

Pepperl+Fuchs GmbH – Lilienthalstraße 200 – 68307 Mannheim

Bei Veröffentlichungen bitte folgende Kontaktdaten angeben:

Tel.: +49 621 776-2222, Fax: +49 621 776-27-2222, www.pepperl-fuchs.com, pa-info@de.pepperl-fuchs.com

Ansprechpartner für Redaktionen: Christa Blas (Tel.: -1420, Fax: -1108), cblas@de.pepperl-fuchs.com

IEC 62061 und ISO 13849-1 – komplementär oder konkurrierend?

Ein Meilenstein für die Normierung sicherheitsrelevanter Technologien war die Publikation der IEC/EN 61508-Reihe, die ursprünglich als Werkzeug für die Entwicklung und Validierung von komplexen elektrischen, elektronischen, programmierbaren elektronischen Systemen gedacht war.

Die IEC 61508 ist jetzt DIE anzuwendende Norm für die funktionale Sicherheit (Safety Integrity Level, SIL) von komplexen Systemen. Eine Menge abgeleiteter Normen existiert bereits – doch, was kommt auf den Maschinenbauer zu?

Ein wenig Geschichte

Traditionell werden Maschinen mit beweglichen Teilen als gefährlich eingestuft. Um das Verletzungsrisiko so gering wie möglich zu halten, wurden und werden daher viele Anstrengungen unternommen, an denen unterschiedlichste Teilnehmer beteiligt sind, zum Beispiel: Berufsgenossenschaften, Maschinenhersteller, Sicherheitskomponentenhersteller und gesetzgebende Organe.

In Europa wurde relativ früh eine Richtlinie nach dem neuen Ansatz für den Maschinensektor publiziert (89/392/EG und folgende). Dieser neue Ansatz sieht eine komplette Harmonisierung der technischen Regulierungen aller Mitgliedstaaten vor.

Seit mehreren Jahren wurden Normen als Teil einer Einigung zwischen den Parteien niedergeschrieben. Eine der bekanntesten Normen in Hinblick auf Sicherheit im Maschinensektor ist die EN 954-1, die Ende 1996 publiziert und unter der Maschinenrichtlinie harmonisiert wurde. Diese Norm ist eine so genannte **B1 Sicherheitsgruppennorm**, die Sicherheitsaspekte bzw. Sicherheitseinrichtungen für eine große Bandbreite von Maschinen behandeln.

Bisheriger Ansatz im Maschinenbausektor

EN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen

Die EN 954-1 basiert auf Ergebnissen einer Risikoanalyse und beschreibt Methoden, um das Risiko in den sicherheitsbezogenen Teilen einer Steuerung zu reduzieren. Hierzu wurden die Maßnahmen in die Kategorien B, 1, 2, 3 und 4 eingeteilt.

EN 954-1 legt klar fest, dass programmierbare Systeme nicht in eine einkanalige Konfiguration für sicherheitsrelevante Applikationen einsetzbar sind. Die (damalige) IEC 1508 wurde bereits als Referenz für solche Systeme zitiert!

Der Fokus dieser Norm liegt demzufolge auf Strukturanforderungen sowie „bewährte“ Komponenten und Prinzipien. Die Sicherheitsintegrität wird erreicht durch Fehlererkennung (Diagnose) und Redundanz (mehrkanaliger Struktur).

Die **Anforderungen an das Sicherheitsmanagement** sind ziemlich verschwommen und vage formuliert: Der Entwickler muss garantieren, dass die sicherheitsrelevante Funktion allen Anforderungen genügt, die im Ergebnis der Risikoanalyse festgeschrieben wurden.

Die abgeleiteten **Applikationsnormen**, oder auch C-Normen genannt, enthalten alle Sicherheitsanforderungen für eine spezielle Maschine oder Maschinenbauart. Als Beispiel sei EN 693 genannt, die die Sicherheitsanforderungen für hydraulische Pressen beschreibt.

Hunderte C-Normen wurden bereits publiziert, die wiederum auf die EN 954-1 verweisen, sodass die Norm EN 954-1 zur Referenznorm für den Maschinenbau wurde!

Der neue Ansatz

Die IEC 61508 – Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

Als während der 70er und 80er Jahre die Anwendung von komplexen und/oder programmierbaren elektronischen Systemen zunahm und entsprechende spezifische Probleme entstanden, wurde schnell klar, dass ein grundlegender Leitfaden fehlte. Insbesondere im Bereich der Software-Entwicklung wurde (und wird immer noch) die Wahrscheinlichkeit, einen systematischen Fehler schon in der Design-Phase zu implementieren, komplett unterschätzt. Die Analyse von Unfällen zeigt mit erschreckender Konsistenz, dass etwas 40% aller Fehler bereits während der Spezifikation entstehen!

Leider können diese systematischen Fehler nicht vollständig beherrscht werden – sie müssen, soweit möglich, vermieden werden. Ein detailliertes Qualitätsmanagementsystem basierend auf dem „Vier-Augenprinzip“ dient hier als klassischer Ansatz, was sich IEC/EN

61508 zur Grundlage machte. Dieses umfangreiche Werk befasst sich mit der funktionalen Sicherheit und wurde ursprünglich geschrieben für

- Hersteller und Anwender programmierbarer sicherheitsrelevanter Systeme
- Verfasser sektororientierter sicherheitsrelevanter Normen, u. a.:
 - Prozessindustrie (IEC/EN 61511)
 - Eisenbahn (EN 50128 Reihe)
 - Medizin (IEC/EN 60601 Reihe)
 - Maschine (IEC/EN 62061)
 - Brennersteuerung (EN 50156)

Heute lässt sich IEC 61508 aber für jedes sicherheitsrelevante System unabhängig von der Technologie anwenden.

Neben den oben beschriebenen Anforderungen wurden auch Ausfallraten gefordert. Somit hängt die Integrität einer Sicherheitsfunktion von zwei Aspekten ab:

- Struktur (wie gehabt)
- Ausfallwahrscheinlichkeit (neu)

Struktur

Die Struktur einer Sicherheitsfunktion muss zwei Anforderungen erfüllen:

- Fehlervermeidung bzw. -aufdeckung: Wird durch den Anteil gefährlicher Fehler bestimmt.
- Fehlerbeherrschung: Wird durch Erhöhen der Kanalanzahl, d.h. durch eine höhere Fehlertoleranz der Hardware, erreicht.

Die folgende Tabelle verdeutlicht den Zusammenhang beider Anforderungen am Beispiel von Strukturanforderungen an komplexen Komponenten (Typ B):

Anteil ungefährlicher Ausfälle	Fehlertoleranz der Hardware		
	0	1	2
< 60 %	-	SIL1	SIL2
60 % - ≤ 90 %	SIL1	SIL2	SIL3
90 % - ≤ 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

Um die Diagnosefähigkeit eines Systems zu klassifizieren, hat die IEC/EN 61508 ein neues Konzept eingeführt – die „Safe Failure Fraction“ (SFF) beschreibt den „Anteil ungefährlicher Ausfälle“.

Ausfallwahrscheinlichkeit

Komponenten leben nicht ewig. Das ist einleuchtend. Dies jedoch zu beschreiben, erfordert viel Mühe. Problematisch bei dem Vorhaben ist, dass die Ausfallraten stark von der jeweiligen Technologie und den Umgebungsbedingungen abhängen.

Jede Komponente hat zudem eigene Fehlermodi, die es zu beschreiben gilt. Zum Beispiel sei die Abhängigkeit von der Betätigung aufgeführt: Ein elektromechanischer Kontakt wird nicht mehr öffnen, wenn er zu oft betätigt wurde (Kontaktmaterial erodierte). Er wird aber auch nicht mehr schließen, wenn er zu selten betätigt wurde (Kontaktmaterial korrodierte). Solche Festlegungen sind in der Norm 2 Betriebsarten zu finden:

- **Betriebsart mit niedriger Anforderungsrate** (PFD_{avg}) beschreibt die bis zu einer sicherheitsrelevanten Anforderung pro Jahr und findet typischerweise in der Prozessindustrie ihre Anwendung.
- **Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung** (PFHD) beschreibt die mindestens einmalige Anforderung pro Jahr und ist typisch für den Maschinenbausektor.

Zur Berechnung stehen einige Hilfsmittel zur Verfügung, zum Beispiel SISTEMA von BGIA oder mittels einer Exceltabelle. Für bestimmte Strukturen (1oo1, 1oo2, 1oo2D etc.) sind einige Berechnungsformeln in Teil 6 der IEC 61508 zu finden. Diese Formeln gehen allerdings davon aus, dass die Fehlerraten konstant sind. Dies trifft aber nicht immer zu (zum Beispiel bei mechanischen Komponenten oder wenn elektrische Systeme am Ende ihrer Lebensdauer sind).

Abgeleitete Sektornormen für den Maschinenbau

Die **Norm IEC/EN 62061** formuliert Empfehlungen für das Design, die Integration und Validierung sicherheitsrelevanter elektrischer, elektronischer und programmierbarer Steuerungen von Maschinen (SRECS). Die technischen Anforderungen aus der IEC/EN 61508 wurden entsprechend zugeschnitten und Fehlerraten (PFH_D) angegeben. Nicht-elektrische Komponenten werden explizit nicht erwähnt, dennoch lässt sich der Rahmen und das Qualitätsmanagement auch hier anwenden. Des Weiteren finden Anwender in dieser Norm und in ISO 13849-1 eine Tabelle mit Beziehungen zwischen SIL und den bisherigen Kategorien aus EN 954. Allgemeine Anforderungen an das Qualitätsmanagement sind Teil der IEC/EN 61508 Norm. IEC/EN 62061 referenziert auf die entsprechenden Stellen.

<Bild 1>

Die **ISO 13849-1** wurde geschrieben, unter anderem um die vielen C-Normen nicht auf einmal als obsolet erscheinen zu lassen. In ihr sollen die alten Kategorien weiter leben, der

Ansatz der IEC 61508 (Qualitätsmanagement, Struktur- und Zuverlässigkeitsanforderungen) aber mit berücksichtigt werden – die Performance Levels waren geboren. Sie bauen einerseits auf die alten Kategorien auf, andererseits beziehen sie Fehlerraten als weiteres Bewertungskriterium mit ein. Als Zuverlässigkeitsparameter wurde jedoch das „Mean-Time-To-Dangerous Failure“ (MTTF_d, mittlere Betriebsdauer bis zum Ausfall) anstelle von Fehlerraten eingeführt, was die Berechnungsformeln unüberschaubar macht. Weiterhin wird der Begriff „Diagnose-Deckungsgrad“ (dc, Diagnostic Coverage) anstelle von „Anteil ungefährlicher Ausfälle“ benutzt (ISO geht davon aus, dass es keine sicheren Fehler gibt ...).

<Bild 2>

Konkurrierend oder ergänzend?

Es lässt sich nicht leugnen, dass beide Normen eigentlich den gleichen Anwendungsbereich ansprechen. Die Ansätze unterscheiden sich jedoch:

Die IEC 62061 besitzt die volle Flexibilität und Variabilität der IEC 61508. Sie eignet sich demnach sehr gut für komplexe Systeme.

Die ISO 13849-1 dagegen beschreibt Systeme mit eingeschränktem Freiheitsgrad und ist angelehnt an die Kategorien der EN 954. Vorteilhaft ist hier, dass der Übergang zwischen Kategorien und modernen Ansätzen mühelos realisiert werden kann. Ein weiterer positiver Effekt ist, dass die C-Normen weiterhin schmerzlos angewendet werden können.

Somit finden beide Normen ihre Anwendung. Wann welche Norm gültig ist, wurde in einem technischen Bericht publiziert (Guidance on the application of ISO 13849-1 & IEC 62061 in the design of safety-related control systems for machinery). Diese Empfehlung wird zudem auch in den Normen zu finden sein.

Hersteller sicherheitsbezogener Komponenten und Systeme unterstützen beide Ansätze und stellen die entsprechenden Daten zur Verfügung.

<Bild 3>

Schlagworte: Funktionale Sicherheit, SIL, Sektornormen Sicherheitstechnik, IEC 62061, ISO 13849, EN 954, Maschinenrichtlinie, Sicherheitsaspekt, Maschinenbausektor, PL, Performance Level

Autor: Dipl.-Ing. Patrick Lerévérénd,
Trainer für Explosionsschutz und Funktionale Sicherheit
Geschäftsbereich Prozessautomation

Co-Autor: Dipl.-Techn.-Red. Xenia Döbling
Technische Redakteurin
Geschäftsbereich Prozessautomation

Zeichen: 8.097, ohne Leerzeichen

Zeichen Kurzfassung: 439, ohne Leerzeichen

Bilder: Nr. MC7522_090116_01, Nr. MC7522_081031_07,
Nr. MC7522_090917_20

Oktober 2009



Bild 1: Aufzug: Sicherheitsfunktion nach SIL bewertet



Bild 2: Windkraftanlage: Sicherheitsfunktion nach ISO 13849-1 (Normvorschlag) bewertet



Bild 3: Drehgeber: für SIL 3 und PLe bewertet