ZVEI:
Die Elektroindustrie

Sicherheit von Maschinen

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

Edition II

Fachverband Automation

IMPRESSUM

Sicherheit von Maschinen

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

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Lyoner Straße 9
60528 Frankfurt am Main
Fachverband Automation
Fachbereich Schaltgeräte, Schaltanlagen, Industriesteuerungen
Technischer Ausschuss
Sicherheitssystem in der Automation

Kontakt:
Dr. Markus Winzenick
Fon: 069 6302-426
Fax: 069 6302-319
Mail: winzenick@zvei.org
www.zvei.org/automation

April 2012

Sicherheit von Maschinen

Sie sind Maschinenhersteller, Systemintegrator oder rüsten Maschinen um?

Was Sie bei der funktionalen Sicherheit zukünftig berücksichtigen sollten!

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

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 (Risikobeurteilung nach EN ISO 12100). Da es in der Technik kein Nullrisiko gibt, gilt es ein akzeptables Restrisiko zu erreichen. Wenn 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 beim Konformitätsnachweis 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 EN 954-1 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, jeder Kategorie ein entsprechendes Systemverhalten zuzuordnen (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 Nachfolgenormen 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-elektronischen (z.B. hydraulischen, pneumatischen oder 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 Geräten.

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 Geräte sind abhängig vom Gerätetyp folgende sicherheitstechnischen Kenngrößen definiert:

- Kategorie (strukturelle Anforderung)
- PL: Performance Level
- $MTTF_d$: Mittlere Zeit bis zu einem gefährlichen 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: Diagnosedeckungsgrad (en: diagnostic coverage)
- CCF: Ausfälle in Folge gemeinsamer Ursache (en: common cause failure)
- T_M: Gebrauchsdauer (en: 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.

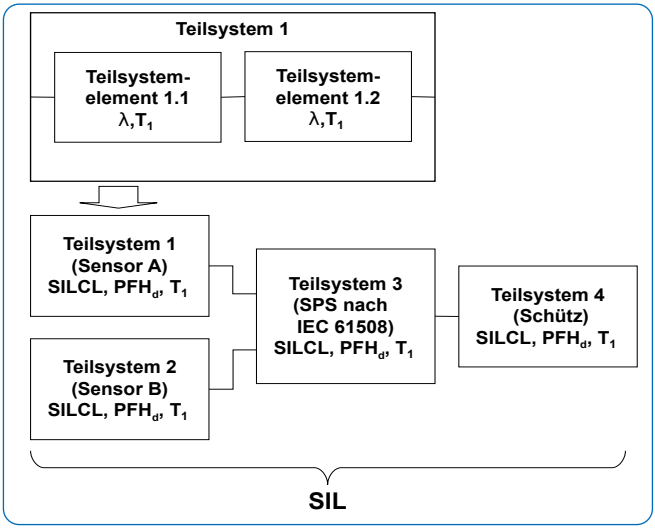
Bei Abweichungen hiervon verweist die EN ISO 13849-1 bei elektrisch/elektronischen Systemen auf die IEC 61508. Bei Kombination mehrerer sicherheitsrelevanter Teile zu einem Gesamtsystem macht die Norm Angaben zur Ermittlung des resultierenden PL.

Für die weitere Validierung verweist die EN ISO 13849-1 auf den Teil 2, der bereits Ende 2003 veröffentlicht wurde. Dieser Teil macht unter anderem Angaben zur Fehlerbetrachtung, Wartung, technischen Dokumentation und zu Hinweisen zum Gebrauch. Die Übergangsfrist von der EN 954-1 zur EN ISO 13849-1, in der beide Normen alternativ angewendet werden konnten, endete in Europa am 31. Dezember 2011.

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 einer Sicherheitsfunktion 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 (Eignung, en: SIL claim limit)
- PFH_d: Wahrscheinlichkeit gefährlicher Ausfalle pro Stunde (en: probability of dangerous failure per hour)
- T_1: Kleinster Wert aus Lebenserwartung oder Prüftest-Intervall (en: life time or proof test interval)

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 (oder ohne konstante Ausfallrate): B_{10}-Wert
- SFF: Anteil sicherer Ausfälle (en: Safe Failure Fraction)

Bei elektromechanischen Geräten wird statt der Ausfallrate vom Hersteller die Ausfalllwahrscheinlichkeit als Funktion der Schaltspiele als B_{10}-Wert angegeben. Die zeitbezogene Ausfallrate und die erwartete 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 PFH_d-Wert der sicherheitsgerichteten Steuerung ermittelt sich aus der Addition der einzelnen PFH_d-Werte der Teilsysteme.

Beim Aufbau einer sicherheitsgerichteten Steuerung hat der Anwender folgende Möglichkeiten:

- Verwendung von Geräten und Teilsystemen, die die EN ISO 13849-1 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 soll die EN ISO 13849-1 angewendet werden.

6. Schritt für Schritt zur Sicherheit – Grundsätzliche Vorgehensweise

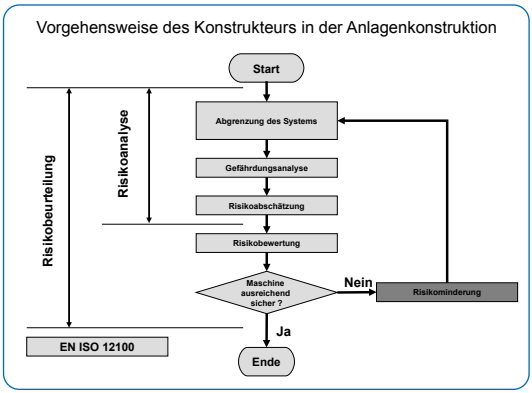
1. Schritt – Risikobeurteilung nach EN ISO 12100

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 immer 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.

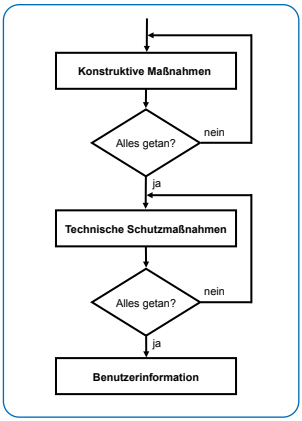
2. Schritt – Bestimmung der Maßahmen zur Minderung der ermittelten Risiken

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:

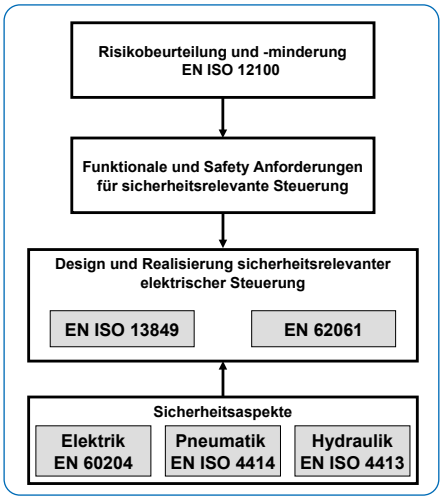
1. Sicherheit der Maschine in sämtlichen Phasen ihrer Lebensdauer;
2. Fähigkeit der Maschine, ihre Funktion auszuführen;
3. Benutzerfreundlichkeit der Maschine;

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



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

1. Beseitigung von Gefährdungen oder Risikoreduzierung durch die Konstruktion
2. Risikominderung durch Schutzeinrichtungen und mögliche ergänzende Schutzmaßnahmen
3. Risikominderung durch Bereitstellung einer Benutzerinformation über das Restrisiko



3. Schritt – Risikominderung durch steuerungstechnische Maßnahmen

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

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

1) Bestimmung der erforderlichen Leistungsfähigkeit

EN ISO 13849-1

Bestimmung des erforderlichen Performance Levels (PL_r)

S = Schwere der Verletzung

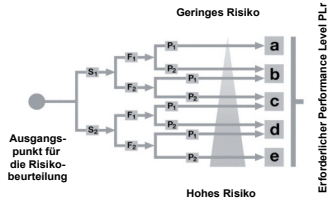
S1 = leichte Verletzung (normalerweise reversibel)
S2 = schwere Verletzung, einschließlich Tod (normalerweise irreversibel)

F = Häufigkeit und/oder Dauer der Gefährdungsexposition

F1 = selten bis öfters und/oder kurze Dauer
F2 = häufig bis dauernd und/oder lange Dauer

P = Möglichkeit zur Vermeidung der Gefährdung

P1 = möglich unter bestimmten Bedingungen
P2 = kaum möglich



EN 62061

Risikoabschätzung und Festlegung des erforderlichen Safety Integrity Levels (SIL)

Auswirkung und Schwere	S	Häufigkeit und Dauer	F	Wahrscheinlichkeit des gef. Ereignisses	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			SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, Verlust von Fingern	3	> 1/Stunde - ≤1/Tag	5	Wahrscheinlich	4				AM	SIL1	SIL2	SIL3
Reversibel, medizinische Behandlung	2	> 1/Tag - ≤2/Woche	4	Möglich	3	unmöglich	5			AM	SIL1	SIL2
Reversibel, Erste Hilfe	1	2/Woche - ≤1/Jahr	3	Selten	2	Möglich	3				AM	SIL1
		> 1/Jahr	2	Vernachlässigbar	1	Wahrscheinlich	1					

AM = Andere Maßnahmen empfohlen

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. Weiterhin 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 und Zweihandsteuerung bei Automatikbetrieb). Eine Sicherheitsfunktion kann durch einen oder mehrere sicherheitsrelevanten Steuerungsteil(e) realisiert sein und mehrere Sicherheitsfunktionen können sich einen oder mehrere sicherheitsrelevanten Steuerungsteil(e) aufteilen (z. B. Logikbaugruppe, Energieübertragungselement(e)).

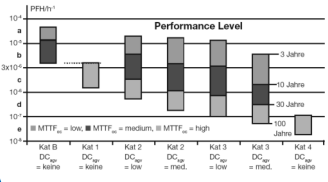
4) Bestimmung der erreichten Leistungsfähigkeit

EN ISO 13849-1	EN 62061
Für jede gewählte SRP/CS und/oder der Kombination von SRP/CS die eine Sicherheitsfunktion ausführt, muss eine Abschätzung des erreichten PL durchgeführt werden. Der PL der SRP/CS muss bestimmt werden durch die Abschätzung folgender Parameter: • des $MTTF_d$ oder B_{10d} Wertes einzelner Komponenten; • der DC; • der CCF; • der Struktur, • des Verhaltens im Fehlerfall; • sicherheitsbezogener Software • systematischer Ausfälle • der Fähigkeit eine Sicherheitsfunktion unter vorhersehbaren Umgebungsbedingungen auszuführen. • Anwendung bewährter Sicherheitsprinzipien	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 für Teilsysteme: • SILCL: SIL-Eignung (en: SIL claim limit) • PFH_d: Wahrscheinlichkeit gefährlicher Ausfälle pro Stunde • T_1: Lebenserwartung

EN ISO 13849-1

Performance level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]		
a	≥ 10^{-5}	PFH_d	< 10^{-4}
b	≥ $3x10^{-6}$	PFH_d	< 10^{-5}
c	≥ 10^{-6}	PFH_d	< $3x10^{-6}$
d	≥ 10^{-7}	PFH_d	< 10^{-6}
e	≥ 10^{-8}	PFH_d	< 10^{-7}

Beziehung zwischen den Kategorien DC, $MTTF_d$ und PL



Anmerkung:
Die PFH-Werte stellen eine notwendige Voraussetzung zur Ermittlung des Performance Levels dar. Darüber hinaus müssen noch zur vollständigen Ermittlung des PL auch Maßnahmen zur Fehlervermeidung wie CCF, Kategorie sowie der DC herangezogen werden.

EN IEC 62061

SIL (IEC 61508)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]		
1	≥ 10^{-6}	PFH_d	< 10^{-5}
2	≥ 10^{-7}	PFH_d	< 10^{-6}
3	≥ 10^{-8}	PFH_d	< 10^{-7}

Sicherheitstechnische Kenngrößen für Teilsystemelemente (Geräte):

- λ: Ausfallrate;
- B_{10d}-Wert: für verschleißbehaftete Bauteile (ohne konstante Ausfallrate)
- T_1: Lebensdauererwartung
- 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	SIL1	SIL2
≥ 60% bis < 90%	SIL1	SIL2	SIL3
≥ 90% bis < 99%	SIL2	SIL3	SIL3
≥ 99%	SIL3	SIL3	SIL3

EN ISO 13849-1	EN IEC 62061

Performance level (PL)	SIL
a	-
b	1
c	
d	2
e	3

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

5) Verifikation

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 sicherheitsbezogenen Steuerungsfunktion muss validiert werden. Es wird die Eignung der sicherheitsbezogenen Steuerungsfunktion für die Anwendung überprüft. Die Validierung kann durch Analyse oder Prüfung erfolgen (z. B. durch gezielte Simulation von Einzel- oder Mehrfachfehlern).

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	Diagnosedeckungsgrad
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 Dangerous Failure	Mittlere Zeit bis zum gefahrbringenden 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 eines 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	Erforderlicher Performance Level
SIL	Safety Integrity Level	Sicherheits-Integritätslevel
SILCL	Safety Integrity Claim Limit	SIL Anspruchsgrenze (Eignung)
SRCF	Safety Related Control Function	Sicherheitsfunktion

Abkürzung	Englischer Begriff	Deutsche Erklärung
SRP/CS	Safety Related Parts of a Control System	Sicherheitsbezogener Teil einer Steuerung
SRECS	Safety Related Electrical Control Systems	Sicherheitsbezogenes elektrisches Steuerungssystem
T_1	Lifetime	Lebenserwartung oder Wiederholungs-prüfung des Sicherheitssystems
T_2	Diagnostic Test Interval	Diagnose Testintervall
T_M	Mission Time	Gebrauchsdauer
β	Susceptibility to Common Cause Failure	Empfindlichkeit für Ausfälle gemeinsamer Ursache
C	Duty Cycle	Betätigungszyklus (pro Stunde) eines elektromechanischen Bauteils
SFF	Safe Failure Fraction	Anteil ungefährlicher Ausfälle (sicher)
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, der von der korrekten Funktion des SRECS, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung abhängt

8. FAQ-Liste

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

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

F: Was ist der Unterschied zwischen SIL und SILCL?

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

F: Gibt es eine Entsprechung zwischen PL und SIL?

A: Über den PFH_d-Wert lässt sich eine Beziehung zwischen PL und SIL bestimmen. (siehe Schritt 4: „Bestimmung der erreichten Leistungsfähigkeit"). Bitte beachten – die Tabelle berücksichtigt nicht die spezifischen Vorgaben der beiden Normen bezüglich zugelassener Struktur, Diagnosedeckungsgrad oder deren systematische Anforderungen.

Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]			Performance level (PL) EN ISO 13849-1	SIL Level (IEC61508)
≥ 10^{-5}	PFH_d	< 10^{-4}	a	-
≥ $3x10^{-6}$	PFH_d	< 10^{-5}	b	1
≥ 10^{-6}	PFH_d	< $3x10^{-6}$	c	
≥ 10^{-7}	PFH_d	< 10^{-6}	d	2
≥ 10^{-8}	PFH_d	< 10^{-7}	e	3

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

A: Entsprechend der beiden Normen lässt sich für zwangsgeführte Kontakte bei redundant ausgeführten (2-kanaligen) Schützen und Relais ein DC von 99 % annehmen.

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

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

A: Nein, in der Regel führt bereits ein Fehler zum Versagen. Für magnetisch betätigte oder RFID – basierte Systeme ist eine Bestätigung einer Hardware-Fehlertoleranz von 1 durch die Hersteller möglich.

F: Gibt es einen PFHd-Wert für verschleißbehaftete Komponenten?

A: Nein, der Anwender kann über den B_{10}-Wert in Abhängigkeit von der Anzahl der Betätigungszyklen einen PFH_d-Wert für verschleißbehaftete Komponenten für den gegebenen Anwendungsfall ermitteln.

F: Was ist der Unterschied zwischen MTBF und MTTF?

A: Die MTBF beschreibt die Zeit zwischen 2 Fehlern, im Gegensatz zur MTTF (Zeit bis ein Fehler auftritt)

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

A: „d" steht für „dangerous" die $MTTF_d$ beschreibt die Zeit bis zum ersten gefahrbringenden Fehler

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

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

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

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

F: Kann ich bei Prozessventilen/Armaturen, die seltener als einmal pro Jahr geschaltet werden (Low Demand), für die Berechnung der MTTF die EN ISO 13849-1 anwenden?

A: 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.

F: Kann ich bei Prozessventilen/Armaturen, die seltener als einmal pro Jahr geschaltet werden (Low Demand), für die Berechnung der Ausfallrate die EN 62061 anwenden?

A: siehe vorige Frage

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

A: Nein. Eine Zertifizierungspflicht auf Basis der beiden Normen besteht nicht separat für die Software sondern orientiert sich an Umfang und Komplexität des Gesamtprojektes. Im Rahmen der Verifikation und Validierung von Sicherheitsfunktionen kann eine Softwareprüfung erforderlich sein. Hinweise hierzu finden sich in EN ISO 13849-1 Kapitel 4.6 und EN 62061 Kapitel 6.9 und 6.10 sowie in EN 61508-3.

F: Kann man jede Komponente mit MTTF für Sicherheitstechnik verwenden?

A: Nein, neben statistischen Kennwerten wie MTTF und B_{10} muss die Komponente auch funktionell für die Funktion geeignet sein und bestimmte Mindestanforderungen wie konstruktive und sicherheitstechnische Anforderungen (Umsetzung und Anwendung von Sicherheitsprinzipien) erfüllen.

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.
Lyoner Straße 9
60528 Frankfurt am Main

Fachverband Automation

Fachbereich Schaltgeräte, Schaltanlagen,
Industriesteuerungen

Technischer Ausschuss
Sicherheitssystem in der Automation