Glossar Funktionale Sicherheit

B10

Der B10-Wert gibt die Lebensdauer (oder Zahl der Schaltspiele) an, bei der wahrscheinlich 10% der Prüflinge ausgefallen sind. Der B10-Wert wird vor allem bei verschleißbehafteten Komponenten (z.B. Schalter, Relais) angegeben.

Mit dem B10-Wert und dem Betätigungszyklus kann die Ausfallrate (MTTF) für elektromechanische Komponenten errechnet werden.
MTTF = B10 / (0,1 x n_{op}), n_{op} ist die Anzahl der jährlichen Schaltspiele in der Applikation.

Beispiel:
B10 : 600‘000 (z.N. Relais)
n_{op} : 150‘000 (1 Schaltung/Minute * 60 Minuten * 10 Stunden * 250 Tage/Jahr)
MTTF : 600‘000 / (0,1 * 150‘000) = 40 Jahre

B10d

Der B10d-Wert gibt die Anzahl von Schaltzyklen an, bis 10% der Komponenten gefährlich ausgefallen sind.
B10d = 50% von B10 (laut DIN EN 13849-1, wenn Herstellerangabe nicht vorhanden)

CCF (Common Cause Failure)

Ausfall in Folge gemeinsamer Ursache (z. B. Kurzschluss). Ausfälle verschiedener Einheiten aufgrund eines einzelnen Ereignisses, wobei diese Ausfälle nicht auf gegenseitiger Ursache beruhen.

DC (Diagnostic Coverage, Diagnosedeckungsgrad)

Abnahme der Wahrscheinlichkeit gefahrbringender Hardwareausfälle, die aus der Ausführung der automatischen Diagnosetests resultiert.

DC_{avg}

Durchschnittlicher Diagnosedeckungsgrad

FIT (Failure In Time)

Masseinheit zur angabe von Ausfallraten elektronischer Bauteile (1 Fit = 1 x 10^{-9}/h)

FMEA (Fehler Mode Effekt Analyse)

Verfahren zur Ermittlung der Art und Weise, in der Komponenten und Systeme ausfallen können und nicht mehr die Sollfunktion erbingen. (gem. E DIN IEC 60300-3-9)

- Ausfallarten
- Auswirkungen der Ausfälle
- Ausfallursachen
- Vermeidung oder Verminderung der Ausfälle

MTTF (Mean Time To Failure, Zeit bis zu einem Ausfall)

Die MTTF ist eine statistische Kenngröße/Kennzahl die über Versuche oder Erfahrungswerte ermittelt wird. Sie gibt keine garantierte Lebensdauer oder garantierte ausfallfreie Zeit an.

$MTTF_d$ (Mean Time To Failure Dangerous, Zeit bis zu einem gefährlichen Ausfall)

MTTFd, beschreibt die mittlere Wahrscheinlichkeit gefahrbringender Ausfälle von sicherheitsrelevanten Bauteilen einer Steuerung, meist in Jahren angegeben.
Als Erwartungswert der Hersteller bemisst er lediglich die Zeit, nach der statistisch rund 63 Prozent aller anfänglich intakten Bauteile gefahrbringend ausgefallen sind.
Der MTTFd-Wert gibt also keine Garantie für eine bestimmte Lebensdauer der Bauteile.

PFH (Probability Failure per Hour)
Wahrscheindlichkeit eines Ausfalls pro Stunde.

PFH_d (Probability of dangerous Failure per Hour)
Wahrscheindlichkeit eines gefahrbringenden Ausfalls pro Stunde.

Bezugswert für Vergleich zwischen PL und SIL

Performance Level (PL) EN ISO 13849-1	Mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde	SIL gem. IEC 61508 und EN IEC 62061	Max. akzeptabler Ausfall des Sicherheits-systems
a	$\geq 10^{-5}$ bis $< 10^{-4}$	–	ein Risikoausfall alle 10.000 Stunden
b	$\geq 3 \times 10^{-6}$ bis $< 10^{-5}$	1	ein Risikoausfall alle 1.250 Tage
c	$\geq 10^{-6}$ bis $< 3 \times 10^{-6}$	1	ein Risikoausfall alle 115,74 Jahre
d	$\geq 10^{-7}$ bis $< 10^{-6}$	2	ein Risikoausfall alle 115,74 Jahre
e	$\geq 10^{-8}$ bis $< 10^{-7}$	3	ein Risikoausfall alle 1.157,41 Jahre

PL (Performance Level)
Der Performance Level ist ein Kennwert für die Zuverlässigkeit, mit der eine Steuerung eine Sicherheitsfunktion erfüllt. Er definiert sich als Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D). In einer fünfstufigen Skala von a bis e steht e für die geringste Ausfallwahrscheinlichkeit.

PL_r (Performance Level Required)
Der erforderliche Performance Level (PL_r) beschreibt die Zuverlässigkeitsanforderung für jede Sicherheitsfunktion der Steuerung, die Konstrukteure im Rahmen der Risikobeurteilung jeweils individuell ermitteln müssen. Dabei können sie für bestimmte Anwendungen die in produktspezifischen C-Normen festgelegten Werte nutzen. Wenn keine C-Norm zur Verfügung steht, bestimmen die Konstrukteure den PL_r durch das Abschätzen der Kriterien Schadensausmaß, Häufigkeit und Aufenthaltsdauer sowie Möglichkeit zur Vermeidung der Gefährdung zum Beispiel mit dem Risikografen der EN ISO 13849 oder ISO 14121. Dieser PL_r ist der Soll-Wert, den die Steuerung erreichen muss.

SF (Sicherheitsfunktion)
Sicherheitsfunktionen dienen der Risikominderung an Maschinen, z. B. der „Vermeidung eines unerwarteten Anlaufs von Motoren bei geöffneter Schutztür“. Die Anforderungen an die „Qualität“ einer Sicherheitsfunktion werden in der Risikoanalyse durch den erforderlichen Performance Level PLr festgelegt. Der tatsächlich erreichte Performance Level PL darf nicht niedriger sein als der PLr.

SFF (Safe Failure Fraction, Anteil sicherer Ausfälle)
Der Anteil ungefährlicher Ausfälle entspricht in etwa dem Diagnosedeckungsgrad (DC), berücksichtigt jedoch auch alle inhärenten Tendenzen für einen Ausfall, bei dem ein sicherer Zustand aktiviert wird. Wenn beispielsweise eine Sicherung durchbrennt, kommt es zu einem Ausfall. Es ist jedoch sehr wahrscheinlich, dass der Ausfall zu einem Drahtbruch führt, was wiederum in den meisten Fällen ein „sicherer" Ausfall ist.

Die meisten mechanischen Geräte mit geringer Komplexität, wie z. B. Not-Halt-Taster und Sicherheitsschalter, verfügen (selbst) über einen relativ geringen SFF-Wert.
Die meisten elektronischen Sicherheitsgeräte wurden mit Redundanz- und Überwachungsfunktionen entwickelt, sodass bei diesen ein Anteil ungefährlicher Ausfälle von über 90 % gängig ist.

Der Wert für den Anteil ungefährlicher Ausfälle wird normalerweise vom Hersteller angegeben.

Der Anteil ungefährlicher Ausfälle kann mithilfe der folgenden Gleichung berechnet werden:

$SFF = (\sum\lambda_S + \sum\lambda_{DD}) / (\sum\lambda_S + \sum\lambda_D)$

λ_S	=	ungefährlichen Aufallrate
λ_D	=	gefährlichen Aufallrate
$\sum\lambda_S + \sum\lambda_D$	=	Gesamtrate der Ausfälle,
λ_{DD}	=	Rate der erkannten gefährlichen Ausfälle

SIL (Safety Integrity Level)
Sicherheits-Integritätslevel (geeignet nur für elektronische Steuerungen, siehe IEC 62061)

SLS
Sicher begrenzte Geschwindigkeit

SOS
Stillstandsüberwachung

SRP/CS (Safety Related Parts of Control Systems)
Sicherheitsbezogenes Teil einer Steuerung

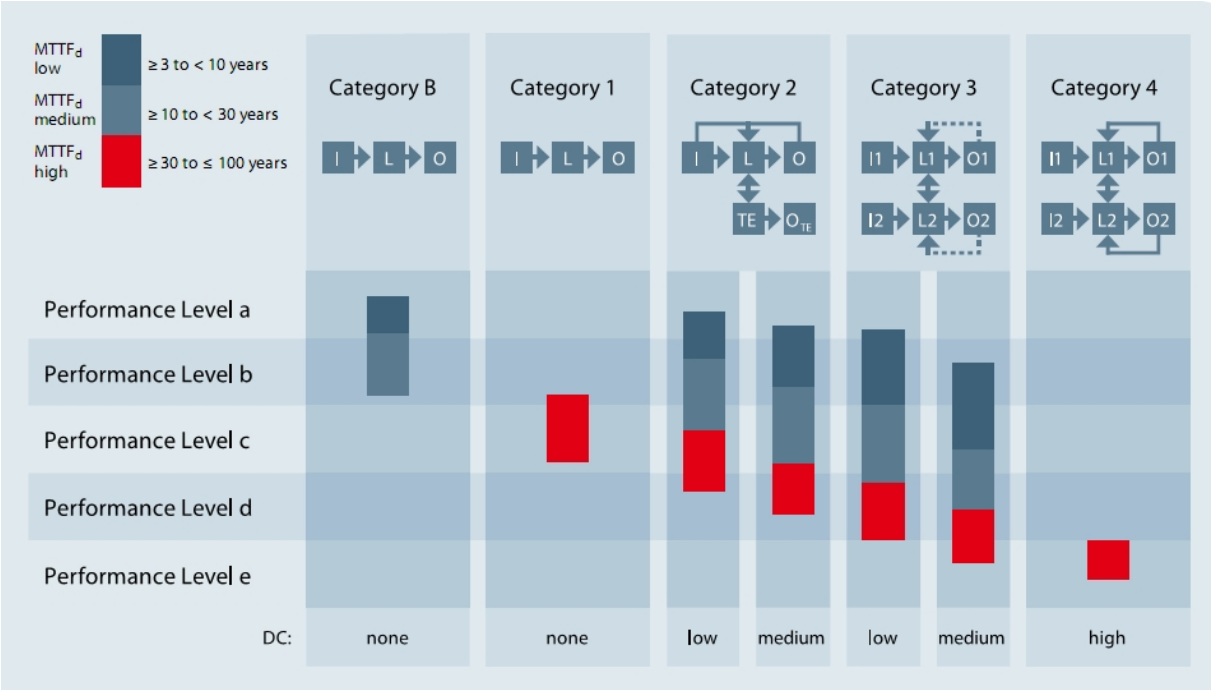
SRECS (Safety Related Electrical Control Systems)
Sicherheitsbezogenes elektrisches Steuerungssystem

STO
Sicherer Halt

T1
Lebensdauer (life time)

T2
Diagnose-Testintervall (diagnostic test interval)

Zuordnung Performance Level ←→ Kategorie



Beziehung zwischen den Kategorien DC_{AVG}, $MTTF_d$ jedes Kanals und des daraus resultierenden PL