4. Was steckt hinter den Kategorien?
Die Kategorien beschreiben das Verhalten der Sicherheitsfunktion im Fehlerfall und die Möglichkeiten zur Fehlererkennung. Dabei unterscheidet man die Kategorien B, 1, 2, 3 und 4.

Kategorie B:
Komponenten sind nach den zutreffenden Normen (grundlegende Sicherheitsprinzipien) gebaut und halten den zu erwartenden Beanspruchungen stand.
Fehlerfall: Verlust der Sicherheitsfunktion möglich
Fehlererkennung: keine (DC = 0)

Kategorie 1:
Anforderungen der Kategorie B müssen erfüllt werden.
Bewährte Bauteile und bewährte Sicherheitsprinzipien sind zu verwenden
Fehlerfall: Verlust der Sicherheitsfunktion möglich, aber weniger wahrscheinlich als bei Kategorie B
Fehlererkennung: keine (DC = 0)

Kategorie 2:
Anforderungen der Kategorie B müssen erfüllt werden.
Anlauftest und periodischer Test der Sicherheitsfunktion, bewährte Sicherheitsprinzipien sind zu verwenden.
Fehlerfall: Verlust der Sicherheitsfunktion zwischen den Testzeitpunkten möglich
Fehlererkennung: Bei jedem Test (DC = niedrig oder mittel)

Kategorie 3:
Anforderungen der Kategorie B müssen erfüllt werden.
Bewährte Sicherheitsprinzipien sind zu verwenden.
Ein einzelner Fehler führt nicht zum Ausfall der Sicherheitsfunktion, wenn immer in angemessener Weise durchführbar.
Fehlerfall: Kein Verlust der Sicherheitsfunktion
Fehlererkennung: Gut, aber nicht vollständig (DC = niedrig oder mittel)

Kategorie 4:
Anforderungen der Kategorie B müssen erfüllt werden.
Bewährte Sicherheitsprinzipien sind zu verwenden.
Ein einzelner Fehler führt nicht zum Ausfall der Sicherheitsfunktion, eine Anhäufung von unerkannten Fehlern darf nicht zum Verlust der Sicherheitsfunktion führen.
Fehlerfall: Kein Verlust der Sicherheitsfunktion
Fehlererkennung: Sehr gut (DC = hoch)

5. Validierung nicht vergessen!
Die EN ISO 13849-2 legt Vorgehensweisen und Bedingungen fest, mit denen eine Sicherheitsfunktion sowie der erreichte Performance Level und die erreichte Kategorie validiert werden können. Für die Kategorien 2, 3, und 4 muss die Validierung der Sicherheitsfunktion auch Prüfung durch geeignete Fehlereinspeisung umfassen.

Unsere Unterstützung für Sie
Eine fundierte Ausbildung in Theorie und Praxis bietet unser Seminar zur EN ISO 13849-1. Anmeldung unter:

www.suva.ch/kurse
>> Kataloge >> Arbeitssicherheit und Gesundheitsschutz >> Deutsch
>> Maschinenbau und Instandhaltung
>> EN ISO 13849-1 Sicherheitsfunktionen für Maschinen - NOST

Produktesicherheit im Maschinenbau –
Wir wissen weiter.

Wir beantworten Ihre Fragen zu den folgenden Themen:

- CE-Konformität
- europäische Richtlinien und Normen
- Sicherheit von Maschinen und Steuerungen

Wir machen für Sie:

- Baumusterprüfungen
- Beurteilungen von Schutzmassnahmen an Maschinen
- Seminare über Produktesicherheit

Profitieren Sie von unserer langjährigen Erfahrung, unserem aktuellen Fachwissen und besuchen Sie unsere Internetseite:
www.suva.ch/certification

Suva
Bereich Technik
Zertifizierungsstelle SCESp 0008
Europäisch notifiziert, Kenn-Nr. 1246
Postfach 4358, CH-6002 Luzern
Tel. +41 41 419 61 31
technik@suva.ch
www.suva.ch/certification

Bestellungen
www.suva.ch/CE13-1.d
Tel. +41 41 419 58 51

Bestellung Normen
Schweizerische Normen-Vereinigung
www.snv.ch
Tel. +41 52 224 54 54

Electrosuisse
www.electrosuisse.ch
Tel. +41 44 956 11 11

Bestellnummer
CE13-1.d - 10.2021

Sicherheitsfunktionen für Maschinen – Das Wichtigste in Kürze

Überblick über den Inhalt der EN ISO 13849-1

suva
CERTIFICATION

Die Richtlinie 2006/42/EG (Maschinenrichtlinie) fordert im Abs. 1.2.1, dass Fehler in der Hardware oder Software einer Maschinensteuerung nicht zu Gefährdungen führen dürfen. Diese Anforderung wird in der Norm EN ISO 13849-1 "Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen" konkretisiert. Das vorliegende Dokument gibt einen Überblick über wesentliche Inhalte der EN ISO 13849-1. Es ersetzt nicht das Lesen und Anwenden der Norm.

1. Bewährtes Verfahren

Für jedes gewählte sicherheitsbezogene Teil der Steuerung oder Kombinationen muss eine Abschätzung des Performance Level (PL) durchgeführt werden.
Der PL der sicherheitsbezogenen Teile der Steuerung muss durch die Abschätzung folgender Aspekte bestimmt werden:

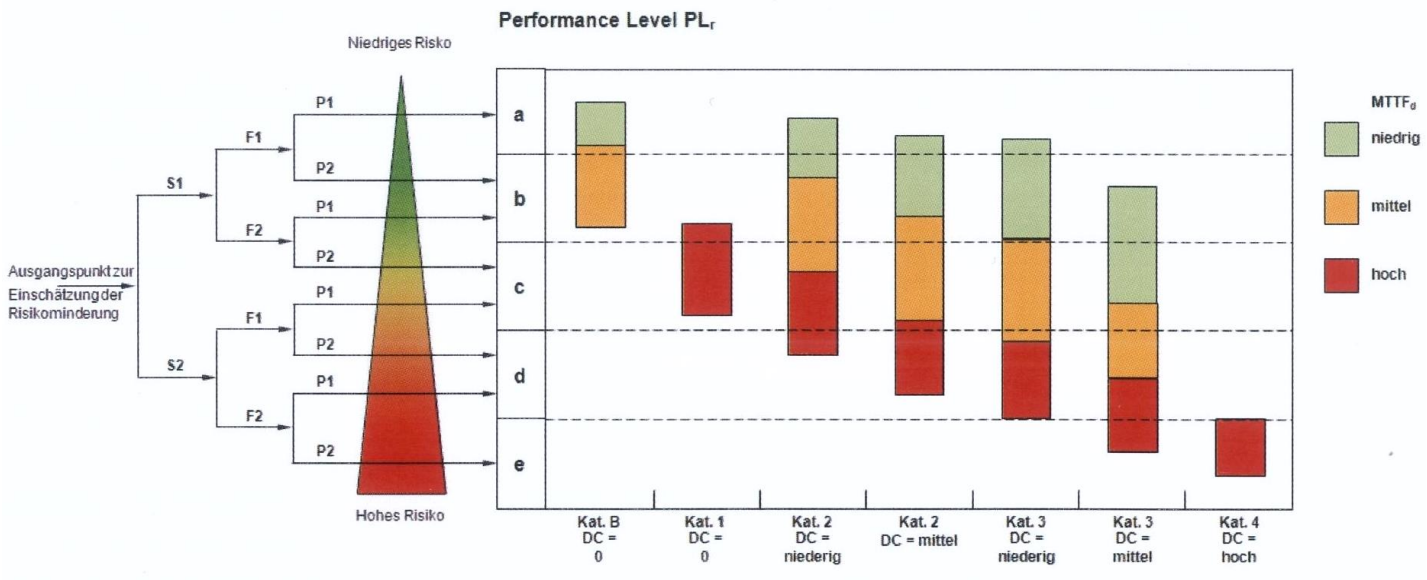
- Architektur der Sicherheitsfunktion (Kategorie)
- Zuverlässigkeit von Bauteilen ($MTTF_D$)
- Qualität von Tests, Diagnosedeckungsgrad (DC)
- Ausfälle infolge gemeinsamer Ursache (CCF)
- Verhalten unter Fehlerbedingung (en)
- sicherheitsbezogener Software
- Massnahmen gegen systematische Fehler
- Fähigkeit, Sicherheitsfunktion unter vorhersehbaren Umgebungsbedingungen auszuführen
- etc.

Die Norm erlaubt ein vereinfachtes Verfahren, basierend auf der Definition der fünf vorgesehenen Architekturen, die spezielle Konstruktionsmerkmale und Verhalten bei einem Fehler erfüllen.
Das vereinfachte Verfahren erlaubt auf Basis der oben gelisteten ersten drei Parametern mit Hilfe der EN ISO 13849-1, Bild 5, den PL zu bestimmen.
Der Vorteil: Der Anwender hat die Möglichkeit, die vorgesehene Architektur zu übernehmen oder er entwirft eine eigene Architektur. In letzterem Fall muss der Anwender aber komplexe mathematische Berechnungen durchführen, welche durch diese Norm nicht unterstützt werden.

2. Begriffe

PL	Performance Level
	Diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen.
$MTTF_D$	Mean time to dangerous failure
	Mittlere Zeit bis zum gefährlichen Ausfall (Anhang C, D)
DC	Diagnostic coverage
	Diagnosedeckungsgrad (Anhang E)
CCF	Common cause failure
	Ausfall infolge gemeinsamer Ursache (Anhang F)

3. Vom Risiko zum Performance Level



Quelle: Bild A.1 und Bild 5 aus EN ISO 13849-1

Folgende Schritte führen vom Risiko zum Performance Level jeder einzelnen Sicherheitsfunktion:

1. Zunächst muss festgestellt werden welcher Performance Level für die entsprechende Sicherheitsfunktion erforderlich ist (PL_r, erforderlicher Performance Level). Der PL_r wird aufgrund der Risikobeurteilung und Verwendung einer Typ-C-Norm oder – falls nicht verfügbar - mit Hilfe des oben gezeigten Diagramms ermittelt (für die Parameter S, F und P siehe Legende zum obenstehenden Bild).
2. Im nächsten Schritt wird der sicherheitsbezogene Teil der Steuerung (SRP/CS) entworfen, der die Sicherheitsfunktion umsetzt.
3. Vom Entwurf des sicherheitsbezogenen Teils der Steuerung werden Kenngrössen der Komponenten ($MTTF_d$), deren Diagnosedeckungsgrad (DC) sowie die Kategorie benötigt. Mit Hilfe dieser Angaben und des oben gezeigten Diagramms kann der erreichte PL abgeschätzt werden. Dabei wird vorausgesetzt, dass alle anderen relevanten Anforderungen erfüllt wurden (Massnahmen gegen CCF, Anforderungen an Software usw.).
4. Der mit dem Entwurf erreichte Performance Level PL muss mindestens so zuverlässig sein wie der erforderliche Performance Level PL_r. ($PL \geq PL_r$).

Legende:

S	**Schwere der Verletzung**
S1	Leichte (üblicherweise reversible) Verletzung
S2	Ernste (üblicherweise irreversible) Verletzung oder Tod
F	**Häufigkeit und/oder Dauer der Gefährdungsexposition**
F1	Selten bis weniger häufig und/oder kurze Dauer der Exposition
F2	Häufig bis dauernd und/oder lange Dauer der Exposition
P	**Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens**
P1	Möglich unter bestimmten Bedingungen
P2	Kaum möglich

$MTTF_D$	**Mittlere Zeit bis zum gefährlichen Ausfall**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre

DC	**Diagnosedeckungsgrad**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC