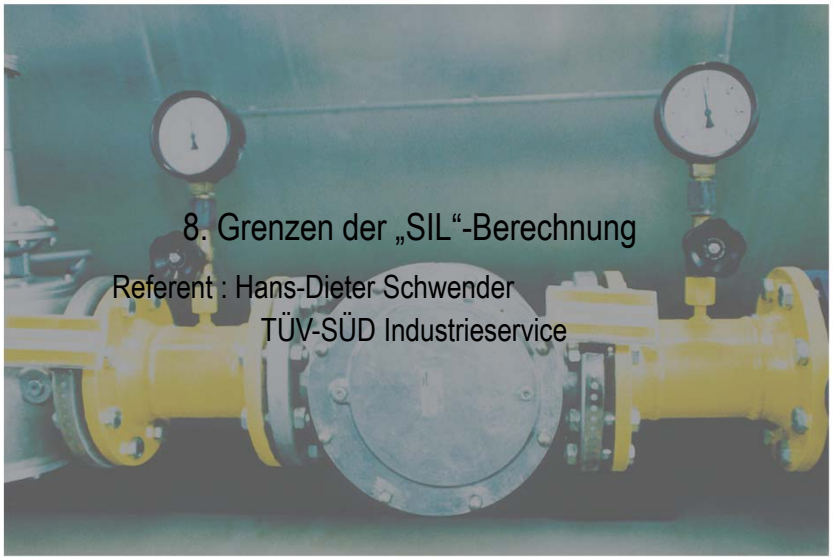
Nennweite:
DN 6 oder DN 8
Anschluss:
G 1/4, 1/4 NPT, G 1/2, 1/2 NPT
NAMUR-Ranschbild
Einbaulage:
Beliebig, Impulsventile vorzugsweise waagerecht

Umgebungs-/ Mediumtemperatur:
Ventil:
-40° ... +65°C (-40° ... +149°F) (Spezial NBR)
-25° ... +80°C (-13° ... +176°F) (HNBR)
Abhängig vom Magnetsystem
Um das Einfrieren der Teile zu vermeiden, muss die Druckluft unter +2°C (+35°F) frei von Feuchtigkeit sein. Bei Freiluftmontage alle Anschlüsse vor Eindringen von Feuchtigkeit schützen.

Material:
Ventilgehäuse: Aluminium 3.0615 mit Oberflächenbehandlung geeignet für harte Umgebungsbedingungen (Geprüft nach DIN 50018: Beanspruchung im Kondenswasser-Wechselklima mit schwefelhaltiger Atmosphäre, DIN 50021/ASTM B117-73: Salzsprühnebelprüfung mit verschiedenen Natriumchloridlösungen, Auslagerung in ammoniakhaltiger Atmosphäre)Messing 2.0401 (Ms 58), Edelstahl 1.4404 (316 L)
Dichtungen: NBR (Sonder-Perbunan) oder HNBR

Zusammenfassung

- Ein zertifizierter Anspruch, dass eine Komponente „SIL…“ ist, bedeutet **nicht automatisch**, dass hierdurch der Sicherheitskreis auch dieses „SIL…“ hat denn;
- SIL ist keine Geräteeigenschaft
- Sondern die Anforderung an einen kompletten Schutzkreis
- Es kann durchaus der Fall sein, dass ein Schutzkreis, in dem alle Komponenten eine „SIL 3“ Eigenschaft haben, lediglich „SIL 2“ oder sogar nur „SIL 1“ erreicht!



8. Grenzen der „SIL“-Berechnung

Referent : Hans-Dieter Schwender
TÜV-SÜD Industrieservice

Was ist, wenn..

- ... eine Komponente keine Kenndaten hat
- … eine rein mech. Komponente eingesetzt ist (Aktor)
- … baumustergeprüfte Geräte eingesetzt werden

Eignung der Komponenten

- Nachweis durch den Hersteller
- Eignungsnachweis durch Betriebsbewährung (proven in use)
- Nachweis durch den Betreiber (Betreiber-Erklärung) → Einsatz in SIS bis SIL 2 einkanalig möglich
- Nachweis durch Baumusterprüfung → Einsatz in SIS bis SIL 2 einkanalig möglich

Nachweis durch den Hersteller

- Eignungsnachweis durch Zertifizierung
  - Auf welcher Datenbasis wurde die Einstufung vorgenommen
  - Wie wurden die Daten ermittelt
  - Welche Auflagen sind mit dem Einsatz verbunden?

Eignungsnachweis durch Betriebsbewährung

- Def. nach DIN EN 61511-1:
  „eine Komponente ist betriebsbewährt, wenn eine entsprechend dokumentierte Untersuchung ergeben hat, dass Nachweise aus früheren Einsätzen belegen, dass die Komponente für den Einsatz in einem sicherheitstechnischen System geeignet ist

- Datenerfassung z.B. nach Namur-Empfehlung NE 93

Störungserfassung für PLT-Schutzeinrichtungen

Firma: _____ Bau: _____ Betrieb: _____

PLT-Stelle: _____ **Risikobereich:** O I O II

Grund: O betriebl. Störungsmeldung O planmäßige IH-Tätigkeit
Fehlerort: O Anregeteil O Signalverarbeitung O Auslöseteil

Ursache: O Gerätebedingt (Bsp.: Fehlfunktion, dejustiert, gestört, etc.)
O Prozessbedingt (Bsp.: chem. beschädigt, verstopft, etc.)
O Sonstige (Bsp.: mech. beschädigt, Bedienungsfehler, etc.)

Fehleranalyse:

Unterscheidung Betriebsbewährung (prior use) und proven in use

Prior use:

- Der **Anwender** dokumentiert, dass das Gerät eine befriedigende Leistung in einer ähnlichen Betriebsumgebung erreicht hat. Das Verständnis dafür, wie sich das Betriebsmittel in einer bestimmten Betriebsumgebung verhält, ist erforderlich, um mit hoher Gewissheit annehmen zu können, dass der beabsichtigte Entwurf, die Sichtprüfung, Prüfung, Instandhaltung und betriebliche Praxis ausreichend sind

Proven in use:

Die Betriebsbewährung des **Herstellers** (en: proven in use) beruht auf dessen Entwurfsgrundlagen (z. B. Temperaturgrenzen, Vibrationsgrenzen, Korrosionsgrenzen, gewünschte Instandhaltungsunterstützung) für sein Gerät.

Durchführung der Betriebsbewährung

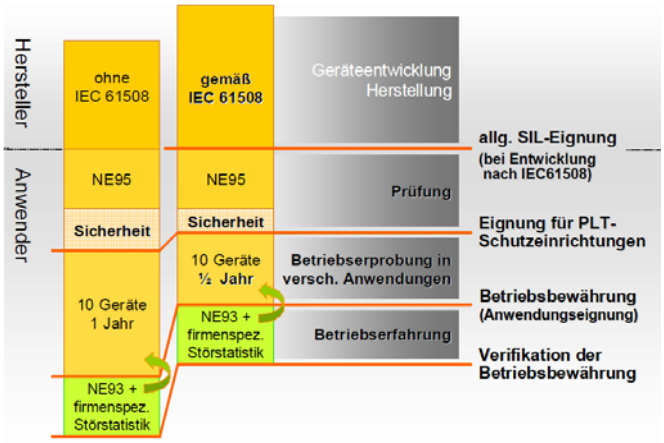
- Nachweis der SIL Eignung (Zertifiziert oder nicht zertifiziert nach DIN EN 61508)
- Nachweis der Eignung zum Einsatz in PLT-Sicherheitseinrichtungen
  - Überprüfung von Konstruktion, Meßgenauigkeit, Erfahrungsrücklauf, Geräteunterlagen…
  - Überprüfung der sicherheitstechnische Aspekte
- Nachweis der Betriebsbewährung (Betriebserprobung z.B. NE130)
  - mind. 10 verschiedene Anwendungen (ges. mind. 10^5 Betriebsstunden)
  - bei unterschiedlichen Prozessbedingungen
  - Dauer 1 Jahr
  - auch bei Vorlage eines Zertifikates nach DIN EN 61508 erforderlich
- Verifikation der Betriebsbewährung
  - Stördatenerfassung (z.B. nach NE93)
  - treten Störungen auf, welche die sicherheitstechn. Funktion beeinträchtigen, so kann die Betriebsbewährung zurückgezogen werden

Nachweis der Betriebsbewährung

- Berücksichtigung der Qualität, des Managements und des Konfigurationsmanagements beim Hersteller;
- geeignete Identifizierung und Spezifikation der Geräte;
- einen Nachweis der Leistungsfähigkeit der Geräte unter ähnlichen betrieblichen Randbedingungen
- den Umfang der Betriebserfahrung

Alle betriebsbewährte Geräte müssen durch eine Versionssnummer gekennzeichnet sein und einem Änderungsmanagement unterliegen. Bei Änderung am Gerät muss beurteilt werden, ob der Nachweis der Betriebsbewährung weiterhin gültig ist!

Betriebsbewährung nach NE 130



Verwendbarkeit in Sicherheitseinrichtung bei Betriebsbewährung

Struktur		Aktorteilsystem	
		1oo1	1oo2
Sensorteilsystem	1oo1	SIL 2	SIL 2
	1oo2	SIL 2	SIL 3
	2oo3	SIL 2	SIL 3

Tabelle 1: Maximal erreichbarer SIL einer PLT-Schutzeinrichtung bei Verwendung unterschiedlicher Strukturen

Kanalrichtwerte nach NE 130

Kanalart	Fehlerrate λ_{DU}	CCF (β)	T_1 (Empf.)
Sensor für p	$1 * 10^{-6}$	5%	8760 Stunden
Sensor für T	$5 * 10^{-7}$	5%	8760 Stunden
Sensor für L	$4 * 10^{-7}$	5%	8760 Stunden
Sensor für F	$1 * 10^{-6}$	5%	8760 Stunden
Aktor	$4 * 10^{-7}$	5%	8760 Stunden

Verweis der VDI/VDE 2180 Blatt 3 (Entw. 2018) Pkt. 8.2.2 auf die NE 130

Prüfintervall (ohne Daten nach DIN EN 61508)

Wenn keine Daten nach DIN EN 61508 vorliegen gibt die DIN EN 50156-1 Tabelle 1 eine Übersicht der vorgeschriebenen Prüfintervalle

Sicherheits-Integritätslevel	Konfiguration [a, c]	Betriebsintervall zwischen zwei Funktionsprüfungen	Diagnose-deckungsgrad
1	1oo1	≤ 1 Monat	kein
	1oo1	≤ 6 Monate	einfach
	1oo1	≤ 1 Jahr	mittel
	2oo2	≤ 1 Monat	kein
	2oo2	≤ 6 Monate	einfach
	2oo2	≤ 1 Jahr	mittel
2	1oo1	≤ 1 Monat	mittel
	1oo1	≤ 1 Jahr	hoch
	2oo2	≤ 1 Monat	mittel
	2oo2	≤ 1 Jahr	hoch
	1oo2	≤ 6 Monate	kein
	1oo2	≤ 1 Jahr	mittel
	2oo3	≤ 1 Monat	kein
	2oo3	≤ 1 Jahr	einfach
3			
	1oo2	≤ 1 Monat	kein[b] (nur Typ A)[e]
	1oo2	≤ 6 Monate	einfach[b]
	1oo2	≤ 1 Jahr	mittel[b]
	2oo3	≤ 1 Monat	kein[b] (nur Typ A)[e]
	2oo3	≤ 6 Monate	einfach[b]
	2oo3	< = 1 Jahr	mittel[b]

Fehlerausschluss

- Im Rahmen der DIN EN 61508, DIN EN 50156-1 und DIN EN ISO 13849-2 ist bei einfach aufgebauten Komponenten (z.B. Lastschütz, SDB…) auch ein Fehlerausschlussverfahren anwendbar.
- z.B nach EN 61511Pkt. 11.4.4
  „Bei der Bestimmung der erreichten HFT können bestimmte Fehler ausgeschlossen werden, vorausgesetzt dass ihre Auftrittswahr-scheinlichkeit sehr klein im Vergleich zu den Anforderungen an die Sicherheits-Integrität ist. Jeder derartige Ausschluss muss begründet und dokumentiert werden.
  ANMERKUNG Weitere Information zum Fehlerausschluss findet sich in ISO13849-1:2006 und ISO13849-2:2012“

Fehlerausschluss

- Hier werden:
  - Beschreibung des Ausfallmechanismus festgehalten
  - Bedingungen (Umgebung, Entwurf…) festgelegt
  - definierte Fehler ausgeschlossen
  - Einzelbetrachtung (begründet) durchgeführt
  - Dokumentation mit allen Randbedingungen erstellt

Fehlerausschluss nach DIN EN 50156-1

Bild 11 – Fehlerbewertung für den fest verdrahteten Teil eines sicherheitsbezogenen Systems

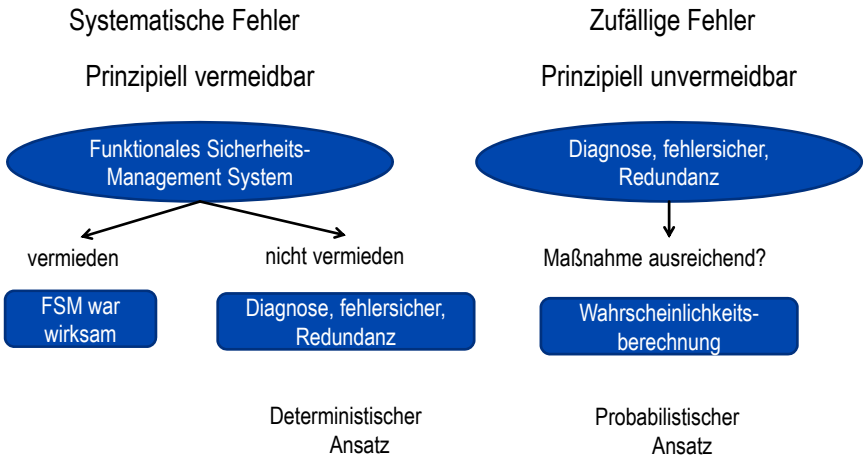
Maßnahmen zum Fehlerausschluss

- Überdimensionierung z.B. durch:
- Nennstrom der Schützkontakte max. 60 % des Nennstrom (I_N)
- Festlegung der Mindestschaltspiele (z.B. nach DIN EN 50156-1 ≥ 3 * 10^6 Schaltspiele)
- Das Schaltverhalten muss für AC 3 – Betrieb (Anlauf eines Drehstrommotors) ausgelegt sein
- Die Schaltung ist mit Sicherung gegen Überlastungen geschützt.
- Thermische Überwachung des Laststromes
- Stärkere Auslegung der Rückstellfeder bei Armaturen
- Ausfälle, welche nicht durch die Überdimensionierung erfasst werden, sind mittels einer FMEDA (failure modes effects and diagnostic analysis) zu analysieren.
  - D.h. zu erwartenden Ausfälle, deren Ursache und entsprechenden Gegenmaßnahmen sind zu dokumentieren
  - die Ausfallrate muss abgeschätzt werden.

Zusammenfassung

- Eignung der Komponenten kann erfolgen durch Hersteller, Betriebsbewährung, Baumusterprüfung
- Richtwerte sind in der NE 130 angegeben (nur begründet verwendbar)
- Fehlerausschlussverfahren möglich (Deterministik)

Fehlerunterscheidung



Definition der Fehlerarten nach DIN EN 61508-4

- **Systematischer Ausfall:**
  „Systematisches Versagen/Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Modifikation des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betreibens, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann“

- **Zufälliger Hardwareausfall:**
  „Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Mechanismen in der Hardware resultiert, die zu einer Verschlechterung der Eigenschaften der Bauteile führen“

Zur Unterscheidung ist folgende Frage hilfreich:
Ist der Ausfall reproduzierbar oder war der Fehler bereits bei der Inbetriebnahme vorhanden?

Unterschied zu el. Komponenten

- Mit der Ermittlung von Ausfällen kann nur dann auf die Wahrscheinlichkeit geschlossen werden, wenn die Ausfälle durch Zufallsprozesse hervorgerufen werden!
- Bei elektronischen Bauteilen sind Defekte nahezu immer Zufallsereignisse
- Softwarebedingte Fehlfunktionen sind nie Zufallsereignisse
- Das Versagen einer mechanischen Komponente kann je nach Betriebsart (HDM / LDM) zufällig oder systematisch bedingt sein.

Anforderungsrate bei mech. Komponenten

Niedrige Anforderungsrate:

- „Wer rastet der rostet“
- Versagen wie bei Software vergleichbar
- Keine Wahrscheinlichkeitsangabe möglich
- Fehlerausschluss mit Begründung möglich
- Im Normalfall ist keine probabilistische Betrachtung möglich

Meist systematisch !

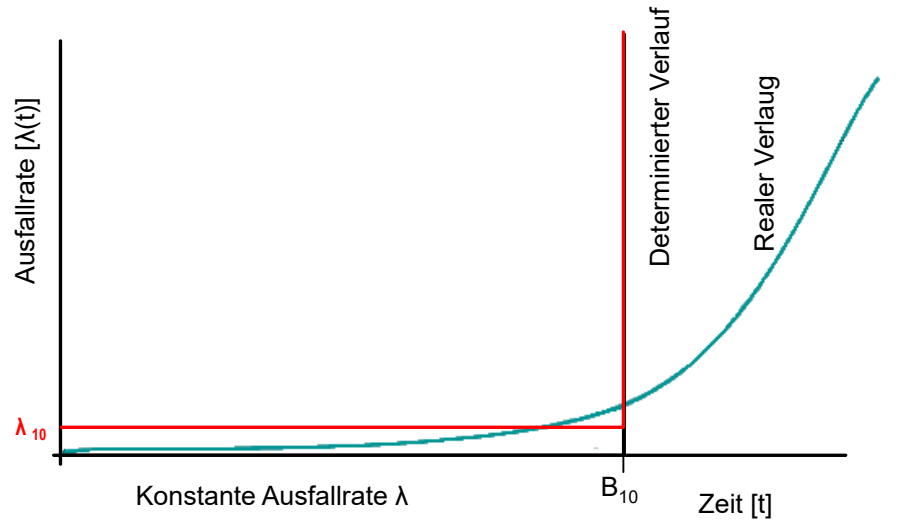
Anforderungsrate bei mech. Komponenten

Hohe Anforderungsrate:

- B_{10}-Wert kann zur Ermittlung einer konstanten Fehlerrate dienen
- Beschreibung mittels der Weibull-Verteilung möglich
- Ausfälle bzw. Defekte finden verschleißbedingt statt
- Lebensdauer ist nicht fest sondern eher Zufall
- Wartung ist essentiell (kein „gedächtnisloses“ System)

Meist Zufall !

Verschleiß



Ausfallrate mechanischer Komponenten

- Der B_{10}-Wert ist die Betriebsdauer (oder Belastung), in der 10% aller Komponenten ausgefallen sind
- Annahme, dass die Ausfallrate bis zum B_{10}-Wert konstant ist
- Damit ergibt sich:

$$F(t) = 10\% = 0{,}1 = \lambda_{10} * t$$

Mit: $t = B_{10}$ $\qquad \lambda_{10} = \frac{0{,}1}{B_{10}}$

wenn B_{10} in Zyklen angegeben ist gilt:

$$\lambda_{10} = \frac{0{,}1}{B_{10}} * f_{Zyklus}$$

Ausfallrate mechanischer Komponenten

- Wird ein Anteil an gefahrbringender Ausfälle (AgA) angegeben, so kann λ_{10D} berechnet werden

$$B_{10D} = \frac{B_{10}}{AgA}$$

Mit: $t = B_{10}$ $\qquad \lambda_{10D} = \frac{0{,}1}{B_{10D}} = \frac{0{,}1 * AgA}{B_{10}}$

wenn B_{10} in Zyklen angegeben ist gilt:

$$\lambda_{10D} = \frac{0{,}1}{B_{10D}} * f_{Zyklus} = \frac{0{,}1 * AgA}{B_{10}} * f_{Zyklus}$$

Ausfallrate mechanischer Komponenten

- Hierbei ist zu beachten:
- Dies ist nur gültig für $\lambda_{10} < B_{10}$ (bzw. B_{10} / f_{Zyklus})
- Bei verschleißbehafteten Komponenten gilt **nicht** :

$$MTTF = 1/\lambda$$

Typische Werte MTTF nach DIN EN ISO 13849-2

Tabelle C.1 — Internationale Normen, die sich mit $MTTF_D$ oder B_{10D} für Bauteile befassen

	Grundlegende und bewährte Sicherheitsprinzipien nach ISO 13849-2:2012	Relevante Normen	Typische Werte: $MTTF_D$ (Jahre) B_{10D} (Zyklen)
Mechanische Bauteile	Tabellen A.1 und A.2	–	$MTTF_D = 150$
Hydraulische Bauteile mit $n_{op} \geq 1\,000\,000$ Zyklen pro Jahr	Tabellen C.1 und C.2	ISO 4413	$MTTF_D = 150$
Hydraulische Bauteile mit 1 000 000 Zyklen pro Jahr $> n_{op} \geq 500\,000$ Zyklen pro Jahr	Tabellen C.1 und C.2	ISO 4413	$MTTF_D = 300$
Hydraulische Bauteile mit 500 000 Zyklen pro Jahr $> n_{op} \geq 250\,000$ Zyklen pro Jahr	Tabellen C.1 und C.2	ISO 4413	$MTTF_D = 600$
Hydraulische Bauteile mit 250 000 Zyklen pro Jahr $> n_{op}$	Tabellen C.1 und C.2	ISO 4413	$MTTF_D = 1\,200$
Pneumatische Bauteile	Tabellen B.1 und B.2	ISO 4414	$B_{10D} = 20\,000\,000$
Relais und Hilfsschütze mit geringer Last	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	$B_{10D} = 20\,000\,000$
Relais und Hilfsschütze mit nominaler Last	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	$B_{10D} = 400\,000$
Näherungsschalter mit geringer Last	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10D} = 20\,000\,000$
Näherungsschalter mit nominaler Last	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10D} = 400\,000$

Zusammenfassung

- Mechanik kann in bestimmten Punkten wie Elektronik betrachtet werden (FSM- System, Vermeidung systematischer Fehler, HFT)
- Probabilistische Betrachtung nur für Zufallsereignisse möglich
- Versagen hat hauptsächlich systematische Ursachen haben (LDM, „wer rastet der rostet“)
- Verschleiß (HDM) kann Zufall sein
- Durch den B10-Wert kann die Weibull - Verteilung in einem bestimmten Bereich durch eine konstante Ausfallrate angenähert werden
- „Ersatzwerte“ werden zwar in verschiedenen Quellen angegeben, die Anwendung muss jedoch wohlüberlegt geschehen (keine falsche Zahlengläubigkeit)
- Fehlerausschluss ist auch möglich

10. Rechenbeispiel

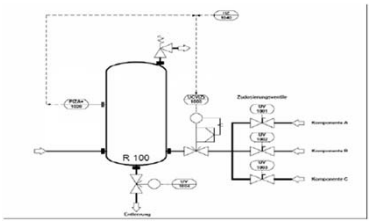
Referent : Hans-Dieter Schwender
TÜV-SÜD Industrieservice

Rechenbeispiel

Fiktiv angenommene Gerätedaten

Sensor (Typ B) inkl. Auswertung:

λ_{DU} = 1,66 * 10^{-7} = 166 FIT
SFF = 89%
HFT = 0
β = 0,1

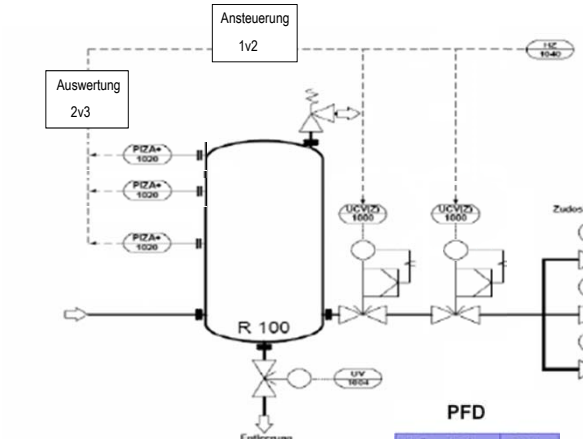


Aktor (Typ A) inkl. Ansteuerung:

λ_{DU} = 1,66 * 10^{-7} = 166 FIT
SFF = 89%
HFT = 0
β = 0,1

Annahme SFF ist konstant und Prüfintervall 1 Jahr

Berechnungsbeispiel



PFD Gesamtsystem

	PFD	HFT	SIL
1v1:	1,45*10^{-3}	0	1
1v2:	1,47*10^{-4}	1	2
2v3:	1,48*10^{-4}	1	2

PFD

10^{-2} … 10^{-1}	SIL 1
10^{-3} … 10^{-2}	SIL 2
10^{-4} … 10^{-3}	SIL 3
10^{-5} … 10^{-4}	SIL 4

SFF \ HFT	0	1	2
< 60%	-----	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

Zusammenhang SFF / HFT

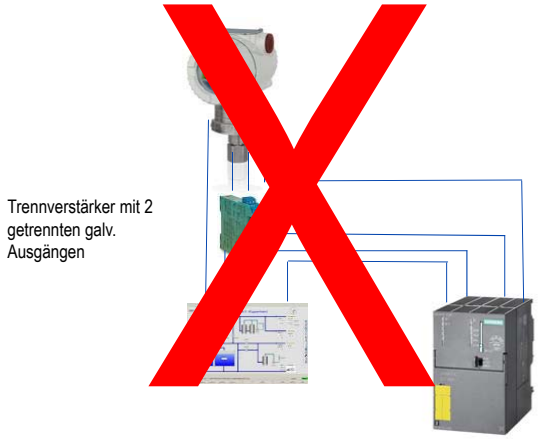
Safe Failure Fraction (SFF)	Type A (simple devices) Hardware Fault Tolerance (HFT)			Type B (complex devices: ASIC, µP) Hardware Fault Tolerance (HFT)		
	0	1	2	0	1 (0)	2 (1)
< 60 %	SIL 1	SIL 2	SIL 3	not allowed	SIL 1	SIL 2
60 % – < 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % – < 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Nach IEC 61511 kann bei betriebsbewährten Geräten die HFT um 1 reduziert werden (gilt nicht für SIL 4)

Verwendung von Teilen einer Sicherheitseinrichtungen für Betriebseinrichtung (z.B. Sensorik)

Anforderung:	Einrichtungen der Sicherheitseinrichtungen sollen als Betriebs- oder Anzeigeeinrichtung mit verwendet werden.
Normativer Ansatz:	Schutzfunktionen sind nach Möglichkeit von anderen Funktionen zu trennen.
Realisierung:	Nach VDI/VDE 2180-3 gilt: Die PLT-Sicherheitseinrichtung kann für PLT-Betriebseinrichtungen verwendet werden, wenn diese rückwirkungs- und rückkopplungsfrei übergeben werden

Verwendung von Sicherheitseinrichtungen für Betriebseinrichtung



Wichtiges

- Nahezu jeder wird eine zertifizierte SPS auswählen
  - Für gewöhnlich der zuverlässigste Teil des Sicherheitskreises, auch ohne Zertifikat
- Viele werden nach einem zertifizierten Transmitter fragen
  - weniger zuverlässig als die SPS, jedoch gewöhnlich robust
- Einige werden nach einem Zertifikat für das Ventil fragen
  - …ein unzuverlässiger Teil des Kreise
- Zu viele werden NICHT nach dem Sicherheitsreport fragen
  - der ESSENTIEL für die Planung ist (überraschenderweise geben sich die Leute mit einem Zertifikat zufrieden)
- Kaum einer fragt nach den Menschen
  - dem am WENIGSTEN verlässlichen Teil (der Teil der durchfunktionales Sicherheitsmanagement abgedeckt wird)

- **Der Teil eines Sicherheitssystems, der am häufigsten ausfällt, ist der Mensch**

Die Wichtigkeit der einzelnen Punkt ist bei allen gleichwertig !

Da wollen wir hin

Auf ein unerwartetes Ereignis vorbereitete sein!

Last Layer Of Protection

Vielen Dank für Ihre Aufmerksamkeit

Wir stehen Ihnen zur Verfügung

Hans-Dieter Schwender

TÜV SÜD Industrie Service GmbH
Leiter Funktionale Sicherheit / MSR-Technik
AN1-MUC

Westendstraße 199
80686 München
Telefon : +49 (0)89 5791 4149
Mobil: +49 (0)151 277 45-659
E-Mail: hans-dieter.schwender@tuev-sued.de