Funktionale Sicherheit für den Maschinensektor

Beim Entwurf und Bau von Sicherheitsschaltungen für Maschinen berücksichtigt man die Kategorien B, 1, 2, 3 und 4 der Norm DIN EN 954-1. Aufgrund neuer Normen hat sich die Ausgangslage für Entwickler und Anwender verändert, und das Thema funktionale Sicherheit ist in das nähere Blickfeld gerückt. In diesem Fachbeitrag wird dargestellt, was funktionale Sicherheit für den Maschinensektor bedeutet.

Nick de With

Wenn man Menschen aus der Praxis fragt, was funktionale Sicherheit ist, erhält man eine große Vielfalt von Antworten. Die häufigste Antwort ist, dass die Maschine sicher arbeiten können muss. An sich ist dieser Gedanke gut, jedoch geht es bei der funktionalen Sicherheit ausschließlich um die an der Maschine angebrachten steuerungstechnischen Sicherheitsfunktionen. Beispiele für derartige Sicherheitsfunktionen sind neben Not-Aus-Tastern, Abschalt- und Bedienungsschutz (Schutzzaun), Lichtschranken und Zweihandsteuerungen (Bild 1).

Die neue Norm DIN EN 62061 (VDE 0113-50) [1] behandelt die funktionale Sicherheit von elektrischen, elektronischen und programmierbaren elektronischen Sicherheitsschaltungen im Maschinensektor. Diese Norm wurde zum 31. 12. 2005 in die Liste der harmonisierten Normen unter der Maschinenrichtlinie 98/37/EG [2] aufgenommen. Befolgt der Anwender diese Norm, gilt das sogenannte „Vermuten von Übereinstimmung“ mit der Maschinenrichtlinie.

Definition von funktionaler Sicherheit

Gemäß der übersetzten Definition aus dem Paragraph 3.2.9 der DIN EN 62061 (VDE 0113-50) ist funktionale Sicherheit: „Der Teil der Sicherheit von der Maschine und dem Maschinen-Steuerungssystem, der abhängig ist vom einwandfreien Funktionieren des sicherheitsgerichteten elektrischen Steuerungssystems (Safety Related Electrical Control System SRECS), sicherheitsgerichteter Systeme, die auf anderen Technologien basieren, sowie externer risikoreduzierender Einrichtungen.“ Wie recht häufig bei Normen, ist auch diese Definition nach einmaligen Lesen nicht direkt zu ergründen. Eine freie Übersetzung ist: „Der Teil der Sicherheit der Maschine, der abhängig ist vom einwandfreien Funktionieren der angebrachten steuerungstechnischen Sicherheitsfunktionen bzw. -maßregeln.“ Kurz gesagt: Welchen risikoreduzierenden Beitrag liefern die steuerungstechnischen Sicherheitsfunktionen an einer Maschine?

In einer steuerungstechnischen Schaltung, die eine Sicherheitsfunktion, zum Beispiel eine Lichtschranken-Absicherung, ausführt, können folgende drei Fehlertypen auftreten:

- zufällige Fehler (Random failure),
- systematische Fehler (Systematic failure) und
- Fehler mit gemeinsamer Ursache (Common cause failure).

Die Unterschiede zwischen diesen Fehlern werden im folgenden näher erläutert.

Will man eine zuverlässige funktionell sichere Sicherheitsschaltung bauen, muss man die drei obengenannten Fehlertypen im Auge haben. Häufig wird angenommen, dass funktionale Sicherheit nur zum Schutz von Mensch und Umwelt dient, aber man kann sie ebenso gut einsetzen, um größere Investitionen wie eine Maschine zu schützen.

Das Besondere an der DIN EN 62061 (VDE 0113-50) besteht darin, dass im Gegensatz zur Norm DIN EN 954-1 [3] nicht nur Anforderungen für die Entwurfsphase der Sicherheitsschaltung spezifiziert werden. Für alle Phasen des Lebenszyklusses der Sicherheitsschaltung werden in der DIN EN 62061 (VDE 0113-50) Anforderungen und Methoden vorgestellt. Nicht nur der Entwurf, sondern auch die Inbetriebnahme, der Einsatz, die Instandhaltung und die Modifikationen einer Sicherheitsschaltung müssen sicher durchgeführt werden können.

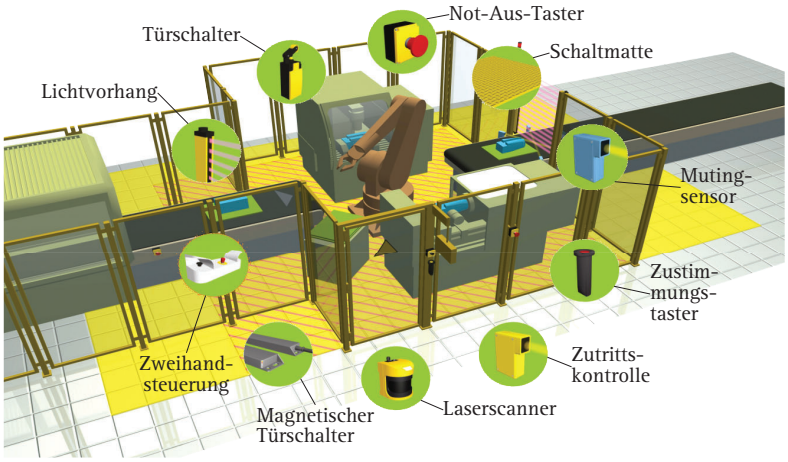

***Bild 1**. Übersicht der Sicherheitsfunktionen an einer Roboterzelle (Quelle: Wieland)*

Dipl.-Ing. Nick de With ist Geschäftsführer bei Functional Safety Consultants Nederland. Er ist verantwortlich für Beratung und Lehrgänge auf dem Gebiet der funktionalen Sicherheit und Maschinensicherheit. Außerdem ist er Mitglied des Niederländischen Normenausschusses NEC 44 und der internationalen Normungs-Arbeitsgruppe IEC TC44/WG7.
E-Mail:

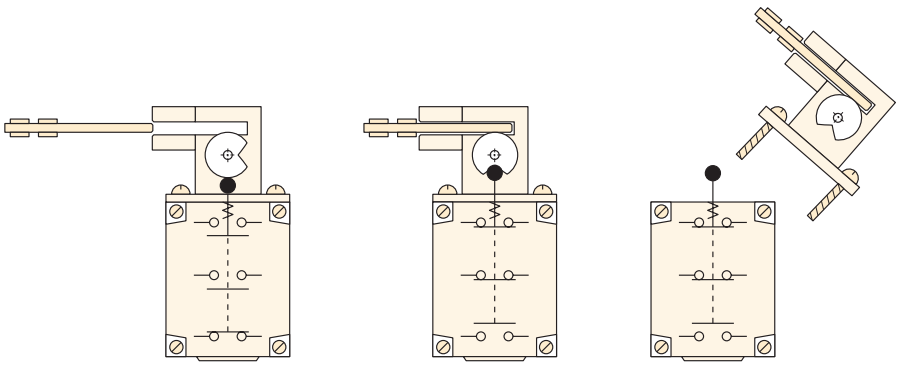

***Bild 2**. Der Fall, dass mechanische Schalter oder betätiger zerstört werden, lässt sich nicht ausschließen*

Ursprung der funktionalen Sicherheit

Jahrelang wurden die deutschen Normen DIN V 19250 [4], DIN V 19251 [5] und DIN V VDE 0801 (**VDE 0801**) [6] für die Entwicklung und den Einsatz elektronischer und programmierbarer elektronischer Sicherheitsprodukte angewandt. Als diese Normen veröffentlicht wurden, waren sie revolutionär, und der Stand der Technik für Sicherheitsanwendungen basierte auf Mikroprozessortechnik. Viele Lieferanten von Sicherheitssystemen ließen ihre Komponenten anhand dieser Normen zertifizieren.

Zu Beginn der 1990er Jahre hat die Arbeitsgruppe IEC/TC65 damit begonnen, eine internationale Norm zu erstellen, was zur Normenreihe DIN EN 61508 (**VDE 0803**) Teil 1 bis 7 [7] führte. Diese Norm unterscheidet sich von ihren Vorgängerinnen, da die Umsetzung bestimmter Anforderungen der Norm von den benötigten Leistungsmerkmalen des Sicherheitssystems abhängig ist. Die benötigten Leistungsmerkmale jeder Sicherheitsfunktion werden in Form eines Safety Integrity Levels (SIL) ausgedrückt. Eine SIL-Stufe gilt für die komplette Kette von Komponenten (Sensor-Logik-Aktuator), aus der die Sicherheitsfunktion aufgebaut ist. Dies steht im Gegensatz zu der vorgenannten DIN EN 954, die sicherheitsgerichtete Komponenten betrachtet.

Die Norm unterscheidet vier SIL-Stufen (SIL 1 bis SIL 4). Für jede steuerungstechnische Sicherheitsfunktion an der Maschine muss mittels einer Risiko-Einschätzung eine SIL-Stufe bestimmt werden. Die Sicherheitsfunktion mit der höchsten SIL-Stufe bestimmt die endgültige SIL-Stufe, deren Anforderungen das Sicherheitssystem (z. B. Sicherheits-SPS) erfüllen muss. Jede SIL-Stufe (**Tabelle**) entspricht einer bestimmten Fehlerwahrscheinlichkeit pro Stunde. Je höher die SIL-Stufe desto kleiner ist die Wahrscheinlichkeit, dass das System ausfällt. Für ein SIL-2-System gilt beispielsweise, dass die Fehlerwahrscheinlichkeit pro Stunde der Sicherheitsfunktion kleiner ist als ein Fehler pro Million Stunden.

Die Normenreihe DIN EN 61508 (**VDE 0803**) ist sehr umfangreich (740 Seiten) und muss als grundlegendes Sicherheitswerk für die Ersteller von Normen betrachtet werden. Die Prozessindustrie hat seit 2003 eine abgeleitete Version davon mit der Bezeichnung DIN EN 61511 (**VDE 0810**) Teil 1 bis 3 [8], und auch der Maschinensektor hat seine eigene Norm nämlich die bereits erwähnte DIN EN 62061 (**VDE 0113-50**). Beide Normen beschreiben, welche Anforderungen die Sicherheitsanwendung erfüllen muss, und verweist Hersteller von Sicherheitskomponenten an die Mutternorm.

Zufällige Fehler

Ein zufälliger Fehler ist ein Fehler, der jederzeit unerwartet in der Hardware eines Sicherheitssystems auftreten kann. Beispiele dafür sind das Durchbrennen einer Sicherung, eine fehlerhafte Speicherzelle in einem Speicherchip, ein fehlerhafter Türschalter oder ein defektes Motorschütz. Man kann zufällige Fehler in zwei Arten aufteilen: permanente und dynamische zufällige Fehler. Permanente zufällige Fehler bleiben solange vorhanden, bis sie repariert werden (z. B. defekte Sicherung). Dynamische Fehler treten nur unter bestimmten Bedingungen auf und sind oft schwer zu entdecken. Nehmen wir zum Beispiel die fehlerhafte Speicherzelle. Solange keine Sicherheitsdaten in diese Speicherzelle geschrieben werden, ist nichts feststellbar. Erst wenn die Zelle tatsächlich benutzt wird, kann es sein, dass die Sicherheitsfunktion nicht ausgeführt wird und somit versagt.

Die DIN EN 62061 (**VDE 0113-50**) gibt an, dass zufällige Fehler auf zwei Arten angegangen werden müssen. Als Erstes werden Maßregeln spezifiziert, um zufällige Fehler zu beherrschen, beispielsweise durch Anwendung von Redundanz oder automatischer Diagnose. Als Zweites wird gefordert, dass eine qualitative und quantitative Zuverlässigkeitsanalyse an der Sicherheitsschaltung durchgeführt wird.

Qualitativ muss untersucht werden, wie das Sicherheitssystem auf zufällige Fehler reagiert. Eine Technik, die man hierbei anwenden kann, ist die Failure Mode and Effect Analysis (FMEA). Anschließend wird das Fehlverhalten mit einer Zuverlässigkeitsberechnung quantifiziert. Es wird berechnet, wie hoch die durchschnittliche Wahrscheinlichkeit ist, dass die Sicherheitsfunktion ausfällt, während der Maschinenprozess verlangt, dass die Sicherheitsfunktion ausgeführt wird. Meistens verwendet man hierfür Standardformeln, wie sie in der Norm wiederzufinden sind. Andere benutzen eine Fehlerbaum-Analyse oder das Markov-Modell.

Safety Integrity Level	Probability of failure per hour (PFH)
SIL 1	10-6 <= PFH < 10-5
SIL 2	10-7 <=PFH < 10-6
SIL 3	10-8<= PFH < 10-7
SIL 4*	10-9 <= PFH < 10-8

***Tabelle** PFH für die verschiedenen SIL-Stufen *Nicht von Anwendung bei Maschinen*

Systematische Fehler

Ein systematischer Fehler ist in vielen Fällen ein verborgener Fehler im Entwurf oder in der Umsetzung des Entwurfs. Systematische Fehler können sowohl in der Hard- als auch in der Software sowie in jeder Lebenszyklusphase des Systems auftreten. Diese Fehler kommen häufig in den Entwurfsspezifikationen, der Bedienungsanleitung oder den Verfahrensweisen vor. Beispiele sind die Wahl einer ver-

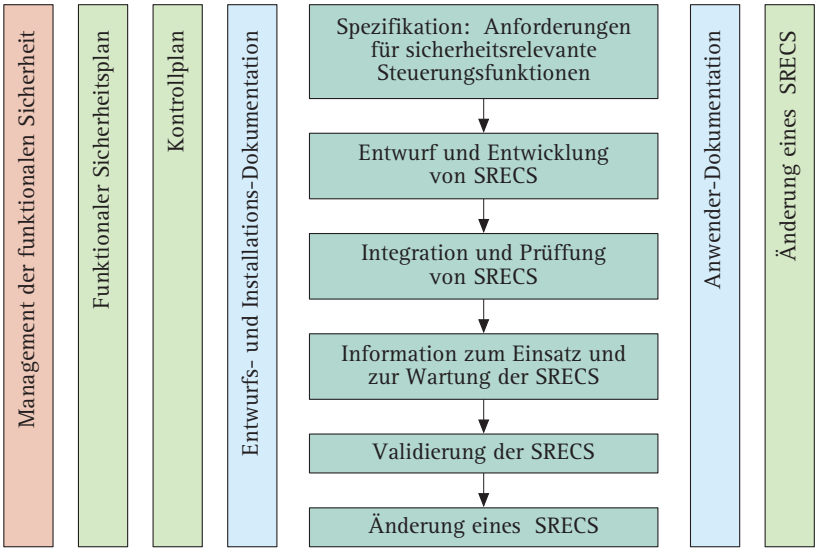

***Bild 3**. Lebenszykluskonzept*

kehrten Entwurfsschaltung aus dem Lieferantenkatalog, das Nicht-Absichern von Sicherheitskontakten eines Sicherheitsrelais oder das Rückstellen einer fehlerhaften Sicherung nach einer Störung. Systematische Fehler können somit überall vorkommen und je früher im Lebenszyklus sie gemacht werden, desto schwieriger ist es, sie zu finden oder sie darauf zu testen.

Auch systematische Fehler können permanent vorhanden sein oder nur unter bestimmten Bedingungen auftreten (zeitweise auftretende systematische Fehler). Ein Beispiel für einen permanent vorhandenen Fehler ist ein Programmierfehler im Sicherheitsprogramm. Die Sicherheitsfunktion muss ausgeführt werden, wenn „A oder B“ auftritt, während der Programmierer „A und B“ programmiert hat. Falls hier kein Test spezifiziert ist, wird dieser Fehler immer in der Software bleiben. Es ist dann auch egal, ob wir ein redundantes System haben oder nicht.

Ein zeitweise auftretender Fehler tritt hingegen nur unter bestimmten Umständen auf. Wenn diese Umstände verschwinden, funktioniert die Sicherheitsfunktion wieder normal. Ein Beispiel dafür ist eine Buskommunikations-Überlastung. Der Feldbus ist aus einem bestimmten Grund überlastet, und die Sicherheitsfunktion ist zeitweise nicht verfügbar. Wenn die Überlast verschwindet, ist alles wieder normal. Zeitweise auftretende systematische Fehler sind am schwierigsten zu finden, und es empfiehlt sich, Spezialisten zu Rate zu ziehen, um sicher zu sein, dass alle Fehlerarten abgedeckt sind.

Die DIN EN 62061 (**VDE 0113-50**) gibt an, dass systematische Hard- und Softwarefehler auf zwei Arten angegangen werden müssen. Einerseits werden Maßregeln spezifiziert, um systematische zufällige Fehler zu verhindern und andererseits werden Beherrschungs-Maßregeln vorgestellt. Die Norm nimmt die systematischen Fehler nicht in die Zuverlässigkeitsberechnung mit auf.

Fehler mit gemeinsamer Ursache

Die letzte Art von Fehlern, die bei Sicherheitssystemen vorkommen können, ist der sogenannte Fehler mit gemeinsamer Ursache. Dieser Fehler kann nur bei Sicherheitssystemen auftreten, die einen redundanten oder dreifach redundanten Aufbau haben. Es sind Fehler, die sich aus einem Ereignis ergeben, das die zwei oder mehr Kanäle gleichzeitig ausfallen lässt (Bild 2). Fehler mit gemeinsamer Ursache sind stets Fehler, die durch Umgebungseinflüsse wie Temperatur, elektromagnetische Felder oder Überschwemmungen verursacht werden.

Die DIN EN 62061 (**VDE 0113-50**) spezifiziert Maßregeln zur Beherrschung von Fehlern mit gemeinsamer Ursache, beispielsweise durch die Anwendung von Diversität bei der Hardware und zwei verschiedenen Teams, welche die Software schreiben. Die Auswirkung der Fehler mit gemeinsamer Ursache wird außerdem in die Zuverlässigkeitsberechnung mit einbezogen.

Auch nicht-technische Anforderungen sind notwendig

Wir können allerlei technische Maßregeln implementieren, die dafür sorgen können, dass das Sicherheitssystem einwandfrei funktioniert. Wenn wir sie nicht gut umsetzen, arbeitet das System immer noch nicht sicher, und die funktionale Sicherheit ist nicht gewährleistet. Die Verfasser der DIN EN 61508 (**VDE 0803**) vergegenwärtigten sich dieses Problem und haben neben technischen Anforderungen auch nicht-technische Anforderungen aufgenommen. Berücksichtigt wird dabei der gesamte Prozess von Auswahl, Entwicklung, Installation, Betrieb, Instandhaltung, Reparatur und Anpassung des Sicherheitssystems.

Um ein funktionssicheres Sicherheitssystem zu erhalten, muss man einen Managementprozess implementieren, der an allen Kanten stimmt. An der Basis von funktionaler Sicherheit liegen denn auch die nicht-technischen Anforderungen der Norm und nicht die tatsächlichen Hard- und Software-Anforderungen. Es geht darum, dass jedes Sicherheitsprojekt, welches wir ausführen, zu einem nachahmbaren funktionssicheren System führt. Wenn wir die Basis nicht unter Kontrolle haben, dann ist funktionale Sicherheit ein Glückstreffer, und wir werden es nie sicher wissen. Die Norm widmet daher das gesamte Kapitel 4 dem „funktionalen Sicherheitsmanagement“.

Behandlung der funktionalen Sicherheit

Die Behandlung der funktionalen Sicherheit verfolgt zwei Ziele. Erstens: wenn man das Projekt erfolgreich ausführen können will, muss man alle technischen und Management-Aktivitäten vorab definieren. Das Definieren dieser Aktivitäten muss anhand eines Sicherheitslebenszyklus (**Bild 3**) erfolgen. Zweitens müssen den Personen, Abteilungen und Organisationen, die von diesem Projekt betroffen sind, deutlich gemacht werden, was ihre Verantwortlichkeiten sind.

Wenn die Schritte, die unternommen werden müssen, um zum richtigen Sicherheitssystem zu gelangen, klar sind, kann man auch die drei vorgenannten Fehlerarten besser verhindern bzw. beherrschen. Dadurch, dass vorab die Schritte bekannt sind, kann man auch dafür sorgen, dass die bestgeeigneten Menschen auf dem richtigen Platz sitzen, mit genügend Unabhängigkeit. Dies ist beispielsweise erforderlich, um den Hard- und Software-Entwurf unabhängig überprüfen zu lassen. Wenn die verantwortlichen Prüfingenieure jedoch an den Entwicklungsleiter berichten, liegt eine unzureichende Unabhängigkeit vor. Viel besser ist es, diese Prüfingenieure zum Beispiel an den Qualitätsmanager berichten zu lassen, der auf der gleichen Ebene

oder auf einer höheren Ebene angesiedelt ist als der Entwicklungsleiter.

DIN EN 954-1 wird zukünftig verschwinden

Die DIN EN 954-1 nennt qualitative Anforderungen für den Entwurf von Sicherheitskomponenten, die mechanisch, elektrisch, pneumatisch oder hydraulisch betätigt werden. Wenngleich auch programmierbare Systeme zum Anwendungsbereich der Norm gehörten, wurde für diese Systeme auf die Norm DIN EN 61508 (VDE 0803) verwiesen. Zur Zeit wird eine Nachfolgerin der Norm DIN EN 954-1, nämlich DIN EN ISO 13849-1 [9], angenommen. Auch diese Norm verlangt eine quantitative Risikobeurteilung, hat aber keine SIL-Stufe sondern eine Leistungsvermögens-Stufe (a bis e) als Ergebnis. Die Norm tritt zum 31. November 2009 in Kraft. Zwischen der DIN EN 62061 (VDE 0113-50) und der DIN EN ISO 13849-1 gibt es große Unterschiede. Es würde zu weit führen, alle Unterschiede in diesem Beitrag aufzuzählen, aber der am meisten ins Auge fallende Unterschied ist, dass die Norm DIN EN ISO 13849-1 keine Lebenszyklusbetrachtung durchführt, sondern sich nur auf den Entwurf konzentriert.

Fazit

Zur Zeit ist bei vielen Betrieben in der Maschinenindustrie eine Tendenz entstanden, bei der SIL ausschließlich mit der wahrscheinlichkeitsbezogenen Zuverlässigkeitberechnung (SIL-Berechnung) assoziiert wird. Und dies obwohl die Norm deutlich über SIL-Stufen qualitative, quantitative Anforderungen, technische und nicht-technische Anforderungen definiert. Die probabilistische Berechnung der Fehlerwahrscheinlichkeit ist nur eine der Anforderungen, die eine Sicherheitsfunktion erfüllen muss.

Literatur

[1] DIN EN 62061 (VDE 0113-50):2005-10 Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbar elektronischer Steuerungssysteme. Berlin · Offenbach: VDE VERLAG

[2] Richtlinie 98/37/EG des europäischen Parlaments und des Rates vom 22. Juni 1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen: eur-lex.europa.eu

[3] DIN EN 954-1:1997-03 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze. Berlin: Beuth

[4] DIN V 19250:1994-05 Leittechnik – Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen.

[5] DIN V 19251:1995-02 Leittechnik – MSR-Schutzeinrichtungen – Anforderungen und Maßnahmen zur gesicherten Funktion.

[6] DIN V VDE 0801 (VDE 0801):1990-01 "Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben

[7] DIN EN 61508 (VDE 0803) Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme. Berlin · Offenbach: VDE VERLAG

[8] DIN EN 61511 (VDE 0810):2005-05 Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie. Berlin · Offenbach: VDE VERLAG

[9] DIN EN ISO 13849-1:2007-07 Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze. Berlin: Beuth