IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen

1 Ausgangslage

Viele Jahre wurde die Sicherheit von Maschinensteuerungen durch die Anwendung der Norm DIN EN 954-1 [1] bewertet. Hier wurden im Wesentlichen strukturelle Aspekte, wie z. B. die Einfehlersicherheit zur Beurteilung herangezogen. Mit der Nachfolgenorm DIN EN 13849-1 [2] hält die Berechnung der Wahrscheinlichkeit für einen gefährlichen Ausfall pro Stunde (Probability of dangerous failure per hour – PFH) von Sicherheitsfunktionen Einzug in den Maschinenbau.

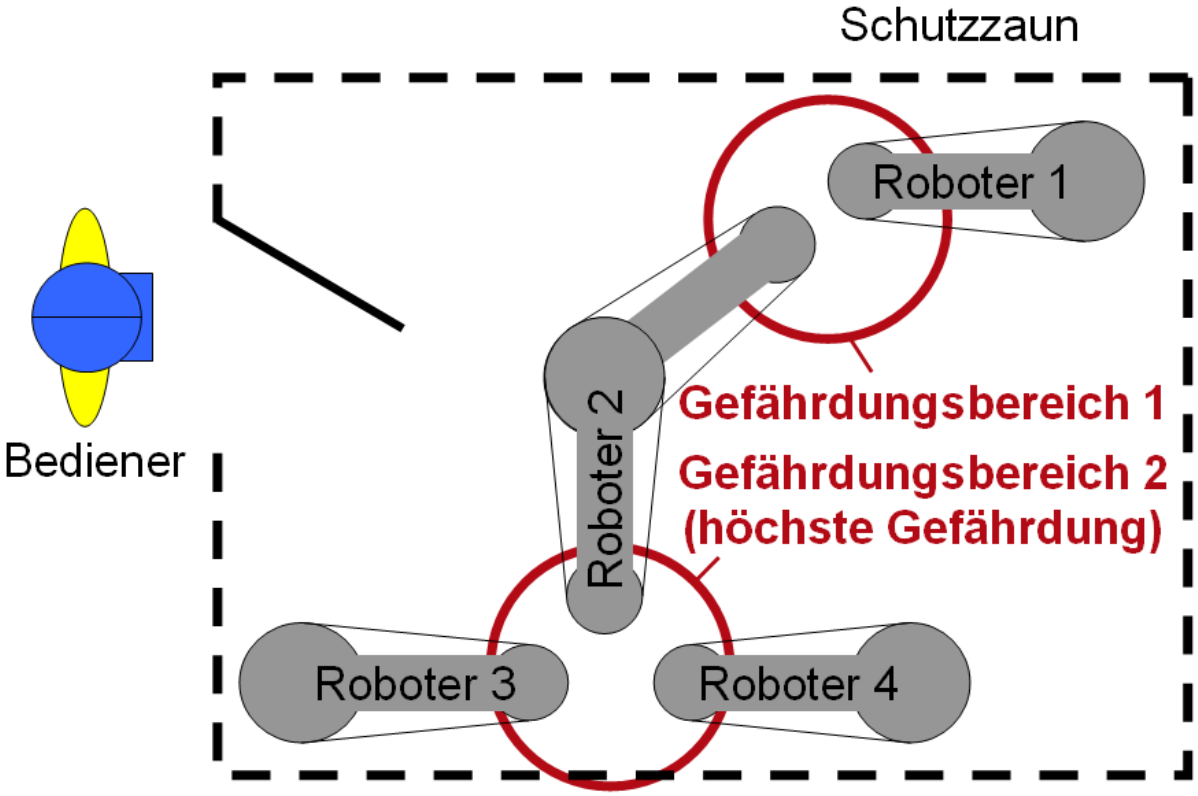
Sicherheitsfunktionen dienen der Risikominderung an Maschinen, z. B. der „Vermeidung eines unerwarteten Anlaufs von Motoren bei geöffneter Schutztür“. Die Anforderungen an die „Qualität“ einer Sicherheitsfunktion werden in der Risikoanalyse durch den erforderlichen Performance Level PL_r festgelegt. Der tatsächlich erreichte Performance Level PL darf nicht niedriger sein als der PLr. Hierbei spielt neben weiteren Aspekten insbesondere die Höhe der PFH eine Rolle. Dazu wird ermittelt, mit welcher Wahrscheinlichkeit ein Steuerungsversagen auftritt, durch das eine Sicherheitsfunktion ausfällt und Personen gefährdet werden können. Bei einfachen Maschinen sind auch deren Sicherheitsfunktionen relativ simpel. Die Ausfallwahrscheinlichkeiten von wenigen Bauteilen müssen hier kombiniert werden, um die PFH für eine komplette Sicherheitsfunktion zu ermitteln. Anspruchsvoller wird es bei komplexen Maschinen mit vielen Bewegungen und speziell dann, wenn sich Gefährdungen überlagern. Von überlagerten Gefährdungen spricht man z. B. dann, wenn am Standort einer Person mehrere gefahrbringende Bewegungen den Bediener verletzen können. In Bild 1 sind zwei Gefährdungsbereiche in einer Roboterzelle dargestellt, auf die das zutrifft. Im Einrichtbetrieb ist der Aufenthalt eines Bedieners in den Gefährdungsbereichen zeitweise erforderlich. Hält sich eine Person im Gefährdungsbereich 1 auf, so stellen die Bewegungen der Roboter 1 und 2 Gefährdungen dar, während dies im Gefährdungsbereich 2 für die Roboter 2, 3 und 4 gilt.

Zur Vermeidung von unerwarteten Bewegungen werden die Antriebsmotoren momentenlos geschaltet und die mechanischen Bremsen fallen ein. Trotz aller sicherheitstechnischen Vorkehrungen besteht eine Restwahrscheinlichkeit dafür, dass es im Fehlerfall z. B. zu einem unerwarteten Anlauf eines Antriebs kommt. Die Wahrscheinlichkeit hierfür wird durch die PFH ausgedrückt. Für den Maschinenbediener spielt es keine Rolle, durch welchen Antrieb er verletzt wird. Für ihn ist die Summe der einzelnen Wahrscheinlichkeiten aller bewegten Maschinenteile relevant [2]. Diese Betrachtungsweise ist Stand der Technik im Bereich der Gefahrstoffe an Arbeitsplätzen. Für den Maschinenbau jedoch stellt sie eine neue Herausforderung dar, denn durch die Addition der einzelnen PFH-Werte vergrößert sich die PFH für die gesamte Sicherheitsfunktion und am Ende wird möglicherweise der zulässige Wert für eine Sicherheitsfunktion überschritten.

Eine zusätzliche Schwierigkeit ergibt sich, wenn die Risikoanalyse an der Maschine für die einzelnen Gefährdungen zu unterschiedlichen PL_r geführt hat. Zur Risikominderung von gefahrbringenden Bewegungen von Robotern sind üblicherweise Sicherheitsfunktionen mit einem PL_r von d erforderlich. Trägt der Roboterarm aber Werkzeuge, von denen zusätzliche Gefährdungen ausgehen, z. B. durch Schweißen, Wasserstrahlschneiden, Laserstrahlung usw., könnte sich hierfür ein anderer PL_r ergeben. Wie soll man diese Überlagerungen bei der Berechnung berücksichtigen?

Zur Lösung der hier beschriebenen Problematik wird im Folgenden ein Verfahren vorgestellt, das in Zusammenarbeit von IFA und dem Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau (FA MFS) entwickelt wurde [4]. Die Anwendung dieses Verfahrens ist nur in den Fällen sinnvoll, bei denen der PL_r für eine Sicherheitsfunktion nicht erreicht wird oder Risiken mit unterschiedlichen PL_r vorliegen.

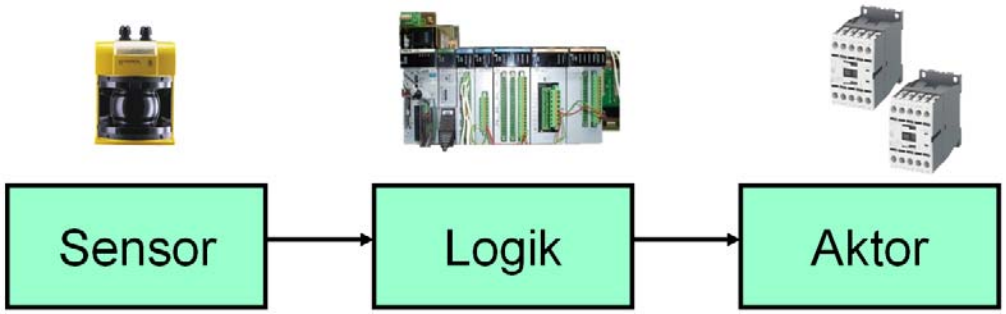
Bild 1: Roboterzelle mit zwei Gefährdungsbereichen



2 Vorgehensweise bei überlagerten Gefährdungen

Sicherheitsfunktionen lassen sich in der Regel in die Abschnitte Sensor, Logik und Aktor aufteilen (s. Bild 2).

Bild 2: Typischer Aufbau einer Sicherheitsfunktion



Die Wahrscheinlichkeit für einen gefährlichen Ausfall pro Stunde berechnet sich dann zu

$PFH_{Sicherheitsfunktion} = PFH_{Sensor} + PFH_{Logik} + PFH_{Aktor}$

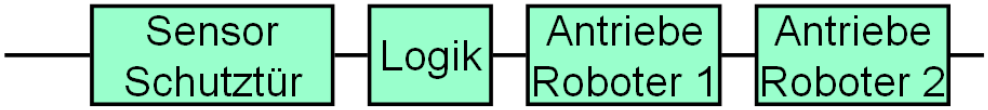
Bei der Überlagerung von gefahrbringenden Bewegungen ist die PFH aller Aktoren zu berücksichtigen, die den Menschen an seinem Standort verletzen können.

Für jeden Gefährdungsbereich sind nun Sicherheitsfunktionen zu definieren, die für eine ausreichende Risikominderung sorgen. Für das Beispiel in Bild 1 könnten diese z. B. lauten:

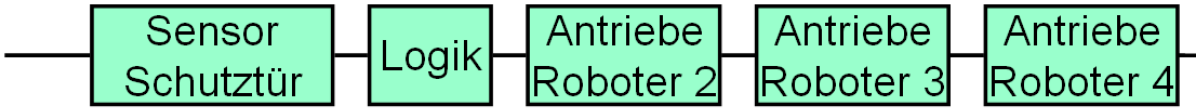
- SF1 Öffnen der Schutztür führt zur Stillsetzung aller Antriebe der Roboter 1 und 2
- SF2 Öffnen der Schutztür führt zur Stillsetzung aller Antriebe der Roboter 2, 3 und 4

In Bild 3 sind Aufbau und Berechnung der PFH für diese beiden Sicherheitsfunktionen skizziert.

Bild 3: Aufbau und PFH der Sicherheitsfunktionen SF1 und SF2



$$PFH_{SF1} = PFH_{Sensor} + PFH_{Logik} + PFH_{Rob1} + PFH_{Rob2}$$



$$PFH_{SF2} = PFH_{Sensor} + PFH_{Logik} + PFH_{Rob2} + PFH_{Rob3} + PFH_{Rob4}$$

Jeder Roboter verfügt über mehrere Antriebe, die jeweils eine PFH aufweisen. Durch die Addition der einzelnen Wahrscheinlichkeiten kann der zulässige PFH-Wert überschritten werden und der PL_r (erforderlicher PL) wird verfehlt. Wurde die Berechnung nach der vereinfachten Methode der DIN EN 13849-1 durchgeführt und ist die PFH nur etwas zu hoch, so könnte man stattdessen eine Markov-Modellierung [5] durchführen. Bei dieser Methode werden die Abschätzungen der DIN EN 13849-1 vermieden, die immer auf der sicheren Seite liegen und zu höheren PFH-Werten führen können. Die Methode der Markov-Modellierung ist jedoch sehr kompliziert und gerade deshalb benutzt die DIN EN 13849-1 einen vereinfachten Ansatz. Aber selbst unter der Anwendung der Markov-Methode gibt es Maschinen mit vielen gefahrbringenden Bewegungen auf engem Raum, sodass die zulässige PFH überschritten wird.

In der Risikoanalyse wurden Sicherheitsfunktionen zur Risikominderung definiert und mit einem PL_r versehen. Nun ist bei komplexen Maschinen mit vielen Aktoren der rechnerische Nachweis einer ausreichenden Risikominderung durch Sicherheitsfunktionen nicht möglich. Heißt das, dass diese Maschinen zu gefährlich sind und so nicht gebaut werden dürften? Die praktische Erfahrung spricht dagegen, denn erhöhte Unfallhäufigkeiten sind nicht festzustellen. Aber wie kann der Nachweis quantitativ erbracht werden?

3 Der Kompromiss

Unter Anwendung der DIN EN 954-1 wurden in der Vergangenheit immer nur Teile von Sicherheitsfunktionen betrachtet. Zum Beispiel gab es in Maschinennormen Anforderungen wie

- Überwachung der Schutztürstellung in Kategorie 1 – Sensor
- Signalverarbeitung in Kategorie 3 – Logik
- Hydraulische Ventile in Kategorie 1 – Aktor

Eine zusammenfassende Betrachtung einer kompletten Sicherheitsfunktion erfolgte nicht, geschweige denn die gleichzeitige Berücksichtigung von mehreren Gefährdungen. Diese Vorgehensweise ist in der Praxis keineswegs durch vermehrt auftretende Unfälle aufgefallen. Insofern erscheint es sinnvoll und zulässig, Sicherheitsfunktionen auf

- Einzelgefährdungen bzw.
- Bewegungen eines einzelnen Maschinenteils

zu begrenzen. Diese Festlegung kann durch den Maschinenhersteller während der Risikoanalyse/Risikobeurteilung erfolgen. Hierbei ist unter Berücksichtigung der bestimmungsgemäßen Handlungen des Bedienpersonals und der Maße der gefährdeten Körperteile der Gefährdungsbereich festzulegen. Die Bewegungen von Maschinenteilen im Gefährdungsbereich stellen die hier relevanten Gefährdungen dar. Einzelne Maschinenteile können dabei durchaus von mehreren Antrieben bewegt werden. Bei der Definition der Sicherheitsfunktionen – und später in der PFH-Berechnung – müssen dann all die Komponenten berücksichtigt werden, die eine gefahrbringende Bewegung des betrachteten Maschinenteils verursachen können. Für das Beispiel der Roboterzelle aus Bild 1 ergeben sich mit dem neuen Ansatz die folgenden Sicherheitsfunktionen:

- SF1: Öffnen der Schutztür führt zur Stillsetzung aller Antriebe von Roboter 1
- SF2: Öffnen der Schutztür führt zur Stillsetzung aller Antriebe von Roboter 2
- SF3: Öffnen der Schutztür führt zur Stillsetzung aller Antriebe von Roboter 3
- SF4: Öffnen der Schutztür führt zur Stillsetzung aller Antriebe von Roboter 4

Dabei wird ein Roboter als einzelnes Maschinenteil aufgefasst, dessen Bewegungen den Bediener gefährden. Jede Sicherheitsfunktion enthält zwar noch immer mehrere Antriebe, aber nur diejenigen eines einzigen Roboters. Die PFH der Sicherheitsfunktionen ist daher deutlich reduziert.

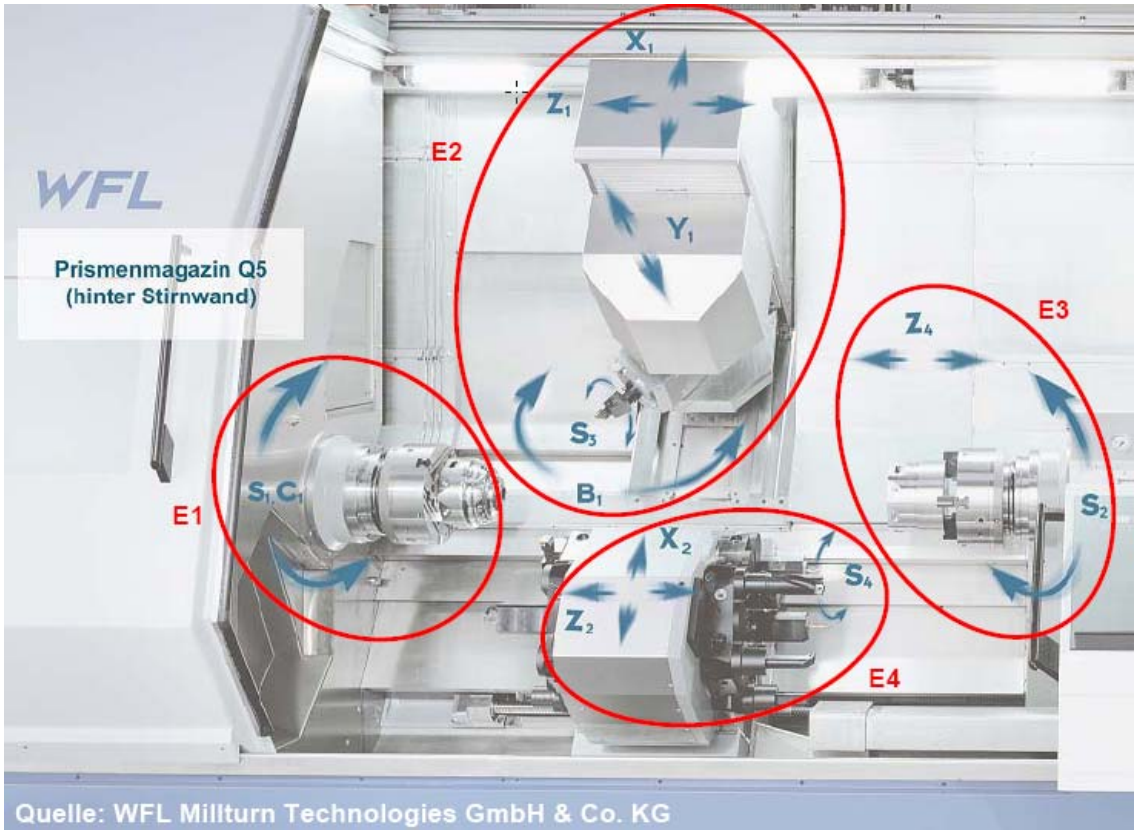
Das hier vorgestellte Prinzip der Berücksichtigung von Einzelgefährdungen löst auch das Problem von überlagerten Gefährdungen mit unterschiedlichem PL_r. Legt man wieder zugrunde, dass ein Roboterarm ein Werkzeug (z. B. Schweißzange, Laserstrahl, Wasserstrahl) trägt, so besteht hierdurch eine über die gefahrbringenden Bewegungen hinausgehende zusätzliche Gefährdung. Zur Risikominderung ist eine weitere Sicherheitsfunktion SF5 erforderlich, die möglicherweise in einem abweichenden Performance Level realisiert werden kann. Insbesondere in diesen Fällen empfiehlt es sich, nur einzelne Gefährdungen (eines Maschinenteils) zu betrachten.

4 Beispiel Werkzeugmaschine

Bild 4 zeigt eine Werkzeugmaschine, in deren Arbeitsraum sich mehrere Bewegungen überlagern, die den Maschinenbediener beispielweise beim Einrichten gefährden. Prinzipiell müssten fast alle Antriebe in einer einzigen Sicherheitsfunktion berücksichtigt werden, denn die Verfahrbereiche der Bewegungen überlagern sich weitgehend und der Einrichter muss hier manuell eingreifen. Die maximal zulässige PFH wird so sicherlich überschritten. Der oben beschriebene Vereinzelungs-ansatz führt auch hier zu einer praktikablen Lösung. Es werden vier Maschinenteile definiert, deren Bewegungen getrennt voneinander betrachtet werden (siehe Markierungen in Bild 4):

- E1: rotatorische (S1) und translatorische (C1 zur außermittigen Bearbeitung) Bewegung der linken Werkstückspindel
- E2: rotatorische (S3) und translatorische (X1, Y1, Z1) Bewegung und Schwenkbewegung (B1) der Frässpindel
- E3: rotatorische (S2) und translatorische (Z4) Bewegung der rechten Werkstückspindel
- E4: rotatorische (S4) und translatorische Bewegung (X2, Z2) einer Werkzeugspindel (der Werkzeugrevolver ist indexiert, sodass dessen rotatorische Bewegung hier nicht betrachtet werden muss)

Bild 4: Unterschiedliche Einzelgefährdungen am Beispiel einer Werkzeugmaschine



Durch die Betrachtung der vier Einzelgefährdungen von Maschinenteilen ergeben sich somit vier Sicherheitsfunktionen SF1 bis SF4, die eine Risikominderung für E1 bis E4 bewirken:

- SF1 berücksichtigt die Bewegungen S1 und C1
- SF2 berücksichtigt die Bewegungen S3, X1, Y1, Z1 und B1
- SF3 berücksichtigt die Bewegungen S2 und Z4
- SF4 berücksichtigt die Bewegungen S4, X2 und Z2

Die Gestaltung der Sicherheitsfunktionen ist abhängig von der Betriebsart der Maschine und den jeweils notwendigen Tätigkeiten. So könnte die Spindel mit einer begrenzten Drehzahl rotieren (Sicher begrenzte Geschwindigkeit/Drehzahl – SLS), nicht benötigte Bewegungen könnten momentenfrei gestellt werden (Sicher abgeschaltetes Moment – STO) und Achsbewegungen wären nur im Zustimm-/Tippbetrieb möglich. Bei allen Sicherheitsfunktionen ist die Anzahl der zu berücksichtigenden Antriebe gegenüber dem ganzheitlichen Ansatz deutlich reduziert und die zulässige PFH kann eingehalten werden.

5 Literatur

[1] DIN EN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (03.97). Beuth, Berlin (1997)

[2] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (12.08). Beuth, Berlin 2008

[3] Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schaefer, M.: Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) Nr. 6, S. 34-37
http://www.dguv.de/ifa/de/pub/grl/pdf/2009_249.pdf

[4] Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Fachausschuss-Informationsblatt Nr. 047, Ausgabe 5/2010. Hrsg.: Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau, Mainz
www.bghm.de, Webcode 796

[5] DIN EN 61508-5: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:1998 und Corrigendum 1999) (11.02). Beuth, Berlin 2002

Autoren: Dipl.-Ing. Ralf Apfeld, Dr. Michael Schaefer
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA),
Sankt Augustin