ZVEI
Automation

Sicherheit von Maschinen

Erläuterungen zur Anwendung der Normen EN 62061 und EN ISO 13849-1

Sicherheit von Maschinen

Erläuterungen zur Anwendung der Normen EN 62061 und EN ISO 13849-1

Sie sind Maschinenhersteller, Systemintegrator oder rüsten Maschinen um?

Was Sie bei der funktionalen Sicherheit zukünftig berücksichtigen sollten!

1. Grundsätzliche Vorgehensweise um die Anforderungen der Maschinenrichtlinie zu erfüllen

Was muss ich tun um eine Maschine richtlinienkonform in den Verkehr zu bringen?
Die EG Maschinenrichtlinie verlangt, dass von Maschinen keine Gefahr ausgehen darf (Gefahrenanalyse nach EN ISO 14121-1). Da es in der Technik kein Nullrisiko gibt, gilt es ein akzeptables Restrisikos zu erreichen. die Sicherheit von Steuerungssystemen abhängt, müssen diese so konstruiert werden, dass die Wahrscheinlichkeit von Funktionsfehlern ausreichend gering ist. Wenn dies nicht möglich ist, dürfen auftretende Fehler nicht zum Verlust der Sicherheitsfunktion führen. Zur Erfüllung der Forderung ist es sinnvoll, harmonisierte Normen zu verwenden, die entsprechend einem Mandat der europäischen Kommission erstellt wurden und im europäischen Amtsblatt veröffentlicht sind (Vermutungswirkung). Nur so kann ein erhöhter Aufwand zum Konformitätsnachweis im Schadensfall vermieden werden.
Im Folgenden werden die beiden Normen EN 62061 und EN ISO 13849-1 gegenübergestellt und eine Auswahlhilfe für den Anwender gegeben.

2. Warum reicht die heutige EN 954-1 zukünftig nicht mehr aus?

In der Vergangenheit wurden die sicherheitsbezogenen Teile von Steuerungen einer Maschine nach der EN 954-1 ausgelegt.
Hierbei bildete das ermittelte Risiko (kategorisiert) die Grundlage. Ziel war es, der Kategorie ein entsprechendes Systemverhalten („Steuerungskategorie“) entgegen zu setzen (Deterministischer Ansatz). Nachdem nun die Elektronik und vor allem die programmierbare Elektronik in der Sicherheitstechnik Einzug gehalten hat, konnte die Sicherheit alleine mit dem einfachen Kategoriensystem der EN 954-1 nicht mehr erfasst werden. Außerdem sind keine Aussagen über Ausfallwahrscheinlichkeiten möglich (Probabilistischer Ansatz).
Abhilfe schaffen nun sowohl die EN 62061 als auch die EN ISO 13849-1 als Nachfolgenorm der EN 954-1.

3. Anwendungsbereiche (Scope) der beiden Normen

EN ISO 13849-1: *„Sicherheitsbezogene Teile von Steuerungen-Teil 1 Allgemeine Gestaltungsleitsätze"*

Diese Norm darf auf SRP/CS (Sicherheitsbezogene Teile von Steuerungen und aller Arten von Maschinen, ungeachtet der verwendeten Technologie und Energie (elektrisch, hydraulisch, pneumatisch, mechanisch, usw.) angewendet werden.

Die EN ISO 13849-1 stellt auch spezielle Anforderungen für SRP/CS mit programmierbaren elektronischen Systemen bereit.

EN 62061: *„Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer Steuerungssysteme"*

Diese Norm legt Anforderungen fest und gibt Empfehlungen für den Entwurf, die Integration und die Validierung von sicherheitsbezogenen elektrischen, elektronischen und programmierbaren elektronischen Steuerungssysteme (SRECS) für Maschinen.

Sie legt keine Anforderungen für die Leistungsfähigkeit von nicht-elektrischen (z.B. hydraulischen, pneumatischen, elektromechanischen) sicherheitsbezogenen Steuerungselementen für Maschinen fest.

4. Kurzbeschreibung EN ISO 13849-1

Die EN ISO 13849-1 setzt auf den bekannten Kategorien der EN 954-1: 1996 auf. Sie betrachtet nun ebenfalls komplette Sicherheitsfunktionen mit allen an ihrer Ausführung beteiligten Geräte.

Mit der EN ISO 13849-1 erfolgt über den qualitativen Ansatz der EN 954-1 hinaus auch eine quantitative Betrachtung der Sicherheitsfunktionen. Aufbauend auf den Kategorien werden hierfür **Performance Level (PL)** verwendet.

Für Bauteile / Geräte sind folgende sicherheitstechnische Kenngrößen notwendig:

- Kategorie (strukturelle Anforderung)
- PL: Performance Level
- $MTTF_d$: Mittlere Zeit bis zu einem gefahrlichen Ausfall (en: mean time to dangerous failure)
- B_{10d}: Anzahl von Zyklen bei denen 10% einer Stichprobe der betrachteten verschleissbehafteten Komponenten gefährlich ausgefallen sind

- DC: Diagnose-Deckungsgrad (en: diagnostic coverage)
- CCF: Fehler gemeinsamer Ursache (en: common causefailure)
- T_M: Mission Time

Die Norm beschreibt die Ermittlung des Performance Level (PL) für sicherheitsrelevante Teile von Steuerungen auf Basis vorgesehener Architekturen (designated architectures) für die vorgesehene Gebrauchsdauer T_M. Bei Abweichungen hiervon verweist die EN ISO 13849-1 auf die IEC 61508. Bei Kombination mehrerer sicherheitsrelevanter Teile zu einem Gesamtsystem macht die Norm Angaben zur Ermittlung des resultierenden PL.

Für weitere Hinweise zur Validierung verweist die EN ISO 13849-1 auf den Teil 2, der bereits Ende 2003 veröffentlicht wurde. Dieser Teil macht Angaben zur Fehlerbetrachtung, Wartung, technischen Dokumentation und zu Hinweisen zum Gebrauch.Die Übergangsfrist von der EN 954-1 zur EN ISO 13849-1 endet im Oktober 2009. In dieser Zeit können beide Normen alternativ angewendet werden.

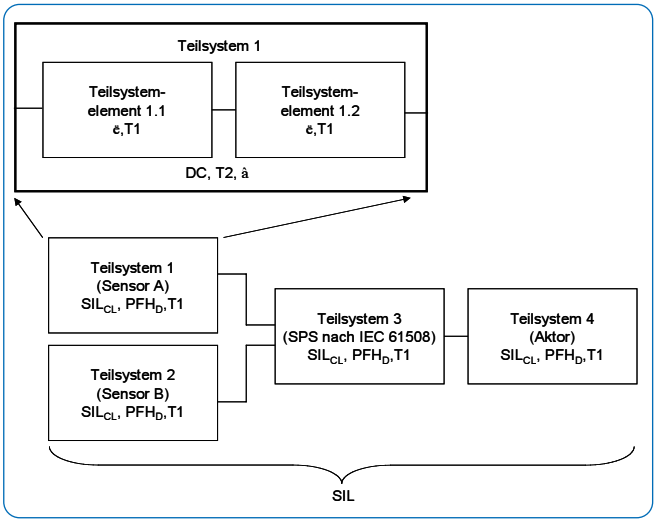
5. Kurzbeschreibung EN 62061

Die EN 62061 stellt eine sektorspezifische Norm unterhalb der IEC 61508 dar. Sie beschreibt die Realisierung sicherheitsrelevanter elektrischer und elektronischer Steuerungssysteme von Maschinen und betrachtet den gesamten Lebenszyklus von der Konzeptphase bis zur Außerbetriebnahme. Basis bilden quantitative und qualitative Betrachtungen von sicherheitsbezogenen Steuerungsfunktionen.

Die Leistungsfähigkeit wird durch den **Safety Integrity Level (SIL)** beschrieben.

Hierbei wird ausgehend von den aus der Risikoanalyse hervorgehenden Sicherheitsfunktionen eine Aufteilung in Teilsicherheitsfunktionen und schließlich eine Zuordnung dieser Teilsicherheitsfunktionen auf reale Geräte, Teilsysteme und Teilsystemelemente genannt, vorgenommen. Es wird sowohl Hardware als auch Software behandelt.

Ein sicherheitsgerichtetes Steuerungssystem besteht aus verschiedenen Teilsystemen. Die Teilsysteme sind durch die Kenngrössen (SIL-Eignung und PFH_D) sicherheitstechnisch beschrieben.



Sicherheitstechnische Kenngrößen für Teilsysteme:

- SILCL: SIL-Anspruchsgrenze (Eignungen: SIL claim limit)
- PFH_D: Wahrscheinlichkeit gefährlicher Ausfalle pro Stunde (en: probability of dangerous failure per hour)
- T_1: Lebensdauer (en: lifetime)
  Diese Teilsysteme wiederum können aus unterschiedlich verschalteten Teilsystemelementen (Geräten) mit den Kenngrößen zur Ermittlung des entsprechenden PFH_D-Wertes des Teilsystems bestehen.

  Sicherheitstechnische Kenngrössen für Teilsystemelemente (Geräte):
- λ: Ausfallrate (en: failure rate);
  für verschleißbehaftete Elemente: B_{10}-Wert
- SFF: Anteil sicherer Ausfälle (en: Safe Failure Fraction)

Bei elektromechanischen Geräten wird die Ausfallrate vom Hersteller bezogen auf eine Anzahl Schaltspiele als B_{10}-Wert angegeben. Die zeitbezogene Ausfallrate und die Lebensdauer müssen an Hand der Schalthäufigkeit für die jeweilige Anwendung bestimmt werden.

Beim Entwurf / Konstruktion festzulegende interne Parameter für das Teilsystem, das aus Teilsystemelementen zusammengesetzt wird:

- T_2: Diagnose-Testintervall (en: diagnostic test interval)
- β: Empfindlichkeit für Fehler gemeinsamer Ursache (en: susceptibility to common cause failure)
- DC: Diagnosedeckungsgrad (en: diagnostic coverage)
  Der PFHD-Wert der sicherheitsgerichteten Steuerung ermittelt sich aus der Addition der einzelnen PFHD-Werte der Teilsysteme.

Beim Aufbau einer sicherheitsgerichteten Steuerung hat der Anwender folgende Möglichkeiten:

- Verwendung von Geräten und Teilsystemen, die die EN 954-1 bzw. IEC 61508 oder EN 62061 bereits erfüllen. Dabei werden in der Norm Angaben gemacht, wie qualifizierte Geräte bei der Realisierung von Sicherheitsfunktionen integriert werden können.
- Entwicklung eigener Teilsysteme.
  – Programmierbare, elektronische Teilsysteme bzw. komplexe Teilsysteme: Anwendung der IEC 61508.
  – Einfache Geräte und Teilsysteme: Anwendung der EN 62061.

Die Norm stellt ein umfassendes System für die Realisierung sicherheitsrelevanter elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme dar. Die EN 62061 ist seit Dezember 2005 harmonisiert.

Für nicht-elektrische Systeme ist die EN 954-1, zukünftig die EN 13849-1 anzuwenden.

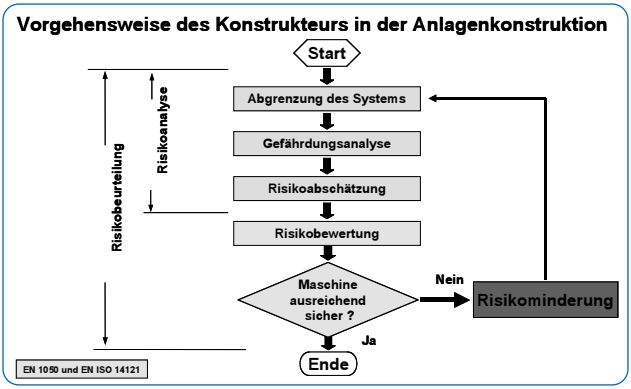
6. Schritt für Schritt zur Sicherheit – Grundsätzliche Vorgehensweise

1. Schritt – Risikobeurteilung nach EN 1050 / EN ISO 14121

Es wird davon ausgegangen, dass eine an einer Maschine vorhandene Gefährdung früher oder später zu einem Schaden führt, falls keine Schutzmaßnahme(n) durchgeführt wird (werden).
Schutzmaßnahmen sind eine Kombination der vom Konstrukteur und der vom Benutzer durchgeführten Maßnahmen. Maßnahmen, die bereits in der Konstruktionsphase getroffen werden können, sind den vom Benutzer

durchgeführten Maßnahmen vorzuziehen und im Allgemeinen wirksamer als diese.
Unter Berücksichtigung der Erfahrungen von Benutzern ähnlicher Maschinen und des Informationsaustausches mit den potentiellen Benutzern (wann immer dies möglich ist) muss der Konstrukteur in der unten angegebenen Reihenfolge vorgehen:

– Festlegen der Grenzen und der bestimmungsgemäßen Verwendung der Maschine;
– Identifizieren von Gefährdungen und zugehörigen Gefährdungssituationen;
– Einschätzen des Risikos für jede identifizierte Gefährdung und Gefährdungssituation;
– Bewerten des Risikos und Treffen von Entscheidungen über die Notwendigkeit zur Risikominderung.



2. Schritt – Bestimmung der Maßahmen zur Reduzierung der ermittelten Risiken

Das zu erreichende Ziel besteht in der größtmöglichen Risikominderung unter Berücksichtigung verschiedener Faktoren. Der Prozess ist iterativ, und es können bei bestmöglicher Anwendung der zur Verfügung stehenden Technologien mehrere aufeinander folgende Wiederholungen erforderlich sein, um das Risiko zu mindern.

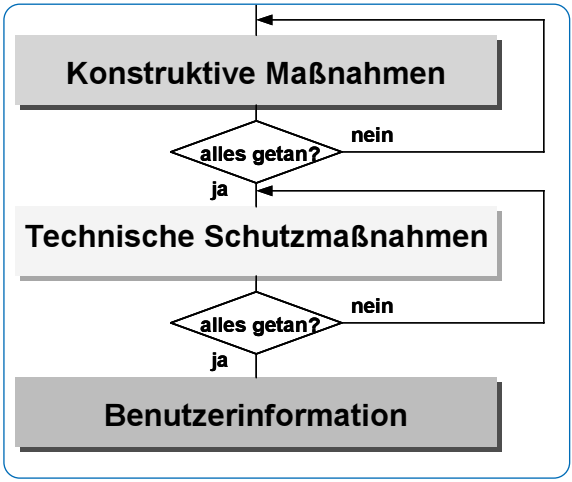
Bei der Durchführung dieses Prozesses ist es erforderlich, die folgende Rangfolge zu berücksichtigen:

1. Sicherheit der Maschine in sämtlichen Phasen ihrer Lebensdauer;
2. Fähigkeit der Maschine, ihre Funktion auszuführen;
3. Benutzerfreundlichkeit der Maschine.

Erst jetzt dürfen die Herstellungs-, Betriebs- und Demontagekosten der Maschine berücksichtigt werden.

Die Gefährdungsanalyse und der Prozess der Risikoreduzierung erfordert, dass Gefährdungen durch eine Hierarchie von Maßnahmen beseitigt oder reduziert werden:

- Beseitigung von Gefährdungen oder Risikoreduzierung durch den Entwurf
- Risikoreduzierung durch Schutzeinrichtungen und mögliche ergänzende Schutzmaßnahmen
- Risikoreduzierung durch Bereitstellung einer Benutzerinformation über das Restrisiko



3. Schritt – Risikoreduzierung durch steuerungstechnische Maßnahmen

Wird die erforderliche Risikominderung durch sicherheitsrelevante Steuerungsteile zur Steuerung einer Schutzmassnahme realisiert, so ist der Entwurf dieser Steuerungsteile ein integraler Teil der gesamten Entwurfsprozedur für die Maschine. Das sicherheitsrelevante Steuerungssystem stellt die Sicherheitsfunktion(en) zukünftig mit einem SIL oder PL bereit, der die erforderliche Risikominderung erreicht.

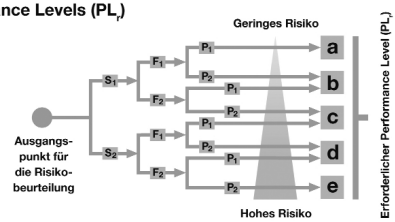
4. Schritt – Steuerungstechnische Umsetzung mit Hilfe von EN 13849-1 bzw. EN 62061

EN ISO 13849-1	EN IEC 62061

1) Bestimmung der erforderlichen Leistungsfähigkeit

Bestimmung des erforderlichen Performance Levels (PL_r)

- **S – Schwere der Verletzung**
  - S_1 = leichte Verletzung (normalerweise reversibel)
  - S_2 = schwere Verletzung, einschließlich Tod (normalerweise irreversibel)
- **F – Häufigkeit und/oder Dauer der Gefährdungsexposition**
  - F_1 = selten bis öfters und/oder kurze Dauer
  - F_2 = häufig bis dauernd und/oder lange Dauer
- **P – Möglichkeiten zur Vermeidung der Gefährdung**
  - P_1 = möglich unter bestimmten Bedingungen
  - P_2 = kaum möglich



EN ISO 13849-1

Risikoabschätzung und Festlegung des erforderlichen Safety Integrity Levels (SIL)

Auswirkungen und Schwere	S	Häufigkeit und Dauer	F	Wahrscheinlichkeit gef. Ereignis	W	Vermeidung	P	Klasse K 3-4	5-7	8-10	11-13	14-15
Tod, Verlust eines Auges oder Armes	4	≤ 1 Stunde	5	häufig	5			SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
permanent, Verlust von Fingern	3	> 1 h – ≤ 1 Tag	5	wahrscheinlich	4				AM	SIL 1	SIL 2	SIL 3
reversibel, medizinische Behandlung	2	> 1 Tag – ≤ 2 Wo.	4	möglich	3	unmöglich	5			AM	SIL 1	SIL 2
reversibel, Erste Hilfe	1	> 2 Wo. – ≤ 1 Jahr	3	selten	2	möglich	3				AM	SIL 1
		> 1 Jahr	2	vernachlässigbar	1	wahrscheinlich	1					

☐ AM = andere Maßnahmen empfohlen

EN IEC 62061

2) Spezifikation

Die Spezifikation der funktionalen Anforderungen muss Details jeder auszuführenden Sicherheitsfunktion beschreiben. Hierzu sind erforderliche Schnittstellen zu anderen Steuerungsfunktionen zu definieren sowie notwendige Fehlerreaktionen festzulegen. Dazu muss der erforderliche SIL oder PL festgelegt werden.

3) Entwurf der Steuerungsarchitektur

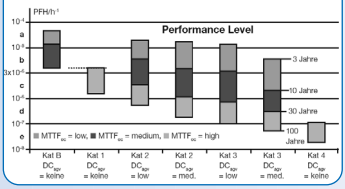
Ein Teil des Prozesses der Risikominderung ist es, die Sicherheitsfunktionen der Maschine zu bestimmen. Dies beinhaltet die Sicherheitsfunktionen der Steuerung, z.B. zur Verhinderung des unerwarteten Anlaufs. Bei der Bestimmung der Sicherheitsfunktionen sollte immer beachtet werden, dass eine Maschine unterschiedliche Betriebszustände (z.B. Automatik- & Einrichtbetrieb) hat und die Schutzmaßnahmen in diesen einzelnen Zuständen durchaus unterschiedlich sein können (z.B. Schleichgangfahrt im Einrichtbetrieb <-> Zweihand bei Automatikbetrieb). Eine Sicherheitsfunktion kann durch eine oder mehrere sicherheitsrelevante Steuerungsteile realisiert sein und mehrere Sicherheitsfunktionen können sich eine oder mehrere sicherheitsrelevante Steuerungsteile aufteilen (z.B. Logikbaugruppe, Energieübertragungselement(e)).

EN ISO 13849-1	EN IEC 62061
4) Bestimmung der <u>erreichten</u> Leistungsfähigkeit	
Für jede gewählte SRP/CS und/oder der Kombination von SRP/CS die eine Sicherheitsfunktion ausführt, muss eine Abschätzung des PL durchgeführt werden. Der PL der SRP/CS muss bestimmt werden durch die Abschätzung folgender Parameter: • des $MTTF_d$-Wertes einzelner Komponenten; • der DC; • des CCF; • der Struktur (Kategorie). • des Verhaltens der Sicherheitsfunktion unter Fehlerbedingung(en); • sicherheitsbezogener Software • systematischer Ausfälle • der Fähigkeit eine Sicherheitsfunktion unter vorhersehbaren Umgebungsbedingungen auszuführen.	Die Auswahl oder der Entwurf der SRECS muss prinzipiell mindestens die folgenden Anforderungen erfüllen: Anforderungen zur Sicherheitsintegrität der Hardware bestehend aus • den strukturellen Einschränkungen zur Sicherheitsintegrität der Hardware • den Anforderungen zur Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle sowie den Anforderungen zur systematischen Sicherheitsintegrität bestehend aus • den Anforderungen zur Vermeidung von Ausfällen und • den Anforderungen zur Beherrschung systematischer Fehler. Die EN 62061 beschreibt auch Anforderungen an die Realisierung von Applikations-Programmen. Sicherheitstechnische Kenngrößen fur Teilsysteme: • SILCL: SIL-Eignung (en: SIL claim limit) • PFH_D: Wahrscheinlichkeit gefährlicher Ausfalle pro Stunde • T_1: Lebensdauer

EN ISO 13849-1

Performance level	durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]
a	$10^{-5} \leq PFH < 10^{-4}$
b	$3 \cdot 10^{-6} \leq PFH < 10^{-5}$
c	$10^{-6} \leq PFH < 3 \cdot 10^{-6}$
d	$10^{-7} \leq PFH < 10^{-6}$
e	$10^{-8} < PFH < 10^{-7}$

Beziehung zwischen den Kategorien DC, $MTTF_d$ und PL



Anmerkung:
Die Tabelle beschreibt die Beziehung zwischen den beiden Konzepten der Normen (PL und SIL). Die in dieser Tabelle zugrundegelegte „PFH-Kopplung" ist zur Beurteilung allerdings allein nicht ausreichend.

EN IEC 62061

durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]	SIL Level
$10^{-6} \leq PFH < 10^{-5}$	SIL 1
$10^{-7} \leq PFH < 10^{-6}$	SIL 2
$10^{-8} < PFH < 10^{-7}$	SIL 3

Sicherheitstechnische Kenngrößen für Teilsystemelemente (Geräte):

- λ: Ausfallrate;
- B_{10}-Wert: für verschleißbehaftete Bauteile:
- T_1: Lebensdauer
- T_2: Diagnose-Testintervall
- β: Empfindlichkeit für Ausfälle gemeinsamer Ursache
- DC: Diagnosedeckungsgrad
- SFF: Anteil sicherer Ausfälle (en: Safe failure Fraction)

SFF	HFT 0	HFT 1	HFT 2
< 60 %	Nicht zulässig	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

EN ISO 13849-1	EN IEC 62061

Performance level	SIL Level
a	--
b	SIL 1
c	SIL 1
d	SIL 2
e	SIL 3

Anmerkung:
Die Tabelle beschreibt die Beziehung zwischen den beiden Konzepten der Normen (PL und SIL). Die in dieser Tabelle zugrundegelegte „PFH-Kopplung“ ist zur Beurteilung allerdings allein nicht ausreichend.

5) Vertifikation

Für jede einzelne Sicherheitsfunktion muss der PL der zugehörigen SRP/CS(en) dem „Erforderlichen Performance Level“, entsprechen. Die PLs verschiedener SRP/CS, die Teil einer Sicherheitsfunktion sind, müssen größer oder gleich dem erforderlichen Performance Level dieser Funktion sein.

Bei der Zusammenschaltung mehrerer SRP/CS kann der endgültige PL mit Hilfe der Tabelle 11 aus der Norm bestimmt werden

Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls jeder SRCF als Folge gefahrbringender zufälliger Hardwareausfälle muss gleich oder kleiner als der in der Spezifikation der Sicherheitsanforderungen festgelegte Ausfallgrenzwert sein.

Der SIL, der durch das SRECS auf Grund der strukturellen Einschränkungen erreicht wird, ist geringer als oder gleich der Niedrigsten SILCL irgendeines Teilsystems, das an der Ausführung der Sicherheitsfunktion beteiligt ist.

6) Validierung

Die Gestaltung einer sicherheitsrelevanten Steuerungsfunktion muss validiert werden. Die Validierung muss zeigen, dass die Kombination für jede Sicherheitsfunktion der sicherheitsrelevanten Teile die entsprechenden Anforderungen erfüllt.

7. Glossar

Abkürzung	Englischer Begriff	Deutsche Erklärung
B_{10d}		Anzahl von Zyklen, bis 10% Komponenten gefahrbringend ausfallen
λ	Failure Rate	Ausfallrate
λ_s		Ausfallrate bei ungefährlichen Fehlern
λ_d		Ausfallrate bei gefahrbringenden Fehlern
CCF	Common Cause Failure	Ausfall in Folge gemeinsamer Ursache
DC	Diagnostic Coverage	Fehleraufdeckungsgrad
DCavg	Average Diagnostic Coverage	Fehleraufdeckungsrate im Durchschnitt
	Designated Architecture	Vorausberechnete Struktur eines SRP/CS
HFT	Hardware Fault Tolerance	Hardware Fehlertoleranz
MTBF	Mean Time Between Failures	Mittlere Ausfallzeit, die im normalen Betrieb vergeht, bevor ein Fehler auftritt.
MTTF	Mean Time To Failure	Mittlere Zeit bis zum Ausfall
$MTTF_d$	Mean Time To	Mittlere Zeit bis zum gefahrbringenden
	Dangerous Failure	Ausfall
MTTR	Mean Time To Repair	Mittlere Reparaturzeit (immer deutlich kleiner als die MTTF)
PFH	Probability Of Failure Per Hour	Wahrscheinlichkeit eines Ausfalls pro Stunde
PFH_D	Probability Of Dangerous Failure Per Hour	Wahrscheinlichkeit des gefahrbringenden Ausfalls pro Stunde
PL	Performance Level	Fähigkeit von sicherheitsbezogenen Teilen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, um die erwartete Risikoreduzierung zu erfüllen.
PL_r	Performance Level Required	Benötigter Performance Level
SIL	Safety Integrity Level	Sicherheits-Integritätslevel
SILCL	Safety Integrity Claim Limit	SIL Anspruchsgrenze (Eignung)

Abkürzung	Englischer Begriff	Deutsche Erklärung
SRP/CS	Safety Related Parts of a Control System	Sicherheitsbezogener Teil einer Steuerung
SRECS	Safety Related Electrical Control Systems	Sicherheitsbezogeneselektrisches Steuerungssystem
T_1	Lifetime	Angenommene Lebensdauer des Sicherheitssystems
T_2	Diagnostic Test Interval	Diagnose Testintervall
T_M	Mission Time	Gebrauchsdauer
β	Susceptibility to Common Cause Failure	Empfindlichkeit für Fehler gemeinsamer Ursache
C	Duty Cycle	Betätigungszyklus (pro Stunde) eines elektromechanischen Bauteils
SFF	Safe Failure Fraction	Anteil ungefährlicher Ausfälle
Security		Umgangssprachlicher Begriff für Sicherheitsdienst oder Wachschutz. Durch Überwachung wird eine Person oder Sache geschützt.
Safety		Sammelbegriff u.a. für funktionale Sicherheit und Maschinensicherheit
Maschinen-sicherheit		Nach erfolgter Gefährdungsanalyse durch Massnahmen erreichte Risikominimierung auf akzeptiertes Restrisiko
Funktionale Sicherheit		Teil der Gesamtsicherheit, bezogen auf die Maschine und das Maschinen-Steuerungssystem, die von der korrekten Funktion des SRECS,sicherheitsbezogenen Systemen anderer Technologie und exter-nen Einrichtungen zur Risikominderung abhängt.

8. FAQ-Liste

Gibt für Magnetventile / Schütze eine SIL oder PL-Angabe?

Nein. Die Angabe eines SIL bzw. PL kann für eine einzelne Komponente nicht gemacht werden.

Was ist der Unterschied zwischen SIL und SILCL?

Die Angabe eines SIL bezieht sich immer auf eine komplette Sicherheitsfunktion während sich der SILCL auf das Teilsystem bezieht.

Gibt es eine Entsprechung zwischen PL und SIL?

Über den PFH-Wert lässt sich eine Beziehung zwischen PL und SIL bestimmen. (siehe Schritt4: „Bestimmung der erreichten Leistungsfähigkeit“).

Performance level (EN13849-1)	durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]	SIL Level nach EN IEC 62061
b	$3 \cdot 10^{-6} \leq PFH < 10^{-5}$	SIL 1
c	$10^{-6} \leq PFH < 3 \cdot 10^{-6}$	SIL 1
d	$10^{-7} \leq PFH < 10^{-6}$	SIL 2
e	$10^{-8} \leq PFH < 10^{-7}$	SIL 3

Welchen Diagnosedeckungsgrad kann ich bei Relais und Schützen mit zwangsgeführten Kontakten in Anspruch nehmen?

Entsprechend der beiden Normen lässt sich für zwangsgeführte Kontakte bei Schützen und Relais ein DC von 99% annehmen.

Voraussetzung hierfür ist eine angemessene Fehlerreaktion oder zumindest eine Warnung vor der Gefährdung.

Kann ich mit einem einzelnen Schutztürschalter die Hardware-Fehlertoleranz von 1 erreichen?

Nein, bereits ein Fehler führt zum Versagen der Schaltung

Gibt es einen PFH-Wert für verschleißbehaftete Komponenten?

Nein, der Anwender kann über den B10-Wert in Abhängigkeit von der Anzahl der Betätigungszyklen einen PFH-Wert für verschleißbehaftete Komponenten für den gegeben Anwendungsfall ermitteln.

Was ist der Unterschied zwischen MTBF und MTTF?

Die MTBF beschreibt die Zeit zwischen 2 Fehlern, im Gegensatz zur MTTF (Zeit bis zum ersten Fehler)

Was bedeutet der Index „d" bei $MTTF_d$?

„d" steht für „dangerous" 2 –> die $MTTF_d$ beschreibt die Zeit bis zum ersten gefahrbringenden Fehler

Darf ich bei der Integration komplexer programmierbarer Elektronik die EN ISO 13849-1 anwenden?

Ja. Jedoch müssen bei Betriebssystemsoftware und Sicherheitsfunktionen nach PL „e" die Anforderungen nach IEC 61508-3 berücksichtigt werden.

Was mache ich, wenn ich vom Hersteller meiner Komponenten keine Kennwerte bekomme?

Die EN ISO 13849-1 bzw. EN IEC 62061 bietet im Anhang ersatzweise Referenzwerte für häufig verwendete Komponenten. Vorzugsweise sollten jedoch die Originalwerte des Herstellers verwendet werden.

Kann ich bei Prozessventilen / Armaturen, die 1- oder 2 mal pro Jahr geschaltet werden (Low Demand), für die Berechnung der MTTF die EN ISO 13849-1 anwenden?

Nein, die EN ISO 13849-1 beschreibt nur den High-demand-mode. Daher lässt sich eine MTTF-Bewertung nur mit zusätzlichen Maßnahmen wie „Zwangsdynamisierung" vornehmen.

Kann ich bei Prozessventilen/Armaturen, die 1- oder 2 mal pro Jahr geschaltet werden (Low Demand), für die Berechnung der Ausfallrate die EN 62061 anwenden?

siehe vorige Frage

Muss Applikations-Software zertifiziert werden? Wenn „Ja" nach welcher Norm?

Nein. Eine Zertifizierungspflicht besteht gemäß der beiden Normen nicht. Jedoch kann es für Anhang IV gemäß Maschinenrichtlinie (z.B. Pressen) eine Zertifizierungspflicht geben. Anforderungen an die Erstellung von SW finden sich sowohl in der EN IEC 62061 als auch in der EN ISO 13849-1 wieder.

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.
Stresemannallee 19
60596 Frankfurt am Main
Fachverband Automation
Fachbereich Schaltgeräte, Schaltanlagen,
Industriesteuerungen
Fachkreis Niederspannungs-Schaltanlagen

Verfasser: Gunther Bernd
Fon: 069 6302-323
Fax: 069 6302-386
Mail: bernd@zvei.org
www.zvei.org/automaton

Trotz größter Sorgfalt keine
Haftung für den Inhalt

Januar 2007