Hilfe zur Anwendung der ISO 13849-1

Safety Evaluation im TIA Selection Tool

https://www.siemens.de/safety-evaluation

Siemens Industry Online Support

Inhaltsverzeichnis

1 Performance Level (PL) und Kategorie (Kat.)

1.1 Performance Level (PL)

In der ISO 13849-1 sind fünf Performance Level (PL a bis PL e) mit definierten Bereichen der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) festgelegt:

Tabelle 1-1 Performance Level (PL)

Performance Level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) 1/h
a	$\geq 10^{-5}$ bis $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ bis $< 10^{-5}$
c	$\geq 10^{-6}$ bis $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ bis $< 10^{-6}$
e	$\geq 10^{-8}$ bis $< 10^{-7}$

Der Performance Level einer Sicherheitsfunktion ergibt sich aus der Summe der Wahrscheinlichkeiten eines Ausfalls je Stunde (PFH_D – Wert) und dem niedrigsten PL aller sicherheitsbezogene Teile einer Steuerung (SRP/CS).

Wenn der Performance Level für ein SRP/CS aufgrund von Anwenderdaten (z.B. Betätigungen) ermittelt werden muss, gilt folgende Methode:

Der maximal erreichbare Performance Level wird durch das vereinfachte Verfahren zur Bewertung aus Tabelle 6 der ISO 13849-1 (siehe nachstehende Tabelle) und die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) aus der Tabelle K.1 der ISO 13849-1 ermittelt.

Tabelle 1-2

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
$MTTF_D$ jedes Kanals							
niedrig	a	n.a.	a	b	b	c	n.a.
mittel	b	n.a.	b	c	c	d	n.a.
hoch	n.a.	c	c	d	d	d	e

Die Safety Evaluation im TIA Selection Tool verwendet ausschließlich die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) und den zugehörige Performance Level (PL) gemäß Tabelle K.1 der ISO 13849-1.

1.2 Kategorie (Kat.) – vorgesehene Architektur

In der Tabelle 10 der ISO 13849-1 (siehe unten) finden sich die grundlegenden Anforderungen für die Kategorien. Es ist seitens des Anwenders sicherzustellen, dass alle Anforderungen für eine Kategorie erfüllt werden. Vollständige Anforderungen sind in Abschnitt 6 der ISO 13849-1 zu finden.

Grundsätzlich kann nur dann ein Performance Level berechnet werden, wenn die Anforderungen an MTTFD jedes Kanals, DCavg und CCF der gewählten Kategorie entsprechen.

Tabelle 1-3 Zusammenfassung der Anforderungen für Kategorien

Kat.	Zusammenfassung der Anforderungen	Systemverhalten	Prinzip zum Erreichen der Sicherheit	$MTTF_D$ jedes Kanals	DC_{avg}	CCF
B	SRP/CS(en) und/oder ihre Schutz-einrichtungen sowie ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt, zusammengebaut und kombiniert werden, dass sie den zu er-wartenden Einflüssen standhalten können. Grundlegende Sicherheitsprinzipien müssen verwendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.	Überwiegend durch die Auswahl von Bauteilen charakterisiert.	niedrig bis mittel	keine	nicht relevant
1	Die Anforderungen von B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheits-prinzipien müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen, aber die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B.	Überwiegend durch die Auswahl von Bauteilen charakterisiert.	hoch	keine	nicht relevant
2	Die Anforderungen von B und die Verwendung bewährter Sicherheits-prinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinen-steuerung getestet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Tests führen. Der Verlust der Sicherheits-funktion wird durch den Test erkannt.	Überwiegend durch die Struktur charakterisiert.	niedrig bis hoch	niedrig bis mittel	siehe Anhang F

Kat.	Zusammenfassung der Anforderungen	Systemverhalten	Prinzip zum Erreichen der Sicherheit	$MTTF_D$ jedes Kanals	DC_{avg}	CCF
3	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet werden, dass: – ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und – wenn immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheits-funktion immer erhalten. Einige, aber nicht alle Fehler werden erkannt. Eine Anhäufung von unerkannten Fehlern kann zum Verlust der Sicherheitsfunktion führen	Überwiegend durch die Struktur charakterisiert	niedrig bis hoch	niedrig bis mittel	siehe Anhang F
4	Die Anforderungen von B und die Ver-wendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet werden, dass: – ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und – der einzelne Fehler bei oder vor der nächsten Anforder-ung der Sicherheits-funktion erkannt wird. Wenn diese Erkenn-ung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheits-funktion immer erhalten. Die Erkennung von Fehleranhäufungen reduziert die Wahrscheinlichkeit des Verlustes der Sicherheitsfunktion (hohe DC). Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern.	Überwiegend durch die Struktur charakterisiert.	hoch	hoch, einschl. der Fehler-anhäuf-ung	siehe Anhang F

2 Diagnose

2.1 Diagnosedeckungsgrad (DC)

Der Wert für den Diagnosedeckungsgrad wird in vier Stufen angegeben:

Tabelle 2-1 Diagnosedeckungsgrad (DC)

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

Zur Abschätzung des Diagnosedeckungsgrades findet sich im Anhang E der ISO 13849-1 die Tabelle E.1 zur Hilfestellung für Ein- und Ausgabeeinheiten.

Tabelle 2-2 Beispiele der ISO 13849-1 für Eingabeeinheiten

Maßnahme	**Diagnosedeckungsgrad DC**
Eingabeeinheit	
Zyklischer Testimpuls durch dynamische Änderung der Eingangssignale	90 %
Plausibilitätsprüfung, z. B. Verwendung der Schließer- und Öffnerkontakte von zwangsgeführten Relais	99 %
Kreuzvergleich von Eingangssignalen ohne dynamischem Test	0 % bis 99 %, abhängig davon, wie oft ein Signalwechsel durch die Anwendung erfolgt
Kreuzvergleich von Eingangssignalen mit dynamischem Test, wenn Kurzschlüsse nicht bemerkt werden können (bei Mehrfach-Ein-/Ausgängen)	90 %
Kreuzvergleich von Eingangssignalen mit unmittelbarem und Zwischenergebnissen in der Logik (L) und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Ausgängen)	99 %
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Betätigungselementen)	90 % bis 99 %, abhängig von der Anwendung
Direkte Überwachung (z. B. elektrische Stellungsüberwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung)	99 %
Fehlererkennung durch den Prozess	0 % bis 99 %, abhängig von der Anwendung; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level e !
Überwachung einiger Merkmale des Sensors (Ansprechzeit, der Bereich analoger Signale, z. B. elektrischer Widerstand, Kapazität)	60 %

Tabelle 2-3 Beispiele der ISO 13849-1 für Ausgabeeinheiten

Maßnahme	Diagnosedeckungsgrad DC
Ausgabeeinheiten	
Überwachung der Ausgänge durch einen Kanal ohne dynamischen Test	0 % bis 99 %, abhängig davon, wie oft ein Signalwechsel durch die Anwendung erfolgt
Kreuzvergleich von Ausgangssignalen ohne dynamischem Test	0 % bis 99 %, abhängig davon, wie oft ein Signalwechsel durch die Anwendung erfolgt
Kreuzvergleich von Ausgangssignalen mit dynamischem Test, ohne Erkennung von Kurzschlüssen (bei Mehrfach-Ein-/Ausgängen)	90 %
Kreuzvergleich von Ausgangssignalen mit unmittelbarem Ergebnis in der Logik (L) und zeitlich und logischer Softwareüberwachung des Programmablaufs und Erkennen statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Ausgängen)	99 %
Redundanter Abschaltpfad mit Überwachung der Betätigungselemente durch die Logik und Testeinrichtung	99 %
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Betätigungselementen)	90 % bis 99 %, abhängig von der Anwendung
Fehlererkennung durch den Prozess	0 % bis 99 %, abhängig von der Anwendung; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level e !
Direkte Überwachung (z. B. elektrische Überwachung der Steuerungs-ventile, Überwachung elektromechanischer Einheiten durch Zwangs-führung)	99 %

3 Zuverlässigkeit

3.1 Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals ($MTTF_D$) und Bauteilgüte (B_{10D})

Für jedes SRP/CS (Teilsystem) nach Tabelle 4 der ISO 13849-1 beträgt der maximale Wert der $MTTF_D$ für jeden Kanal 100 Jahre. Für SRP/CS (Teilsysteme) der Kategorie 4 erhöht sich der maximale Wert der $MTTF_D$ für jeden Kanal auf 2 500 Jahre. Der Wert der $MTTF_D$ jedes Kanals wird in drei Stufen angegeben:

Tabelle 3-1 Mittlere Zeit jedes Kanals bis zum gefahrbringenden Ausfall ($MTTF_D$)

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre

Mit dem B_{10} – Wert (Anzahl Schaltspiele nach dem 10% der Prüflinge ausgefallen sind) und dem Anteil gefahrbringender Ausfälle (%) wird der B_{10D} – Wert ermittelt:

B_{10D} = B_{10} / Anteil gefahrbringender Ausfälle

Anmerkung: Ist nur der B_{10D} – Wert bekannt, dann kann dieser direkt in die Eingabemaske B10 eingetragen und der Anteil gefahrbringenden Ausfälle auf 100% gesetzt werden.

Mit dem B_{10D} und der Anzahl Betätigungen pro Jahr wird der $MTTF_D$ für verschleißbehaftete Komponenten bestimmt.

Die Berechnung erfolgt auf folgenden Annahmen:

1 Tag = 24 Stunden; 1 Woche = 7 Tage; 1 Monat = 30 Tage; 1 Jahr = 365 Tage.

Die folgende Tabelle C.1 der ISO 13849-1 zeigt mögliche Wertebereiche für B_{10D} und $MTTF_D$ sowie weitere relevante Normen auf.

Wichtiger Hinweis: die Angaben des Herstellers von Bauteilen sind den Werten aus der folgen-den Tabelle C.1 der ISO 13849-1 immer vorzuziehen.

Tabelle 3-2 Internationale Normen, die sich mit $MTTF_D$ oder $B10_D$ für Bauteile befassen

	Grundlegende und bewährte Sicherheits-prinzipien nach ISO 13849-2:2003	**Andere relevante Normen**	**Typische Werte: $MTTF_D$ (Jahre) B_{10D} (Zyklus)**
Mechanische Bauteile	Tabellen A.1 und A.2	–	$MTTF_D$ = 150
Hydraulische Bauteile mit n_{op} ≥ 1 000 000 Zyklen pro Jahr	Tabellen C.1 und C.2	ISO 4413	$MTTF_D$ = 150
Hydraulische Bauteile mit 1 000 000 Zyklen pro Jahr > n_{op} ≥ 500 000 Zyklen pro Jahr	Tabellen C.1 und C.2	ISO 4413	$MTTF_D$ = 300
Hydraulische Bauteile mit 500 000 Zyklen pro Jahr > n_{op} ≥ 250 000 Zyklen pro Jahr	Tabellen C.1 und C.2	ISO 4413	$MTTF_D$ = 600
Hydraulische Bauteile mit 250 000 Zyklen pro Jahr > n_{op}	Tabellen C.1 und C.2	ISO 4413	$MTTF_D$ = 1 200
Pneumatische Bauteile	Tabellen B.1 und B.2	ISO 4414	B_{10D} = 20 000 000
Relais und Hilfsschütze mit geringer Last	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	B_{10D} = 20 000 000
Relais und Hilfsschütze mit nominaler Belastung	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	B_{10D} = 400 000
Näherungsschalter mit geringer Last	Tabellen D.1 und D.2	IEC 60947 ISO 14119	B_{10D} = 20 000 000
Näherungsschalter mit nominaler Last	Tabellen D.1 und D.2	IEC 60947 ISO 14119	B_{10D} = 400 000
Schütze mit geringer Last	Tabellen D.1 und D.2	IEC 60947	B_{10D} = 20 000 000
Schütze mit nominaler Last	Tabellen D.1 und D.2	IEC 60947	B_{10D} = 1 300 000 (siehe Anmerkung 1)
Positionsschalter [a]	Tabellen D.1 und D.2	IEC 60947 ISO 14119	B_{10D} = 20 000 000
Positionsschalter (mit separatem Betätiger, Zuhaltung) [a]	Tabellen D.1 und D.2	IEC 60947 ISO 14119	B_{10D} = 2 000 000
Not-Halt-Geräte [a]	Tabellen D.1 und D.2	IEC 60947 ISO 13850	B_{10D} = 100 000
Druck-Taster (z. B. Zustimmungsschalter) [a]	Tabellen D.1 und D.2	IEC 60947	B_{10D} = 100 000

ANMERKUNG 1 $B10_D$ wird abgeschätzt als zweimal B10 (50 % gefährlicher Ausfall), wenn keine anderen Angaben vorliegen (z. B. Produktnorm).

ANMERKUNG 2 „Nominale Last“ oder „geringe Last“ sollten die Sicherheitsprinzipien berücksichtigen, die in ISO 13849-2 beschrieben sind, wie Überdimensionierung des Strom-Nennwerts. „Geringe Last“ bedeutet z. B. 20 %.

ANMERKUNG 3 Not-Halt-Geräte nach IEC 60947-5-5 und ISO 13850 sowie Zustimmungsschalter nach IEC 60947-5-8 können als Teilsystem der Kategorie 1 oder Kategorie 3/4 abgeschätzt werden, je nach Anzahl der elektrischen Ausgangskontakte und der Fehlererkennung im nachgeordneten SRP/CS. Jedes Kontaktelement (einschließlich der mechanischen Betätigung) kann als ein Kanal mit entsprechendem *B*10D-Wert betrachtet werden. Für Zustimmungsschalter nach IEC 60947-5-8 umfasst dies die Öffnungsfunktion durch Durchdrücken oder Loslassen. In einigen Fällen kann es möglich sein, dass der Maschinenhersteller einen Fehlerausschluss nach ISO 13849-2, Tabelle D.8, unter Berücksichtigung der jeweiligen Anwendungs- und Umgebungsbedingungen des Gerätes anwenden kann.

[a] Falls Fehlerausschluss für Zwangsöffnung möglich ist.

4 Resistenz

4.1 Abschätzung der Anfälligkeit gegenüber Ausfällen infolge gemeinsamer Ursache (CCF)

Ab Kategorie 2 müssen Maßnahmen gegen CCF berücksichtigt werden.

Mit der Tabelle F.1 der ISO 13849-1 können die verschiedenen Maßnahmen mit Punkten bewertet werden (siehe auch „CCF ermitteln“).

Die Gesamtpunktzahl muss >= 65 Punkte betragen, damit die Maßnahmen gegen CCF erfüllt sind.

Wenn die ermittelte Gesamtpunktzahl < 65 ist, dann sind die Maßnahmen gegen CCF nicht erfüllt.

Somit sind auch die Anforderungen der Kategorie nicht erfüllt und es kann kein Performance Level ermittelt werden, bzw. es ist keine Aussage möglich.