Niederspannungsschalt- und Steuergeräte – Gesichtspunkte der funktionalen Sicherheit

Leitfaden, wie Niederspannungs-schalt- und Steuergeräte in Anwendungen der funktionalen Sicherheit verwendet werden können.

Picture Siemens AG

CAPIEL

european coordinating committee of manufacturers of electrical switchgear and controlgear

Philippe Sauer
CAPIEL Präsident

Karlheinz Kaul
CAPIEL Vice-Präsident

Statements der CAPIEL Präsidenten

In den letzten Jahren wurden Maschinen immer komplexer. Durch die Europäische Maschinenrichtlinie wurden auch die Anforderungen immer höher. Daher ist die Europäische Union in Bezug auf funktionale Sicherheit in Maschinensystemen sehr einflussreich.

Dieses hat auch große Auswirkungen auf CAPIEL Produkte. Einige CAPIEL Produkte erfüllen wohl nicht die Definition eines "Sicherheitsbauteils", aber sie können trotzdem Merkmale oder Funktionalitäten besitzen die es erlauben, von Maschinenbauern in Sicherheitsanwendungen eingesetzt werden zu können.

Als CAPIEL ist es eine unserer wichtigsten Pflichten, mit den Aufsichtsbehörden zusammen zu arbeiten, um sicherzustellen, dass Merkmale und Funktionalitäten mit unseren allgemeinen Sicherheitszielen übereinstimmen. Es ist unsere Verantwortung, dass dies für Entwickler und Anwender von elektrischen Produkten, Systemen und Lösungen klar definiert und verständlich ist, und richtig interpretiert werden kann.

Diese Broschüre bietet Informationen zur Anwendung der jetzigen Normen und der EU Maschinenrichtlinie, um Niederspannungsschalt- und Steuergeräte in Anwendungen mit funktionaler Sicherheit verwenden zu können.

Wir hoffen dass es Ihr Interesse findet.

Mit freundlichen Grüßen

Philippe Sauer & **Karlheinz Kaul**

CAPIEL ist das europäische Komitee zur Koordinierung von Herstellern elektrischer Schalt- und Steuergeräte

CAPIEL bietet insbesondere verschiedene **Start-, Steuer- & Sicherheitslösungen für Maschinen an**.

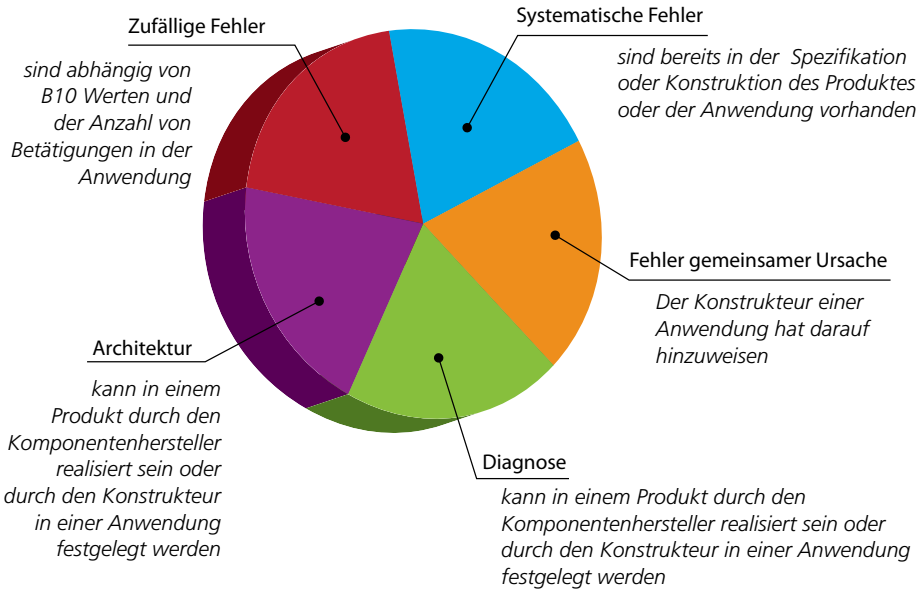
CAPIEL spielt eine aktive Rolle bei neuen Technologien, besonders bezüglich Innovationen in den Bereichen Umweltschutz und Nachhaltigkeit, aber auch in der Gesundheit und der Sicherheit.

Sicherheitsfaktoren

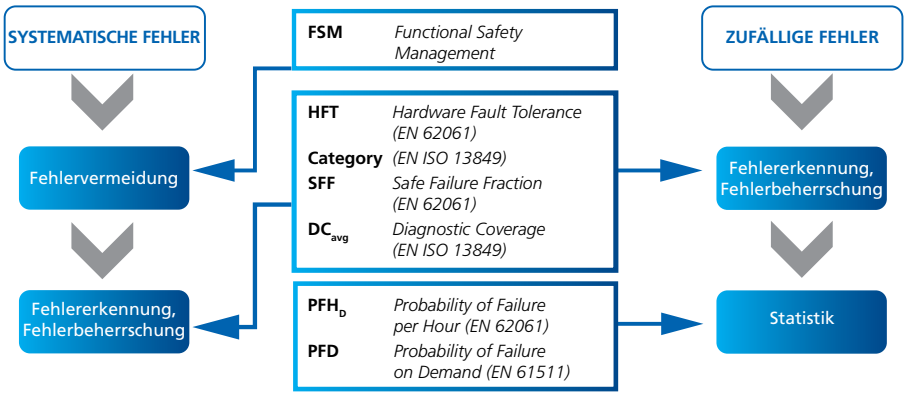
- Die Maschinenrichtlinie 2006/42/EC wird seit 2009 angewendet.
  Maschinenbauer müssen sich überlegen, wie sie Sicherheitssysteme sicher machen und die Konformität mit der Maschinenrichtlinie (2006/42/EC), vorzugsweise unter Anwendung der folgenden harmonisierten EN Normen, nachweisen können:
  - EN ISO 13849
  - EN 62061 (gleich mit IEC 62061)
- Damit die EN-Standards effektiv umgesetzt werden können, bieten die CAPIEL-Hersteller Daten bezüglich der funktionalen Sicherheit zur Unterstützung der Maschinenbauer bei der Auslegung passender Sicherheitssysteme an. (Siehe Seite 11)
- Das Format der in diesem Dokument angebotenen Daten ist wichtig für die vereinfachten Rechenmethoden, wie in EN ISO 13849 und EN 62061.
- Funktionale Sicherheit ist auch wichtig in der Prozessindustrie, in explosiver Umgebung, in der Bahntechnik und anderen Bereichen. Dafür gibt es eine Anzahl von anzuwendenden Richtlinien und Normen, wie z.B.:
  - ATEX Richtlinie 94/9/EC (wird ersetzt durch 2014/34/EU): EN 50495
  - Prozess Industrie: EN 61511
  - Bahn Anwendungen: EN 50155

Faktoren der funktionalen Sicherheit für elektromechanische Produkte

- Um eine Maschine sicher zu machen, ist es notwendig mehrere Faktoren zu berücksichtigen:



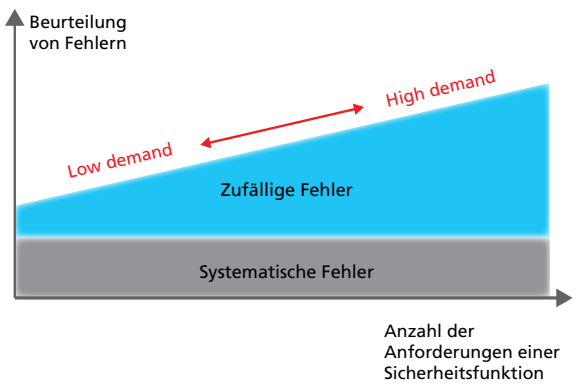
Warum ist es notwendig, zwischen Fehlern zu unterscheiden?



- Der Unterschied zwischen systematischen und zufälligen Fehlern liegt in der Art ihrer Ursache.
- Systematische Fehler entstehen meist bei der Gestaltung eines Systems. Diese Fehler sind meist bereits von Anfang an im Produkt oder System vorhanden (z.B. falsche Anforderungen oder Spezifikation, falsche Dimensionierung, Software Fehler).
- Zufällige Fehler sind schwer vorauszusagen, weil es praktisch unmöglich ist den Fehler vor dem Ausfall zu erkennen. Darum werden hier statistische Methoden angewendet.

Was ist der Unterschied zwischen “low demand” und “high demand”?

- Im low demand mode mit verschleißbehafteten Komponenten ist es am wichtigsten, die systematischen Fehler zu reduzieren. Für high demand und low demand sind aber die gleichen Maßnahmen einzustellen, wie z.B. „Fehlervermeidung“, „Qualitätsmanagement“, die Verwendung von „bewährten Prinzipien“ oder „Felderfahrung“.



Mode of operation

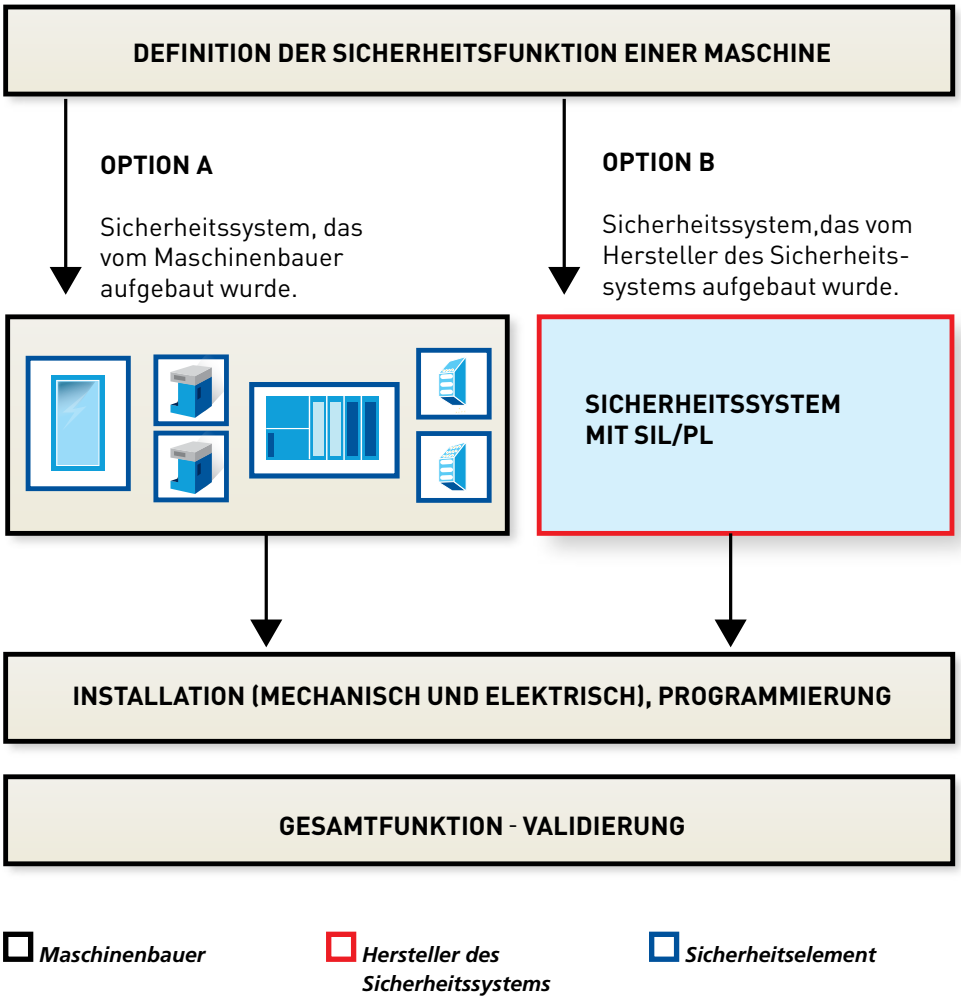
Demand:
- *Die Sicherheitsfunktion wird ausgeführt, um die Anlage in einen definierten sicheren Zustand zu bringen*

Low demand mode
- *Häufigkeit der Sicherheitsanforderungen ≤ 1 / a*
- *Der Verlust der Sicherheitsfunktion führt nicht sofort zu einer gefährlichen Situation*

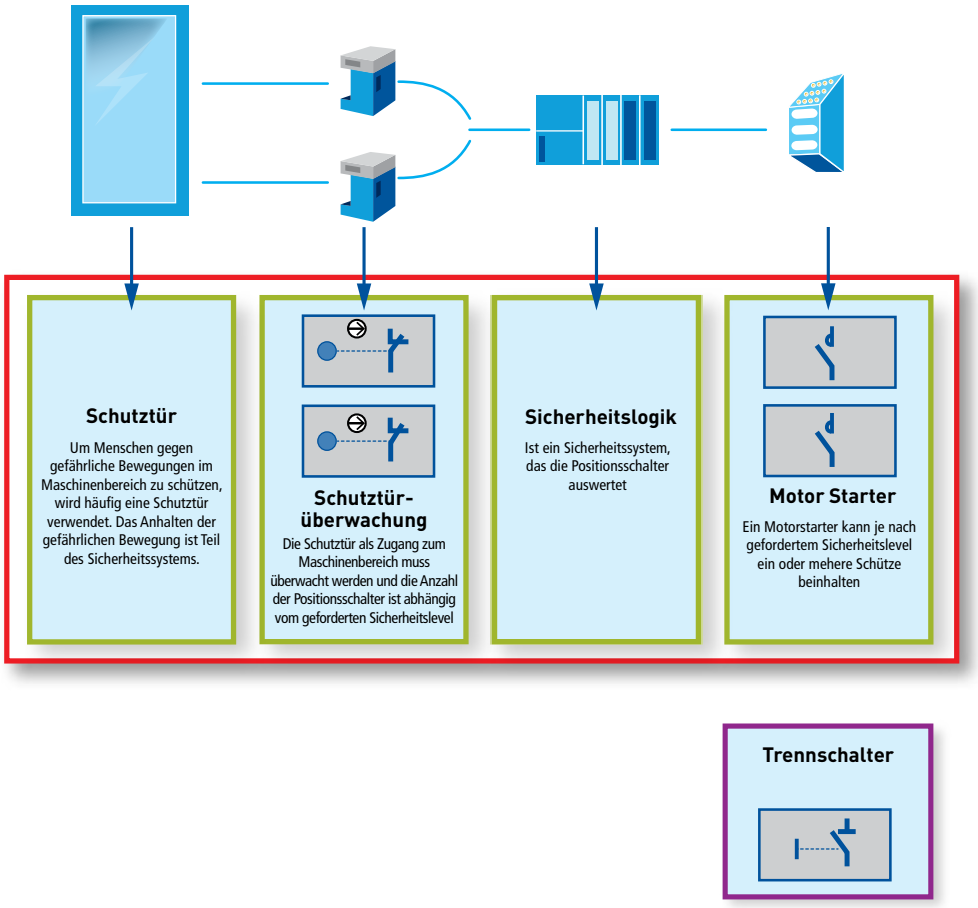
High demand mode
- *Häufigkeit der Sicherheitsanforderungen > 1 / a*
- *Der Verlust der Sicherheitsfunktion führt direkt zu einer gefährlichen Situation*

Verantwortlichkeiten

- Der Maschinenbauer ist verantwortlich für die gesamte Entwicklung und die Sicherheit der Maschine.
- Das ist grundlegend, egal ob Option A oder B im untenstehenden Diagramm verwendet wird.
- Bei der Auswahl der verwendeten Produkte entscheidet der Maschinenbauer, ob er aus Sicherheitselementen Sicherheitsteilsysteme aufbaut oder vorgefertigte Teilsysteme verwendet.



Realisierungsebenen von Sicherheitsprodukten



Sicherheitssystem

Beispiel : Schutzhaube mit Überwachung und Auslösefunktion (kein einzelnes CAPIEL Produkt)

Sicherheitsteil-system

Beispiel : Teilfunktion, um eine gefährliche Bewegung eines Fließbandes zu stoppen, realisiert durch einen sicheren Motorstarter

Andere Beispiele: Sicherheitsrelais

Sicherheits-element

Beispiel : Schütz (mit B_{10d})

Andere Beispiele : Türüberwachungs-schalter, Relais mit Spiegelkontakten, NOT HALT Einrichtung, Zuhalteeinrichtung

Allgemeines Element

Beispiel : Netzfreischalter

Andere Beispiele : Schütz (ohne B_{10d}), Relais, Druckschalter, Anschlusselement, Standard-SPS, Hilfsschalter, Lasttrenner, Anzeigesäulen. alle Beispiele ohne Sicherheitsfunktion

Welches Produkt braucht welche Sicherheitskennwerte - Übersicht

Jede Realisierungsebene benötigt verschiedene Daten, damit der Maschinenbauer die geforderten PL/SIL für die Sicherheitsfunktion ermitteln kann. Die folgende Tabelle zeigt die benötigten Daten:

Vom Hersteller bereitgestellte Informationen	Realisierungsebenen							
	Sicherheits-system		Sicherheit-steilsystem		Sicherheit-selement		Allgemeines Element	
	TB	WB	TB	WB	TB	WB	TB	WB
SIL und/oder PL	■	■						
SILCL und/oder PL			■	■				
PFH_D und/oder PFD	■	■	■	■				
Operation limit		■		■		■		■
$MTTF_d$ oder MTTF und RDF					■			
B_{10d} oder B_{10} und RDF						■		
MTBF							■	
B_{10}								■
T_M	■	■	■	■	■	■	■	■

■ ***Pflichtfeld, Daten erforderlich,***

■ ***Optionales Feld, Daten optional (Anwendungsabhängig),***

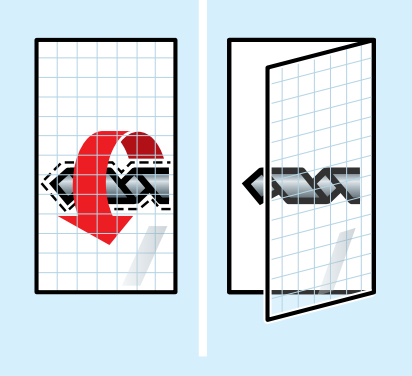
TB **Zeitbasiert *(Time based), z.B. elektronsche Produkte***

WB **Verschleißbasiert *(Wear based), z.B. elektro-mechanische Produkte***

PL *Performance Level (EN ISO 13849)*
SIL *Safety Integrity Level (EN 61508)*
SILCL *Safety Integrity Level Claim Limit (EN 62061)*
PFH_D *Probability Failure per Hour (EN 62061)*
T_M *Mission time (EN ISO 13849)*
MTBF *Mean Time Between Failure (EN ISO 13849)*

$MTTF_d$ *Mean Time To Dangerous Failure (EN ISO 13849)*
RDF *Ratio of Dangerous Failures*
B_{10} *10% der Geräte ist ausgefallen (EN ISO 13849)*
B_{10d} *10% der Geräte ist gefährlich ausgefallen (EN ISO 13849)*
PFD *Probability of failure on Demand (EN 61511)*
Operation limit *max. Anzahl der Betätigungen die in der Berechnung des PFH_D verwendet wurden*

Fallbeispiel: High Demand Anwendung



Picture Eaton Industries GmbH

Eine bewegliche Schutztür wird durch Positionsschalter überwacht (eventuell zwei, abhängig vom geforderten PL/SIL). Der Aktuator wird bei der Berechnung nicht berücksichtigt.

Bedingungen für dieses Beispiel:

- Diese Schutztür wird 4 mal pro Stunde geöffnet (C=4).
- 2-kanalige Architektur
- B_{10} = 1 000 000
- RDF = 20%
- CCF, β = 10% (Common Cause Factor EN 62061)
- T_1 = 20 Jahre (Proof Test Interval EN 62061) ≈ 200 000 Stunden
- DC = 0

Berechnung des SIL Claim für das Teilsystem 1:

Der Anteil gefahrbringender Fehler (RDF) und der B_{10} wird vom Hersteller bereitgestellt, z.B. 20% und 1 000 000*. Der B_{10d} Wert wie in der EN ISO 13849 verwendet, kann wie folgt ermittelt werden:

$$B_{10d} = \frac{B_{10}}{RDF} = \frac{1\,000\,000}{0.2} = 5\,000\,000$$

Die gesamte Fehlerrate λ_D nach EN/IEC 62061 des Positionsschalters, wie folgt:

$$\lambda_D = \frac{0.1 \times C}{B_{10d}} = \frac{0.1 \times 4}{5\,000\,000} = 8 \times 10^{-8}$$

In diesem Beispiel ist die Funktion der Sensoren nicht überwacht, deshalb gilt λ_{DD}=0. Ebenso ist λ_S =0, weil "schließt nicht Fehler" nicht zur Sicherheitsfunktion beitragen und deshalb nicht für die SFF Berechnung berücksichtigt werden dürfen.

➡ $SFF = (\lambda_{DD} + \lambda_S) / (\lambda_D + \lambda_S) = (0+0)/(8 \times 10^{-8} + 0) = 0$

Für die Berechnung des SFF sind nur Fehler relevant, die zur Sicherheitsfunktion beitragen. Die „no effect failures" werden nicht für die Berechnung des SFF verwendet**.

$PFH_D \approx 2 * \lambda_D^2 * T_1/2 + \beta * \lambda_D$

$PFH_D \approx 2 * (8 \times 10^{-8})^2 * 200\,000/2 + 0{,}1 * 8 \times 10^{-8} = 8 \times 10^{-9}$ [1/h]

**Siehe auch "CAPIEL WHITE PAPER, Low voltage controlgear products and functional safety", www.capiel.eu.*
***Siehe auch EN 61508-4 2nd Ed Abschnitt 3.6.14/15*

3 Faktoren aus der Anwendung/Berechnung

2-kanalig = HFT = 1

SFF = 0

PFH_D =8 x 10^{-9}

Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Element oder Teilsystem ausgeführt wird:

Hardwarefehlertoleranz (HFT)			Anteil sicherer Ausfälle (SFF)
HFT 0	**HFT 1**	HFT 2	
Nicht zulässig	SIL 1	SIL 2	**< 60%**
SIL 1	SIL 2	SIL 3	60% – < 90%
SIL 2	SIL 3	SIL 3	90% – < 99%
SIL 3	SIL 3	SIL 3	≥ 99%

(Referenz: EN 62061)

Sicherheits Integritätslevel - Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher Anforderungsrate betrieben wird:

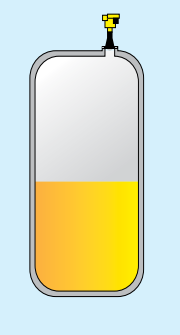
Wahrscheinlichkeit eines gefahr-bringenden Ausfalls pro Stunde (PFH_D)	Sicherheits Integritätslevel (SIL)
$10^{-6} \leq PFH_D < 10^{-5}$	SIL 1
$10^{-7} \leq PFH_D < 10^{-6}$	SIL 2
$10^{-8} \leq PFH_D < 10^{-7}$	SIL 3

(Referenz: EN 62061)

Das Ergebnis für das Sicherheitsteilsyste 1 = SILCL 1

In diesem Beispiel ist der PFH Wert gut genug für SIL 3, der SIL wird jedoch durch SFF und HFT auf SIL 1 begrenzt.

Fallbeispiel: Low Demand Anwendung



Picture Vega Grieshaber KG

Ein Füllstandsmesser in der Prozessindustrie überwacht das Füllstandsniveau im Reaktor.

Nach der IEC 61511 gibt es 3 Möglichkeiten der Ermittlung:

- Berechnung nach IEC 61508
- prior use (Felderfahrung)
- Fehlerausschluß

Arbeiten im Low Demand Mode:

- Die hauptsächlichen Fehler sind systematische Fehler; zufällige Fehler sind nicht von der Anzahl der Betätigungen abhängig.
- B_{10} Wert ist nicht für die PFD Berechnung verwendbar
- Die Fehlerrate ist meistens aus Felderfahrung ermittelt

Für low demand Anwendungen in der Prozessindustrie können die Ausfallraten aus Datenbanken oder aus dem Sicherheitshandbuch des Herstellers verwendet werden.
Herstellerangaben: $\lambda_D = 20$ FIT $= 20 \times 10^{-9} = 2 \times 10^{-8}$ Fehler/h
Anwenderangabe: T_1=1 Jahr (8760 Stunden)
PFD $= \lambda_D * T_1/2$

3 Faktoren aus der Anwendung/Berechnung

1-kanalig = HFT = 0
SFF = 0
PFD = 8.76 x10^{-5}

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

Hardwarefehlertoleranz (HFT)			Anteil sicherer Ausfälle (SFF)
HFT 0	HFT 1	HFT 2	
SIL 1	SIL 2	SIL 3	**SFF < 60%**
SIL 2	SIL 3	SIL 4	60% ≤ SFF ≤ 90%
SIL 3	SIL 4	SIL 4	90% ≤ SFF ≤ 99%
SIL 3	SIL 4	SIL 4	SFF ≥ 99%

(Referenz: IEC 61508-2)

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

Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Anforderung (PFD_{avg})	Sicherheits Integritätslevel (SIL)
$10^{-2} \leq PFD_{avg} < 10^{-1}$	SIL 1
$10^{-3} \leq PFD_{avg} < 10^{-2}$	SIL 2
$10^{-4} \leq PFD_{avg} < 10^{-3}$	SIL 3
$10^{-5} \leq PFD_{avg} < 10^{-4}$	SIL 4

(Referenz: IEC 61508-1)

Das Ergebnis für das Sicherheitsteilsystem 1 = SIL 1

In diesem Beispiel ist der PFD Wert gut genug für SIL 4, der SIL wird jedoch durch SFF und HFT auf SIL 1 begrenzt.

Folgerungen

- Der Maschinenbauer ist für die gesamte Entwicklung und Sicherheit der Maschine verantwortlich.
- Bei der Konstruktion einer Maschine hat der Maschinenbauer folgende Möglichkeiten:
  - Die Auswahl eines für seine Anwendung geeigneten Sicherheitssystems. Dabei stellt der Lieferant alle notwendigen Sicherheitsdaten bei.
  - Die Auswahl und Kombination geeigneter Sicherheitsteilsysteme um damit ein Sicherheitssystem zu erstellen, das den geforderten Level für die Sicherheitsfunktion erfüllt.
  - Er entwickelt mit Sicherheitselementen ein Sicherheitsteilsystem und kombiniert es mit weiteren Sicherheitsteilsystemen um damit ein Sicherheitssystem zu erstellen, das den geforderten Level für die Sicherheitsfunktion erfüllt.
- Wenn ein allgemeines Element für eine Sicherheitsanwendung verwendet wird, muss der Maschinenbauer begründen, wie er es als Sicherheitselement verwenden will. Das beinhaltet die Herleitung aller Werte für die funktionale Sicherheit und die Eignung für die geplante Funktion.
  Die Tabelle auf Seite 7 zeigt, welche Sicherheitswerte durch den Komponentenhersteller bereitgestellt werden.
- Statistische Ermittlungsmethoden sind nicht immer für die Ermittlung von Zuverlässigkeit verwendbar. Bevor ein neues System erstellt wird, muss immer die systematische Analyse aller möglichen Ursachen von Fehlern in einem System und seinen Komponenten durchgeführt werden.
- Die Berechnung ist lediglich eine von mehreren Verifikationsmaßnahmen die dazu dient zu zeigen, dass der notwendige Sicherheitslevel erreicht wurde.
- Statistikdaten für zufällige Fehler werden durch den Komponentenhersteller bereitgestellt, können von verschiedenen Datenbanken bezogen werden oder sind Ergebnis von Felderfahrung.
- Einige Beispiele für allgemeine Datenbanken:
  - Exida Electrical & Mechanical Component Reliability Handbook
  - MIL HDBK 217F
  - NAMUR NE 93
  - RAC FMD 91
  - SN29500
  - SN31920
  - VDE 2180
  - IEC/TR 62380
  - IEC 61709
  - White paper CAPIEL PG5

Verweise

EN 61508	Functional safety of electrical/ electronic/programmable electronic safety-related systems
EN 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN 61511	Functional safety – Safety instrumented systems for the process industry sector
EN ISO 13849-1	Safety of machinery – Safety-related parts of control systems Part 1: General principles for design
EN ISO 13849-2	Safety of machinery – Safety-related parts of control systems Part 2: Validation
EN 60947-series	Low-voltage switchgear and controlgear
EN 61649	Weibull analysis
VDMA 66413	VDMA-Specification
EN 50495	Safety devices required for the safe functioning of equipment with respect to explosion risks
EN 50155	Railway applications – Electronic equipment used on rolling stock

CAPIEL
Mitglieder

CAPIEL AUF EINEN BLICK

CAPIEL vertritt **9 nationale Verbände** aus 8 europäischen Ländern mit **mehr als 550 Herstellern**.

Mitglieder der nationalen Verbände, vertreten durch CAPIEL beinhalten Klein-, Mittel- und Großbetriebe, die **120,000 Menschen beschäftigen** und gemeinsam einen **Umsatz von € 18,25 Mrd**. erzielen.

CAPIEL Mitglieder sind **Global Player**, wie Siemens, Schneider Electric, ABB, Eaton, Rockwell Automation usw.

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

www.capiel.eu