Hilfe zur Anwendung der IEC 62061

Safety Evaluation im TIA Selection Tool

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

Siemens Industry Online Support

Inhaltsverzeichnis

1 Sicherheitsintegrität und -architektur

1.1 Sicherheits-Integritätslevel (SIL)

Drei Sicherheits-Integritätslevel (SIL1, SIL 2 und SIL 3) sind mit definierten Bereichen der Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (PFHD) festgelegt:

Tabelle 1-1 Sicherheits-Integritätslevel (SIL)

Sicherheits-Integritätslevel (SIL)	Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde 1/h (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2	≥ 10^{-7} bis < 10^{-6}
1	≥ 10^{-6} bis < 10^{-5}

Der Sicherheits-Integritätslevel einer Sicherheitsfunktion ergibt sich aus der Summe der Wahrscheinlichkeiten eines gefahrbringenden Ausfalls je Stunde (PFH_D) und dem niedrigsten SIL CL aller Teilsysteme.

1.2 Strukturelle Einschränkung von Teilsystemen (SIL CL)

Der maximal erreichbare SIL eines Teilsystems wird mit SIL CL (SIL Claim Limit) angegeben (SIL Eignung). Der SIL CL ist abhängig von

- der Architektur (HFT),
- dem Anteil sicherer Ausfälle (SFF) und
- indirekt der Diagnose (DC).

Eine 1-kanalige Architektur entspricht einer Hardware-Fehlertoleranz (HFT) von 0 und eine 2-kanalige Architektur einer Hardware-Fehlertoleranz (HFT) von 1.

Beispiel mit HFT = 0

- 1 Komponente (mechanisch und elektrisch 1-kanalig, ein Positionsschalter)

Beispiele mit HFT = 1

- 2 Komponenten (mechanisch und elektrisch 2-kanalig, zwei Positionsschalter)
- 1 Komponente (mechanisch 1-kanalig und elektrisch 2-kanalig, Not-Halt Befehlsgerät).

Der Anteil sicherer Ausfälle (SFF) ist abhängig von dem Diagnosedeckungsgrad (DC).

Tabelle 1-2 Strukturelle Einschränkung von Teilsystemen (SIL CL)

Anteil sicherer Ausfälle (SFF)	**Hardware-Fehlertoleranz (HFT)**		
	0	**1**	**2**
< 60%	Nicht erlaubt (siehe Anmerkung)	SIL 1	SIL 2
60% bis < 90%	SIL 1	SIL 2	SIL 3
90% bis < 99%	SIL 2	SIL 3	SIL 3
≥ 99%	SIL 3	SIL 3	SIL 3

Anmerkung: SIL 1 ist mit bewährten Bauteilen (z.B. Positionsschalter, Not-Halt Befehlsgerät, Schütz) gemäß ISO 13849-1 erreichbar.

Der SIL CL kann strukturell auf SIL 2 eingeschränkt sein, wenn ein Fehlerausschluss gemacht wird, der zu einem gefahrbringenden Ausfall des Teilsystems führen könnte.

Beispiel: ein Positionsschalter mit getrenntem Betätiger (1 Komponente), der elektrisch 2-kanalig ausgewertet wird.

Ausnahme: mit einem Not-Halt Befehlsgerät, das elektrisch 2-kanalig ausgewertet wird, kann grundsätzlich SIL 3 erreicht werden.

2 Diagnose

2.1 Diagnosedeckungsgrad (DC)

Zur Abschätzung des Diagnosedeckungsgrades kann als Alternative die Tabelle E.1 der ISO 13849-1 zur Hilfestellung herangezogen werden.

Beispiele aus der Tabelle E.1 der ISO 13849-1 für Ein- und Ausgabeeinheiten:

Tabelle 2-1 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 2-2 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 Gefahrbringende Ausfallrate (λ_D) und Bauteilgüte (B_{10})

Mit dem B10 – Wert (Anzahl Schaltspiele nach dem 10% der Prüflinge ausgefallen sind), dem Anteil gefahrbringender Ausfälle (%) und der Anzahl Betätigungen pro Stunde wird die gefahrbringende Ausfallrate (λ_D) für verschleißbehaftete Komponenten ermittelt.

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} ($B_{10D} = B_{10}$ / Anteil gefahrbringender Ausfälle) 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 3-1 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.

3.2 Proof-Test-Intervall oder Gebrauchsdauer (T1)

Grundsätzlich wird für den Zeitraum T1 die Gültigkeit der sicherheitstechnischen Kenngrößen vorausgesetzt.

Der T1 - Wert ist der kleinere Wert des Intervalls für den Proof-Test oder der Gebrauchsdauer: dabei stellt der Proof-Test eine Prüfung eines Teilsystems dar, mit dem ein „Wie-Neu-Zustand“ nachgewiesen werden kann und die Gebrauchsdauer den erlaubten Verwendungszeitraum.

In den meisten Fällen kann der T1 - Wert mit der Gebrauchsdauer der verwendeten Komponente angenommen werden.

4 Resistenz

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

Ab einer 2-kanaligen Architektur müssen Maßnahmen gegen CCF berücksichtigt werden.

Mit der Tabelle F.1 der IEC 62061 können die verschiedenen Maßnahmen mit Punkten bewertet werden (siehe auch „CCF ermitteln“).

Die ermittelte Gesamtpunktzahl dient dann zur Abschätzung des Faktors der Ausfälle infolge gemeinsamer Ursache (CCF – Faktor oder β) durch Verwendung der Tabelle F.2 der IEC 62061.

Dieser CCF – Faktor kann 10%, 5%, 2% oder 1% betragen.

Anmerkung: es wird empfohlen zuerst den CCF – Faktor mit 10% anzunehmen. Eine Reduzierung des CCF – Faktors hat eine Verbesserung des PFH_D zur Folge; dies muss dann entsprechend der Tabelle F.1 der IEC 62061 nachgewiesen werden.