

Fünf Antworten zur

Kaum eine Norm hat so viel Aufsehen erregt, wie die EN ISO 13849. Einigen Steuerungstechnikern war sie zu heiß. Sie kämpften in Brüssel für die Verlängerung der EN 954-1. Mit Erfolg. Doch der Tag wird kommen, an dem der probabilistische Ansatz allein gültig ist. Vorher gilt es noch fünf Fragen zu klären.

TEXT: Nicole Wittmann, A&D FOTOS: Fiessler; Inmas; Pilz; Sick; Wieland

Kaum eine Norm wurde so heiß diskutiert wie die EN ISO 13849. Letztlich hat die Debatte um ihr Inkrafttreten zum Ende des vergangenen Jahres die neue Maschinenrichtlinie in den Schatten gestellt, die seit 29. Dezember 2009 die Sicherheit beim Inverkehrbringen von Maschinen in den Mitgliedsstaaten der Europäischen Union bestimmt. Im November und Dezember haben die Spekulationen über eine Verlängerung der Vorgängernorm EN 954-1 das allgemeine Interesse erregt. Dennoch – auch mit Übergangsfrist – die Neue kommt. Ab dem Neujahrstag 2012 ist sie die allein gültige Norm für die Auslegung sicherheitsgerichteter Steuerungen. Grund genug, ein wenig genauer hinzublicken, was die Norm eigentlich besagt. Fünf Experten beantworten fünf Fragen zur EN ISO 13849.

1 *Worauf ist zu achten, wenn sich innerhalb einer Maschine oder Anlage Gefährdungen mit unterschiedlichen PL-Werten überlagern?*

Götz Fiessler: Die EN ISO 13849-1 beinhaltet ausführlich wie Reihenschaltungen aus mehreren Subsystemen (SRP/CS) behandelt werden müssen. Dabei wird immer das schwächste Glied der Sicherheitskette zuerst betrachtet. Der



Götz Fiessler ist Geschäftsführer von Fiessler Elektronik in Esslingen

Performance Level (PL) dieser Sicherheitsfunktion gibt letztendlich den maximalen PL der Gesamtanlage an. Denn eine Sicherheitskette reißt dort, wo die Kette das schwächste Glied hat.

Aber nicht nur das schwächste Glied muss bei der Betrachtung des Gesamt-PL einer Anlage betrachtet werden. Die Anzahl der Subsysteme und auch der PFH (Wahrscheinlichkeit eines Ausfalls pro Stunde) spielen hier eine Rolle. Sollen an einer Maschine oder Anlage Gefährdungen mit unterschiedlichen PLr-Werten betrachtet werden, die sich überlagern, so muss hier die Gefahr mit dem höchsten PLr als federführend betrachtet werden: Die Gefährdung mit dem höchsten PLr-Wert bildet die Grundlage des PLr für die gesamte Anlage.

Abweichend davon kann man einzelne Gefährdungen dann separat betrachten, wenn diese sich nicht gegenseitig beeinflussen.

2 *Die Norm EN ISO 13849-1 kann für alle Steuerungen verwendet werden, die EN 62061 beschreibt ausschließlich Anforderungen für elektrische Steuerungen. Wie grenzen sich die beiden Normen noch voneinander ab?*

Silvia Schmidt: Ganz alleine steht die ISO 13849 in der Normenwelt nicht da. Die IEC 62061 zum Beispiel, ist auch in Europa harmonisiert, und stellt für pro-



Silvia Schmidt ist Managerin für Normen und CE-Kennzeichnung bei Inmas in Bremen

grammierbare Steuerungen ein wichtiges Normenwerk dar. Wie genau die Anwendungsbereiche der unterschiedlichen Normen anzuwenden sind, wird in der IEC 62061 definiert. Auch bei den Begrifflichkeiten unterscheiden sich die Normen. Hantieren die Steuerungsnormen normalerweise mit dem SIL Level, so verwendet die harmonisierte ISO 13849 den Performance Level (PL). Der PL wird mit Hilfe eines Graphen ermittelt. Viele

EN ISO 13849

Unternehmen missbrauchen diesen Graphen zur Einschätzung in ihrer Risikobeurteilung. Hiervon ist aber laut Berufsgenossenschaft abzuraten, da der Einfluss der Eintrittswahrscheinlichkeit nicht berücksichtigt wird. Bessere Methoden zur Risikoeinschätzung finden sich in der ISO/TR 14121-2. Diese nicht harmonisierte Norm vervollständigt den harmonisierten Teil 1 und unterstützt Hersteller mit konkreten Vorschlägen und Beispielen bei der Risikobeurteilung.

3 *Muss der Maschinenbauer die Daten überprüfen, die ihm die Bauteilehersteller liefern? Wie ist zu verfahren, wenn es noch keine zuverlässigen Zahlen gibt?*

Matthias Wimmer: Diese Frage ist im Zusammenhang mit den neuen Vor-

schriften für die funktionale Sicherheit oder der neuen Maschinenrichtlinie nicht neu. Dahinter steht die eher grundsätzliche Überlegung, inwieweit der Maschinenbauer generell den Angaben eines Lieferanten trauen kann. Komponentenhersteller, die Produkte im Anwendungsbereich der neuen Normen anbieten, stellen gewöhnlich auch verlässliche sicherheitstechnische Kenndaten zur Verfügung. Konstrukteure sind vom Gesetz her nicht verpflichtet, diese Werte zu überprüfen. Aus diesem Grund führt auch eine freiwillige Überprüfung nicht automatisch zu einer höheren Rechtssicherheit, sondern erleichtert allenfalls den Nachweis in einem konkreten Problemfall.

Wenn für eine Komponente keine sicherheitstechnischen Kenndaten vorlie-



Matthias Wimmer
ist Consultant
im Technischen
Büro Hannover
von Pilz

gen, können Maschinenbauer entsprechend der Norm einer dreistufigen Vorgehensweise folgen. Diese beginnt mit der direkten Nachfrage beim Hersteller der Komponente. Sollte dies zu keinem Ergebnis führen, können Konstrukteure als nächstes auf Standardwerte aus der EN ISO 13849-1 (siehe Tabelle C1) für bestimmte, einfache Komponenten wie Schalter und Schütze sowie mechanische,

hydraulische und pneumatische Bauteile zurückgreifen. Wird die eingesetzte Komponente hiervon nicht abgedeckt, kann für die MTTFd (Mittlere Zeit bis zum gefahrbringenden Ausfall einer Komponente) ein Wert von zehn Jahren verwendet werden. Der Nachteil ist jedoch, dass dies in der Praxis in einem sehr niedrigen Performance Level – maximal PLc – resultiert. Die MTTFd ist dann die maßgebliche beschränkende Größe (siehe Tabelle K1 der EN ISO 13849-1).

4 Ist der MTTFd-Wert allein ausreichend für die Bewertung von Sicherheitsfunktionen?

Hans-Jörg Stubenrauch: Der MTTFd stellt den probabilistischen (wahrscheinlichkeitsbezogenen) Aspekt der Bewertung von Sicherheitsfunktionen mit einem Wert dar. Dieser Wert beschreibt die Zuverlässigkeit der verwendeten Bauteile oder der gesamten Schaltung und wird als „Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall“ in Jahren definiert. Die Berücksichtigung dieses Aspekts ist sinnvoll, aber es ist nur ein Teilaspekt. Eine weite-

re Minimalforderung ist, dass die verwendeten Bauteile dem Stand der Technik (zum Beispiel einer Produktnorm) genügen.



Hans-Jörg Stubenrauch ist Manager Safety Solutions bei Sick in Waldkirch

Die Bewertung einer kompletten Sicherheitsfunktion umfasst neben dem MTTFd die Struktur (Kategorie), des Diagnosedeckungsgrades DC, der Maßnahmen gegen *common cause failure* (CCF) in der Anwendung, den Gestaltungsprozess, die Einsatzbedingungen und die systematischen Ausfälle, um die gefahrbringenden Fehler zu beherrschen. Allein mit einem hohen MTTFd von zum Beispiel 30 Jahren darf nach ISO 13849-1 ein Bauteil nicht in Sicherheitsfunktionen verwendet werden.

diese Parameter sollen gemeinsam in die Berechnung des PFH-Wertes (Wahrscheinlichkeit eines Ausfalls pro Stunde) oder des Performance Levels eingehen.



Christof Sofsky ist Business Development Manager Safety bei Wieland Electric Bamberg

Aufgrund der Deckelung ist aber gerade bei der Wahl der Komponenten auf eine ausgeglichene Zuverlässigkeit der einzelnen Kanäle zu achten, da ansonsten ein Kanal mit deutlich höherem MTTFd als 100 Jahren am Ende auf 100 Jahre abgeschnitten wird, der zweite, eventuell deutlich schlechtere Kanal mit einem sehr geringen MTTFd durch die Anwendung der Symmetrierungsformel das Gesamtergebnis bis auf zwei Drittel des höheren Wertes herunterziehen kann (in dem Fall rechnerisch mindestens 66,7 Jahre). Legt man zugrunde, dass 30 bis 100 Jahre als hoher MTTFd eingestuft sind, lässt sich dennoch damit in jedem Fall ein Erreichen des PLe realisieren, unter der Maßgabe, dass auch alle anderen Aspekte (Diagnose, Struktur und CCF) erfüllt sind.

Innerhalb eines Kanals kann mit höheren Werten gerechnet werden, doch aufgrund der Formel ist klar, dass der MTTFd-Wert mit steigender Kettenlänge immer schlechter wird und ein einziger schlechter Wert innerhalb dieser Kette sich nicht durch andere gute Werte kompensieren lässt. □

> MORE@CLICK AD7060900

5 Welche Auswirkung hat die Deckelung des MTTFd jedes Kanals auf 100 Jahre bei längeren Steuerungsketten?

Christof Sofsky: Grundsätzlich hat die Deckelung den Sinn, die zweifelsohne wichtige Bauteilzuverlässigkeit gegenüber anderen wichtigen Einflussfaktoren, wie Struktur und Diagnose nicht überzubewerten. All

Sicherheits-Lichtvorhänge



über 50 Jahre Erfahrung für Ihre Sicherheit

Innovative Sicherheitstechnik
weltweiter Kunden- und Vertriebservice
individuelle Kundenlösungen

FISSLER
ELEKTRONIK

Tel. +49 (0) 711-91 96 97-0
Fax +49 (0) 711-91 96 97-50
info@fiessler.de

www.fiessler.de

- große Reichweite bis 60 m
- integriertes Schaltgerät
- programmierbare Ausblendfunktion
- montagefreundlich, kompakte Bauform
- Innovations-Anerkennungsträger des Landes Baden-Württemberg