SHARING COMPETENCE

Pfannenberg
ELEKTROTECHNIK FÜR DIE INDUSTRIE

Funktionale Sicherheit normenkonform realisieren

Normensituation: Funktionelle Sicherheit

Maschinenindustrie

Elektrik
Hydraulik
Pneumatik
Mechanik

EN ISO 13849

IEC 62061

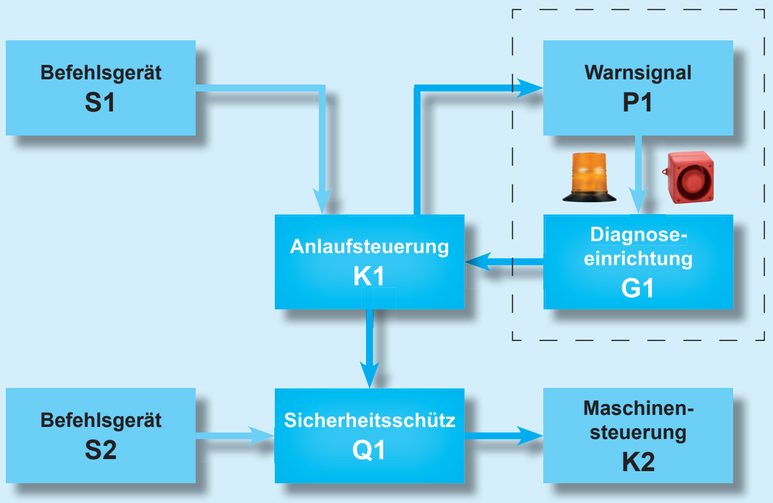
IEC 61508

IEC 61511

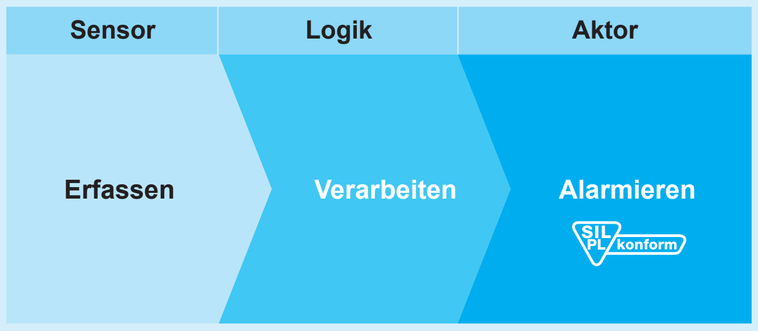
Elektrik
Elektronik
programm. Elek.
(E/E/PE)

Prozessindustrie

Maschinen-Sicherheit z. B. Anlaufwarneinrichtung



Safety Loop

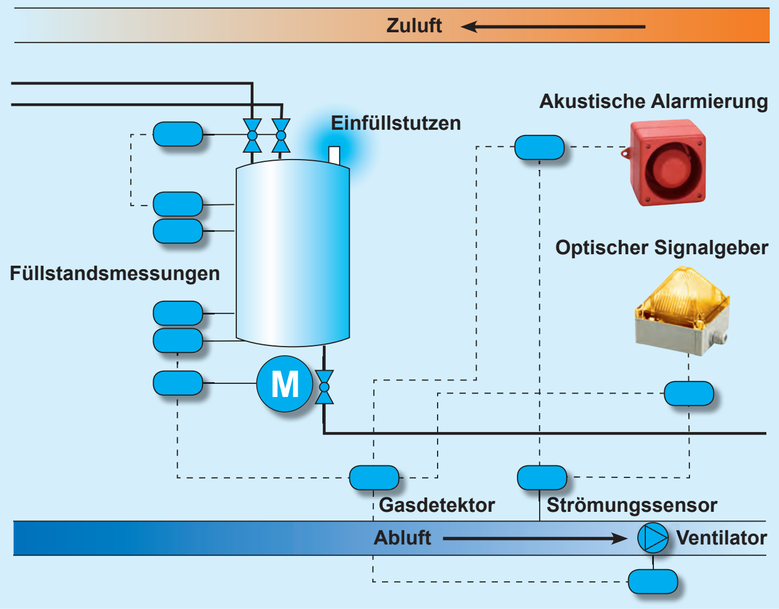


Aktoren 100 % konform zu SIL/PL:

Quadro- und PMF-Blitzleuchten

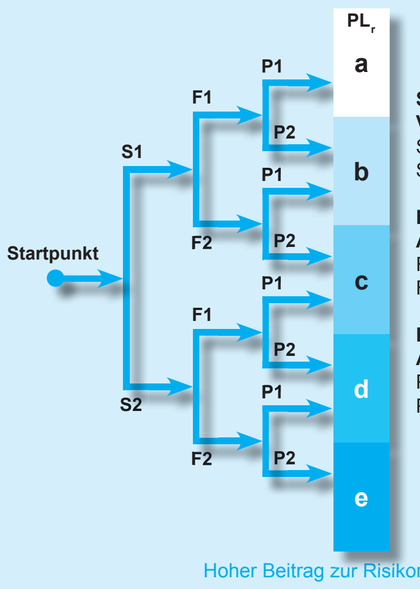
DS-Schallgeber

Prozess-Sicherheit z. B. Gasalarm



Risikograf nach DIN EN ISO 13849

Niedriger Beitrag zur Risikoreduzierung



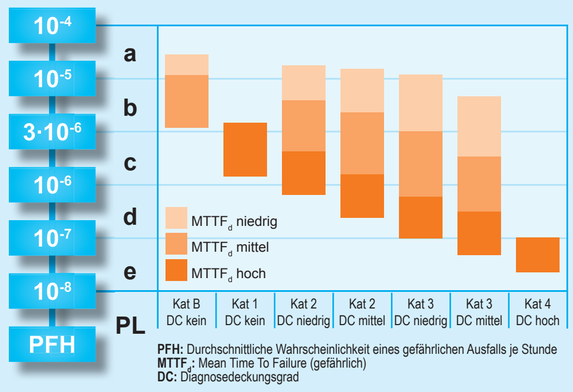
Hoher Beitrag zur Risikoreduzierung

S: Schwere der Verletzung
S1: leicht oder reversibel
S2: schwer, irreversibel

F: Häufigkeit des Auftretens
F1: selten
F2: oft oder dauernd

P: Möglichkeit der Abwendbarkeit
P1: möglich
P2: eher unmöglich

Performance Level (PL) nach DIN EN ISO 13849



PFH: Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde
$MTTF_d$: Mean Time To Failure (gefährlich)
DC: Diagnosedeckungsgrad

$MTTF_d$ für jeden Kanal		DC	
	$MTTF_d$ (in a)		DC in %
niedrig	3 bis < 10	kein	< 60
mittel	10 bis < 30	niedrig	60 bis < 90
hoch	30 bis < 100	mittel	90 bis < 99
nicht möglich	ab 100	hoch	ab 99

Kenngrößen

Anteil sichere Ausfälle (SFF), Diagnosedeckungsgrad (DC)

$$SFF = \frac{\lambda_s}{\lambda_{ges}} \text{ ohne Diagnose} \qquad SFF = \frac{\lambda_s + \lambda_{dd}}{\lambda_{ges}} \text{ mit Diagnose}$$

$$DC = \frac{\lambda_{dd}}{\lambda_d} \qquad SFF = \frac{\lambda_s + DC \cdot \lambda_d}{\lambda_s + \lambda_d}$$

$$\lambda_{ges} = \lambda_s + \lambda_d \qquad \lambda_d = \lambda_{dd} + \lambda_{du}$$

s: safe
d: dangerous
dd: dangerous detected
du: dangerous undetected

Sicherheitsintegrität, Normenvergleich, PFH, PFD, Anforderungen

Sicherheitsintegrität (Typ B) nach IEC 61508				SIL/PL (ISO 13849)	
	HFT				
SFF	0	1	2	SIL	PL
< 60%	–	SIL 1	SIL 2	1	b, c
60% bis < 90%	SIL 1	SIL 2	SIL 3	2	d
90% bis < 99%	SIL 2	SIL 3	SIL 4	3	e
99% bis > 99%	SIL 3	SIL 4	SIL 4	4	–

Anforderung nach IEC 61508, Typ B (teilweise unbekanntes Ausfallverhalten)
Vergleich SIL/PL (IEC 61508/ DIN EN ISO 13849)

SIL	PFH(d)	PFD(d)
	in 1/h	
1	$<10^{-5}$	$< 10^{-1}$
2	$<10^{-6}$	$< 10^{-2}$
3	$<10^{-7}$	$< 10^{-3}$
4	$<10^{-8}$	$< 10^{-4}$

Kenngrößen (IEC 61508)
SIL Safety Integrity Level
SFF Anteil ungefährlicher Ausfälle
PF Ausfallwahrscheinlichkeit
PFH PF pro Stunde
PFD PF pro Anforderung

Lexikon A–P

β (Beta-Faktor bzw. Common Cause-Faktor)
Maß für den CCF; Anteil von Ausfällen, die eine gemeinsame Ursache haben.

CCF (Common Cause Failure)
Ausfall infolge gemeinsamer Ursache.

DC (Diagnostic Coverage)
Maß für die Wirksamkeit der Diagnose, der bestimmt werden kann als Verhältnis der Ausfallrate der bemerkten gefährlichen Ausfälle und der Ausfallrate der gesamten gefährlichen Ausfälle.

DC_{avg}
Durchschnittlicher Diagnosedeckungsgrad.

HFT (Hardware-Fehlertoleranz)
Fähigkeit eines SRECS, eines Teilsystems oder Teilsystem-Elements, eine geforderte Funktion beim vorhandensein von Fehlern oder Ausfällen weiter auszuführen.

KAT (Kategorie)
Einstufung der sicherheitsbezogenen Teile einer Steuerung bezüglich ihres Widerstandes gegen Fehler und ihres nachfolgenden Verhaltens bei einem Fehler, das erreicht wird durch die Struktur der Anordnung der Teile, die Fehlererkennung und/oder ihre Zuverlässigkeit.

λ
Durchschnittliche Wahrscheinlichkeit eines Ausfalls.

λ_D
Rate gefährlicher Ausfälle.

λ_S
Rate sicherer Ausfälle.

$MTTF_d$ (Mean Time To Dangerous Failure)
Mittlere Zeit bis zum gefährlichen Ausfall.

Muting
Überbrückungsfunktion: Ein zeitlich begrenztes bestimmungsgemäßes Aufheben der Sicherheitsfunktion mit zusätzlicher Sensorik.

PFH / PFH_d (Probability of [Dangerous] Failure per Hour)
Wahrscheinlichkeit eines (gefährlichen) Ausfalls pro Stunde bei kontinuierlicher Nutzung.

PFD (Probability of Failure per hour on Demand)
Ausfallwahrscheinlichkeit bei Auslösen/Anforderung der Sicherheitsfunktion.

PL (Performance Level)
Diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen.

PL_r (Performance Level, erforderlicher)
Performance Level, um die erforderliche Risikominderung für eine Sicherheitsfunktion zu erreichen.

Hierarchische Gliederung der EN-Normen

Auszug relevanter Normen für die Anwendung optischer und akustischer Signalgeräte

Sicherheitsgrundnormen
z. B. EN ISO 12100

Typ A-Normen
Gestaltungsleitsätze und Grundbegriffe für Maschinen

Sicherheitsgruppennormen
z. B. EN ISO 13849-1
EN 62061

Zum Beispiel:

Typ B-Normen

EN 61310	Anzeigen, Kennzeichnen und Bedienen
EN 981	System akustische und optische Gefahrensignale
EN 842	Optische Gefahrensignale
EN ISO 7731	Gefahrensignale für Arbeitsstätten

Fachnormen

Zum Beispiel:

Typ C-Normen

EN 15093/15094	Walzmaschinen	EN 692/693	Pressen
EN 415	Verpackungsmaschinen	EN 1034	Papiermaschinen
EN ISO 11111	Textilmaschinen	EN 1248/1247	Gießereimaschinen
EN 1010	Druckmaschinen		

Lexikon R–Z

Risiko
Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes.

SFF (Safe Failure Fraction)
Anteil sicherer Ausfälle, Anteil an der Gesamtausfallrate eines Teilsystems, der nicht zu einem gefahrbringenden Ausfall führt.

Sicherheitsfunktion
Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann.

SIL (Safety Integrity Level)
Diskrete Stufe (eine von vier möglichen) zur Spezifizierung der Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-System zugeordnet werden, wobei der SIL 3 (SIL 4 in der Prozessindustrie) die höchste Stufe und der SIL 1 die niedrigste ist.

SIL_{CL} (SIL-Anspruchsgrenze)
Maximaler SIL, der für ein SRECS-Teilsystem in Bezug auf strukturelle Einschränkungen und systematische Sicherheitsintegrität beansprucht werden kann.

SRCF (Safety Related Control Function)
Von einem SRECS ausgeführte Steuerungsfunktion mit einem festgelegten Integritätslevel, die dazu vorgesehen ist, den sicheren Zustand der Maschine aufrechtzuerhalten oder einen unmittelbaren Anstieg des Risikos zu verhindern.

SRECS (Safety Related Electronic Control System)
Elektronisches Steuerungssystem an einer Maschine, dessen Ausfall zu einer unmittelbaren Erhöhung des Risikos führt.

SRP/CS (Safety Related Part of Control System)
Teil einer Steuerung, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt.

T_1 (Wiederholungsprüfung)
Wiederkehrende Prüfung zur Aufdeckung von Ausfällen in einem sicherheitsbezogenen System, so dass nötigenfalls das System in einen „Wie-Neu"-Zustand gebracht oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand herangebracht werden kann. Technisch ist eine Wiederholungsprüfung für die meisten Geräte nicht realisierbar.

T_M (Gebrauchsdauer)
Zeitraum, der die vorgegebene Verwendung der SRP/CS abdeckt.

Pfannenberg GmbH Werner-Witt-Straße 1 · D-21035 Hamburg · Telefon +49 40 734 12-0 · Telefax +49 40 734 12-101 · sales.support@pfannenberg.com · www.pfannenberg.com