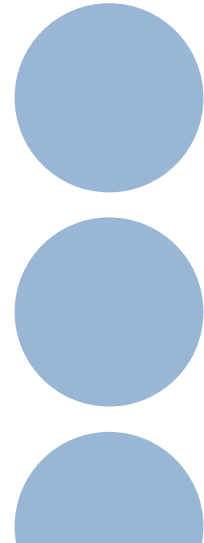


Risikominderung 2

Anforderungen an Steuerungseinrichtungen

ID 063994



1

Beispiele sicherheitsrelevanter Steuerungsfunktionen

- Zustimmungseinrichtung
- Achsgeschwindigkeiten bei offenen Bedienertüren
- Schutztürverriegelungen
- Not-Halt-Einrichtungen
- Spindeldrehzahlen
- Verhinderung unerwarteter Bewegungen
- Berührungslos wirkende Schutzeinrichtungen (BWS)

ID 015545

2

DIN EN ISO 13849-1: Wesentliche Merkmale

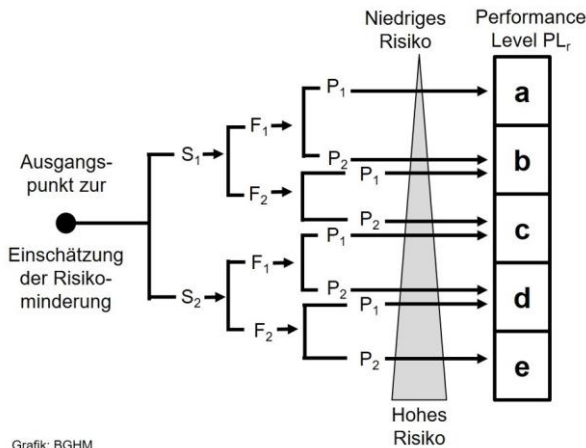
DEUTSCHE NORM		Entwurf	August 2021		
DIN EN ISO 13849-1			DIN		
ICS 13.110	<div>Entwurf</div>		Einsprüche bis 2021-09-09 Vorgesehen als Ersatz für DIN EN ISO 13849-1:2016-06; Ersatz für E DIN EN ISO 13849-1:2020-08		
Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (ISO/DIS 13849-1.2:2021); Deutsche und Englische Fassung prEN ISO 13849-1:2021					
Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (ISO/DIS 13849-1.2:2021); German and English version prEN ISO 13849-1:2021					
Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception (ISO/DIS 13849-1.2:2021); Version allemande et anglaise prEN ISO 13849-1:2021					

- Besonderer Risikograph
- Performance Level (PL), wird bestimmt aus:
 - Kategorie (wie bisher) mit Erweiterungen:
 - MTTF_d „Bauteilgüte“
 - DC : „Fehlererkennung“
 - CCF: Fehler gemeinsamer Ursache
- Software Anforderungen

ID 032282

3

Erforderliche Risikominderung und PL



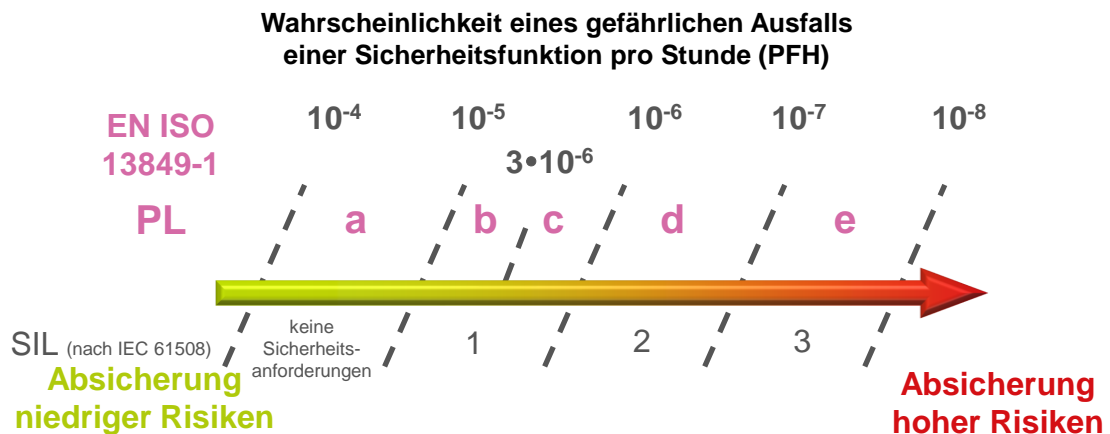
- S: Schwere der Verletzung
F: Häufigkeit und/oder Dauer
der Gefährdungsexposition
P: Möglichkeiten zur
Vermeidung der Gefährdung

Quelle Inhalt nach BGIA Report 02/2008

ID 032282

4

Erforderliche Risikominderung und PL



Quelle: Institut für Arbeitsschutz der DGUV (IFA)

ID 032285

5

Veranschaulichung PFH

Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFH):

Was bedeutet z. B. $PFH = 10^{-6}$?

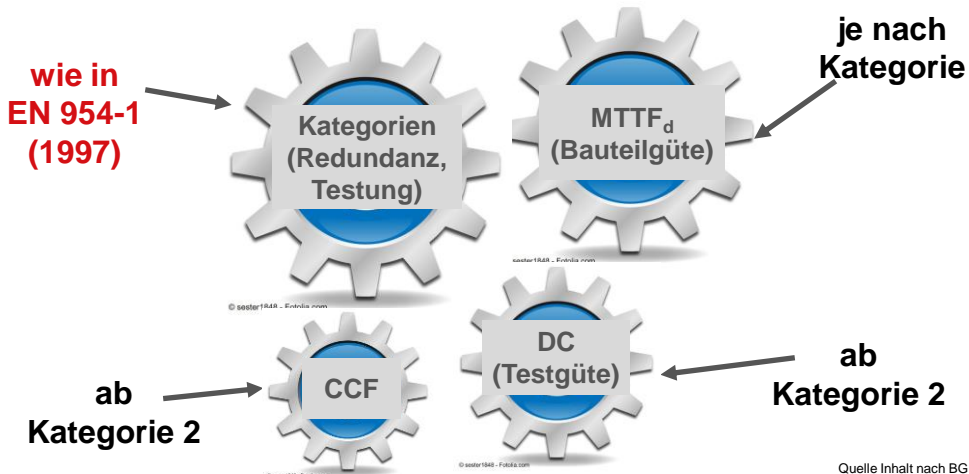
Im Mittel kommt es zu einem gefährlichen Ausfall der Sicherheitsfunktion innerhalb 10^6 (1 Million) Stunden.

→ entspricht ca. 114 Jahre oder 41667 Tage

ID 032290

6

Erweiterung des Kategorie-Begriffs



ID 032291

7

Steuerungskategorie

Kat. B	Sicherheitsbezogene Teile müssen den zu erwartenden Einflüssen standhalten.	Ein Fehler kann zum Verlust der Sicherheitsfunktion führen.
Kat. 1	Verwendung von sicherheitstechnisch bewährten Bauteilen und Prinzipien.	Ein Fehler kann z. Verlust der Sicherheitsfunktion führen. Wahrscheinlichkeit dafür ist geringer als in Kat. B.
Kat. 2	Sicherheitsfunktion muss in geeigneten Zeitabständen geprüft werden.	Ein Fehler kann z. Verlust der Sicherheitsfunktion führen. Aufdeckung des Fehlers erfolgt automatisch.
Kat. 3	Ein Fehler darf nicht zum Verlust der Sicherheitsfunktion führen.	Einfehlersicherheit: Anhäufung von Fehlern kann zum Verlust der Sicherheitsfunktion führen.
Kat. 4	Ein einzelner Fehler, wie auch die Anhäufung von Fehlern, dürfen nicht Verlust der Sicherheitsfunktion führen.	Wenn Fehler auftreten, bleibt die Sicherheitsfunktion erhalten.

ID 009388

8

MTTF_d - Mean Time To Failure (dangerous)

MTTF_d: Mittelwert der Betriebsdauer ohne gefährlichen Ausfall in einem einzelnen Kanal der Steuerung

Bezeichnung	Wertebereich MTTF _d
niedrig	3 Jahre ≤ MTTF _d < 10 Jahre
mittel	10 Jahre ≤ MTTF _d < 30 Jahre
hoch	30 Jahre ≤ MTTF _d ≤ 100 Jahre

MTTF_d ist ein statistischer Mittelwert und keine garantierte Lebensdauer!

Quelle: Institut für Arbeitsschutz der DGUV (IFA)

ID 032293

9

Diagnosedeckungsgrad DC

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \lambda_{du}}$$

Ausfallrate erkannter gefährlicher Ausfälle
Ausfallrate aller gefährlicher Ausfälle

Bezeichnung	Wertebereich DC
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC



**Beispielwerte für DC in
EN 13849-1 Anhang E**

Quelle: Institut für Arbeitsschutz der DGUV (IFA)

ID 032295

10

Maßnahmen gegen CCF

CCF: Ausfälle verschiedener Teile durch gemeinsame Ursache

Maßnahmenliste mit Punktesystem (Maximalsumme: 100 Punkte)

- | | |
|--|-----------|
| • Trennung der Signalpfade | 15 Punkte |
| • Diversität | 20 Punkte |
| • Schutz gegen z. B. Überspannung / Überdruck | 15 Punkte |
| • Bewährte Bauteile | 5 Punkte |
| • FMEA | 5 Punkte |
| • Kompetenz / Training der Entwickler | 5 Punkte |
| • EMV oder Filterung des Druckmediums und Schutz gegen Verschmutzung | 25 Punkte |
| • Temperatur, Feuchte, Schock, Vibration usw. | 10 Punkte |

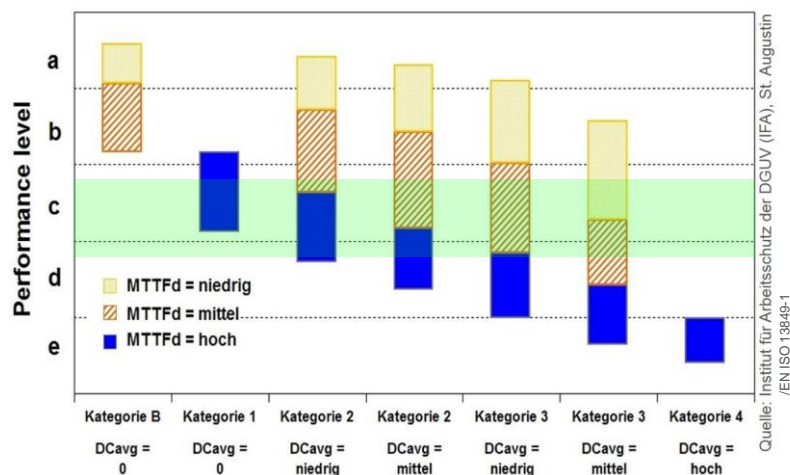
Ziel: mindestens 65 Punkte

Quelle: Institut für Arbeitsschutz der DGUV (IFA)

ID 040021

11

Vielfalt der Realisierungsmöglichkeiten



ID 032292

12